Alexey L. Gorodentsev

Algebra II

Textbook for Students of Mathematics

Springer

Algebra II

Alexey L. Gorodentsev

Algebra II

Textbook for Students of Mathematics

Springer

Alexey L. Gorodentsev
Faculty of Mathematics
National Research University
"Higher School of Economics"
Moscow, Russia

Originally published in Russian as "Algebra. Uchebnik dlya studentov-matematikov. Chast' 2", © MCCME 2015

ISBN 978-3-319-50852-8 ISBN 978-3-319-50853-5 (eBook)
DOI 10.1007/978-3-319-50853-5

Library of Congress Control Number: 2017930683

Mathematics Subject Classification (2010): 11.01, 12.01, 13.01, 14.01, 15.01, 16.01, 18.01, 20.01

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This is the second part of a 2-year course of abstract algebra for students beginning a professional study of higher mathematics.[1] This textbook is based on courses given at the Independent University of Moscow and at the Faculty of Mathematics at the National Research University Higher School of Economics. In particular, it contains a large number of exercises that were discussed in class, some of which are provided with commentary and hints, as well as problems for independent solution that were assigned as homework. Working out the exercises is of crucial importance in understanding the subject matter of this book.

Moscow, Russia — Alexey L. Gorodentsev

[1] Throughout this book, the first volume will be referred to as *Algebra I*.

Contents

Notation and Abbreviations

$\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	The integer, positive integer, rational, real, and complex numbers
$\mathbb{F}_q$	The finite field of q elements
$\|M\|$	The cardinality of a finite set M
Id_X	The identity map $X \xrightarrow{\sim} X$
$n \mid m$	n divides m
$\mathbb{F}^*, K^*$	The multiplicative groups of the nonzero elements in a field $\mathbb{F}$ and the invertible elements in a ring K
$[a]$, $[a]_U$, $[a]_p$	The equivalence class of an element a modulo some equivalence relation, e.g., modulo a subgroup U or a prime number p
$\mathrm{Hom}(X, Y)$	The set of homomorphisms $X \to Y$
$\mathrm{Hom}_A(U, W)$	The set of maps $U \to W$ commuting with a set of operators A acting on U and W
$\mathrm{Hom}_{\mathcal{C}}(X, Y)$	The set of morphisms $X \to Y$ in a category $\mathcal{C}$
$\mathrm{End}(X)$, $\mathrm{End}_A(U)$, etc.	The same for the endomorphisms $X \to X$
$\mathrm{Aut}(X)$, $\mathrm{Aut}_A(U)$, etc.	The same for the groups of invertible morphisms $X \xrightarrow{\sim} X$
$A \otimes B$	The tensor product of commutative rings or modules over the same commutative ring
$U \otimes_R W$	The tensor product of a right R-module U and a left R-module W
$S_n, A_n \lhd S_n$	The symmetric group $\mathrm{Aut}\{1, 2, \dots, n\}$ and its normal subgroup of even permutations
$(g_1, g_2, \dots, g_n) \in S_n$	The permutation $g : k \mapsto g_k$
$\|i_1, i_2, \dots, i_m\rangle \in S_n$	The cyclic permutation $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_m \mapsto i_1$
λ, $\|\lambda\|$, $\ell(\lambda)$	A Young diagram $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_m)$, its weight $\|\lambda\| = \sum_i \lambda_i$, and its length $\ell(\lambda) = m$
$\lambda(g), \lambda(N), \lambda(a), \lambda(T)$	The cyclic types of a permutation $g \in S_N$ or a nilpotent linear endomorphism $N \in \mathrm{End}(V)$ and the shapes of an array a or a filling T

λ^t, a^t, A^t	The transposed Young diagram, array, and matrix for a given Young diagram λ, array a, and matrix A
V, V^*	Dual vector spaces
$\langle \xi, v \rangle = \xi(v) = \mathrm{ev}_v(\xi)$	The contraction between a vector $v \in V$ and a covector $\xi \in V^*$
$f^* : W^* \to U^*$	The dual map to a linear map $f : U \to W$
$\mathbb{A}(V), \mathbb{P}(V)$	The affine and projective spaces associated with a vector space V
$\mathbb{A}^n = \mathbb{A}(\Bbbk^n), \mathbb{P}_n = \mathbb{P}(\Bbbk^{n+1})$	The coordinate affine and projective spaces of dimension n
$\mathrm{GL}(V),\ \mathrm{O}(V),\ \mathrm{U}(V)$	The groups of linear, orthogonal, and unitary transformations of a vector space V
$\mathrm{PGL}(V)$	The group of linear projective transformations of a projective space $\mathbb{P}(V)$
$\mathrm{SL}(V),\ \mathrm{SO}(V),\ \text{etc.}$	The subgroups of the previous groups formed by the linear transformations of determinant 1
$\mathrm{GL}_n(\Bbbk), \mathrm{SL}_n(\Bbbk), \text{etc.}$	The groups of $n \times n$ matrices obtained from the previous groups for $V = \Bbbk^n$
$V^{\otimes n}, S^n V, \Lambda^n V$	The nth tensor, symmetric, and exterior powers of a vector space V
$\mathsf{T}(V), SV, \Lambda V$	The tensor, symmetric, and exterior (Grassmannian) algebras of a vector space V
$\mathrm{Sym}^n V, \mathrm{Alt}^n V \subset V^{\otimes n}$	The subspaces of symmetric and skew-symmetric tensors
$\mathbb{S}^\lambda V$	The irreducible Schur's representation of $\mathrm{GL}(V)$ associated with a Young diagram λ
$\Lambda, \omega : \Lambda \xrightarrow{\sim} \Lambda$	The $\mathbb{Z}$-algebra of symmetric functions and its canonical involution
$e_i, h_i, p_i \in \Lambda$	The elementary, complete, and Newton's symmetric polynomials numbered by their degrees i
$m_\lambda, e_\lambda, h_\lambda, s_\lambda \in \Lambda$	Numbered by the Young diagrams λ, the monomial, elementary, complete, and Schur's bases of Λ over $\mathbb{Z}$
$p_\lambda \in \mathbb{Q} \otimes \Lambda$	The Newton basis of $\mathbb{Q} \otimes \Lambda$ over $\mathbb{Q}$ numbered by the Young diagrams λ
$\mathrm{res}_H^G W, \mathrm{ind}_H^G V, \mathrm{coind}_H^G V$	Restricted, induced, and coinduced representations
M_λ, S_λ	The tabloid and Specht's S_n-modules indexed by a Young diagram λ of weight $\lvert\lambda\rvert = n$
$\mathcal{S}et, \mathcal{T}op, \mathcal{G}rp, \mathcal{A}b, \mathcal{C}mr$	The categories of sets, topological spaces, groups, abelian groups, and commutative rings with units
$R\text{-}\mathcal{M}od, \mathcal{M}od\text{-}R, \mathcal{V}ec_\Bbbk$	The categories of left and right modules over a ring R and vector spaces over a field $\Bbbk$
$\mathcal{F}un(\mathcal{C}, \mathcal{D})$	The category of functors $\mathcal{C} \to \mathcal{D}$
$\mathcal{P}re\mathcal{S}h(\mathcal{C}, \mathcal{D}) = \mathcal{F}un(\mathcal{C}^{\mathrm{opp}}, \mathcal{D})$	The category of presheaves $\mathcal{C} \to \mathcal{D}$

$\varphi^* : K^Y \to K^X$	The pullback homomorphism $f \mapsto f \circ \varphi$ associated with a map of sets $\varphi : X \to Y$
$Z(f), Z(I) \subset \mathbb{P}(V)$	The zero sets of a homogeneous polynomial $f \in SV^*$ and a homogeneous ideal $I \subset SV^*$
$V(f), V(I) \subset \mathbb{A}[V]$	The affine hypersurface $f(v) = 0, f \in SV^*$ and the zero set of an ideal $I \subset SV^*$
$X \subset \mathbb{A}^n$, $I(X)$, $\Bbbk[X]$	An affine algebraic variety, its ideal, and the coordinate algebra
$\mathcal{D}(f) \subset X$	The principal open set $f(x) \neq 0$ provided by a regular function $f \in \Bbbk[X]$ on an affine algebraic variety X
$\mathrm{Dom}(f), \mathrm{Dom}(\varphi) \subset X$	The domains of regularity for a rational function f and a rational map φ on algebraic manifold X
$D(f)$	The discriminant of a polynomial $f \in \Bbbk[x]$
$\overline{\Bbbk}$, $\overline{A}_B$	An algebraic closure of a field $\Bbbk$ and the integral closure of a commutative ring A in a commutative ring $B \supset A$
$\mu_\zeta \in \Bbbk[x]$, $\deg_{\Bbbk} \zeta \in \mathbb{N}$	The minimal polynomial and degree over a field $\Bbbk$ of an element ζ, algebraic over $\Bbbk$, of some $\Bbbk$-algebra
$\boldsymbol{\mu}_n$, Φ_n	The multiplicative group of nth roots of unity and the nth cyclotomic polynomial
F_p	The Frobenius endomorphism and the corresponding Frobenius element in the Galois group of a cyclotomic field
$\deg \mathbb{K}/\Bbbk = \dim_{\Bbbk} \mathbb{K}$	The degree of a finite extension of fields $\mathbb{K} \supset \Bbbk$
$\mathrm{Aut}_{\Bbbk}(\mathbb{F})$	The group of automorphisms of a field $\mathbb{F}$ over a subfield $\Bbbk \subset \mathbb{F}$
$\mathrm{Gal}\,\mathbb{K}/\Bbbk$, $\mathrm{Gal}\,f/\Bbbk$	The Galois groups of a Galois extension of fields $\mathbb{K} \supset \Bbbk$ and of a separable polynomial $f \in \Bbbk[x]$

Chapter 1
Tensor Products

1.1 Multilinear Maps

Let K be a commutative ring, and let $V_1, V_2, \dots, V_n$ and W be K-modules. A map

$$\varphi : V_1 \times V_2 \times \cdots \times V_n \to W \tag{1.1}$$

is called *multilinear* or *n-linear* if φ is linear in each argument while all the other arguments are fixed, i.e.,

$$\varphi(\dots, \lambda v' + \mu v'', \dots) = \lambda\, \varphi(\dots, v', \dots) + \mu\, \varphi(\dots, v'', \dots)$$

for all $\lambda, \mu \in K$, $v', v'' \in V_i$, $1 \leqslant i \leqslant n$. For example, the 1-linear maps $V \to V$ are the ordinary linear endomorphisms of V, and the 2-linear maps $V \times V \to K$ are the bilinear forms on V. The multilinear maps (1.1) form a K-module with the usual addition and multiplication by constants defined for maps taking values in a K-module. We denote the K-module of multilinear maps (1.1) by $\mathrm{Hom}(V_1, V_2, \dots, V_n; W)$, or by $\mathrm{Hom}_K(V_1, V_2, \dots, V_n; W)$ when explicit reference to the ground ring is required.

1.1.1 Multilinear Maps Between Free Modules

Let $V_1, V_2, \dots, V_n$ and W be free modules of finite ranks $d_1, d_2, \dots, d_n$ and d respectively. Then the module of multilinear maps (1.1) is also free of rank $d \cdot d_1 \cdot d_2 \cdots d_n$. To see this, choose a basis $e_1^{(\nu)}, e_2^{(\nu)}, \dots, e_{d_\nu}^{(\nu)}$ in every V_ν and a basis $e_1, e_2, \dots, e_d$ in W. Every map (1.1) is uniquely determined by its values on

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_1

all collections of the basis vectors

$$\varphi\left(e^{(1)}_{j_1},\, e^{(2)}_{j_2},\, \dots,\, e^{(n)}_{j_n}\right) \in W, \tag{1.2}$$

because for an arbitrary collection of vectors $v_1, v_2, \dots, v_n$, where each $v_\nu \in V_\nu$ is linearly expressed through the basis as

$$v_\nu = \sum_{j_\nu=1}^{d_\nu} x^{(\nu)}_{j_\nu}\, e^{(\nu)}_{j_\nu}, \tag{1.3}$$

it follows from the multilinearity of φ that

$$\varphi(v_1, v_2, \dots, v_n) = \sum_{j_1 j_2 \dots j_n} x^{(1)}_{j_1} \cdot x^{(2)}_{j_2} \cdots x^{(n)}_{j_n} \cdot \varphi\left(e^{(1)}_{j_1}, e^{(2)}_{j_2}, \dots, e^{(n)}_{j_n}\right). \tag{1.4}$$

Every vector (1.2) is uniquely expanded as

$$\varphi\left(e^{(1)}_{j_1},\, e^{(2)}_{j_2},\, \dots,\, e^{(n)}_{j_n}\right) = \sum_{i=1}^{d} a_{i j_1 j_2 \dots j_n} \cdot e_i.$$

Thus, the multilinear maps (1.1) are in bijection with the $(n+1)$-dimensional matrices

$$A = \left(a_{i j_1 j_2 \dots j_n}\right)$$

of size $d \times d_1 \times d_2 \times \cdots \times d_n$ with elements $a_{i j_1 j_2 \dots j_n} \in K$. For $n = 1$, such a matrix is the usual 2-dimensional $d \times d_1$ matrix $\left(a_{ij}\right)$ of a linear map $V \to W$, where $d_1 = \dim V$, $d = \dim W$. For $n = 2$, a bilinear map $V_1 \times V_2 \to W$ is encoded by the three-dimensional matrix of size $d \times d_1 \times d_2$ formed by the constants $\left(a_{i j_1 j_2}\right)$, etc. A map φ is recovered from its matrix by the formula

$$\varphi(v_1, v_2, \dots, v_n) = \sum_{i, j_1, \dots, j_n} a_{i j_1 j_2 \dots j_n} \cdot x^{(1)}_{j_1} \cdot x^{(2)}_{j_2} \cdots x^{(n)}_{j_n} \cdot e_i. \tag{1.5}$$

The addition and multiplication by constants in $\mathrm{Hom}(V_1, V_2, \dots, V_n; W)$ has the effect on matrices $\left(a_{i j_1 j_2 \dots j_n}\right)$ of componentwise addition and multiplication by constants. Therefore, $\mathrm{Hom}(V_1, V_2, \dots, V_n; W)$ is isomorphic to the K-module of $(n+1)$-dimensional matrices of size $d \times d_1 \times d_2 \times \cdots \times d_n$ with elements from K. The latter module is free with a basis formed by the matrices $E_{i j_1 j_2 \dots j_n}$ having 1 in the position $(i j_1 j_2 \dots j_n)$ and 0 everywhere else. The corresponding basis of $\mathrm{Hom}(V_1, V_2, \dots, V_n; W)$ consists of the multilinear maps

$$\begin{gathered}\delta^{i}_{j_1, j_2, \dots, j_n} : V_1 \times V_2 \times \cdots \times V_n \to W, \\ \left(e^{(1)}_{k_1}, e^{(2)}_{k_2}, \dots, e^{(n)}_{k_n}\right) \mapsto \begin{cases} e_i & \text{if } k_\nu = j_\nu \text{ for all } \nu, \\ 0 & \text{otherwise.} \end{cases}\end{gathered} \tag{1.6}$$

An arbitrary collection of vectors (1.3) is mapped to

$$\delta^{i}_{j_1,j_2,\ldots,j_n} : (v_1, v_2, \ldots, v_n) \mapsto x^{(1)}_{j_1} \cdot x^{(2)}_{j_2} \cdots x^{(n)}_{j_n} \cdot e_i. \tag{1.7}$$

In particular, if $K = \Bbbk$ is a field and $V_1, V_2, \ldots, V_n,\ W$ are finite-dimensional vector spaces over $\Bbbk$, then $\dim \operatorname{Hom}(V_1, V_2, \ldots, V_n; W) = \dim W \cdot \prod_\nu \dim V_\nu$.

1.1.2 Universal Multilinear Map

Given a multilinear map of K-modules

$$\tau : V_1 \times V_2 \times \cdots \times V_n \to U \tag{1.8}$$

and an arbitrary K-module W, composing τ with the linear maps $F : U \to W$ assigns the map

$$\operatorname{Hom}(U, W) \to \operatorname{Hom}(V_1, V_2, \ldots, V_n; W), \quad F \mapsto F \circ \tau, \tag{1.9}$$

which is obviously linear in F.

Definition 1.1 A multilinear map (1.8) is called *universal* if for every K-module W, the linear map (1.9) is an isomorphism of K-modules. In the expanded form, this means that for every K-module W and multilinear map $\varphi : V_1 \times V_2 \times \cdots \times V_n \to W$, there exists a unique K-linear map $F : U \to W$ such that $\varphi = F \circ \tau$, i.e., the two solid multilinear arrows in the diagram

$$\begin{tikzcd} & U \arrow[dd, dashed, "F"] \\ V_1 \times V_2 \times \cdots \times V_n \arrow[ur, "\tau"] \arrow[dr, "\varphi"'] & \\ & W \end{tikzcd}$$

are uniquely completed to a commutative triangle by the dashed linear arrow.

Lemma 1.1 *For every two universal multilinear maps*

$$\tau_1 : V_1 \times V_2 \times \cdots \times V_n \to U_1, \tau_2 : V_1 \times V_2 \times \cdots \times V_n \to U_2$$

there exists a unique linear isomorphism $\iota : U_1 \xrightarrow{\sim} U_2$ *such that* $\tau_2 = \iota\tau_1$.

Proof By the universal properties of τ_1, τ_2, there exists a unique pair of linear maps

$$F_{21} : U_1 \to U_2 \quad \text{and} \quad F_{12} : U_2 \to U_1$$

that fit in the commutative diagram

$$\begin{tikzcd}
U_1 \arrow[dd, equal, "\mathrm{Id}_{U_1}"'] \arrow[dr, dashed, "F_{21}"] & & & & U_2 \arrow[dd, equal, "\mathrm{Id}_{U_2}"] \arrow[dl, dashed, "F_{12}"'] \\
& U_2 \arrow[dl, dashed, "F_{12}"] & V_1 \times V_2 \times \cdots \times V_n \arrow[l, "\tau_2"'] \arrow[r, "\tau_1"] \arrow[ull, "\tau_1"'] \arrow[dll, "\tau_1"] \arrow[urr, "\tau_2"] \arrow[drr, "\tau_2"'] & U_1 \arrow[dr, dashed, "F_{21}"'] & \\
U_1 & & & & U_2
\end{tikzcd}$$

Since the factorizations $\tau_1 = \varphi \circ \tau_1$ and $\tau_2 = \psi \circ \tau_2$ are unique and hold for $\varphi = \mathrm{Id}_{U_1}$, $\psi = \mathrm{Id}_{U_2}$, we conclude that $F_{21}F_{12} = \mathrm{Id}_{U_2}$ and $F_{12}F_{21} = \mathrm{Id}_{U_1}$. $\square$

1.2 Tensor Product of Modules

The universal multilinear map (1.8) is denoted by

$$\begin{aligned} \tau : V_1 \times V_2 \times \cdots \times V_n &\to V_1 \otimes V_2 \otimes \cdots \otimes V_n, \\ (v_1, v_2, \dots, v_n) &\mapsto v_1 \otimes v_2 \otimes \cdots \otimes v_n, \end{aligned} \tag{1.10}$$

and called *tensor multiplication*. The target module $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ is called the *tensor product* of K-modules $V_1, V_2, \dots, V_n$, and its elements are called *tensors*. The image of tensor multiplication consists of the tensor products $v_1 \otimes v_2 \otimes \cdots \otimes v_n$, called *tensor monomials* or *decomposable tensors*. The decomposable tensors do not form a vector space, because the map (1.10) is *not linear* but multilinear.[1] We will see soon that the decomposable tensors form a quite thin set within $V_1 \otimes V_2 \otimes \cdots \otimes V_n$. Over an infinite ground ring K, a random tensor is most likely an indecomposable linear combination of monomials $v_1 \otimes v_2 \otimes \cdots \otimes v_n$.

Exercise 1.1 Deduce from the universal property of the tensor product that $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ is linearly generated by the tensor monomials.

[1]The formula (1.5) shows that an n-linear map is described in coordinates by means of nth-degree polynomials.

1.2.1 Existence of Tensor Product

Although Lemma 1.1 states that the tensor product is unique up to a unique isomorphism commuting with the tensor multiplication, Definition 1.1 does not vouch for the existence of the tensor product. In this section we construct $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ in terms of generators and relations. Then this description will be clarified in Theorems 1.1 and 1.2.

Given a collection of K-modules $V_1, V_2, \ldots, V_n$, write $\mathcal{V}$ for the free K-module with a basis formed by all n-literal words $[v_1 v_2 \ldots v_n]$, where the ith letter is an arbitrary vector $v_i \in V_i$. Let $\mathcal{R} \subset \mathcal{V}$ be the submodule generated by all linear combinations

$$[\cdots (\lambda u + \mu w) \cdots] - \lambda [\cdots u \cdots] - \mu [\cdots w \cdots], \tag{1.11}$$

where the left and right dotted fragments remain unchanged in all three words. We put

$$\begin{aligned} V_1 \otimes V_2 \otimes \cdots \otimes V_n &\stackrel{\text{def}}{=} \mathcal{V}/\mathcal{R}, \\ v_1 \otimes v_2 \otimes \cdots \otimes v_n &\stackrel{\text{def}}{=} [v_1 v_2 \ldots v_n] \pmod{\mathcal{R}}. \end{aligned} \tag{1.12}$$

Thus, the K-module $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ consists of all finite K-linear combinations of tensor monomials $v_1 \otimes v_2 \otimes \cdots \otimes v_n$, where $v_i \in V_i$, satisfying the distributivity relations

$$\cdots \otimes (\lambda u + \mu w) \otimes \cdots = \lambda \cdot (\cdots \otimes u \otimes \cdots) - \mu \cdot (\cdots \otimes w \otimes \cdots). \tag{1.13}$$

Lemma 1.2 *The map*

$$\tau : V_1 \times \cdots \times V_n \to \mathcal{V}/\mathcal{R}, (v_1, \ldots, v_n) \mapsto [v_1 \ldots v_n] \pmod{\mathcal{R}},$$

is the universal multilinear map.

Proof The multilinearity of τ is expressed exactly by the relations (1.13), which hold by definition. Let us check the universal property. For every map of sets

$$\varphi : V_1 \times V_2 \times \cdots \times V_n \to W,$$

there exists a unique linear map $F : \mathcal{V} \to W$ acting on the basis by the rule

$$[v_1 v_2 \ldots v_n] \mapsto \varphi(v_1, v_2, \ldots, v_n).$$

This map is correctly factorized through the quotient map $\mathcal{V} \twoheadrightarrow \mathcal{V}/\mathcal{R}$ if and only if $\mathcal{R} \subset \ker F$. Since F is linear and φ is multilinear, for every linear generator (1.11) of $\mathcal{R}$, the equalities

$$\begin{aligned} & F\big([\dots(\lambda u+\mu w)\dots]-\lambda\,[\dots u\dots]-\mu\,[\dots w\dots]\big) \\ &\quad = F\big([\dots(\lambda u+\mu w)\dots]\big)-\lambda\,F\big([\dots u\dots]\big)-\mu\,F\big([\dots w\dots]\big) \\ &\quad = \varphi(\dots,\,(\lambda u+\mu w),\,\dots)-\lambda\,\varphi(\dots,\,u,\,\dots)-\mu\,\varphi(\dots,\,w,\,\dots)=0 \end{aligned}$$

hold. Therefore, the prescription $v_1\otimes v_2\otimes\cdots\otimes v_n\mapsto\varphi(v_1,v_2,\dots,v_n)$ actually assigns a well-defined linear map $\mathcal{V}/\mathcal{R}\to W$. □

Theorem 1.1 (Tensor Product of Free Modules) *Let modules V_i be free with a (not necessarily finite) basis E_i. Then the tensor product $V_1\otimes V_2\otimes\cdots\otimes V_n$ is free with a basis formed by the tensor products of basis vectors*

$$e_1\otimes e_2\otimes\cdots\otimes e_n,\ \textit{where } e_i\in E_i. \tag{1.14}$$

In particular, if all V_i are of finite rank, then $\operatorname{rk} V_1\otimes V_2\otimes\cdots\otimes V_n=\prod\operatorname{rk}V_i$.

Proof Let us temporarily consider the symbols (1.14) just as formal records, and write $\mathcal{W}$ for the free module with a basis formed by all these records. By Sect. 1.1.1, there exists a unique multilinear map $\tau : V_1\times V_2\times\cdots\times V_n\to\mathcal{W}$ such that $\tau(e_1,e_2,\dots,e_n)=e_1\otimes e_2\otimes\cdots\otimes e_n$. It is universal, because for every multilinear map $\varphi : V_1\times V_2\times\cdots\times V_n\to W$, the condition $\varphi=F\circ\tau$ on a linear map $F:\mathcal{W}\to W$ forces F to act on the basis of $\mathcal{W}$ by the rule

$$F\,(e_1\otimes e_2\otimes\cdots\otimes e_n)=\varphi(e_1,e_2,\dots,e_n),$$

and this prescription actually assigns the well-defined linear map $F:\mathcal{W}\to W$. By Lemma 1.1, there exists a unique K-linear isomorphism $\mathcal{W}\xrightarrow{\sim}V_1\otimes V_2\otimes\cdots\otimes V_n$ that maps the formal records (1.14) to the actual tensor products of the basis vectors $e_1\otimes e_2\otimes\cdots\otimes e_n\in V_1\otimes V_2\otimes\cdots\otimes V_n$. Therefore, these tensor products also form a basis. □

Example 1.1 (Polynomial Rings) The tensor product of n copies of the K-module of polynomials $K[x]$, i.e., the nth tensor power $K[x]^{\otimes n}=K[x]\otimes K[x]\otimes\cdots\otimes K[x]$, is isomorphic to the module of polynomials in n variables $K[x_1,x_2,\dots,x_n]$ via the map $x^{m_1}\otimes x^{m_2}\otimes\cdots\otimes x^{m_n}\mapsto x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$.

Example 1.2 (Segre Varieties) Let $V_1,V_2,\dots,V_n$ be finite-dimensional vector spaces over an arbitrary field $\Bbbk$. It follows from Theorem 1.1 that the tensor product $V_1\otimes V_2\otimes\cdots\otimes V_n$ is linearly generated by the decomposable tensors $v_1\otimes v_2\otimes\cdots\otimes v_n$. Considered up to proportionality,[2] the collection of decomposable tensors in the projective space $\mathbb{P}\,(V_1\otimes V_2\otimes\cdots\otimes V_n)$ is called a *Segre variety*.

[2]Note that all the tensors proportional to a given decomposable tensor are decomposable, because $\lambda\cdot v_1\otimes v_2\otimes\cdots\otimes v_n=(\lambda v_1)\otimes v_2\otimes\cdots\otimes v_n$.

We will see in Example 2.8 on p. 50 that this Segre variety actually is algebraic and can be described by a system of homogeneous quadratic equations, necessary and sufficient for the complete decomposability of a tensor $t \in V_1 \otimes V_2 \otimes \cdots \otimes V_n$ in a tensor product of n vectors. On the other hand, the Segre variety can be described parametrically as the image of the *Segre embedding* $s : \mathbb{P}_{m_1} \times \cdots \times \mathbb{P}_{m_n} \to \mathbb{P}_m$, mapping the product of projective spaces $\mathbb{P}_{m_i} = \mathbb{P}(V_i)$ to the projectivization of the tensor product of the underlying vector spaces $\mathbb{P}_m = \mathbb{P}(V_1 \otimes V_2 \otimes \cdots \otimes V_n)$. It sends a collection of 1-dimensional subspaces spanned by nonzero vectors $v_i \in V_i$ to the 1-dimensional subspace spanned by the decomposable tensor

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n \in V_1 \otimes V_2 \otimes \cdots \otimes V_n.$$

Exercise 1.2 Verify that the map s is well defined and injective.

Note that the expected dimension of the Segre variety equals $\sum m_i = -n + \sum \dim V_i$ and is much less than $\dim \mathbb{P}(V_1 \otimes V_2 \otimes \cdots \otimes V_n) = \prod \dim V_i - 1$. However, the Segre variety does not lie in a hyperplane and linearly spans the whole ambient space. Also note that by construction, the Segre variety is ruled by n families of projective spaces of dimensions $m_1, m_2, \ldots, m_n$.

1.2.2 Linear Maps as Tensors

For two vector spaces U, W there exists a bilinear map

$$W \times U^* \to \operatorname{Hom}(U, V) \tag{1.15}$$

that sends a pair $(w, \xi) \in W \times U^*$ to the linear map

$$w \otimes \xi : U \to W, \quad u \mapsto w \cdot \xi(u). \tag{1.16}$$

If the vector w and covector ξ are both nonzero, then $\operatorname{rk} w \otimes \xi = 1$. In this case, the image of the linear map (1.16) has dimension 1 and is spanned by the vector $w \in W$, and the kernel $\ker(w \otimes \xi) = \operatorname{Ann}(\xi) \subset U$ has codimension 1.

Exercise 1.3 Convince yourself that every linear operator $F : U \to W$ of rank 1 is of the form (1.16) for appropriate nonzero covector $\xi \in U^*$ and vector $w \in W$ uniquely up to proportionality determined by F.

By the universal property of tensor product, the bilinear map (1.15) produces the unique linear map

$$W \otimes U^* \to \operatorname{Hom}(U, W) \tag{1.17}$$

sending a decomposable tensor $\xi \otimes w \in W \otimes U^*$ to the linear map (1.16). If both vector spaces U, W are finite-dimensional, then the map (1.17) is an isomorphism of vector spaces. To check this, we fix some bases $\boldsymbol{w} = (u_1, u_2, \ldots, u_n)$ in U and $\boldsymbol{w} = (w_1, w_2, \ldots, w_m)$ in W, and write $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$ for the basis in U^*

dual to $\boldsymbol{u}$. Then the mn tensors $w_i \otimes u_j^*$ form a basis in $W \otimes U^*$ by Lemma 1.2. The corresponding linear maps (1.16) act on the basis of U as

$$w_i \otimes u_j^* : u_k \mapsto \begin{cases} w_i & \text{for } k = j, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the matrix of the operator $w_i \otimes u_j^*$ in the bases $\boldsymbol{u}$, $\boldsymbol{w}$ is exactly the standard basis matrix $E_{ij} \in \mathrm{Mat}_{m\times n}(\Bbbk)$. So the basis of $U^* \otimes V$ built from the bases $\boldsymbol{u}$, $\boldsymbol{w}$ via Theorem 1.1 goes to the standard basis of $\mathrm{Hom}(U, W)$ associated with the bases $\boldsymbol{u}, \boldsymbol{w}$.

In the language of projective geometry, the rank-one operators $U \to W$, considered up to proportionality, form the Segre variety $S \subset \mathbb{P}(\mathrm{Hom}(U, W))$, the image of the Segre embedding

$$s : \mathbb{P}_{m-1} \times \mathbb{P}_{n-1} = \mathbb{P}(W) \times \mathbb{P}(U^*) \hookrightarrow \mathbb{P}(\mathrm{Hom}(U, W)) = \mathbb{P}_{mn-1}.$$

For points $w \in \mathbb{P}_{m-1} = \mathbb{P}(W)$, $\xi \in \mathbb{P}_{n-1} = \mathbb{P}(U^*)$ with the homogeneous coordinates

$$\boldsymbol{x} = (x_1 : x_2 : \cdots : x_n) \quad \text{and} \quad \boldsymbol{y} = (y_1 : y_2 : \cdots : y_n)$$

in the bases $\boldsymbol{w}$ and $\boldsymbol{u}^*$ respectively, the map s takes the pair (w, ξ) to the linear operator whose matrix in the bases $\boldsymbol{u}$, $\boldsymbol{w}$ is $\boldsymbol{x}^t \cdot \boldsymbol{y} = \left(x_i y_j\right)$. The set of all rank-1 matrices $A = \left(a_{ij}\right) \in \mathrm{Mat}_{m\times n}(\Bbbk)$ considered up to proportionality is described in $\mathbb{P}_{mn-1} = \mathbb{P}\left(\mathrm{Mat}_{m\times n}(\Bbbk)\right)$ by a system of homogeneous quadratic equations

$$\det \begin{pmatrix} a_{ij} & a_{ik} \\ a_{\ell j} & a_{\ell k} \end{pmatrix} = a_{ij}a_{\ell k} - a_{ik}a_{\ell j} = 0$$

for all $1 \leqslant i < \ell \leqslant m$, $1 \leqslant j < k \leqslant n$. These equations certify the vanishing of all 2×2 minors in A. Their solution set, the Segre variety $S \subset \mathbb{P}_{mn-1}$, is bijectively parameterized by $\mathbb{P}_{m-1} \times \mathbb{P}_{n-1}$ as $a_{ij} = x_i y_j$. This parameterization takes two families of "coordinate planes" $\{\boldsymbol{x} \times \mathbb{P}_{n-1}\}_{\boldsymbol{x}\in\mathbb{P}_{m-1}}$ and $\{\mathbb{P}_{m-1} \times \boldsymbol{y}\}_{\boldsymbol{y}\in\mathbb{P}_{n-1}}$ on $\mathbb{P}_{m-1} \times \mathbb{P}_{n-1}$ to two families of projective spaces ruling the Segre variety S. They consist of all rank-1 matrices with prescribed ratios either between the rows or between the columns. Note that $\dim S = \dim(\mathbb{P}_{m-1} \times \mathbb{P}_{n-1}) = m + n - 2$ is much less than $\dim \mathbb{P}_{mn-1} = mn - 1$ for $m, n \gg 0$. However, S does not lie in any hyperplane of $\mathbb{P}_{mn-1}$.

Example 1.3 (The Segre Quadric in $\mathbb{P}_3$) For $\dim U = \dim W = 2$, the Segre embedding $\mathbb{P}_1 \times \mathbb{P}_1 \hookrightarrow \mathbb{P}_3 = \mathbb{P}\left(\mathrm{Mat}_2(\Bbbk)\right)$ assigns the bijection between $\mathbb{P}_1 \times \mathbb{P}_1$ and the determinantal *Segre quadric*

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\Bbbk) \ : \ ad - bc = 0 \right\}$$

considered in Example 17.6 of Algebra I. A pair of points

$$w = (x_0 : x_1) \in W, \xi = (y_0 : y_1) \in \mathbb{P}\left(U^*\right)$$

is mapped to the matrix

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \cdot \begin{pmatrix} y_0 & y_1 \end{pmatrix} = \begin{pmatrix} x_0y_0 & x_0y_1 \\ x_1y_0 & x_1y_1 \end{pmatrix}. \tag{1.18}$$

The two families of "coordinate lines" $\{w \times \mathbb{P}_1\}_{w\in\mathbb{P}(W)}$, $\{\mathbb{P}_1 \times \xi\}_{\xi\in\mathbb{P}(U^*)}$ go to the two families of lines ruling the Segre quadric and formed by the rank-one matrices with prescribed ratios

$$\begin{aligned} ([\text{top row}] : [\text{bottom row}]) &= (x_0 : x_1), \\ ([\text{left column}] : [\text{right column}]) &= (y_0 : y_1). \end{aligned}$$

Every line lying on the Segre quadric belongs to exactly one of these two ruling families. All the lines in each family have no intersections, whereas every two lines from different families intersect, and every point on S is the intersection point of two lines from different families.

Exercise 1.4 Prove all these claims.

1.2.3 Tensor Products of Abelian Groups

The description of the tensor product $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ given in Sect. 1.2 is not so explicit as one could want. For nonfree modules V_i, it may not be easy to understand from that description even whether the tensor product is zero.

As an example, let us describe the tensor products of finitely generated $\mathbb{Z}$-modules, i.e., the abelian groups. First, we claim that $\mathbb{Z}/(m) \otimes \mathbb{Z}/(n) = 0$ for all coprime $m, n \in \mathbb{Z}$. Indeed, the class $[n] = n \pmod m$ is invertible in the residue ring $\mathbb{Z}/(m)$ in this case, and therefore, every element $a \in \mathbb{Z}/(m)$ can be written as $a = n \cdot a'$ with $a' = [n]^{-1}a \in \mathbb{Z}/(m)$. On the other hand, $nb = 0$ in $\mathbb{Z}/(n)$ for all $b \in \mathbb{Z}/(n)$. Hence, for all decomposable tensors $a \otimes b \in \mathbb{Z}/(m) \otimes \mathbb{Z}/(n)$,

$$a \otimes b = (n \cdot a') \otimes b = n \cdot (a' \otimes b) = a' \otimes (n \cdot b) = \alpha' \otimes 0 = \alpha' \otimes (0 \cdot 0) = 0 \cdot (\alpha' \otimes 0) = 0.$$

Since the decomposable tensors span $\mathbb{Z}/(m) \otimes \mathbb{Z}/(n)$ over $\mathbb{Z}$, this is the zero module. Now we compute $\mathbb{Z}/(p^n) \otimes \mathbb{Z}/(p^m)$ for a prime p and all $n \leqslant m$. Consider the multiplication map

$$\mu : \mathbb{Z}/(p^n) \times \mathbb{Z}/(p^m) \to \mathbb{Z}/(p^n), \quad \left([a]_{p^n}, [b]_{p^m}\right) \mapsto [ab]_{p^n} = ab \cdot [1]_{p^n}. \tag{1.19}$$

It is certainly well defined and $\mathbb{Z}$-bilinear. Let us verify that it is universal. Since for every bilinear map $\varphi : \mathbb{Z}/(p^n) \times \mathbb{Z}/(p^m) \to W$, the equality $\varphi([a]_{p^n}, [b]_{p^m}) = ab \cdot \varphi\left([1]_{p^n}, [1]_{p^m}\right)$ holds, a linear map $F : \mathbb{Z}/(p^n) \to W$ such that $\varphi = F \circ \mu$ has to send the generator $[1]_{p^n}$ of the module $\mathbb{Z}/(p^n)$ to the vector $\varphi\left([1]_{p^n}, [1]_{p^m}\right)$. Therefore, such a linear map F is unique if it exists. It indeed exists by Proposition 14.1 of Algebra I, because the basis linear relation $p^n \cdot [1]_{p^n} = 0$ on the generator $[1]_{p^n}$ of $\mathbb{Z}/(p^n)$ holds for the vector $\varphi\left([1]_{p^n}, [1]_{p^m}\right)$ in W as well:

$$\begin{aligned} p^n \cdot \varphi\left([1]_{p^n}, [1]_{p^m}\right) &= \varphi\left(p^n \cdot [1]_{p^n}, [1]_{p^m}\right) = \varphi\left(0, [1]_{p^m}\right) = \varphi\left(0 \cdot 0, [1]_{p^m}\right) \\ &= 0 \cdot \varphi\left(0, [1]_{p^m}\right) = 0\,. \end{aligned}$$

Since the multiplication map (1.19) is the universal bilinear map, then

$$\mathbb{Z}/(p^n) \otimes \mathbb{Z}/(p^m) \simeq \mathbb{Z}/\left(p^{\min(n,m)}\right).$$

Finally, $\mathbb{Z} \otimes A \simeq A$ for every $\mathbb{Z}$-module A, because the multiplication map $\mu : \mathbb{Z} \times A \to A$, $(n, a) \mapsto na$, is obviously the universal bilinear map too, because for every bilinear map $\varphi : \mathbb{Z} \times A \to W$, a linear map $F : A \to W$ such that $F\mu = \varphi$ should be and actually is defined by the prescription $a \mapsto \varphi(1, a)$. Computation of the tensor product of two arbitrary abelian groups

$$A = \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{\left(p_1^{n_1}\right)} \oplus \cdots \oplus \frac{\mathbb{Z}}{\left(p_\alpha^{n_\alpha}\right)} \quad \text{and} \quad B = \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{\left(q_1^{m_1}\right)} \oplus \cdots \oplus \frac{\mathbb{Z}}{\left(q_\beta^{m_\beta}\right)}$$

is reduced to the three particular cases considered above by means of the canonical isomorphisms stating the distributivity of the tensor product with respect to direct sums, and the commutativity and associativity of the tensor product. We establish these isomorphisms in the next section.

Exercise 1.5 Prove that for every module V over an arbitrary commutative ring K, the multiplication $K \otimes V \to V$, $\lambda \otimes v \mapsto \lambda v$, is a well-defined linear isomorphism of K-modules.

1.3 Commutativity, Associativity, and Distributivity Isomorphisms

In this section we consider arbitrary modules over a commutative ring K. It is often convenient to define linear maps

$$f : V_1 \otimes V_2 \otimes \cdots \otimes V_n \to W \tag{1.20}$$

by indicating the values of f on the decomposable tensors, that is, by the prescription

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto f(v_1, v_2, \ldots, v_n). \tag{1.21}$$

Since the decomposable tensors linearly generate $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ over K, we know from Proposition 14.1 of Algebra I that there exists at most one linear map (1.20) acting on the decomposable tensors by the rule (1.21), and it exists if and only if all the linear relations between the decomposable tensors in $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ hold between the vectors $f(v_1, v_2, \ldots, v_n)$ in W as well. Since the linear relations between the decomposable tensors are linearly generated by the multilinearity relations from formula (1.13) on p. 5, we get the following useful criterion.

Lemma 1.3 *If the vectors $f(v_1, v_2, \ldots, v_n)$ in (1.21) depend multilinearly*[3] *on the vectors $v_1, v_2, \ldots, v_n$, then there exists a unique linear map (1.20) acting on the decomposable tensors by the rule (1.21).* □

Proposition 1.1 (Commutativity Isomorphism) *The map*

$$U \otimes W \xrightarrow{\sim} W \otimes U, u \otimes w \mapsto w \otimes u,$$

is a well-defined linear isomorphism.

Proof Since the prescription $u \otimes w \mapsto w \otimes u$ is bilinear in u, w, it assigns the well-defined homomorphism of K-modules $U \otimes W \to W \otimes U$. For the same reason, there exists the well-defined K-linear map $W \otimes U \to U \otimes W$, $w \otimes u \mapsto u \otimes w$. These two maps are inverse to each other, because both of their compositions act identically on the decomposable tensors spanning $U \otimes W$ and $W \otimes U$ over K. □

Proposition 1.2 (Associativity Isomorphism) *The maps*

$$V \otimes (U \otimes W) \xleftarrow{\sim} V \otimes U \otimes W \xrightarrow{\sim} (V \otimes U) \otimes W$$

taking $v \otimes u \otimes w$, respectively, to $v \otimes (u \otimes w)$ and $(v \otimes u) \otimes w$ are well-defined linear isomorphisms.

Proof The tensor $v \otimes (u \otimes w) \in V \otimes (U \otimes W)$ depends 3-linearly on (v, u, w). Hence, by Lemma 1.3, there exists the well-defined linear map $V \otimes U \otimes W \to V \otimes (U \otimes W)$, $v \otimes u \otimes w \mapsto v \otimes (u \otimes w)$. The inverse map is constructed in two steps as follows. For all $v \in V$, the tensor $v \otimes u \otimes w$ depends bilinearly on u, w. Therefore, there exists the linear map $\tau_v : U \otimes W \to V \otimes U \otimes W$, $u \otimes w \mapsto v \otimes u \otimes w$. Since this map depends linearly on v, the tensor $\tau_v(t) = v \otimes t$ is bilinear in $v \in V$ and $t \in U \otimes W$. By Lemma 1.3, there exists the linear map $V \otimes (U \otimes W) \to V \otimes U \otimes W$, $v \otimes (u \otimes w) \mapsto v \otimes u \otimes w$, which is certainly inverse to the map

$$V \otimes U \otimes W \to V \otimes (U \otimes W), \quad v \otimes u \otimes w \mapsto v \otimes (u \otimes w).$$

The arguments establishing the isomorphism $V \otimes U \otimes W \xrightarrow{\sim} (V \otimes U) \otimes W$ are similar. □

[3] That is, are linear in each v_i while all the other v_j are fixed.

Proposition 1.3 (Distributivity Isomorphisms) *For every K-module V and family of K-modules U_x, $x \in X$, the maps*

$$V \otimes \Big(\bigoplus_{x\in X} U_x \Big) \xrightarrow{\sim} \bigoplus_{x\in X} (V \otimes U_x) , \quad v \otimes (u_x)_{x\in X} \mapsto (v \otimes u_x)_{x\in X} , \tag{1.22}$$

$$\Big(\bigoplus_{x\in X} U_x \Big) \otimes V \xrightarrow{\sim} \bigoplus_{x\in X} (U_x \otimes V) , \quad (u_x)_{x\in X} \otimes v \mapsto (u_x \otimes v)_{x\in X} , \tag{1.23}$$

are well-defined isomorphisms of K-modules.

Proof It is enough to prove only (1.22). Then (1.23) follows by the commutativity isomorphism from Proposition 1.1. The map (1.22) is well defined, because the family $(v \otimes u_x)_{x\in X}$ depends bilinearly on the vector $v \in V$ and the family

$$(u_x)_{x\in X} \in \bigoplus_{x\in X} U_x.$$

The inverse map is constructed as follows. For every $x \in X$ there exists a well-defined linear map $\varphi_x : V \otimes U_x \to V \otimes \bigoplus_{x\in X} U_x$ sending $v \otimes u \in V \otimes U_x$ to $v \otimes (w_\nu)_{\nu\in X}$, where the family $(w_\nu)_{\nu\in X} \in \bigoplus_{x\in X} U_x$ has $w_x = u$ and $w_\nu = 0$ for all other $\nu \neq x$. The sum of the maps φ_x over all $x \in X$ gives the map

$$\varphi : \bigoplus_{x\in X} (V \otimes U_x) \to V \otimes \bigoplus_{x\in X} U_x, \quad (v_x \otimes u_x)_{x\in X} \mapsto \sum_{x\in X} \varphi_x (v_x \otimes u_x) . \tag{1.24}$$

It is well defined, because $v_x \otimes u_x = 0$ for all but finitely many $x \in X$ by the definition of direct sum $\bigoplus_{x\in X} (V \otimes U_x)$, and therefore, the rightmost sum in (1.24) is finite.

Exercise 1.6 Show that for every set of K-module homomorphisms $\varphi_x : U_x \to W$, a well-defined linear map $\sum \varphi_x : \bigoplus_{x\in X} U_x \to W$ is given by the rule

$$(u_x)_{x\in X} \mapsto \sum_{x\in X} \varphi_x (u_x) .$$

Write $v \otimes u_x \in \bigoplus_{x\in X} (V \otimes U_x)$ for the family $(w_\nu)_{\nu\in X}$ in which

$$w_x = v \otimes u_x \in V \otimes U_x$$

and $w_\nu = 0$ for all other $\nu \neq x$. The vectors $v \otimes u_x$ for $v \in V$, $u_x \in U_x$, $x \in X$ span $\bigoplus_{x\in X} (V \otimes U_x)$. Since $\psi\varphi (v \otimes u_x) = v \otimes u_x$, we conclude that $\psi\varphi = \mathrm{Id}$. Now write $u_x \in \bigoplus_{x\in X} U_x$ for the family $(w_\nu)_{\nu\in X}$ in which $w_x = u_x$ and $w_\nu = 0$ for all other $\nu \neq x$. The tensors $v \otimes u_x$ with $v \in V$, $u_x \in U_x$, $x \in X$ span the tensor product $V \otimes \big(\bigoplus_{x\in X} U_x \big)$. Since $\varphi\psi (v \otimes u_x) = v \otimes u_x$, we conclude that $\varphi\psi = \mathrm{Id}$. □

1.4 Tensor Product of Linear Maps

For a finite collection of K-linear maps $f_i : U_i \to W_i$ between modules over a commutative ring K, the tensor

$$f_1(u_1) \otimes f_2(u_2) \otimes \cdots \otimes f_n(u_n) \in W_1 \otimes W_2 \otimes \cdots \otimes W_n$$

depends multilinearly on the vectors $(u_1, u_2, \dots, u_n) \in U_1 \times U_2 \times \cdots \times U_n$. Hence, there exists the linear map

$$f_1 \otimes f_2 \otimes \cdots \otimes f_n : U_1 \otimes U_2 \otimes \cdots \otimes U_n \to W_1 \otimes W_2 \otimes \cdots \otimes W_n$$

such that $u_1 \otimes u_2 \otimes \cdots \otimes u_n \mapsto f_1(u_1) \otimes f_2(u_2) \otimes \cdots \otimes f_n(u_n)$.
It is called the *tensor product of maps* $f_i : U_i \to W_i$.

Example 1.4 (Kronecker Matrix Product) Consider two vector spaces U, W with bases $u_1, u_2, \dots, u_n$ and $w_1, w_2, \dots, w_m$ respectively, and let the linear operators $f : U \to U$, $g : W \to W$ have matrices $F = (\varphi_{ij})$ and $G = (\gamma_{k\ell})$ in these bases. By Theorem 1.1 on p. 6, the tensors $u_j \otimes w_\ell$ form a basis in $U \otimes W$. The matrix of the operator $f \otimes g$ in this basis has size $(mn) \times (mn)$, and its entry at the intersection of the (i, k)th row with the (j, ℓ)th column equals $\varphi_{ij}\gamma_{k\ell}$, because

$$f \otimes g\,(u_j \otimes w_\ell) = \Big(\sum_i u_i\varphi_{ij}\Big) \otimes \Big(\sum_k w_k\gamma_{k\ell}\Big) = \sum_{i,k} \varphi_{ij}\gamma_{k\ell} \cdot u_i \otimes w_k.$$

This matrix is called the *Kronecker product* of matrices F, G. If the basis in $U \otimes W$ is ordered lexicographically,

$$u_1 \otimes w_1, \dots, u_1 \otimes w_m, u_2 \otimes w_1, \dots, u_2 \otimes w_m, \dots, u_n \otimes w_1, \dots, u_n \otimes w_m,$$

then the Kronecker product turns into the block matrix

$$F \otimes G = (\varphi_{ij}) \otimes (\gamma_{k\ell}) = \begin{pmatrix} \varphi_{11}G & \varphi_{12}G & \cdots & \varphi_{1n}G \\ \varphi_{21}G & \varphi_{22}G & \cdots & \varphi_{2n}G \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{n1}G & \varphi_{n2}G & \cdots & \varphi_{nn}G \end{pmatrix},$$

which consists of n^2 blocks of size $m \times m$, each proportional to the matrix G.

Lemma 1.4 *For every epimorphism of K-modules $f : U \twoheadrightarrow W$ and every K-module V, the map* $\mathrm{Id}_V \otimes f : V \otimes U \to V \otimes W$ *is surjective.*

Proof All decomposable tensors $v \otimes w \in V \otimes W$ certainly lie in the image of $f \otimes \mathrm{Id}_V$. □

Lemma 1.5 *For every monomorphism of K-modules $f : U \hookrightarrow W$ and every free K-module F, the map $\mathrm{Id}_F \otimes f : F \otimes U \to F \otimes W$ is injective.*

Proof If $F \simeq K$ has rank one, then the multiplication maps

$$K \otimes U \xrightarrow{\sim} U, \quad \lambda \otimes u \mapsto \lambda u,$$
$$K \otimes W \xrightarrow{\sim} W, \quad \mu \otimes w \mapsto \mu w,$$

are bijective by Exercise 1.5, and they transform the map $\mathrm{Id}_F \otimes f : K \otimes U \to K \otimes W$ into the map $f : U \to W$. Thus, $\mathrm{Id}_F \otimes f$ is injective as soon as f is injective. An arbitrary free module F with a basis E is the direct sum $F \simeq \bigoplus_{e \in E} Ke$ of rank-one modules Ke, numbered by the basis vectors $e \in E$. By Proposition 1.3 and Exercise 1.5,

$$\begin{aligned} F \otimes U &\simeq \bigoplus_{e \in E} (Ke \otimes U) \simeq \bigoplus_{e \in E} U_e, \\ F \otimes W &\simeq \bigoplus_{e \in E} (Ke \otimes W) \simeq \bigoplus_{e \in E} W_e, \end{aligned} \tag{1.25}$$

where $U_e = U$, $W_e = W$ are just the copies of U, W marked by $e \in E$ to indicate the summands $Ke \otimes U \simeq U$, $Ke \otimes W \simeq W$ from which these copies come. The isomorphisms (1.25) identify the map $\mathrm{Id}_F \otimes f$ with the map

$$\bigoplus_{e \in E} U_e \to \bigoplus_{e \in E} U_e, \quad (u_e)_{e \in E} \mapsto \big(f(u_e)\big)_{e \in E},$$

which is injective as soon as the map f is injective. □

Caution 1.1 For a nonfree module F, the map $\mathrm{Id}_F \otimes f : F \otimes U \to F \otimes W$ may be noninjective even if the both the modules U, W in the monomorphism $f : U \hookrightarrow W$ are free. For example, the tensor product of the $\mathbb{Z}$-module monomorphism

$$f : \mathbb{Z} \hookrightarrow \mathbb{Z}, \quad z \mapsto 2z,$$

with the identity endomorphism of $\mathbb{Z}/(2)$ is the zero map

$$f \otimes \mathrm{Id}_{\mathbb{Z}/(2)} : \mathbb{Z}/(2) \to \mathbb{Z}/(2), \quad [1]_2 \mapsto [0]_2.$$

1.5 Tensor Product of Modules Presented by Generators and Relations

Recall[4] that a K-module V generated by some vectors $v_1, v_2, \dots, v_n$ can be presented as the quotient module $V = K^n/R_{\boldsymbol{v}}$, where $R_{\boldsymbol{v}} \subset K^n$ consists of all $(x_1, x_2, \dots, x_n) \in K^n$ such that $x_1v_1 + x_2v_2 + \dots + x_nv_n = 0$ in V. Let $V_1 \simeq F_1/R_1$, $V_2 \simeq F_2/R_2$ be two K-modules presented in this way. We are going to describe the tensor product $V_1 \otimes V_2$ as the quotient of the free module $F_1 \otimes F_2$ by some relation submodule. To describe the generating relations, write $\iota_1 : R_1 \hookrightarrow F_1$, $\iota_2 : R_2 \hookrightarrow F_2$ for the inclusions of the relation submodules R_1, R_2 for V_1, V_2 in the corresponding free modules. By Lemma 1.5, the monomorphisms $\iota_1 \otimes \mathrm{Id}_{F_1} : R_1 \otimes F_2 \hookrightarrow F_1 \otimes F_2$, $\mathrm{Id}_{F_1} \otimes \iota_2 : F_1 \otimes R_2 \hookrightarrow F_1 \otimes F_2$ allow us to consider the tensor products $R_1 \otimes F_2$, $F_1 \otimes R_2$ as the submodules of the free module $F \otimes G$. Write

$$R_1 \otimes F_2 + F_1 \otimes R_2 \subset F_1 \otimes F_2$$

for their linear span.

Theorem 1.2 *For every commutative ring K, free K-modules F_1, F_2, and relation submodules $R_1 \subset F_1$, $R_2 \subset F_2$, one has*

$$(F_1/R_1) \otimes (F_1/R_1) \simeq (F_1 \otimes F_2) \,/\, (R_1 \otimes F_2 + F_1 \otimes R_2)\,.$$

Proof Let $V_1 = F_1/R_1$, $V_2 = F_2/R_2$, $S = R_1 \otimes F_2 + F_1 \otimes R_2 \subset F_1 \otimes F_2$. For all $f_1 \in F_1, f_2 \in F_2$, the class $[f_1 \otimes f_2]_S = f_1 \otimes f_2 \pmod{S} \in (F_1 \otimes F_2)\,/S$ depends only on the classes

$$[f_1]_{R_1} = f_1 \pmod{R_1} \in V_1 \quad \text{and} \quad [f_2]_{R_2} = f_2 \pmod{R_2} \in V_2,$$

because

$$(f_1 + r_1) \otimes (f_2 + r_2) = f_1 \otimes f_2 + (r_1 \otimes f_2 + f_1 \otimes r_2 + r_1 \otimes r_2) \equiv f_1 \otimes f_2 \pmod{S}$$

for all $r_1 \in R_1$, $r_2 \in R_2$. Hence, there exists the well-defined bilinear map

$$\overline{\tau} : V_1 \times V_2 \to (F_1 \otimes F_2)\,/S, \quad ([f_1]_{R_1}, [f_2]_{R_2}) \mapsto [f_1 \otimes f_2]_S, \tag{1.26}$$

[4] See Sect. 14.1.2 of Algebra I.

that fits in the commutative diagram

$$\begin{tikzcd} F_1 \times F_2 \arrow[r, "\tau"] \arrow[d, "\pi_1\times\pi_2"'] & F_1 \otimes F_2 \arrow[d, "\pi"] \\ V_1 \times V_2 \arrow[r, "\overline{\tau}"] & (F_1 \otimes F_2)/S \end{tikzcd} \tag{1.27}$$

where $\pi_1 : F_1 \twoheadrightarrow V_1$, $\pi_2 : F_2 \twoheadrightarrow V_2$, $\pi : F_1 \otimes F_2 \twoheadrightarrow (F_1 \otimes F_2)/S$ are the quotient maps and $\tau : F_1 \times F_2 \to F_1 \otimes F_2$ is the universal bilinear map. We have to show that the bilinear map (1.26) is universal. For every bilinear map $\varphi : V_1 \times V_2 \to W$, the composition

$$\varphi \circ (\pi_1 \times \pi_2) : F_1 \times F_2 \to W, \quad (f_1, f_2) \mapsto \varphi\left([f_1]_{R_1}, [f_2]_{R_2}\right),$$

is bilinear. Hence, there exists a unique linear map $\psi : F_1 \otimes F_2 \to W$ such that $\psi \circ \tau = \varphi \circ (\pi_1 \times \pi_2)$, i.e., $\psi(f_1 \otimes f_2) = \varphi\left([f_1]_{R_1}, [f_2]_{R_2}\right)$ for all $f_1 \in F_1, f_2 \in F_2$. Therefore, ψ annihilates both submodules $R_1 \otimes F_2, F_1 \otimes R_2 \subset F_1 \otimes F_2$ spanning S, and is factorized through the linear map

$$\overline{\psi} : (F_1 \otimes F_2)/S \to W$$

such that $\overline{\psi} \circ \pi \circ \tau = \varphi \circ (\pi_1 \times \pi_2)$. Hence,

$$\overline{\psi} \circ \overline{\tau} \circ (\pi_1 \times \pi_2) = \overline{\psi} \circ \pi \circ \tau = \varphi \circ (\pi_1 \times \pi_2).$$

Since $\pi_1 \times \pi_2$ is surjective, we conclude that $\varphi = \overline{\psi} \circ \overline{\tau}$. It remains to show that such a factorization of φ through $\overline{\tau}$ is unique. Let a linear map $\eta : (F_1 \otimes F_2)/S \to W$ also satisfy $\eta \circ \overline{\tau} = \varphi$. Then

$$\eta \circ \pi \circ \tau = \eta \circ \overline{\tau} \circ (\pi_1 \times \pi_2) = \varphi \circ (\pi_1 \times \pi_2) = \overline{\psi} \circ \pi \circ \tau.$$

Therefore $\eta \circ \pi = \overline{\psi} \circ \pi$ by the universal property of τ. Since π is surjective, $\eta = \overline{\psi}$. □

Example 1.5 (Tensor Products of Abelian Groups Revisited) Theorem 1.2 brings all the computations made in Sect. 1.2.3 into one line:

$$\forall\, m, n \in \mathbb{Z} \quad \mathbb{Z}/(m) \otimes \mathbb{Z}/(n) \simeq \mathbb{Z}/(m, n) \simeq \mathbb{Z}/\left(\mathrm{GCD}(m, n)\right).$$

Problems for Independent Solution to Chapter 1

Problem 1.1 For arbitrary modules L, M, N over a commutative ring K with unit, construct the canonical isomorphisms **(a)** $\mathrm{Hom}(L \oplus M, N) \simeq \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(M, N)$, **(b)** $\mathrm{Hom}(L, M \oplus N) \simeq \mathrm{Hom}(L, M) \oplus \mathrm{Hom}(L, N)$, **(c)** $\mathrm{Hom}(L \otimes M, N) \simeq \mathrm{Hom}(L, \mathrm{Hom}(M, N))$.

Problem 1.2 Write the canonical decomposition of the $\mathbb{Z}$-module $\mathbb{Z}/(270) \otimes \mathbb{Z}/(360)$ as the direct sum of indecomposable modules $\mathbb{Z}/(p^m)$.

Problem 1.3 Write the canonical decompositions as the direct sum of indecomposable modules for the following $\mathbb{Z}$-modules: **(a)** $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(270), \mathbb{Z}/(360)\big)$, **(b)** $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(360), \mathbb{Z}/(270)\big)$, **(c)** $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(m), \mathbb{Z}/(n)\big)$ for coprime $m, n \in \mathbb{Z}$, **(d)** $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(p^m), \mathbb{Z}/(p^n)\big)$ for prime $p \in \mathbb{N}$.

Problem 1.4 Describe the following groups[5] of $\mathbb{Z}$-linear automorphisms of $\mathbb{Z}$-modules: **(a)** $\mathrm{Aut}\big(\mathbb{Z}/(p^n)\big)$ for prime $p \in \mathbb{N}$, **(b)** $\mathrm{Aut}\big(\mathbb{Z}/(30)\big)$, **(c)** $\mathrm{Aut}\big(\mathbb{Z}/(2) \oplus \mathbb{Z}\big)$.

Problem 1.5 Describe the tensor product of $\Bbbk[x]$-modules

$$\Bbbk[x]/(f) \otimes \Bbbk[x]/(g)$$

for an arbitrary field $\Bbbk$ and $f, g \in \Bbbk[x]$.

All the remaining problems are about finite-dimensional vector spaces over an arbitrary field $\Bbbk$.

Problem 1.6 Show that a collection of vectors $(v_1, v_2, \dots, v_n) \in V_1 \times V_2 \times \cdots \times V_n$ is annihilated by all multilinear maps $\varphi : V_1 \times V_2 \times \cdots \times V_n \to W$ if and only if some v_i is equal to 0.

Problem 1.7 Use the isomorphism $V \otimes U^* \simeq \mathrm{Hom}(U, V)$ to write linear maps $A : U \to V$ and $B : V \to W$ as $A = \sum a_\nu \otimes \alpha_\nu$, $B = \sum b_\mu \otimes \beta_\mu$ with $a_\nu \in V$, $\alpha_\nu \in U^*$, $b_\mu \in W$, and $\beta_\mu \in V^*$. Using only these vectors and covectors, write in the same way the composition $BA \in \mathrm{Hom}(U, W) \simeq U^* \otimes W$.

Problem 1.8 Let vectors $e_i \in V$ and covectors $x_i \in V^*$ form a pair of dual bases. Describe the linear endomorphism of V corresponding to the *Casimir tensor* $\sum e_i \otimes x_i \in V \otimes V^*$ under the isomorphism $V \otimes V^* \xrightarrow{\sim} \mathrm{End}\, V$. Does the Casimir tensor depend on the choice of dual bases?

Problem 1.9 Check that there is a well-defined linear map

$$\widehat{\tau} : \mathrm{End}(V) \simeq V \otimes V^* \to (V \otimes V^*)^* \simeq \mathrm{End}(V)^*$$

[5] Where the group operation is the composition of automorphisms.

sending a decomposable tensor $v \otimes \xi$ to the linear form $v' \otimes \xi' \mapsto \xi(v') \cdot \xi'(v)$. It provides the vector space $\operatorname{End}(V)$ with a correlation.[6] Describe the bilinear form on $\operatorname{End}(V)$ corresponding to this correlation. Is it symmetric? Is it degenerate? Write an explicit formula for the quadratic form $\tau(f) = \langle f, \widehat{\tau} f \rangle$ in terms of the matrix F of an endomorphism f in an arbitrary basis of V.

Problem 1.10 Construct the canonical[7] isomorphisms

$$\begin{aligned}\operatorname{End}\big(\operatorname{Hom}(U,W)\big) &\simeq \operatorname{Hom}\big(U \otimes \operatorname{Hom}(U,W),\ W\big)\\ &\simeq \operatorname{Hom}\big(U,\ \operatorname{Hom}(U,W)^* \otimes W\big).\end{aligned}$$

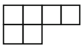
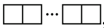
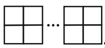
Describe the endomorphism of the vector space $\operatorname{Hom}(U,W)$ corresponding to the linear map $c : U \otimes \operatorname{Hom}(U,W) \to W$, $u \otimes f \mapsto f(u)$. Prove that the linear map $\widetilde{c} : U \to \operatorname{Hom}(U,W)^* \otimes W$ corresponding to c is injective for $W \neq 0$.

Problem 1.11 Construct the canonical isomorphism

$$\operatorname{End}(U \otimes V \otimes W) \simeq \operatorname{Hom}\big(\operatorname{Hom}(U,V) \otimes \operatorname{Hom}(V,W),\ \operatorname{Hom}(U,W)\big)$$

and describe the linear map $\operatorname{Hom}(U,V) \otimes \operatorname{Hom}(V,W) \to \operatorname{Hom}(U,W)$ corresponding to the identity endomorphism of $U \otimes V \otimes W$.

Problem 1.12 Let $f : \Bbbk^n \to \Bbbk^n$ and $g : \Bbbk^m \to \Bbbk^m$ be two diagonalizable linear operators with eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_n$ and $\mu_1, \mu_2, \dots, \mu_m$. Describe the eigenvalues of $f \otimes g$.

Problem 1.13 For a nilpotent operator $\eta \in \operatorname{End} V$ of cyclic type $\lambda(\eta)$, describe the cyclic type of the operator $\eta \otimes \eta \in \operatorname{End}(V^{\otimes 2})$. To begin with, let the diagram λ be **(a)** $(4,2) =$ , **(b)** $(n) =$ , **(c)** $(n,n) =$ , **(d)** (m,n) with $m > n$.

Problem 1.14 Construct the canonical isomorphisms between the vector space of n-linear forms $V \times V \times \cdots \times V \to \Bbbk$ and

(a) $(V^*)^{\otimes n} = V^* \otimes V^* \otimes \cdots \otimes V^*$,
(b) $\left(V^{\otimes n}\right)^* = (V \otimes V \otimes \cdots \otimes V)^*$.

Which of them remain valid for infinite-dimensional V?

Problem 1.15 Find the dimension of the space of all bilinear forms $\varphi : V \times V \to \Bbbk$ such that **(a)** $\varphi(v,v) = 0$ for all $v \in V$, **(b)** $\varphi(u,w) = \varphi(w,u)$ for all $u, w \in V$.

[6] Recall that a *correlation* on a vector space W is a linear map $\widehat{\beta} : W \to W^*$. The correlations are in bijection with the bilinear forms $\beta : W \times W \to \Bbbk$, $\beta(u,w) = \langle u, \widehat{\beta} w \rangle$ (see Sect. 16.1 of Algebra I).

[7] That is, independent of any extra data on U and W, such as the choice of bases.

Problem 1.16 Find the dimension of the space of 3-linear forms $\varphi : V \times V \times V \to \Bbbk$ such that for all $u, v, w \in V$:

(a) $\varphi(u, u, u) = 0$,
(b) $\varphi(u, v, w) = \varphi(v, u, w)$,
(c) $\varphi(u, v, w) = \varphi(v, w, u)$,
(d) $\varphi(u, v, w) = \varphi(v, u, w) = \varphi(u, w, v)$,
(e) $\varphi(u, v, v) = \varphi(u, u, v) = 0$,
(f) $\varphi(u, v, w) + \varphi(v, w, u) + \varphi(w, u, v) = 0$,
(g) $\varphi(u, v, w) = \varphi(v, u, w) = \varphi(u, w, w)$.

Chapter 2
Tensor Algebras

2.1 Free Associative Algebra of a Vector Space

Let V be a vector space over an arbitrary field $\Bbbk$. We write $V^{\otimes n} \stackrel{\text{def}}{=} V \otimes V \otimes \cdots \otimes V$ for the tensor product of n copies of V and call it the *nth tensor power* of V. We also put $V^{\otimes 0} \stackrel{\text{def}}{=} \Bbbk$ and $V^{\otimes 1} \stackrel{\text{def}}{=} V$. The infinite direct sum

$$\mathsf{T}V \stackrel{\text{def}}{=} \bigoplus_{n \geqslant 0} V^{\otimes n}$$

is called the *tensor algebra* of V. The multiplication in $\mathsf{T}V$ is provided by the tensor multiplication of vectors $V^{\otimes k} \times V^{\otimes m} \to V^{\otimes(k+m)}$, $(t_k, t_m) \mapsto t_k \otimes t_m$. For every basis E of V over $\Bbbk$, all the tensor monomials $e_1 \otimes e_2 \otimes \cdots \otimes e_d$ with $e_i \in E$ form a basis of $V^{\otimes d}$. These monomials are multiplied just by writing them sequentially with the sign $\otimes$ between them:

$$\begin{aligned}(e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_k}) \cdot \big(e_{j_1} \otimes e_{j_2} \otimes \cdots \otimes e_{j_m}\big) \\ = e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_k} \otimes e_{j_1} \otimes e_{j_2} \otimes \cdots \otimes e_{j_m}.\end{aligned}$$

Thus, $\mathsf{T}V$ is an associative but not commutative $\Bbbk$-algebra. It can be thought of as the algebra of polynomials in noncommuting variables $e \in E$ with coefficients in $\Bbbk$. From this point of view, the subspace $V^{\otimes d} \subset \mathsf{T}V$ consists of all homogeneous polynomials of degree d.

Another name for $\mathsf{T}V$ is the *free associative $\Bbbk$-algebra with unit* spanned by the vector space V. This name emphasizes the following *universal property* of the $\Bbbk$-linear map $\iota : V \hookrightarrow \mathsf{T}V$ embedding V into $\mathsf{T}V$ as the subspace $V^{\otimes 1}$ of linear homogeneous polynomials.

Proposition 2.1 (Universal Property of Free Associative Algebras) *For every associative $\Bbbk$-algebra A with unit and $\Bbbk$-linear map $f : V \to A$, there exists a unique homomorphism of $\Bbbk$-algebras $\widetilde{f} : \mathsf{T}V \to A$ such that $f = \widetilde{f} \circ \iota$. Thus, for every*

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_2

$\Bbbk$-algebra A, the homomorphisms of $\Bbbk$-algebras $\mathsf{T}V \to A$ are in bijection with the linear maps $V \to A$.

Exercise 2.1 Let $\iota' : V \to T'$, where T' is an associative $\Bbbk$-algebra with unit, be another linear map satisfying the universal property from Proposition 2.1. Show that there exists a unique isomorphism of $\Bbbk$-algebras $\psi : \mathsf{T}V \xrightarrow{\sim} T'$ such that $\psi\iota = \iota'$.

Proof (of Proposition 2.1) A homomorphism of $\Bbbk$-algebras $\widetilde{f} : \mathsf{T}V \to A$ such that $f = \widetilde{f} \circ \iota$ maps every decomposable tensor $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ to the product $f(v_1) \cdot f(v_2) \cdots f(v_n)$ in A, and therefore $\widetilde{f}$ is unique, because the decomposable tensors span $\mathsf{T}V$. Since the product $f(v_1) \cdot f(v_2) \cdots f(v_n)$ is multilinear in v_i, for each $n \in \mathbb{N}$ there exists the linear map

$$f_n : V \otimes V \otimes \cdots \otimes V \to A, \quad v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto f(v_1) \cdot f(v_2) \cdots f(v_n).$$

We put $f_0 : \Bbbk \to A$, $1 \mapsto 1$, and define $\widetilde{f} : \mathsf{T}V \to A$ to be the sum of all the f_n:

$$\widetilde{f} : \bigoplus_{n \geqslant 0} V^{\otimes n} \to A, \quad \sum_{n \geqslant 0} t_n \mapsto \sum_{n \geqslant 0} \varphi_n(t_n) \in A.$$

Since every tensor polynomial $t = \sum t_n \in \mathsf{T}V$ has a finite number of nonzero homogeneous components $t_n \in V^{\otimes n}$, the map $\widetilde{f}$ is a well-defined algebra homomorphism. $\square$

2.2 Contractions

2.2.1 Complete Contraction

For dual vector spaces V, V^* and two decomposable tensors of equal degree $t = v_1 \otimes v_2 \otimes \cdots \otimes v_n \in V^{\otimes n}$, $\vartheta = \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \in V^{*\otimes n}$, the product

$$\langle t, \vartheta \rangle \stackrel{\text{def}}{=} \prod_{i=1}^{n} \xi_i(v_i) = \prod_{i=1}^{n} \langle v_i, \xi_i \rangle \in \Bbbk \tag{2.1}$$

is called the *complete contraction* of t with ξ. For a fixed

$$\vartheta = \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \in V^{*\otimes n},$$

the constant $\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n, \vartheta \rangle \in \Bbbk$ depends multilinearly on the vectors $v_1, v_2, \ldots, v_n \in V$. Hence, there exists a unique linear form

$$c_\vartheta : V^{\otimes n} \to \Bbbk, \quad v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto \langle v_1 \otimes v_2 \otimes \cdots \otimes v_n, \vartheta \rangle .$$

Since the covector $c_\vartheta \in V^{\otimes n*}$ depends multilinearly on $\xi_1, \xi_2, \dots, \xi_n$, there exists a unique linear map

$$V^{*\otimes n} \to V^{\otimes n*}, \quad \vartheta \mapsto c_\vartheta . \tag{2.2}$$

In other words, the complete contraction assigns a well-defined pairing[1] between the vector spaces $V^{\otimes n}$ and $V^{*\otimes n}$,

$$V^{\otimes n} \times V^{*\otimes n} \to \Bbbk, \quad (t, \vartheta) \mapsto \langle\, t,\ \vartheta\, \rangle . \tag{2.3}$$

Proposition 2.2 *For a finite-dimensional vector space V, the pairing (2.3) is perfect, i.e., the linear map (2.2) is an isomorphism.*

Proof Choose dual bases $e_1, e_2, \dots, e_n \in V$ and $x_1, x_2, \dots, x_n \in V^*$. Then the tensor monomials $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_r}$ and $x_{j_1} \otimes x_{j_2} \otimes \cdots \otimes x_{j_s}$ form bases in $V^{\otimes n*}$ and $V^{*\otimes n}$ dual to each other with respect to the full contraction pairing (2.1). $\square$

Corollary 2.1 *For every finite-dimensional vector space V, there is a canonical isomorphism*

$$\left(V^*\right)^{\otimes n} \xrightarrow{\sim} \mathrm{Hom}(V, \dots, V\,;\, \Bbbk) \tag{2.4}$$

mapping the decomposable tensor $\vartheta = \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \in V^{*\otimes n}$ to the n-linear form

$$V \times V \times \cdots \times V \to \Bbbk, \quad (v_1, v_2, \dots, v_n) \mapsto \prod_{i=1}^{n} \xi_i(v_i).$$

Proof The universal property of tensor product $V^{\otimes n}$ asserts that the dual space $\left(V^{\otimes n}\right)^*$, that is, the space of linear maps $V^{\otimes n} \to \Bbbk$, is isomorphic to the space of n-linear forms $V \times V \times \cdots \times V \to \Bbbk$. It remains to compose this isomorphism with the isomorphism (2.2). $\square$

2.2.2 Partial Contractions

Given a pair of injective but not necessarily order-preserving maps

$$\{1, 2, \dots, p\} \overset{I}{\hookleftarrow} \{1, 2, \dots, m\} \overset{J}{\hookrightarrow} \{1, 2, \dots, q\},$$

[1] See Sect. 7.2 of Algebra I.

we write $I = (i_1, i_2, \dots, i_m)$ and $J = (j_1, j_2, \dots, j_m)$ for the sequences of their values $i_\nu = I(\nu), j_\nu = J(\nu)$. The *partial contraction* in the indices I, J is the linear map

$$c_J^I : V^{*\otimes p} \otimes V^{\otimes q} \to V^{*\otimes (p-m)} \otimes V^{\otimes (q-m)} \tag{2.5}$$

sending a decomposable tensor $\xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_p \otimes v_1 \otimes v_2 \otimes \cdots \otimes v_q$ to the product

$$\prod_{\nu=1}^{m} \langle v_{j_\nu}, \xi_{i_\nu} \rangle \cdot \Big(\bigotimes_{i \notin I} \xi_i\Big) \otimes \Big(\bigotimes_{j \notin J} v_j\Big), \tag{2.6}$$

obtained by contracting the i_νth tensor factor of $V^{*\otimes p}$ with the j_νth tensor factor of $V^{\otimes q}$ for $\nu = 1, 2, \dots, m$ and leaving all the other tensor factors in their initial order. Note that the different choices of injective maps I, J lead to different partial contraction maps (2.5) even if the maps have equal images and differ only in the order of sequences $i_1, i_2, \dots, i_m$ and $j_1, j_2, \dots, j_m$.

Exercise 2.2 Verify that the linear map (2.5) is well defined by its values (2.6) on the decomposable tensors.

Example 2.1 (Inner Product of Vector and Multilinear Form) Consider an n-linear form $\varphi : V \times V \times \cdots \times V \to \Bbbk$ as a tensor from $V^{*\otimes n}$ by means of the isomorphism from Corollary 2.1, and contract this tensor with a vector $v \in V$ at the first tensor factor. The result of such a contraction is called the *inner product* of the n-linear form φ with the vector v, and is denoted by $v \llcorner \varphi \in V^{*\otimes (n-1)}$. This tensor can be viewed as the $(n-1)$-linear form on V obtained from the form φ by setting the first argument equal to v. In other words,

$$v \llcorner \varphi(u_1, u_2, \dots, u_{n-1}) = \varphi\,(v,\, u_1, u_2, \dots, u_{n-1})$$

for all $u_1, u_2, \dots, u_{n-1} \in V$. Indeed, since both sides of the equality are linear in φ, it is enough to verify it only for the n-linear forms φ coming from the decomposable tensors

$$\xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \in V^{*\otimes n},$$

because the latter span $V^{*\otimes n}$. For such φ, we have

$$\begin{aligned}
\varphi\,(v,\, u_1, u_2, \dots, u_{n-1}) &= \langle v \otimes u_1 \otimes u_2 \otimes \cdots \otimes u_{n-1},\, \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \rangle \\
&= \langle v,\, \xi_1 \rangle \cdot \langle u_1,\, \xi_2 \rangle \cdot \langle u_2,\, \xi_3 \rangle \cdots \langle u_{n-1},\, \xi_n \rangle \\
&= \langle u_1 \otimes u_2 \otimes \cdots \otimes u_{n-1},\, \langle v,\, \xi_1 \rangle \cdot \xi_2 \otimes \cdots \otimes \xi_n \rangle \\
&= \big\langle u_1 \otimes u_2 \otimes \cdots \otimes u_{n-1},\, c_1^1\,(v \otimes \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n) \big\rangle \\
&= v \llcorner \varphi\,(u_1, u_2, \dots, u_{n-1})\,.
\end{aligned}$$

Exercise 2.3 Verify that for every pair of vector subspaces $U, W \subset V$, one has $U^{\otimes n} \cap W^{\otimes n} = (U \cap W)^{\otimes n}$ in $V^{\otimes n}$.

2.2.3 Linear Support and Rank of a Tensor

It follows from Exercise 2.3 that for every tensor $t \in V^{\otimes n}$, the intersection of all vector subspaces $U \subset V$ such that $t \in U^{\otimes n}$ is the minimal subspace of V with respect to inclusions whose nth tensor power contains t. It is called the *linear support* of t and denoted by $\mathrm{Supp}(t) \subset V$. Its dimension is denoted by $\mathrm{rk}\, t \stackrel{\text{def}}{=} \dim \mathrm{Supp}(t)$ and called the *rank* of the tensor t. Tensors t with $\mathrm{rk}\, t < \dim V$ are called *degenerate*. If we think of tensors as polynomials in noncommutative variables, then the degeneracy of a tensor t means that t depends on fewer than $\dim V$ variables for an appropriate choice of basis in V. For example, every tensor $t \in V^{\otimes n}$ of rank 1 can be written as $\lambda \cdot e^{\otimes n} = \lambda \cdot e \otimes e \otimes \cdots \otimes e$ for some nonzero vector $e \in \mathrm{Supp}(t)$ and $\lambda \in \Bbbk$. For a practical choice of such special coordinates and the computation of $\mathrm{rk}\, t$, we need a more effective description of $\mathrm{Supp}(t)$.

Let $t \in V^{\otimes n}$ be an arbitrary tensor. For every sequence $J = j_1 j_2 \dots j_{n-1}$ of $n-1$ distinct but not necessarily increasing indices $1 \leqslant j_\nu \leqslant n$, write

$$c_t^J : V^{*\otimes(n-1)} \to V, \quad \xi \mapsto c^{1,2,\dots,(n-1)}_{j_1,j_2,\dots,j_{n-1}}(\xi \otimes t) \tag{2.7}$$

for the contraction map that pairs all $(n-1)$ factors of $V^{*\otimes(n-1)}$ with the $(n-1)$ factors of t chosen in the order determined by J, that is, the νth factor of $V^{*\otimes(n-1)}$ is contracted with the j_νth factor of t for each $\nu = 1, 2, \dots, n-1$. The result of such a contraction is a linear combination of vectors that appear in monomials of t at the position not represented in J. This linear combination certainly belongs to $\mathrm{Supp}(t)$.

Theorem 2.1 *For every $t \in V^{\otimes n}$, the subspace* $\mathrm{Supp}(t) \subset V$ *is spanned by the images of the $n!$ contraction maps* (2.7) *corresponding to all possible choices of J.*

Proof Let $\mathrm{Supp}(t) = W \subset V$. We have to show that every linear form $\xi \in V^*$ annihilating all the subspaces $\mathrm{im}\left(c_t^I\right) \subset W$ has to annihilate all of W as well. Assume the contrary. Let $\xi \in V^*$ be a linear form having nonzero restriction on the subspace W and annihilating all the subspaces $c_t^J\left(V^{*\otimes(n-1)}\right)$. Write $\xi_1, \xi_2, \dots, \xi_d$ for a basis in V^* such that $\xi_1 = \xi$ and the restrictions of $\xi_1, \xi_2, \dots, \xi_k$ to W form a basis in W^*. Let $w_1, w_2, \dots, w_k$ be the dual basis of W. Expand t as a linear combination of tensor monomials built out of the w_i. Then

$$\xi\left(c_t^J(\xi_{\nu_1} \otimes \xi_{\nu_2} \otimes \cdots \otimes \xi_{\nu_{n-1}})\right)$$

is equal to the complete contraction of t with the monomial $\xi_{\mu_1} \otimes \xi_{\mu_2} \otimes \cdots \otimes \xi_{\mu_n}$ whose indices $\mu_1, \mu_2, \dots, \mu_n$ form the permutation of the indices $1, \nu_1, \nu_2, \dots, \nu_{n-1}$ uniquely determined by J. The result of this contraction equals the coefficient of the monomial $w_{\mu_1} \otimes w_{\mu_2} \otimes \cdots \otimes w_{\mu_n}$ in the expansion of t. Varying J and $\nu_1, \nu_2, \dots, \nu_{n-1}$ allows us to obtain every monomial $w_{\mu_1} \otimes w_{\mu_2} \otimes \cdots \otimes w_{\mu_n}$ containing w_1. Our assumption on $\xi = \xi_1$ forces the coefficients of all these monomials in t to vanish. Therefore, $w_1 \notin \mathrm{Supp}(t)$. Contradiction. □

2.3 Quotient Algebras of a Tensor Algebra

There are three kinds of ideals in a noncommutative ring R. A subring $I \subset R$ is called a *left ideal* if $xa \in I$ for all $a \in I$, $x \in R$. Symmetrically, I is called a *right ideal* if $ax \in I$ for all $a \in I$, $x \in R$. If $I \subset R$ is both a left and right ideal, then I is called a *two-sided ideal* or simply an *ideal* of R. The two-sided ideals are exactly the kernels of ring homomorphisms, because for a homomorphism of rings $\varphi : R \to S$ and $a \in R$ such that $\varphi(a) = 0$, the equality $\varphi(xay) = \varphi(x)\varphi(a)\varphi(y) = 0$ holds for all $x, y \in R$. Conversely, if an additive abelian subgroup $I \subset R$ is a two-sided ideal, then the quotient group[2] R/I inherits the well-defined multiplication by the usual rule $[a][b] \stackrel{\text{def}}{=} [ab]$.

Exercise 2.4 Check this.

Therefore, the quotient map $R \twoheadrightarrow R/I$ is a homomorphism of rings with kernel I. It follows from the factorization theorem for a homomorphism of abelian groups[3] that an arbitrary homomorphism of rings $\varphi : R \to S$ is factorized into a composition of the surjective quotient map $R \twoheadrightarrow R/\ker\varphi \simeq \operatorname{im}\varphi$ followed by the monomorphism $R/\ker\varphi \simeq \operatorname{im}\varphi \hookrightarrow S$.

The algebra of polynomials on a vector space V introduced in Sect. 11.2.1 of Algebra I and the algebra of Grassmannian polynomials from Sect. 9.4 of Algebra I can be described uniformly as the quotient algebras of the free associative algebra by appropriate two-sided ideals spanned by the *commutativity* and *skew-commutativity* relations. The details follow in the next four sections.

2.3.1 Symmetric Algebra of a Vector Space

Let V be a vector space over an arbitrary field $\Bbbk$. Write $\mathcal{I}_{\mathrm{sym}} \subset \mathsf{T}V$ for the two-sided ideal generated by the $\Bbbk$-linear span of all the differences

$$u \otimes w - w \otimes u \in V \otimes V. \tag{2.8}$$

The ideal $\mathcal{I}_{\mathrm{sym}}$ consists of finite linear combinations of the tensors obtained from the differences (2.8) by taking left and right products with arbitrary elements of $\mathsf{T}V$.

[2] See Sect. 6.6.1 of Algebra I.

[3] See Proposition 2.1 of Algebra I.

Therefore, the intersection $\mathcal{I}_{\text{sym}} \cap V^{\otimes n}$ is linearly spanned by the differences

$$(\cdots \otimes v \otimes w \otimes \cdots) - (\cdots \otimes w \otimes v \otimes \cdots), \tag{2.9}$$

where the right dotted fragments in both decomposable tensors are the same, as are the left dotted fragments as well. The whole ideal $\mathcal{I}_{\text{sym}}$ is the direct sum of these homogeneous components:

$$\mathcal{I}_{\text{sym}} = \bigoplus_{n \geqslant 0} \left(\mathcal{I}_{\text{sym}} \cap V^{\otimes n}\right).$$

The quotient algebra $SV \stackrel{\text{def}}{=} \mathsf{T}V/\mathcal{I}_{\text{sym}}$ is called the *symmetric algebra* of the vector space V. The multiplication in SV is induced by the tensor multiplication in $\mathsf{T}V$ and denoted by the dot sign $\cdot$, which is, however, usually omitted. The relations (2.8) force all vectors $u, w \in V$ to commute in SV. As a vector space, the symmetric algebra splits into the direct sum of homogeneous components

$$SV = \bigoplus_{n \geqslant 0} S^n V, \text{ where } S^n V \stackrel{\text{def}}{=} V^{\otimes n}/(\mathcal{I}_{\text{sym}} \cap V^{\otimes n}).$$

The space $S^n V$ is called the *nth symmetric power* of V. Note that $S^0 V = \Bbbk$ and $S^1 V = V$. The inclusion $\iota : V \hookrightarrow SV$, which maps V to $S^1 V$, has the following universal property.

Exercise 2.5 (Universal Property of Free Commutative Algebras) Show that for every commutative $\Bbbk$-algebra A and linear map $f : V \to A$, there exists a unique homomorphism of $\Bbbk$-algebras $\widetilde{f} : SV \to A$ such that $f = \widetilde{\varphi} \circ \iota$. Also show that for every linear map $\iota' : V \to S'$ to a commutative algebra S' that possesses the same universal property, there exists a unique isomorphism of algebras $\psi : S' \xrightarrow{\sim} SV$ such that $\psi\iota' = \iota$.

For this reason, the symmetric algebra SV is also called the *free commutative* $\Bbbk$-*algebra with unit* spanned by V. For every basis $e_1, e_2, \dots, e_d$ of V, the commutative monomials $e_1^{m_1} e_2^{m_2} \cdots e_d^{m_d}$ of total degree $\sum_i m_i = n$ form a basis in $S^n V$, as we have seen in Proposition 11.2 of Algebra I. Thus, the choice of basis in V assigns the isomorphism of $\Bbbk$-algebras $SV \simeq \Bbbk[e_1, e_2, \dots, e_d]$.

Exercise 2.6 Calculate $\dim S^n V$ for $\dim V = d$.

2.3.2 Symmetric Multilinear Maps

An n-linear map $\varphi : V \times V \times \cdots \times V \to U$ is called *symmetric* if $\varphi(v_{g_1}, v_{g_2}, \dots, v_{g_n}) = \varphi(v_1, v_2, \dots, v_n)$ for all permutations $g \in S_n$. The symmetric multilinear maps form a subspace of the vector space $\operatorname{Hom}(V, \dots, V; U)$ of all n-linear maps. We denote this subspace by $\operatorname{Sym}^n(V, U) \subset \operatorname{Hom}(V, \dots, V; U)$.

Given a symmetric n-linear map $\varphi : V \times V \times \cdots \times V \to U$, then for every vector space W, the right composition of linear maps $F : U \to W$ with φ assigns the linear map

$$\varrho_\varphi : \mathrm{Hom}(U, W) \to \mathrm{Sym}^n(V, W), \quad F \mapsto F \circ \varphi.$$

A symmetric multilinear map φ is called *universal* if ϱ_φ is an isomorphism for all W. The universal symmetric n-linear map is also called the n-ary *commutative multiplication* of vectors.

Exercise 2.7 Verify that the target spaces of any two universal symmetric n-linear maps are isomorphic by means of the unique linear map commuting with the commutative multiplication.

Proposition 2.3 *The universal symmetric n-linear map*

$$\sigma_n : V \times V \times \cdots \times V \to U$$

is provided by tensor multiplication followed by factorization through the commutativity relations, i.e.,

$$\sigma_n : V \times V \times \cdots \times V \overset{\tau}{\dashrightarrow} V^{\otimes n} \overset{\pi}{\twoheadrightarrow} S^n(V).$$

Proof By the universal property of tensor multiplication $\tau : V \times V \times \cdots \times V \to V^{\otimes n}$, every n-linear map $\varphi : V \times V \times \cdots \times V \to W$ is uniquely factorized as $\varphi = \widetilde{F} \circ \tau$ for some linear map $\widetilde{F} : V^{\otimes n} \to W$. If the multilinear map φ is symmetric, then the linear map $\widetilde{F}$ annihilates the commutativity relations (2.8):

$$\begin{aligned}
&\widetilde{F}\big((\cdots \otimes v \otimes w \otimes \cdots) - (\cdots \otimes w \otimes v \otimes \cdots)\big)\\
&\quad = \widetilde{F}(\cdots \otimes v \otimes w \otimes \cdots) - \widetilde{F}(\cdots \otimes w \otimes v \otimes \cdots)\\
&\quad = \varphi(\ldots, v, w, \ldots) - \varphi(\ldots, w, v, \ldots) = 0.
\end{aligned}$$

Hence, there exists a linear map $F : S^n V \to W$ such that

$$F(v_1 v_2 \ldots v_n) = \varphi(v_1, v_2, \ldots, v_n)$$

and $\widetilde{F} = F\pi$, where $\pi : V^{\otimes n} \twoheadrightarrow S^n V$ is the factorization by the symmetry relation. Therefore, $\varphi = \widetilde{F} \circ \tau = F\pi\tau = F\sigma$. Given another linear map $F' : S^n V \to W$ such that $\varphi = F'\sigma = F'\pi\tau$, the universal property of τ forces $F'\pi = F\pi$. Since π is surjective, this leads to $F' = F$. □

Corollary 2.2 *For an arbitrary (not necessarily finite-dimensional) vector space V, the nth symmetric power $S^n V$ and the space* $\mathrm{Sym}^n(V, \Bbbk)$ *of symmetric n-linear forms $V \times V \times \cdots \times V \to \Bbbk$ are canonically dual to each other.*

Proof Right composition with the commutative multiplication

$$\sigma_n : V \times V \times \cdots \times V \to S^n V,$$

which takes a covector $\xi : S^n V \to \Bbbk$ to the symmetric n-linear form

$$\xi \circ \sigma_n : V \times V \times \cdots \times V \to \Bbbk,$$

establishes an isomorphism $(S^n V)^* \xrightarrow{\sim} \mathrm{Sym}^n(V, \Bbbk)$ by the universal property of σ_n.
□

2.3.3 The Exterior Algebra of a Vector Space

Write $\mathcal{I}_{\text{skew}} \subset \mathsf{T}V$ for the two-sided ideal generated by the $\Bbbk$-linear span of all proper squares $v \otimes v \in V \otimes V$, $v \in V$.

Exercise 2.8 Convince yourself that the $\Bbbk$-linear span of all proper squares $v \otimes v \in V \otimes V$ contains all the sums $u \otimes w + w \otimes u$ with $u, w \in V$ and is linearly generated by these sums if $\operatorname{char} \Bbbk \neq 2$.

As in the commutative case, the ideal $\mathcal{I}_{\text{skew}}$ splits into the direct sum of homogeneous components

$$\mathcal{I}_{\text{skew}} = \bigoplus_{n \geqslant 0} \left(\mathcal{I}_{\text{skew}} \cap V^{\otimes n} \right),$$

where the degree-n component $\mathcal{I}_{\text{skew}} \cap V^{\otimes n}$ is linearly generated over $\Bbbk$ by the decomposable tensors $\cdots \otimes v \otimes v \otimes \cdots$, containing a pair of equal sequential factors. By Exercise 2.8, all the sums

$$(\cdots \otimes v \otimes w \otimes \cdots) + (\cdots \otimes w \otimes v \otimes \cdots). \tag{2.10}$$

also belong to $\mathcal{I}_{\text{skew}} \cap V^{\otimes n}$. The quotient algebra $\Lambda V \stackrel{\text{def}}{=} \mathsf{T}V / \mathcal{I}_{\text{skew}}$ is called the *exterior* or *Grassmannian algebra* of the vector space V. The multiplication in ΛV is induced by the tensor multiplication in $\mathsf{T}V$. It is called the *exterior* or *Grassmannian* multiplication and is denoted by the wedge sign $\wedge$. The skew-symmetry relations imply that all the vectors from V anticommute and have zero squares in ΛV, i.e., $u \wedge w = -w \wedge u$ and $u \wedge u = 0$ for all $u, w \in V$. A permutation of factors in any monomial multiplies the monomial by the sign of the permutation,

$$v_{g_1} \wedge v_{g_2} \wedge \cdots \wedge v_{g_k} = \mathrm{sgn}(g) \cdot v_1 \wedge v_2 \wedge \cdots \wedge v_k \quad \forall\, g \in S_k.$$

The algebras possessing this property are commonly called *skew commutative* in mathematics and *supercommutative* in physics. We will shorten both names to *s-commutativity*.

As a vector space over $\Bbbk$, the Grassmannian algebra splits into the direct sum of homogeneous components

$$\Lambda V = \bigoplus_{n \geqslant 0} \Lambda^n V, \text{ where } \Lambda^n V = V^{\otimes n} / (\mathcal{I}_{\text{skew}} \cap V^{\otimes n}).$$

The vector space $\Lambda^n V$ is called the *nth exterior power* of V. Note that $\Lambda^0 V = \Bbbk$ and $\Lambda^1 V = V$. As in the symmetric case, the inclusion $\iota : V \hookrightarrow \Lambda V$, mapping V to $\Lambda^1 V$, has a universal property.

Exercise 2.9 (Universal Property of Free s-Commutative Algebras) Show that for every s-commutative $\Bbbk$-algebra L and linear map $f : V \to L$, there exists a unique homomorphism of $\Bbbk$-algebras $\widetilde{f} : \Lambda V \to L$ such that $f = \widetilde{f} \circ \iota$. Also show that for every linear map $\iota' : V \to \Lambda'$ to an s-commutative algebra Λ' possessing the same universal property, there exists a unique isomorphism of algebras $\psi : \Lambda' \xrightarrow{\sim} \Lambda V$ such that $\psi \iota' = \iota$.

For this reason, the algebra ΛV is also called the *free s-commutative* $\Bbbk$*-algebra* spanned by V.

2.3.4 Alternating Multilinear Maps

An n-linear map $\varphi : V \times V \times \cdots \times V \to U$ is called *alternating* if

$$\varphi(v_{g_1}, v_{g_2}, \ldots, v_{g_n}) = \operatorname{sgn}(g) \cdot \varphi(v_1, v_2, \ldots, v_n)$$

for all permutations $g \in S_n$. We write $\operatorname{Alt}^n(V, U) \subset \operatorname{Hom}(V, \ldots, V; U)$ for the subspace of alternating n-linear maps.

Associated with every alternating n-linear map $\varphi : V \times V \times \cdots \times V \to U$ and vector space W is the linear map

$$\operatorname{Hom}(U, W) \to \operatorname{Alt}^n(V, W), \quad F \mapsto F \circ \varphi. \tag{2.11}$$

The map φ is called the *universal alternating n-linear map* or the *n-ary s-commutative multiplication* of vectors if the linear map (2.11) is an isomorphism for all vector spaces W.

Exercise 2.10 Prove that the universal alternating n-linear map

$$\alpha_n : V \times V \times \cdots \times V \to U$$

is provided by tensor multiplication followed by factorization by the skew-commutativity relations, i.e., $\alpha_n : V \times \ldots \times V \overset{\tau}{\dashrightarrow} V^{\otimes n} \overset{\pi}{\twoheadrightarrow} \Lambda^n(V)$, and verify that the target spaces of every two universal symmetric n-linear maps are isomorphic by means of the unique linear map commuting with the s-commutative multiplication.

Corollary 2.3 *For an arbitrary (not necessarily finite-dimensional) vector space V, the nth exterior power $\Lambda^n V$ and the space $\mathrm{Alt}^n(V, \Bbbk)$ of alternating n-linear forms $V \times V \times \cdots \times V \to \Bbbk$ are canonically dual to each other.*

Proof The same as for Corollary 2.2 on p. 28. □

Proposition 2.4 *For every basis $e_1, e_2, \ldots, e_d$ of V, a basis in $\Lambda^d V$ is formed by the Grassmannian monomials*

$$e_I \overset{\text{def}}{=} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n} \tag{2.12}$$

numbered by all $I = (i_1, i_2, \ldots, i_n)$ with $1 \leqslant i_1 < i_2 < \cdots < i_n \leqslant d$. In particular, $\dim \Lambda^n V = \binom{d}{n}$ *and* $\dim \Lambda V = 2^d$.

Proof Write U for the vector space of dimension $\binom{d}{n}$ with the basis $\{u_I\}$ numbered by the same multi-indices I as the Grassmannian monomials (2.12). We know from Sect. 1.1.1 on p. 1 that every n-linear map $\alpha : V \times V \times \cdots \times V \to U$ is uniquely determined by its values on all the collections of basis vectors $\alpha(e_{j_1}, e_{j_2}, \ldots, e_{j_n})$, and these values may be arbitrary. Let us put $\alpha(e_{j_1}, e_{j_2}, \ldots, e_{j_n}) = 0$ if some arguments coincide, and $\alpha(e_{j_1}, e_{j_2}, \ldots, e_{j_n}) = \mathrm{sgn}(g)\cdot u_I$, where $I = (j_{g_1}, j_{g_2}, \ldots, j_{g_n})$ is the strictly increasing permutation of the indices $j_1, j_2, \ldots, j_n$ if all the indices are distinct. The resulting n-linear map $\alpha : V \times V \times \cdots \times V \to U$ is alternating and universal, because for every n-linear alternating map $\varphi : V \times V \times \cdots \times V \to W$, there exists a unique linear operator $F : U \to W$ such that $\varphi = F \circ \alpha$, namely, the operator acting on the basis of U as $F(u_I) = \varphi(e_{i_1}, e_{i_2}, \ldots, e_{i_n})$. By Exercise 2.10, there exists a linear isomorphism $U \xrightarrow{\sim} \Lambda^n V$ sending the basis vectors u_I to the s-symmetric products $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n} = e_I$. This forces the latter to form a basis in $\Lambda^n V$. □

Corollary 2.4 *For every basis $e_1, e_2, \ldots, e_d$ of V, the exterior algebra ΛV is isomorphic to the Grassmannian polynomial algebra $\Bbbk\langle e_1, e_2, \ldots, e_d \rangle$ defined in Sect. 9.4 of Algebra I.* □

2.4 Symmetric and Alternating Tensors

Starting from this point, we will always assume by default that $\mathrm{char}\,\Bbbk = 0$. For every $n \in \mathbb{N}$, the symmetric group S_n acts on $V^{\otimes n}$ by permutations of factors in the decomposable tensors:

$$g(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = v_{g_1} \otimes v_{g_2} \otimes \cdots \otimes v_{g_n} \quad \forall\, g \in S_n. \tag{2.13}$$

Since $v_{g_1} \otimes v_{g_2} \otimes \cdots \otimes v_{g_n}$ is multilinear in $v_1, v_2, \ldots, v_n$, there exists a well-defined linear operator $g : V^{\otimes n} \to V^{\otimes n}$ acting on decomposable tensors by formula (2.13). The subspaces of S_n-invariant and sign-alternating tensors are denoted by

$$\operatorname{Sym}^n V \stackrel{\text{def}}{=} \{t \in V^{\otimes n} \mid \forall\, g \in S_n,\ g(t) = t\}, \tag{2.14}$$

$$\operatorname{Alt}^n V \stackrel{\text{def}}{=} \{t \in V^{\otimes n} \mid \forall\, g \in S_n,\ g(t) = \operatorname{sgn}(g) \cdot t\}, \tag{2.15}$$

and called, respectively, the spaces of *symmetric* and *alternating* tensors of degree n on V.

2.4.1 Symmetrization and Alternation

If $\operatorname{char} \Bbbk = 0$, then for all $n \geqslant 2$, the tensor power $V^{\otimes n}$ is projected onto the subspaces of symmetric and alternating tensors, respectively, by means of the *symmetrization* and *alternation* maps

$$\operatorname{sym}_n : V^{\otimes n} \to \operatorname{Sym}^n V, \quad t \mapsto \frac{1}{n!} \sum_{g \in S_n} g(t), \tag{2.16}$$

$$\operatorname{alt}_n : V^{\otimes n} \to \operatorname{Alt}^n V, \quad t \mapsto \frac{1}{n!} \sum_{g \in S_n} \operatorname{sgn}(g) \cdot g(t). \tag{2.17}$$

Exercise 2.11 For all $t \in V^{\otimes n}$, $s \in \operatorname{Sym}^n V$, $a \in \operatorname{Alt}^n V$, and $n \geqslant 2$, prove that **(a)** $\operatorname{sym}_n(s) = s$, **(b)** $\operatorname{alt}_n(a) = a$, **(c)** $\operatorname{sym}_n(a) = \operatorname{alt}_n(s) = 0$, **(d)** $\operatorname{sym}_n(t) \in \operatorname{Sym}^n V$, **(e)** $\operatorname{alt}_n(t) \in \operatorname{Alt}^n V$.

Therefore, the symmetrization and alternation maps satisfy the relations

$$\operatorname{sym}_n^2 = \operatorname{sym}_n, \quad \operatorname{alt}_n^2 = \operatorname{alt}_n, \quad \operatorname{sym}_n \circ \operatorname{alt}_n = \operatorname{alt}_n \circ \operatorname{sym}_n = 0. \tag{2.18}$$

Example 2.2 (Tensor Square Decomposition) For $n = 2$, the symmetrization and alternation maps form a pair of complementary projectors,[4] that is,

$$\operatorname{sym}_2 + \operatorname{alt}_2 = (\mathrm{Id} + s_{12})/2 + (\mathrm{Id} - s_{12})/2 = \mathrm{Id},$$

where $s_{12} \in S_2$ is a transposition. Therefore, there exists the direct sum decomposition

$$V^{\otimes 2} = \operatorname{Sym}^2 V \oplus \operatorname{Alt}^2 V. \tag{2.19}$$

[4] See Example 15.3 in Algebra I.

If we interpret $V^{\otimes 2}$ as the space of bilinear forms on V^*, then the decomposition (2.19) turns out to be the decomposition of the space of bilinear forms into the direct sum of subspaces of symmetric and alternating forms considered in Sect. 16.1.6 of Algebra I.

Example 2.3 (Tensor Cube Decomposition) For $n = 3$, the direct sum $\mathrm{Sym}^3 V \oplus \mathrm{Alt}^3 V$ does not exhaust all of $V^{\otimes 3}$.

Exercise 2.12 Find codim $\left(\mathrm{Sym}^3 V \oplus \mathrm{Alt}^3 V\right)$ in $V^{\otimes 3}$.

To find the complement to $\mathrm{Sym}^3 V \oplus \mathrm{Alt}^3 V$ in $V^{\otimes 3}$, write $T = |123\rangle \in S_3$ for the cyclic permutation and consider the difference

$$p = \mathrm{Id} - \mathrm{sym}_3 - \mathrm{alt}_3 = \mathrm{Id} - \left(\mathrm{Id} + T + T^2\right)/3. \tag{2.20}$$

Exercise 2.13 Verify that $p^2 = p$ and $p \circ \mathrm{alt}_3 = \mathrm{alt}_3 \circ p = p \circ \mathrm{sym}_3 = \mathrm{sym}_3 \circ p = 0$.

Since $\mathrm{sym}_3 + \mathrm{alt}_3 + p = \mathrm{Id}_{V^{\otimes 3}}$, there exists the direct sum decomposition

$$V^{\otimes 3} = \mathrm{Sym}^3 V \oplus \mathrm{Alt}^3 V \oplus \mathrm{im}(p),$$

where $\mathrm{im}(p) = \{t \in V^{\otimes 3} \mid t + Tt + T^2 t = 0\}$ consists of all cubic tensors annihilated by averaging over the action of a 3-cycle. An example of such a tensor is provided by $[u, [v, w]]$, where $[a, b] \overset{\text{def}}{=} a \otimes b - b \otimes a$ means the commutator in the tensor algebra.

Exercise 2.14 (Jacobi Identity) Verify that $[u, [v, w]] + [v, [w, u]] + [w, [u, v]] = 0$ in $V^{\otimes 3}$ for all $u, v, w \in V$.

If we think of $V^{\otimes 3}$ as the space of 3-linear forms on V^*, then $\mathrm{im}(p)$ consists of all 3-linear forms $t : V^* \times V^* \times V^* \to \Bbbk$ satisfying the *Jacobi identity*:

$$t(\xi, \eta, \zeta) + t(\eta, \zeta, \xi) + t(\zeta, \xi, \eta) = 0$$

for all $\xi, \eta, \zeta \in V^*$.

For larger n, the decomposition of $V^{\otimes n}$ by the "symmetry types" of tensors becomes more complicated. It is the subject of the representation theory of the symmetric group, which will be discussed in Chap. 7 below.

2.4.2 Standard Bases

Let us fix a basis $e_1, e_2, \ldots, e_d$ in V and break the basis monomials

$$e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_n} \in V^{\otimes n}$$

into a disjoint union of S_n-orbits. Since the monomials of every S_n-orbit appear in the expansion of every symmetric tensor $t \in \mathrm{Sym}^n V$ with equal coefficients, a basis in $\mathrm{Sym}^n V$ is formed by the *monomial symmetric tensors*

$$e_{[m_1,m_2,\dots,m_d]} \stackrel{\text{def}}{=} \left(\begin{array}{c} \text{sum of all tensor monomials formed by} \\ m_1 \text{ factors } e_1,\, m_2 \text{ factors } e_2, \dots, m_d \text{ factors } e_d \end{array} \right) \tag{2.21}$$

numbered by the sequences $(m_1, m_2, \dots, m_d)$ of nonnegative integers satisfying the condition

$$m_1 + m_2 + \cdots + m_d = n.$$

It follows from the orbit length formula[5] that the sum on the right-hand side of (2.21) consists of $n!/(m_1!m_2! \cdots m_d!)$ summands, because the stabilizer of each summand is formed by $m_1!\, m_2! \cdots m_d!$ independent permutations of equal tensor factors.

Similarly, a basis in $\mathrm{Alt}^n V$ is formed by the *monomial alternating tensors*

$$e_I = e_{\langle i_1,i_2,\dots,i_n\rangle} \stackrel{\text{def}}{=} \sum_{g\in S_n} \mathrm{sgn}(g) \cdot e_{i_{g(1)}} \otimes e_{i_{g(2)}} \otimes \cdots \otimes e_{i_{g(n)}} \tag{2.22}$$

numbered by strictly increasing sequences of positive integers

$$I = (i_1, i_2, \dots, i_n), \quad 1 \leqslant i_1 < i_2 < \cdots < i_n \leqslant d.$$

Remark 2.1 (Bases (2.21) *and* (2.22) *for Infinite-Dimensional V)* We do not actually need to assume that $d = \dim V < \infty$ in both formulas (2.21), (2.22). They make sense for an arbitrary, not necessarily finite, basis E in V under the following agreement on notation. Let us fix some total ordering on the set E and number once and for all the elements of every finite subset $X \subset E$ in increasing order by integer indices $1, 2, \dots, |X|$. Then a basis in $S^n V$ is formed by the monomial tensors (2.21), where $d, m_1, m_2, \dots, m_d \in \mathbb{N}$ are any *positive* integers such that $m_1 + m_2 + \cdots + m_d = n$, and $e_1, e_2, \dots, e_d$ run through the (numbered) subsets of cardinality d in E. Similarly, a basis in $\mathrm{Alt}^n V$ is formed by the monomials (2.22), where $e_{i_1}, e_{i_2}, \dots, e_{i_n}$ run through the (numbered) subsets of cardinality n in E.

Proposition 2.5 *If* $\mathrm{char}(\Bbbk) = 0$*, then the restriction of the quotient map*

$$V^{\otimes n} \twoheadrightarrow S^n V$$

to the subspace $\mathrm{Sym}^n \subset V^{\otimes n}$ *and the restriction of the quotient map*

$$V^{\otimes n} \twoheadrightarrow \Lambda^n V$$

[5] See Proposition 12.2 of Algebra I.

to the subspace $\mathrm{Alt}^n \subset V^{\otimes n}$ *establish the isomorphisms of vector spaces*

$$\pi_{\mathrm{sym}} : \mathrm{Sym}^n V \xrightarrow{\sim} S^n V \quad \textit{and} \quad \pi_{\mathrm{sk}} : \mathrm{Alt}^n V \xrightarrow{\sim} \Lambda^n V.$$

These isomorphisms act on the basis monomial tensors (2.21) *and* (2.22) *by the rules*

$$e_{[m_1,m_2,\dots,m_d]} \mapsto \frac{n!}{m_1!\cdot m_2!\,\cdots\, m_d!}\cdot e_1^{m_1} e_2^{m_2}\cdots e_d^{m_d}, \tag{2.23}$$

$$e_{\langle i_1,i_2,\dots,i_d\rangle} \mapsto n!\cdot e_{i_1}\wedge e_{i_2}\wedge\cdots\wedge e_{i_d}. \tag{2.24}$$

Proof The projection π_{sym} maps each of the $n!/(m_1!m_2!\cdots m_d!)$ summands in (2.21) to the commutative monomial $e_1^{m_1}e_2^{m_2}\dots e_d^{m_d}$. Similarly, the projection π_{sk} sends each of the $n!$ summands in (2.22) to the Grassmannian monomial $e_{i_1}\wedge e_{i_2}\wedge\cdots\wedge e_{i_n}$. □

Caution 2.1 In spite of Proposition 2.5, the subspaces $\mathrm{Sym}^n V$, $\mathrm{Alt}^n V \subset V^{\otimes n}$ should not be confused with the quotient spaces $S^n V$ and $\Lambda^n V$ of the tensor power $V^{\otimes n}$. If $\mathrm{char}\,\Bbbk = p > 0$, then many symmetric tensors and all the alternating tensors of degree larger than p are *annihilated* by projections $V^{\otimes n} \twoheadrightarrow S^n V$ and $V^{\otimes n} \twoheadrightarrow \Lambda^n V$. Even if $\mathrm{char}\,\Bbbk = 0$, the isomorphisms from Proposition 2.5 *do not* identify the monomial bases of tensor spaces directly with the standard monomials in the polynomial rings. Both isomorphisms contain some combinatorial factors, which should be taken into account whenever we need either to pull back the multiplication from the polynomial (respectively exterior) algebra to the space of symmetric (respectively alternating) tensors or push forward the contractions of tensors into the polynomial algebras.

2.5 Polarization of Polynomials

It follows from Proposition 2.5 that for every homogeneous polynomial $f \in S^n V^*$, there exists a unique symmetric tensor $\widetilde{f} \in \mathrm{Sym}^n V^*$ mapped to f under the factorization by the commutativity relations $(V^*)^{\otimes n} \twoheadrightarrow S^n V^*$ on p. 23 allows us to treat $\widetilde{f}$ as the symmetric n-linear form

$$\widetilde{f} : V\times V\times\,\dots\,\times V \to \Bbbk, \quad \widetilde{f}(v_1,v_2,\dots,v_n) \overset{\text{def}}{=} \left\langle v_1\otimes v_2\otimes\,\cdots\,\otimes v_n, \widetilde{f}\right\rangle.$$

This form is called the *complete polarization* of the polynomial f. For $n = 2$, the polarization $\widetilde{f}$ of a quadratic form $f \in S^2V^*$ coincides with that defined in Chap. 17 of Algebra I by the equality

$$2\widetilde{f}(u,w) = f(u+w) - f(u) - f(w).$$

For arbitrary n, the complete polarization of every monomial $x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d}$ of degree $n = m_1 + m_2 + \cdots + m_d$ is given by the first formula from Proposition 2.5 and equals

$$\frac{m_1!\, m_2! \, \cdots \, m_d!}{n!} \cdot x_{[m_1, m_2, \ldots, m_d]}. \tag{2.25}$$

The complete polarization of an arbitrary polynomial can be computed using (2.25) and the linearity of the polarization map $\pi_{\text{sym}}^{-1} : S^n V^* \xrightarrow{\sim} \operatorname{Sym}^n V^*, f \mapsto \widetilde{f}$. By Remark 2.1 on p. 34, this works for every (not necessarily finite) basis in V^* as well.

2.5.1 Evaluation of Polynomials on Vectors

Associated with every polynomial $f \in S^n V^*$ is the *polynomial function*

$$f : V \to \Bbbk, \quad v \mapsto f(v) \stackrel{\text{def}}{=} \widetilde{f}(v, v, \ldots, v). \tag{2.26}$$

Note that the value of f on v is well defined even for infinite-dimensional vector spaces and does not depend on any extra data on V, such as the choice of basis. Now assume that $\dim V < \infty$, fix dual bases $e_1, e_2, \ldots, e_d \in V$, $x_1, x_2, \ldots, x_d \in V^*$, and identify the symmetric algebra SV^* with the polynomial algebra $\Bbbk[x_1, x_2, \ldots, x_d]$. Then the value of a polynomial $f(x_1, x_2, \ldots, x_n)$ at a vector $v = \sum \alpha_i e_i \in V$ coincides with the result of the substitution $x_i = \alpha_i$ in f:

$$f(v) = f(\alpha_1, \alpha_2, \ldots, \alpha_d). \tag{2.27}$$

Indeed, for every monomial $f = x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d}$, the complete contraction of $v^{\otimes n}$ with

$$\widetilde{f} = \frac{m_1! \cdot m_2! \, \cdots \, m_d!}{n!} x_{[m_1, m_2, \ldots, m_d]}$$

is the sum of $n!/(m_1! \cdot m_2! \, \cdots \, m_d!)$ equal products

$$\begin{aligned} &\frac{m_1! \cdot m_2! \, \cdots \, m_d!}{n!} \cdot x_1(v)^{m_1} \cdot x_2(v)^{m_2} \cdots x_d(v)^{m_d} \\ &= \frac{m_1! \cdot m_2! \, \cdots \, m_d!}{n!} \cdot \alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_d^{m_d}. \end{aligned}$$

It coincides with the result of the substitution $(x_1, x_2, \ldots, x_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ in the monomial

$$\frac{n!}{m_1! m_2! \, \cdots \, m_d!} x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d}.$$

We conclude that the evaluation of a polynomial $f \in \Bbbk[x_1, x_2, \dots, x_d]$ at the coordinates of a vector $v \in V$ depends only on $f \in S^n V^*$ and $v \in V$ but not on the choice of dual bases in V, V^*.

2.5.2 Combinatorial Formula for Complete Polarization

Since the value of a symmetric n-linear form does not depend on the order of arguments, let us write

$$\widetilde{f}\left(v_1^{m_1}, v_2^{m_2}, \dots, v_n^{m_k}\right)$$

for the value of $\widetilde{f}$ at m_1 vectors v_1, m_2 vectors $v_2, \dots, m_k$ vectors v_k with $\sum_\nu m_\nu = n$.

Exercise 2.15 Show that for every polynomial $f \in S^n V^*$ and all vectors $v_1, v_2, \dots, v_k \in V$, one has

$$\begin{aligned} f(v_1 + v_2 + \dots + v_k) &= \widetilde{f}((v_1 + v_2 + \dots + v_k)^n) \\ &= \sum_{m_1 m_2 \dots m_k} \frac{n!}{m_1! m_2! \cdots m_k!} \cdot \widetilde{f}\left(v_1^{m_1}, v_2^{m_2}, \dots, v_k^{m_k}\right), \end{aligned} \tag{2.28}$$

where the summation is over all integers $m_1, m_2, \dots, m_k$ such that

$$m_1 + m_2 + \dots + m_k = n$$

and $0 \leqslant m_\nu \leqslant n$ for all ν.

Proposition 2.6 *Let V be a vector space, not necessarily finite-dimensional, over a field $\Bbbk$ of characteristic zero. Then for every homogeneous polynomial $f \in S^n V^*$,*

$$n! \cdot \widetilde{f}(v_1, v_2, \dots, v_n) = \sum_{I \subsetneq \{1,\dots,n\}} (-1)^{|I|} f\Big(\sum_{i \notin I} v_i\Big), \tag{2.29}$$

where the left summation is over all subsets $I \subsetneq \{1, 2, \dots, n\}$ including $I = \varnothing$, for which $|\varnothing| = 0$. For example, for $f \in S^3 V^*$, one has

$$6\widetilde{f}(u, v, w) = f(u + v + w) - f(u + v) - f(u + w) - f(v + w) + f(u) + f(v) + f(w).$$

Proof Consider the expansion (2.28) from Exercise 2.15 for $k = n = \deg f$. Its right-hand side contains the unique term depending on all the vectors $v_1, v_2, \dots, v_n$, namely $n! \cdot \widetilde{f}(v_1, v_2, \dots, v_n)$. For every proper subset $I \subsetneq \{1, 2, \dots, n\}$, the summands of (2.28) that do not contain vectors v_i with $i \in I$ appear in (2.28) with the same coefficients as they do in the expansion of $f\left(\sum_{i \notin I} v_i\right)$, because the latter is obtained from $f(v_1+v_2+\cdots+v_n)$ by setting $v_i = 0$ for all $i \in I$. Therefore, all terms that do not depend on some of the v_i can be removed from (2.28) by the standard combinatorial inclusion–exclusion procedure. This leads to the required formula

$$\begin{aligned} &n! \cdot \widetilde{f}(v_1, v_2, \dots, v_n) \\ &\quad = f\Big(\sum_\nu v_\nu\Big) - \sum_{\{i\}} f\Big(\sum_{\nu \neq i} v_\nu\Big) + \sum_{\{i,j\}} f\Big(\sum_{\nu \neq i,j} v_\nu\Big) - \sum_{\{i,j,k\}} f\Big(\sum_{\nu \neq i,j,k} v_\nu\Big) + \cdots . \end{aligned}$$

□

2.5.3 Duality

Assume that $\operatorname{char} \Bbbk = 0$ and $\dim V < \infty$. The complete contraction between $V^{\otimes m}$ and $V^{*\otimes m}$ provides the spaces $S^m V$ and $S^m V^*$ with the perfect pairing[6] that couples polynomials $f \in S^n V$ and $g \in S^n V^*$ to a complete contraction of their complete polarizations $\widetilde{f} \in V^{\otimes m}$ and $\widetilde{g} \in V^{*\otimes m}$.

Exercise 2.16 Verify that for every pair of dual bases

$$e_1, e_2, \dots, e_d \in V, \quad x_1, x_2, \dots, x_d \in V^*,$$

all the nonzero couplings between the basis monomials are exhausted by

$$\left\langle e_1^{m_1} e_2^{m_2} \cdots e_d^{m_d},\, x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d} \right\rangle = \frac{m_1! m_2! \cdots m_d!}{n!}. \tag{2.30}$$

Note that the monomials constructed from the dual basis vectors become the dual bases of the polynomial rings only after rescaling by the same combinatorial factors as in Proposition 2.5.

2.5.4 Derivative of a Polynomial Along a Vector

Associated with every vector $v \in V$ is the linear map

$$i_v : V^{*\otimes n} \to V^{*\otimes(n-1)}, \quad \varphi \mapsto v \llcorner \varphi, \tag{2.31}$$

provided by the inner multiplication[7] of n-linear forms on V by v, which takes an n-linear form $\varphi \in V^{*\otimes n}$ to the $(n-1)$-linear form

$$v \llcorner \varphi(v_1, v_2, \dots, v_{n-1}) = \varphi(v,\ v_1, v_2, \dots, v_{n-1}).$$

[6] See Sect. 7.1.4 of Algebra I.

[7] See Example 2.1 on p. 24.

The map (2.31) preceded by the complete polarization map

$$S^n V^* \simeq \mathrm{Sym}^n V^* \subset V^{*\otimes n}$$

and followed by the quotient map $V^{*\otimes(n-1)} \twoheadrightarrow S^{n-1}V^*$ gives the linear map

$$\mathrm{pl}_v : S^n V^* \to S^{n-1}V^*, \quad f(x) \mapsto \mathrm{pl}_v f(x) \stackrel{\text{def}}{=} \widetilde{f}(v, x, x, \dots, x), \tag{2.32}$$

which depends linearly on $v \in V$. This map fits in the commutative diagram

$$\begin{tikzcd} V^{*\otimes n} \supset \mathrm{Sym}^n V^* \arrow[r, "v\llcorner"] \arrow[d, "\pi_{\mathrm{sym}}"', "\wr"] & V^{*\otimes(n-1)} \arrow[d, "\pi_{\mathrm{sym}}"] \\ S^n V^* \arrow[r, "\mathrm{pl}_v"] & S^{n-1} V^* \end{tikzcd} \tag{2.33}$$

The polynomial $\mathrm{pl}_v f(x)\widetilde{f}(v, x, \dots x) \in S^{n-1}(V^*)$ is called the *polar* of v with respect to f. For $n = 2$, the polar of a vector v with respect to a quadratic form $f \in S^2V^*$ is the linear form $w \mapsto \widetilde{f}(v, w)$ considered[8] in Sect. 17.4.3 of Algebra I.

In terms of dual bases $e_1, e_2, \dots, e_d \in V$, $x_1, x_2, \dots, x_d \in V^*$, the contraction of the first tensor factor in $V^{*\otimes n}$ with the basis vector $e_i \in V$ maps the complete symmetric tensor $x_{[m_1,m_2,\dots,m_n]}$ either to the complete symmetric tensor containing the $(m_i - 1)$ factors x_i or to zero for $m_i = 0$. By formula (2.23) from Proposition 2.5,

$$\mathrm{pl}_{e_i} x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d} = \frac{m_i}{n} x_1^{m_1} \cdots x_{i-1}^{m_{i-1}} x_i^{m_i - 1} x_{i+1}^{m_{i+1}} \cdots x_d^{m_d} = \frac{1}{n} \frac{\partial}{\partial x_i} x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d}.$$

Since $\mathrm{pl}_v f$ is linear in both v and f, we conclude that for every $v = \sum \alpha_i e_i$, the polar polynomial of v with respect to f is nothing but the *derivative* of the polynomial f along the vector v divided by $\deg f$, i.e.,

$$\mathrm{pl}_v f = \frac{1}{\deg(f)} \partial_v f = \frac{1}{\deg(f)} \sum_{i=1}^{d} \alpha_i \frac{\partial f}{\partial x_i}.$$

Note that this forces the right-hand side of the formula to be independent of the choice of dual bases in V and V^*. It follows from the definition of polar map that the derivatives along vectors commute, $\partial_u \partial_w = \partial_w \partial_u$, and satisfy the following

[8]Recall that the zero set of this form in $\mathbb{P}(V)$ is the hyperplane intersecting the quadric $Z(f) \subset \mathbb{P}(V)$ along its apparent contour viewed from v.

remarkable relation:

$$m! \, \frac{\partial^m f}{\partial u^m}(w) = n! \, \widetilde{f}(\underbrace{u, u, \dots, u}_{m}, \underbrace{w, w, \dots, w}_{n}) = (n-m)! \, \frac{\partial^{n-m} f}{\partial w^{n-m}}(u), \tag{2.34}$$

which holds for all $u, w \in V, f \in S^n V^*$, and $0 \leqslant m \leqslant n$.

Exercise 2.17 Prove the *Leibniz rule* $\partial_v(f \cdot g) = \partial_v(f) \cdot g + f \cdot \partial_v(g)$.

Exercise 2.18 Show that

$$\widetilde{f}(v_1, v_2, \dots, v_n) = \frac{1}{n!} \partial_{v_1} \partial_{v_2} \cdots \partial_{v_n} f$$

for every polynomial $f \in S^n V^*$ and all vectors $v_1, v_2, \dots, v_n \in V$.

Example 2.4 (Taylor Expansion) For $k = 2$, the expansion (2.28) from Exercise 2.15 turns into the identity

$$f(u+w) = \widetilde{f}(u+w, \, u+w, \, \dots, \, u+w) = \sum_{m=0}^{n} \binom{n}{m} \cdot \widetilde{f}(u^m, w^{n-m}),$$

where $n = \deg f$, which holds for every polynomial $f \in S^n V^*$ and all vectors $u, w \in V$. The relations (2.34) allow us to rewrite this identity as the *Taylor expansion* for f at u:

$$f(u+w) = \sum_{m=0}^{\deg f} \frac{1}{m!} \, \partial_w^m f(u). \tag{2.35}$$

Note that this is an exact equality in the polynomial ring SV^*, and its right-hand side actually is completely symmetric in u, w, because of the same relations in (2.34).

2.5.5 Polars and Tangents of Projective Hypersurfaces

Let $S = Z(F) \subset \mathbb{P}(V)$ be a projective hypersurface defined by a homogeneous polynomial equation $F(x) = 0$ of degree n. For every line $\ell = (pq) \subset \mathbb{P}(V)$, the intersection $\ell \cap S$ consists of all points $\lambda p + \mu q \in \ell$ such that $(\lambda : \mu)$ satisfies the homogeneous equation $f(\lambda, \mu) = 0$ obtained from the equation $F(x) = 0$ via the substitution $x \leftarrow \lambda p + \mu q$. Over an algebraically closed field $\Bbbk$, the binary form $f(\lambda, \mu) \in \Bbbk[\lambda, \mu]$ either is zero or is completely factorized into a product of n forms linear in λ, μ:

$$f(\lambda, \mu) = \prod_i (\alpha_i'' \lambda - \alpha_i' \mu)^{s_i} = \prod_i \det{}^{s_i} \begin{pmatrix} \lambda & \alpha_i' \\ \mu & \alpha_i'' \end{pmatrix}, \tag{2.36}$$

where $a_i = (\alpha_i' : \alpha_i'')$ are distinct points on $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ and $\sum_i s_i = n$. In the first case, the line ℓ lies on S. In the second case, the intersection $\ell \cap S$ consists of points $a_i = \alpha_i' p + \alpha_i'' q$. The exponent s_i of the linear form $\alpha_i''\mu - \alpha_i'\lambda$ in the factorization (2.36) is called the *intersection multiplicity* of the hypersurface S and the line ℓ at the point a_i, and is denoted by $(S, \ell)_{a_i}$. If $(S, \ell)_{a_i} = 1$, then a_i is called a *simple* (or *transversal*) intersection point. Otherwise, the intersection of ℓ and S at a_i is called *multiple*. Note that the total number of intersections counted with their multiplicities equals the degree of S.

Let $p \in S$. Then a line $\ell = (p, q)$ is called *tangent* to the hypersurface $S = Z(F)$ at p if either $\ell \subset S$ or $(S, \ell)_a \geqslant 2$. In other words, the line ℓ is tangent to S at p if the polynomial $F(p + tq) \in \Bbbk[t]$ either is the zero polynomial or has a multiple root at zero. It follows from formulas (2.35), (2.34) that the Taylor expansion of $F(p + tq)$ at p starts with

$$F(p + tq) = t\binom{d}{1}\widetilde{F}(p^{n-1}, q) + t^2\binom{d}{2}\widetilde{F}(p^{n-2}, q^2) + \cdots .$$

Therefore, $\ell = (p, q)$ is tangent to S at p if and only if $\widetilde{F}(p^{n-1}, q) = 0$. This is a straightforward generalization of Lemma 17.4 from Algebra I.

If $F(p^{n-1}, x)$ does not vanish identically as a linear form in x, then the linear equation $F(p^{n-1}, x) = 0$ on $x \in V$ defines a hyperplane in $\mathbb{P}(V)$ filled by the lines (pq) tangent to S at p. This hyperplane is called the *tangent space* to S at p and is denoted by

$$T_p = \left\{x \in \mathbb{P}(V) \mid \widetilde{F}(p^{n-1}, x) = 0\right\}.$$

In this case, the point p is called a *smooth point* of S. The hypersurface $S \subset \mathbb{P}(V)$ is called *smooth* if every point $p \in S$ is smooth.

If $F(p^{n-1}, x)$ is the zero linear form in x, the hypersurface S is called *singular* at p, and the point p is called a *singular point* of S.

By formulas (2.34), the coefficients of the polynomial $F(p^{n-1}, x) = \partial_x F(p)$, considered as a linear form in x, are equal to the partial derivatives of F evaluated at the point p. Therefore, the singularity of a point $p \in S = Z(F)$ is expressed by the equations

$$\frac{\partial F}{\partial x_i}(p) = 0 \quad \text{for all } i,$$

in which case every line ℓ passing through p has $(S, \ell)_p \geqslant 2$, i.e., is tangent to S at p. Thus, the tangent lines to S at p fill the whole ambient space $\mathbb{P}(V)$ in this case.

If q is either a smooth point on S or a point outside S, then the polar polynomial

$$\mathrm{pl}_q F(x) = \widetilde{F}(q, x^{n-1})$$

does not vanish identically as a homogeneous polynomial of degree $n-1$ in x, because otherwise, all partial derivatives of $\mathrm{pl}_q F(x) = \widetilde{F}(q, x^{n-1})$ in x would also vanish, and in particular,

$$\widetilde{F}(q^{n-1}, x) = \frac{\partial^{n-2}}{\partial q^{n-2}} \mathrm{pl}_q F(x) = 0$$

identically in x, meaning that q would be a singular point of S, in contradiction to our choice of q. The zero set of the polar polynomial $\mathrm{pl}_q F \in S^{n-1}V^*$ is denoted by

$$\mathrm{pl}_q S \stackrel{\text{def}}{=} Z\left(\mathrm{pl}_q F\right) = \left\{x \in \mathbb{P}(V) \mid \widetilde{F}(q, x^{n-1}) = 0\right\} \tag{2.37}$$

and called the *polar hypersurface* of the point q with respect to S. If S is a quadric, then $\mathrm{pl}_q S$ is exactly the polar hyperplane of q considered in Sect. 17.4.3 of Algebra I. As in that case, for a hypersurface S of arbitrary degree, the intersection $S \cap \mathrm{pl}_q S$ coincides with the *apparent contour* of S viewed from the point q, that is, with the locus of all points $p \in S$ such that the line (pq) is tangent to S at p.

More generally, for an arbitrary point $q \in \mathbb{P}(V)$, the locus of points

$$\mathrm{pl}_q^{n-r} S \stackrel{\text{def}}{=} \left\{x \in \mathbb{P}(V) \mid \widetilde{F}(q^{n-r}, x^r) = 0\right\}$$

is called the *rth-degree polar* of the point q with respect to S or the *rth-degree polar* of S at q for $q \in S$. If the polynomial $\widetilde{F}(q^{n-r}, x^r)$ vanishes identically in x, we say that the rth-degree polar is *degenerate*. Otherwise, the rth-degree polar is a projective hypersurface of degree r. The linear[9] polar of S at a smooth point $q \in S$ is simply the tangent hyperplane to S at q,

$$T_q S = \mathrm{pl}_q^{n-1} S.$$

The quadratic polar $\mathrm{pl}_q^{n-2} S$ is the quadric passing through q and having the same tangent hyperplane at q as S. The cubic polar $\mathrm{pl}_q^{n-3} S$ is the cubic hypersurface passing through q and having the same quadratic polar at q as S, etc. The rth-degree polar $\mathrm{pl}_q^{n-2} S$ at a smooth point $q \in S$ passes through q and has $\mathrm{pl}_q^{r-k} \mathrm{pl}_q^{n-r} S = \mathrm{pl}_q^{n-k} S$ for all $1 \leqslant k \leqslant r-1$, because

$$\begin{aligned} \mathrm{pl}_q^{r-k} \mathrm{pl}_q^{n-r} F(x) &= \widetilde{\mathrm{pl}_q^{n-r} F}\left(q^{r-k}, x^k\right) = \widetilde{F}\left(q^{n-r}, q^{r-k}, x^k\right) = \widetilde{F}\left(q^{n-k}, x^k\right) \\ &= \mathrm{pl}_q^{n-k} F(x). \end{aligned}$$

[9]That is, of first degree.

2.5.6 Linear Support of a Homogeneous Polynomial

Let V be a finite-dimensional vector space and $f \in S^n V^*$ a polynomial. We write $\mathrm{Supp} f$ for the minimal[10] vector subspace $W \subset V^*$ such that $f \in S^n W$, and call this subspace the *linear support* of f. For char $\Bbbk = 0$, the linear support of a polynomial f coincides with the linear support of the symmetric tensor[11] $\widetilde{f} \in \mathrm{Sym}^n V^*$, the complete polarization of f. By Theorem 2.1, it is linearly generated by the images of the $(n-1)$-tuple contraction maps

$$c_t^J : V^{\otimes(n-1)} \to V^*, \quad t \mapsto c^{1,2,\dots,(n-1)}_{j_1,j_2,\dots,j_{n-1}}(t \otimes \widetilde{f}),$$

coupling all the $(n-1)$ factors of $V^{\otimes(n-1)}$ with some $n-1$ factors of $\widetilde{t} \in V^{*\otimes n}$ in the order indicated by the sequence $J = (j_1, j_2, \dots, j_{n-1})$. For the symmetric tensor $\widetilde{f}$, such a contraction does not depend on J and maps every decomposable tensor $v_1 \otimes v_2 \otimes \cdots \otimes v_{n-1}$ to the linear form on V proportional to the $(n-1)$-tuple derivative $\partial_{v_1}\partial_{v_2}\cdots\partial_{v_{n-1}} f \in V^*$.

Therefore, $\mathrm{Supp}(f)$ is linearly generated by all $(n-1)$-tuple partial derivatives

$$\frac{\partial^{m_1}}{\partial x_1^{m_1}}\frac{\partial^{m_2}}{\partial x_2^{m_2}}\cdots\frac{\partial^{m_d}}{\partial x_d^{m_d}} f(x), \text{ where } \sum m_\nu = n-1. \tag{2.38}$$

The coefficient of x_i in the linear form (2.38) depends only on the coefficients of the monomial

$$x_1^{m_1}\cdots x_{i-1}^{m_{i-1}} x_i^{m_i+1} x_{i+1}^{m_{i+1}}\cdots x_d^{m_d}$$

in f. Writing the polynomial f in the form

$$f = \sum_{\nu_1+\cdots+\nu_d=n} \frac{n!}{\nu_1!\nu_2!\cdots\nu_d!}\, a_{\nu_1\nu_2\dots\nu_d}\, x_1^{\nu_1}x_2^{\nu_2}\cdots x_d^{\nu_d} \tag{2.39}$$

turns the linear form (2.38) into

$$n!\cdot\sum_{i=1}^d a_{m_1\dots m_{i-1}(m_i+1)m_{i+1}\dots m_d} x_i. \tag{2.40}$$

Altogether, we get $\binom{n+d-2}{d-1}$ such linear forms, which are in bijection with the nonnegative integer solutions $m_1, m_2, \dots, m_d$ of the equation $m_1+m_2+\cdots+m_d=n-1$.

[10] With respect to inclusions.

[11] See Sect. 2.2.3 on p. 25.

Proposition 2.7 *Let $\Bbbk$ be a field of characteristic zero, V a finite-dimensional vector space over $\Bbbk$, and $f \in S^n V^*$ a polynomial written in the form (2.39) in some basis of V^*. If $f = \varphi^n$ is the proper nth power of some linear form $\varphi \in V^*$, then the $d \times \binom{n+d-2}{d-1}$ matrix built from the coefficients of linear forms (2.40) has rank 1. In this case, there are at most n linear forms $\varphi \in V^*$ such that $\varphi^n = f$, and they differ from one another by multiplication by the nth roots of unity lying in $\Bbbk$. Over an algebraically closed field $\Bbbk$, the converse is true as well: if all the linear forms (2.40) are proportional, then $f = \varphi^n$ for some linear form φ, which is also proportional to the forms (2.40).*

Proof The equality $f = \varphi^n$ means that $\mathrm{Supp}(f) \subset V^*$ is the 1-dimensional subspace spanned by φ. In this case, all linear forms (2.40) are proportional to φ. Such a form $\psi = \lambda\varphi$ has $\psi^n = f$ if and only if $\lambda^n = 1$ in $\Bbbk$. Conversely, let all the linear forms (2.40) be proportional, and let $\psi \neq 0$ be one of them. Then $\mathrm{Supp}(f) = \Bbbk \cdot \psi$ is the 1-dimensional subspace spanned by ψ. Hence $f = \lambda\psi^n$ for some $\lambda \in \Bbbk$, and therefore, $f = \varphi^n$ for[12] $\varphi = \sqrt[n]{\lambda} \cdot \psi$. □

Example 2.5 (Binary Forms of Rank 1) We know from Example 11.6 of Algebra I that a homogeneous binary form of degree n,

$$f(x_0, x_1) = \sum_k a_k \cdot \binom{n}{k} \cdot x_0^{n-k} x_1^k,$$

is the proper nth power of some linear form $\alpha_0 x_0 + \alpha_1 x_1$ if and only if the ratio of sequential coefficients $a_i : a_{i+1} = \alpha_0 : \alpha_1$ does not depend on i. This is equivalent to the condition

$$\mathrm{rk}\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = 1,$$

which is expanded to a system of homogeneous quadratic equations $a_i a_{j+1} = a_{i+1} a_j$ in the coefficients of f. Proposition 2.7 leads to the same result, because the columns of the above matrix are exactly the coefficients of linear forms (2.40) divided by $n!$.

Corollary 2.5 *The proper nth powers of linear forms $\varphi \in V^*$ form the projective algebraic variety*

$$\mathcal{V}_n \stackrel{\text{def}}{=} \{\varphi^n \mid \varphi \in V^*\} \subset \mathbb{P}(S^n V^*) \tag{2.41}$$

in the space of all degree-n hypersurfaces[13] *in $\mathbb{P}(V)$. This variety is described by the system of quadratic equations representing the vanishing of all 2×2 minors in the $d \times \binom{n+d-2}{d-1}$ matrix built from the coefficients of linear forms (2.40).* □

[12] Here we use that $\Bbbk$ is algebraically closed.

[13] See Sect. 11.3.3 of Algebra I.

Definition 2.1 (Veronese Variety) The projective algebraic variety (2.41) is called the *Veronese variety*.

Exercise 2.19 (Veronese Embedding) Verify that the prescription $\varphi \mapsto \varphi^n$ gives the well-defined injective map $\mathbb{P}(V^*) \hookrightarrow \mathbb{P}(S^n V^*)$ whose image coincides with the Veronese variety (2.41).

2.6 Polarization of Grassmannian Polynomials

It follows from Proposition 2.5 on p. 34 that for every Grassmannian polynomial $\omega \in \Lambda^n V^*$ over a field of characteristic zero, there exists a unique alternating tensor $\widetilde{\omega} \in \operatorname{Alt}^n V^* \subset V^{*\otimes n}$ mapped to ω under the factorization by the skew-commutativity relations $\pi_{\mathrm{sk}} : V^{*\otimes n} \twoheadrightarrow \Lambda^n V^*$. It can be viewed as the alternating n-linear form

$$\widetilde{\omega} : V \times V \times \cdots \times V \to \Bbbk, \quad \widetilde{\omega}(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \langle\, v_1 \otimes v_2 \otimes \cdots \otimes v_n,\, \widetilde{\omega}\,\rangle\,,$$

called the *complete polarization* of the Grassmannian polynomial $\omega \in \Lambda^n V^*$. If the covectors x_i form a basis of V^*, then by formula (2.24) on p. 35, the complete polarization of the Grassmannian monomial $x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_n}$ equals

$$\frac{1}{n!}\, x_{\langle i_1, i_2, \dots, i_n\rangle} = \operatorname{alt}_n \left(x_{i_1} \otimes x_{i_2} \otimes \cdots \otimes x_{i_n}\right). \tag{2.42}$$

The polarization of an arbitrary Grassmannian polynomial can be computed using this formula and the linearity of the polarization map

$$\pi_{\mathrm{sk}}^{-1} : \Lambda^n V^* \xrightarrow{\sim} \operatorname{Alt}^n V^*, \quad \omega \mapsto \widetilde{\omega}. \tag{2.43}$$

By Remark 2.1 on p. 34, this procedure is also well defined for infinite-dimensional vector spaces.

2.6.1 Duality

Similarly to the symmetric case, for a finite-dimensional vector space V over a field of characteristic zero, there exists a perfect pairing between the spaces $\Lambda^n V$ and $\Lambda^n V^*$ coupling polynomials $\tau \in \Lambda^n V$ and $\omega \in \Lambda^n V^*$ to the complete contraction of their complete polarizations $\widetilde{\tau} \in V^{\otimes n}$ and $\widetilde{\omega} \in V^{*\otimes n}$.

Exercise 2.20 Convince yourself that the nonzero couplings between the basis monomials $e_I \in \Lambda^n V$ and $x_J \in \Lambda^n V^*$ are exhausted by

$$\langle\, e_I,\, x_I \,\rangle = 1/n!. \tag{2.44}$$

2.6.2 Partial Derivatives in an Exterior Algebra

By analogy with Sect. 2.5.4, the *derivative* of a Grassmannian polynomial $\omega \in \Lambda^n V^*$ along a vector $v \in V$ is defined by the formula

$$\partial_v \omega \stackrel{\text{def}}{=} \deg \omega \cdot \mathrm{pl}_v \omega ,$$

where the *polarization map* $\mathrm{pl}_v : \Lambda^n V^* \to \Lambda^{n-1} V^*$, $\omega \mapsto \pi_{\mathrm{sk}}(v \llcorner \widetilde{\omega})$, is composed of the inner multiplication (2.31) preceded by the complete polarization (2.43) and followed by the quotient map $\pi_{\mathrm{sk}} : V^{*\otimes(n-1)} \twoheadrightarrow \Lambda^{n-1} V^*$. Thus, pl_v fits in the commutative diagram

$$\begin{tikzcd} V^{*\otimes n} \supset \mathrm{Alt}^n V^* \arrow[r, "v\llcorner"] \arrow[d, "\pi_{\mathrm{sk}}"'] & V^{*\otimes(n-1)} \arrow[d, "\pi_{\mathrm{sk}}"] \\ \Lambda^n V^* \arrow[r, "\mathrm{pl}_v"] & \Lambda^{n-1} V^* \end{tikzcd} \tag{2.45}$$

which is similar to the diagram from formula (2.33) on p. 39. Since $\mathrm{pl}_v \omega$ is linear in v, it follows that

$$\partial_v = \sum \alpha_i \, \partial_{e_i} \quad \text{for} \quad v = \sum \alpha_i e_i .$$

If ω does not depend on x_i, then certainly $\partial_{e_i} \omega = 0$. Therefore, a nonzero contribution to $\partial_v x_I$ is given only by the derivations ∂_{e_i} with $i \in I$. Formula (2.42) implies that

$$\partial_{e_{i_1}} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_n} = x_{i_2} \wedge x_{i_3} \wedge \cdots \wedge x_{i_n}$$

for every collection of indices $i_1, i_2, \dots, i_n$, not necessarily increasing. Hence,

$$\begin{aligned} \partial_{e_{i_k}} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_n} &= \partial_{e_{i_k}} (-1)^{k-1} x_{i_k} \wedge x_{i_1} \wedge \cdots \wedge x_{i_{k-1}} \wedge x_{i_{k+1}} \cdots x_{i_n} \\ &= (-1)^{k-1} \partial_{e_{i_k}} x_{i_k} \wedge x_{i_1} \wedge \cdots \wedge x_{i_{k-1}} \wedge x_{i_{k+1}} \cdots x_{i_n} \\ &= (-1)^{k-1} x_{i_1} \wedge \cdots \wedge x_{i_{k-1}} \wedge x_{i_{k+1}} \cdots x_{i_n} . \end{aligned}$$

In other words, the derivation along the basis vector that is dual to the kth variable from the left in the monomial behaves as $(-1)^{k-1} \frac{\partial}{\partial x_{i_k}}$, where the *Grassmannian partial derivative* $\frac{\partial}{\partial x_i}$ takes x_i to 1 and annihilates all x_j with $j \neq i$, exactly as in the symmetric case. However, the sign $(-1)^k$ in the previous formula forces the Grassmannian partial derivatives to satisfy the *Grassmannian Leibniz rule*, which differs from the usual one by an extra sign.

Exercise 2.21 (Grassmannian Leibniz Rule) Prove that for every homogeneous Grassmannian polynomial $\omega, \tau \in \Lambda V^*$ and vector $v \in V$, one has

$$\partial_v(\omega \wedge \tau) = \partial_v(\omega) \wedge \tau + (-1)^{\deg \omega} \omega \wedge \partial_v(\tau). \tag{2.46}$$

Since the Grassmannian polynomials are linear in each variable, it follows that $\partial_v^2 \omega = 0$ for all $v \in V$, $\omega \in \Lambda V$. The relation $\partial_v^2 = 0$ forces the Grassmannian derivatives to be skew commutative, i.e.,

$$\partial_u \partial_w = -\partial_w \partial_u \quad \forall\, u, w \in V.$$

2.6.3 Linear Support of a Homogeneous Grassmannian Polynomial

Let V be a finite-dimensional vector space over a field $\Bbbk$ of characteristic zero. For the needs of further applications, in this section we switch between V^* and V and consider $\omega \in \Lambda^n V$. The *linear support* $\operatorname{Supp} \omega$ is defined to be the minimal (with respect to inclusions) vector subspace $W \subset V$ such that $\omega \in \Lambda^n W$. It coincides with the linear support of the complete polarization $\widetilde{\omega} \in \operatorname{Alt}^n V$, and is linearly generated by all $(n-1)$-tuple partial derivatives[14]

$$\partial_J \omega \overset{\text{def}}{=} \partial_{x_{j_1}} \partial_{x_{j_2}} \cdots \partial_{x_{j_{n-1}}} \omega = \frac{\partial}{\partial_{e_{j_1}}} \frac{\partial}{\partial_{e_{j_2}}} \cdots \frac{\partial}{\partial_{e_{j_{n-1}}}} \omega,$$

where $J = j_1 j_2 \dots j_{n-1}$ runs through all sequences of $n-1$ distinct indices from the set $\{1, 2, \dots, d\}$, $d = \dim V$. Up to a sign, the order of indices in J is not essential, and we will not assume the indices to be increasing, because this simplifies the notation in what follows. Let us expand ω as a sum of basis monomials

$$\omega = \sum_I a_I e_I = \sum_{i_1 i_2 \dots i_n} \alpha_{i_1 i_2 \dots i_n} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}, \tag{2.47}$$

where $I = i_1 i_2 \dots i_n$ also runs through the n-tuples of distinct but not necessarily increasing indices, and the coefficients $\alpha_{i_1 i_2 \dots i_n} \in \Bbbk$ are alternating in $i_1 i_2 \dots i_n$. Nonzero contributions to $\partial_J \omega$ are given only by the monomials $a_I e_I$ with $I \supset J$. Therefore, up to a common sign,

$$\partial_J \omega = \pm \sum_{i \notin J} \alpha_{j_1 j_2 \dots j_{n-1} i}\, e_i. \tag{2.48}$$

[14]Compare with Sect. 2.5.6 on p. 43.

Proposition 2.8 *The following conditions on a Grassmannian polynomial $\omega \in \Lambda^n V$ written in the form (2.47) are equivalent:*

1. $\omega = u_1 \wedge u_2 \wedge \cdots \wedge u_n$ *for some* $u_1, u_2, \dots, u_n \in V$.
2. $u \wedge \omega = 0$ *for all* $u \in \mathrm{Supp}(\omega)$.
3. *for any two collections* $i_1 i_2 \dots i_{m+1}$ *and* $j_1 j_2 \dots j_{m-1}$ *consisting of* $n+1$ *and* $n-1$ *distinct indices, the following Plücker relation holds:*

$$\sum_{\nu=1}^{m+1} (-1)^{\nu-1} a_{j_1 \dots j_{m-1} i_\nu} a_{i_1 \dots \widehat{i_\nu} \dots i_{m+1}} = 0, \tag{2.49}$$

where the hat in $a_{i_1 \dots \widehat{i_\nu} \dots i_{m+1}}$ *means that the index* i_ν *should be omitted.*

Proof Condition 1 holds if and only if ω belongs to the top homogeneous component of its linear span, $\omega \in \Lambda^{\dim \mathrm{Supp}(\omega)} \mathrm{Supp}(\omega)$. Condition 2 means the same because of the following exercise.

Exercise 2.22 Show that $\omega \in \Lambda U$ is homogeneous of degree $\dim U$ if and only if $u \wedge \omega = 0$ for $u \in U$.

The Plücker relation (2.49) asserts the vanishing of the coefficient of

$$e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_{m+1}}$$

in the product $\left(\partial_{j_1 \dots j_{m-1}} \omega\right) \wedge \omega$. In other words, (2.49) is the coordinate form of condition 2 written for the vector $u = \partial_{j_1 \dots j_{m-1}} \omega$ from the formula (2.48). Since these vectors linearly generate the subspace $\mathrm{Supp}(\omega)$, the whole set of Plücker relations is equivalent to condition 2. □

Example 2.6 (The Plücker Quadric) Let $n = 2$, $\dim V = 4$, and let e_1, e_2, e_3, e_4 be a basis of V. Then the expansion (2.47) for $\omega \in \Lambda^2 V$ looks like $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j$, where the coefficients a_{ij} form a skew-symmetric 4×4 matrix. The Plücker relation corresponding to $(i_1, i_2, i_3) = (2, 3, 4)$ and $j_1 = 1$ is

$$a_{12} a_{34} - a_{13} a_{24} + a_{14} a_{23} = 0. \tag{2.50}$$

All other choices of (i_1, i_2, i_3) and $j_1 \notin \{i_1, i_2, i_3\}$ lead to exactly the same relation.

Exercise 2.23 Check this.

For $j_1 \in \{i_1, i_2, i_3\}$, we get the trivial equality $0 = 0$. Thus for $\dim V = 4$, the set of decomposable Grassmannian quadratic forms $\omega \in \Lambda^2 V$ is described by just one quadratic equation, (2.50).

Exercise 2.24 Convince yourself that the Eq. (2.50) in $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j$ is equivalent to the condition[15] $\omega \wedge \omega = 0$.

[15]Compare with Problem 17.20 of Algebra I.

2.6.4 Grassmannian Varieties and the Plücker Embedding

Given a vector space V of dimension d, the set of all vector subspaces $U \subset V$ of dimension m is denoted by $\mathrm{Gr}(m, V)$ and called the *Grassmannian*. When the origin of V is not essential or $V = \Bbbk^d$, we write $\mathrm{Gr}(m, d)$ instead of $\mathrm{Gr}(m, V)$. Thus, $\mathrm{Gr}(1, V) = \mathbb{P}(V)$, $\mathrm{Gr}(\dim V - 1, V) = \mathbb{P}(V^*)$. The Grassmannian $\mathrm{Gr}(m, V)$ is embedded into the projective space $\mathbb{P}(\Lambda^m V)$ by means of the *Plücker map*

$$p_m : \mathrm{Gr}(m, V) \to \mathbb{P}(\Lambda^m V), \quad U \mapsto \Lambda^m U \subset \Lambda^m V, \tag{2.51}$$

sending every m-dimensional subspace $U \subset V$ to its highest exterior power $\Lambda^m U$, which is a 1-dimensional vector subspace in $\Lambda^m V$. If U is spanned by vectors $u_1, u_2, \dots, u_m$, then $p_m(U) = u_1 \wedge u_2 \wedge \cdots \wedge u_m$ up to proportionality.

Exercise 2.25 Check that the Plücker map is injective.

The image of the map (2.51) consists of all Grassmannian polynomials $\omega \in \Lambda^m V$ completely factorizable into a product of m vectors. Such polynomials are called *decomposable*. By Proposition 2.8, they form a projective algebraic variety given by the system of quadratic Eq. (2.49) in the coefficients of the expansion (2.47).

Example 2.7 (The Plücker Quadric, Geometric Continuation of Example 2.6) For $\dim V = 4$, the Grassmannian $\mathrm{Gr}(2, 4) = \mathrm{Gr}(2, V)$ can be viewed as the set of lines $\ell = \mathbb{P}(U)$ in $\mathbb{P}_3 = \mathbb{P}(V)$. The Plücker embedding (2.51) maps a line $(ab) \subset \mathbb{P}_3$ to the point $a \wedge b \in \mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$ and establishes a bijection between the lines in $\mathbb{P}_3$ and the points of the smooth quadric

$$P = \left\{\omega \in \Lambda^2 V \mid \omega \wedge \omega = 0\right\}$$

in $\mathbb{P}_5$, called the *Plücker quadric*.

2.6.5 The Grassmannian as an Orbit Space

The Grassmannian $\mathrm{Gr}(m, d)$ admits the following matrix description. Fix some basis $(e_1, e_2, \dots, e_d)$ in V. Given a vector subspace $U \subset V$ with a basis $(u_1, u_2, \dots, u_m)$, consider the $m \times d$ matrix A_u whose ith row is formed by the coordinates of the vector u_i in the chosen basis of V. Every other basis of U,

$$(w_1, w_2, \dots, w_m) = (u_1, u_2, \dots, u_m) \cdot C_{uw},$$

where $C_{wu} \in \mathrm{GL}_m(\Bbbk)$ is an invertible transition matrix, leads to the matrix A_w expressed through A_u by the formula

$$A_w = C_{uw}^t A_u.$$

Exercise 2.26 Check this.

Therefore, the bases in U are in bijection with the $m \times d$ matrices of rank m forming one orbit of the action of $\mathrm{GL}_m(\Bbbk)$ on $\mathrm{Mat}_{m\times d}(\Bbbk)$ by left multiplication, $G : A \mapsto GA$ for $G \in \mathrm{GL}_m$, $A \in \mathrm{Mat}_{m\times d}$. Hence the Grassmannian $\mathrm{Gr}(m, d)$ can be viewed as the set of all $m \times d$ matrices of rank m considered up to left multiplication by nondegenerate $m \times m$ matrices. Note that for $m = 1$, this agrees with the description of projective space $\mathbb{P}_{d-1} = \mathrm{Gr}(1, d)$ as the set of nonzero rows $(x_1, x_2, \dots, x_d) \in \Bbbk^d = \mathrm{Mat}_{1\times d}$ considered up to multiplication by nonzero constants $\lambda \in \Bbbk^* = \mathrm{GL}_1(\Bbbk)$. Thus, the matrix A_u formed by the coordinate rows of some basis vectors $u_1, u_2, \dots, u_m$ in U is the direct analogue of the homogeneous coordinates in projective space.

Exercise 2.27 (Plücker Coordinates) Verify that the coefficients $\alpha_{i_1 i_2 \dots i_n}$ in the expansion (2.47) written for $\omega = u_1 \wedge u_2 \wedge \cdots \wedge u_m$ are equal to the $m \times m$ minors of the matrix A_u.

These minors are called the *Plücker coordinates* of the subspace $U \subset V$ spanned by the vectors u_i.

Example 2.8 (Segre Varieties Revisited, Continuation of Example 1.2) Let $W = V_1 \oplus V_2 \oplus \cdots \oplus V_n$ be a direct sum of finite-dimensional vector spaces V_i. For $k \in \mathbb{N}$ and nonnegative integers $m_1, m_2, \dots, m_n$ such that $\sum_\nu m_\nu = k$ and

$$0 \leqslant m_i \leqslant \dim V_i,$$

denote by $W_{m_1,m_2,\dots,m_n} \subset \Lambda^k W$ the linear span of all products $w_1 \wedge w_2 \wedge \cdots \wedge w_k$ formed by m_1 vectors from V_1, m_2 vectors from V_2, etc.

Exercise 2.28 Show that the well-defined isomorphism of vector spaces

$$\Lambda^{m_1} V_1 \otimes \Lambda^{m_2} V_2 \otimes \cdots \otimes \Lambda^{m_n} V_n \xrightarrow{\sim} W_{m_1,m_2,\dots,m_n}$$

is given by the prescription $\omega_1 \otimes \omega_2 \otimes \cdots \otimes \omega_n \mapsto \omega_1 \wedge \omega_2 \wedge \cdots \wedge \omega_n$, and verify that

$$\Lambda^k W = \bigoplus_{m_1,m_2,\dots,m_n} W_{m_1,m_2,\dots,m_n} \simeq \bigoplus_{m_1,m_2,\dots,m_n} \Lambda^{m_1} V_1 \otimes \Lambda^{m_2} V_2 \otimes \cdots \otimes \Lambda^{m_n} V_n.$$

Thus, the tensor product $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ can be identified with the component $W_{1,1,\dots,1} \subset \Lambda^n W$. Under this identification, the decomposable tensors

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n$$

go to the decomposable Grassmannian monomials $v_1 \wedge v_2 \wedge \cdots \wedge v_n$. Therefore, the Segre variety from Example 1.2 on p. 6 is the intersection of the Grassmannian variety $\mathrm{Gr}(n, W) \subset \mathbb{P}(\Lambda^n W)$ with the projective subspace $\mathbb{P}(W_{1,1,\dots,1}) \subset \mathbb{P}(\Lambda^n W)$. In particular, the Segre variety is actually an algebraic variety described by the system of quadratic equations from Proposition 2.8 on p. 48 restricted to the linear subspace $W_{1,1,\dots,1} \subset \Lambda^n W$.

Problems for Independent Solution to Chapter 2

Problem 2.1 Let V be a finite-dimensional vector space of over a field $\Bbbk$ of characteristic zero. Show that the following vector spaces are canonically isomorphic: **(a)** $\mathrm{Sym}^n(V^*)$, **(b)** $\mathrm{Sym}^n(V)^*$, **(c)** $(S^nV)^*$, **(d)** $S^n(V^*)$, **(e)** symmetric n-linear forms $V \times V \times \cdots \times V \to \Bbbk$, **(f)** functions $V \to \Bbbk$, $v \mapsto f(v)$, where f is a homogeneous polynomial of degree n in the coordinates of v with respect to some basis in V.

Problem 2.2 For the same V and $\Bbbk$ as in the previous problem, show that the following vector spaces are canonically isomorphic: **(a)** $\mathrm{Alt}^n(V^*)$, **(b)** $\mathrm{Alt}^n(V)^*$, **(d)** $(\Lambda^nV)^*$, **(d)** $\Lambda^n(V^*)$, **(e)** alternating n-linear forms $V \times V \times \cdots \times V \to \Bbbk$.

Problem 2.3 Which of the isomorphisms from the previous two problems hold

(a) over a field $\Bbbk$ of any positive characteristic?
(b) for an infinite-dimensional vector space V?

Problem 2.4 (Aronhold's Principle) Let V be a finite-dimensional vector space over a field $\Bbbk$ of zero characteristic. Prove that the subspace of symmetric tensors $\mathrm{Sym}^n(V) \subset V^{\otimes n}$ is linearly generated by the proper nth tensor powers $v^{\otimes n} = v \otimes v \otimes \cdots \otimes v$ of vectors $v \in V$. Write the symmetric tensor

$$u \otimes w \otimes w + w \otimes u \otimes w + w \otimes w \otimes u \in \mathrm{Sym}^3(V)$$

as a linear combination of proper tensor cubes.

Problem 2.5 Is there a linear change of coordinates that makes the polynomial

$$9\,x^3 - 15\,yx^2 - 6\,zx^2 + 9\,xy^2 + 18\,z^2x - 2\,y^3 + 3\,zy^2 - 15\,z^2y + 7\,z^3$$

depend on at most two variables?

Problem 2.6 Ascertain whether the cubic Grassmannian polynomial

$$-\xi_1 \wedge \xi_2 \wedge \xi_3 + 2\,\xi_1 \wedge \xi_2 \wedge \xi_4 + 4\,\xi_1 \wedge \xi_3 \wedge \xi_4 + 3\,\xi_2 \wedge \xi_3 \wedge \xi_4$$

is decomposable. If it is, write down an explicit factorization. If not, explain why.

Problem 2.7 Let V be a vector space of dimension n. Fix some nonzero element $\eta \in \Lambda^nV$. Check that for all k, m with $k + m = n$, the perfect pairing between Λ^kV and Λ^mV is well defined by the formula $\omega_1 \wedge \omega_2 = \langle\, \omega_1, \omega_2 \,\rangle \cdot \eta$. Given a vector $v \in V$, describe the linear operator $\Lambda^{m-1}V \to \Lambda^m V$ dual with respect to this pairing to the left multiplication by $v : \Lambda^k V \to \Lambda^{k+1}V$, $\omega \mapsto v \wedge \omega$.

Problem 2.8 Verify that the Taylor expansion for the polynomial $\det(A)$ in the space of linear operators $A : V \to V$ has the following form:

$$\det(\lambda A + \mu B) = \sum_{p+q=n} \lambda^p \mu^q \cdot \operatorname{tr}\left(\Lambda^p A \cdot \Lambda^q B^*\right),$$

where $\Lambda^p A : \Lambda^p V \to \Lambda^p V$, $v_1 \wedge v_2 \wedge \cdots \wedge v_p \mapsto A(v_1) \wedge A(v_2) \wedge \ldots \wedge A(v_p)$ is the pth exterior power of A and $\Lambda^q B^* : \Lambda^p V \to \Lambda^p V$ is dual to $\Lambda^q B : \Lambda^q V \to \Lambda^q V$ with respect to the perfect pairing from Problem 2.7.

Problem 2.9 Write $\mathbb{P}_N = \mathbb{P}(S^2V^*)$ for the space of quadrics in $\mathbb{P}_n = \mathbb{P}(V)$, and $S \subset \mathbb{P}_N$ for the locus of all singular quadrics. Show that:

(a) S is an algebraic hypersurface of degree $n+1$,
(b) a point $Q \in S$ is a smooth point of S if and only if the corresponding quadric $Q \subset \mathbb{P}_n$ has just one singular point,
(c) the tangent hyperplane $T_Q S \subset \mathbb{P}_N$ to S at such a smooth point $Q \in S$ is formed by all quadrics in $\mathbb{P}_n$ passing through the singular point of the quadric $Q \subset \mathbb{P}_n$.

Problem 2.10 Find all singular points of the following plane projective curves[16] in $\mathbb{P}_2 = \mathbb{P}(\mathbb{C}^3)$: **(a)** $(x_0 + x_1 + x_2)^3 = 27\, x_0x_1x_2$, **(b)** $x^2y + xy^2 = x^4 + y^4$, **(c)** $(x^2 - y + 1)^2 = y^2(x^2 + 1)$.

Problem 2.11 Write an explicit rational parameterization[17] for the plane projective quartic

$$\left(x_0^2 + x_1^2\right)^2 + 3\, x_0^2 x_1 x_2 + x_1^3 x_2 = 0$$

using the projection of the curve from its singular point to some line.[18]

Problem 2.12 For a diagonalizable linear operator $F : V \to V$ with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, find the eigenvalues of $F^{\otimes n}$ for all $n \in \mathbb{N}$.

Problem 2.13 Prove that for every collection of linear operators

$$F_1, F_2, \ldots, F_m : V \to V$$

[16] Though the last two curves are given by their affine equations within the standard chart $U_0 \subset \mathbb{P}_2$, the points at infinity should also be taken into account.

[17] That is, a triple of rational functions $x_0(t), x_1(t), x_2(t) \in \Bbbk(t)$ such that $f(x_0(t), x_1(t), x_2(t)) = 0$ in $\Bbbk(t)$, where $f \in \Bbbk[x_0, x_1, x_2]$ is the equation of the curve.

[18] Compare with Example 11.7 and the proof of Proposition 17.6 in Algebra I.

and constants $\lambda_1, \lambda_2, \dots, \lambda_m \in \Bbbk$, one has $\lambda_1 F_1^{\otimes n} + \lambda_2 F_2^{\otimes n} + \dots + \lambda_m F_m^{\otimes n} = 0$ for all $n \in \mathbb{N}$ only if $\lambda_i = 0$ for all i.

Problem 2.14 Express the following quantities in terms of the coefficients of the characteristic polynomial of F for an arbitrary linear operator $F : V \to V$: **(a)** $\operatorname{tr} F^{\otimes 2}$, **(b)** $\operatorname{tr} F^{\otimes 3}$, **(c)** $\det F^{\otimes 2}$, **(d)** $\det F^{\otimes 3}$, **(e)** the trace and determinant of the map $\mathrm{Ad}_F : \mathrm{End}(V) \to \mathrm{End}(V)$, $G \mapsto FGF^{-1}$, assuming that F is invertible, **(f)** the trace and determinant of the map $S^2F : S^2V^* \to S^2V^*$ that sends a quadratic form $q : V \to \Bbbk$ to the composition $q \circ F : V \to \Bbbk$.

Problem 2.15 Let F be a diagonalizable linear operator on an n-dimensional vector space over a field $\Bbbk$ of characteristic zero. Express the eigenvalues of the operators

$$S^nF : v_1 v_2 \cdots v_n \mapsto F(v_1)F(v_2)\cdots F(v_n),$$

$$\Lambda^nF : v_1 \wedge v_2 \wedge \cdots \wedge v_n \mapsto F(v_1) \wedge F(v_2) \wedge \cdots \wedge F(v_n),$$

through the eigenvalues of F, and prove the following two identities in $\Bbbk[\![t]\!]$: **(a)** $\det(E - tF)^{-1} = \sum_{k \geqslant 0} \operatorname{tr}\bigl(S^kF\bigr) \cdot t^k$, **(b)** $\det(E + tF) = \sum_{k \geqslant 0} \operatorname{tr}\bigl(\Lambda^kF\bigr) \cdot t^k$.

Problem 2.16 (Splitting Principle) Prove that the answers you got in the previous two problems hold for nondiagonalizable linear operators F as well. Use the following arguments, known as a *splitting principle*. Interpret the relation on F you are going to prove as the identical vanishing of some polynomial with rational coefficients in the matrix elements f_{ij} of F considered as independent variables. Then prove the following claims:

(a) If a polynomial $f \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ evaluates to zero at all points of some dense subset of $\mathbb{C}^n$, then f is the zero polynomial. (Thus, it is enough to check that the relation being proved holds for some set of *complex* matrices dense in $\mathrm{Mat}_n(\mathbb{C})$.)

(b) The diagonalizable matrices are dense in $\mathrm{Mat}_n(\mathbb{C})$. Hint: every Jordan block[19] can be made diagonalizable by a small perturbation of the diagonal elements of the cell.

(c) The polynomial identity being proved is not changed under conjugation[20] $F \mapsto gFg^{-1}$ of the matrix $F = \bigl(f_{ij}\bigr)$ by any invertible matrix $g \in \mathrm{GL}_n(\mathbb{C})$. (Thus, it is enough to check the required identity only for the *diagonal* matrices.)[21]

[19] See Sect. 15.3.1 of Algebra I.

[20] This is clear if the identity in question expresses some basis-independent properties of the *linear operator* but not its matrix in some specific basis.

[21] Even for the diagonal matrices with distinct eigenvalues, because the conjugation classes of these matrices are dense in $\mathrm{Mat}_n(\mathbb{C})$ as well.

Problem 2.17 Use the splitting principle to prove the Cayley–Hamilton identity $\chi_F(F) = 0$ by reducing the general case to the diagonal F.

Problem 2.18 Prove that for every $F \in \mathrm{Mat}_{n^2}(\mathbb{C})$, one has $e^{F\otimes E+E\otimes F} = e^F \otimes e^F$ in $\mathrm{Mat}_{n^2}(\mathbb{C})$, where E is the identity matrix.

Problem 2.19* Prove the identity $\log\det(E-A) = \operatorname{tr}\log(E-A)$ in the ring of formal power series with rational coefficients in the matrix elements a_{ij} of the $n\times n$ matrix A. Show that for all small enough complex matrices $A \in \mathrm{Mat}_n(\mathbb{C})$, this identity becomes a true numerical identity in $\mathbb{C}$.

Problem 2.20 Let V be a vector space of dimension 4 over $\mathbb{C}$ and $g \in S^2V^*$ a nondegenerate quadratic form with the polarization $\widetilde{g} \in \mathrm{Sym}^2 V^*$. Write $G \subset \mathbb{P}_3 = \mathbb{P}(V)$ for the projective quadric defined by the equation $g(x) = 0$.

(a) Prove that there exists a unique symmetric bilinear form $\Lambda^2\widetilde{g}$ on the space Λ^2V such that

$$\Lambda^2\widetilde{g}(\, v_1\wedge v_2,\, w_1\wedge w_2\,) \stackrel{\text{def}}{=} \det\begin{pmatrix}\widetilde{g}(v_1,w_1) & \widetilde{g}(v_1,w_2)\\ \widetilde{g}(v_2,w_1) & \widetilde{g}(v_2,w_2)\end{pmatrix}$$

for all decomposable bivectors.

(b) Check that this form is symmetric and nondegenerate, and write its Gram matrix in the monomial basis $e_i\wedge e_j$ constructed from a g-orthonormal basis e_1, e_2, e_3, e_4 of V.

(c) Show that the Plücker embedding $\mathrm{Gr}(2,V) \hookrightarrow \mathbb{P}_3 = \mathbb{P}(V)$ from Example 2.7 on p. 49, which establishes a one-to-one correspondence between the lines in $\mathbb{P}_3 = \mathbb{P}(V)$ and the points of the Plücker quadric $P = \{\omega \in \Lambda^2V \mid \omega\wedge\omega = 0\}$ in $\mathbb{P}_5 = \mathbb{P}(\Lambda^2V)$, maps the tangent lines to G bijectively to the intersection $P \cap \Lambda^2G$, where $L^2G \subset \mathbb{P}_5$ is the quadric given by the symmetric bilinear form $\Lambda^2\widetilde{g}$.

Problem 2.21 (Plücker–Segre–Veronese Interaction) Let U be a vector space of dimension 2 over $\mathbb{C}$. Consider the previous problem for the vector space $V = \operatorname{End} U$ and the quadratic form $g = \det$, whose value on an endomorphism $f : U \to U$ is $\det f \in \mathbb{C}$ and the zero set is the Segre quadric[22] $G \subset \mathbb{P}_3 = \mathbb{P}(V)$ consisting of endomorphisms of rank one.

(a) Construct canonical isomorphisms

$$S^2V \simeq \mathrm{Sym}^2 V \simeq \left(S^2U^*\otimes S^2U\right)\oplus\left(\Lambda^2U^*\otimes\Lambda^2U\right),$$
$$\Lambda^2V \simeq \mathrm{Alt}^2 V \simeq \left(S^2U^*\otimes\Lambda^2U\right)\oplus\left(\Lambda^2U^*\otimes S^2U\right).$$

(b) Show that the Plücker embedding sends two families of lines on the Segre quadric to the pair of smooth conics $P\cap\Lambda_+$, $P\cap\Lambda_-$ cut out of the Plücker

[22] See Example 1.3 on p. 8 and Example 17.6 from Algebra I.

quadric $P \subset \mathbb{P}\left(\Lambda^2 \operatorname{End}(U)\right)$ by the complementary planes

$$\Lambda_- = \mathbb{P}\left(S^2U^* \otimes \Lambda^2 U\right) \quad \text{and} \quad \Lambda_+ = \mathbb{P}\left(\Lambda^2 U^* \otimes S^2 U\right),$$

the collectivizations of components of the second decomposition in (a).

(c) Check that the two conics $P \cap \Lambda_-$ and $P \cap \Lambda_+$ in (b) are the images of the quadratic Veronese embeddings

$$\mathbb{P}(U^*) \hookrightarrow \mathbb{P}\left(S^2U^*\right) = \mathbb{P}\left(S^2U^* \otimes \Lambda^2 U\right), \quad \xi \mapsto \xi^2,$$
$$\mathbb{P}(U) \hookrightarrow \mathbb{P}\left(S^2U\right) = \mathbb{P}\left(\Lambda^2U^* \otimes S^2 U\right), \quad v \mapsto v^2.$$

In other words, there is the following commutative diagram:

$$\begin{tikzcd}
\mathbb{P}_1^+ = \mathbb{P}(U) \arrow[rr, hook, "\text{Veronese}"'] & & \mathbb{P}(S^2U) = \Lambda_+ \arrow[d, hook] \\
\mathbb{P}_1^+ \times \mathbb{P}_1^- \arrow[u, "\pi_+"] \arrow[d, "\pi_-"] \arrow[r, "\text{Segre}", "\sim"'] & G \subset \mathbb{P}\operatorname{End}(U) \arrow[r, dashed, "\text{Plücker}"] & \mathbb{P}\begin{pmatrix} \Lambda^2U^* \otimes S^2U \\ \oplus \\ S^2U^* \otimes \Lambda^2 U \end{pmatrix} \\
\mathbb{P}_1^- = \mathbb{P}(U^*) \arrow[rr, hook, "\text{Veronese}"] & & \mathbb{P}(S^2U^*) = \Lambda_- \arrow[u, hook]
\end{tikzcd}$$

where the Plücker embedding is dashed, because it takes lines to points.

Problem 2.22 (Hodge Star) Under the conditions of Problem 2.20, verify that for every nondegenerate quadratic form g on V, the linear operator $* : \Lambda^2 V \to \Lambda^2 V$, $\omega \mapsto \omega^*$, is well defined by the formula

$$\omega_1 \wedge \omega_2^* = \Lambda^2\widetilde{g}(\omega_1, \omega_2) \cdot e_1 \wedge e_2 \wedge e_3 \wedge e_4 \quad \forall\, \omega_1, \omega_2 \in \Lambda^2 V,$$

where e_1, e_2, e_3, e_4 is a g-orthonormal basis of V. Check that, up to a scalar complex factor of modulus one, the star operator does not depend on the choice of orthonormal basis. Describe the eigenspaces of the star operator and indicate their place in the diagram from Problem 2.21.

Problem 2.23 (Grassmannian Exponential) Let V be a vector space over a field $\Bbbk$ of *arbitrary* characteristic. The *Grassmannian exponential* is defined for decomposable $\omega \in \Lambda^{2m}$ by the assignment $e^{\omega} \stackrel{\text{def}}{=} 1 + \omega$. For an arbitrary even-degree homogeneous Grassmannian polynomial $\zeta \in \Lambda^{2m} V$, we write $\zeta = \sum \omega_i$, where all ω_i are decomposable, and put $e^{f} \stackrel{\text{def}}{=} \prod e^{\omega_i}$. Verify that this product depends neither on an ordering of factors nor on the choice of expression[23] $\zeta = \sum \omega_i$. Prove that the exponential map $\Lambda^{\text{even}}V \hookrightarrow \Lambda^{\text{even}}V$, $\zeta \mapsto e^{\zeta}$, is an injective homomorphism of the additive group of even-degree Grassmannian polynomials to the multiplicative group of even-degree Grassmannian polynomials with unit constant term. Show that over a field of characteristic zero, $\partial_\alpha e^{\zeta} = e^{\zeta} \wedge \partial_\alpha \zeta$ for all $\alpha \in V^*$, and $e^{\zeta} = \sum_{k \geqslant 0} \frac{1}{k!} \zeta^{\wedge k}$.

Problem 2.24 Let V be a finite-dimensional vector space. Show that the subspaces

$$\mathcal{I}_{\text{sym}} \cap (V \otimes V) \subset V \otimes V \quad \text{and} \quad \mathcal{I}_{\text{skew}} \cap (V^* \otimes V^*) \subset V^* \otimes V^*,$$

which generate the ideals of the commutativity and skew-commutativity relations[24] $\mathcal{I}_{\text{sym}} \subset \mathsf{T}V$, $\mathcal{I}_{\text{skew}} \subset \mathsf{T}V^*$, are the annihilators of each other under the perfect pairing between $V \otimes V$ and $V^* \otimes V^*$ provided by the complete contraction.

Problem 2.25 (Koszul and de Rham Complexes) Let $e_1, e_2, \dots, e_n$ be a basis of a vector space V over a field $\Bbbk$ of characteristic zero. Write x_i and ξ_i for the images of the basis vector e_i in the symmetric algebra SV and the exterior algebra ΛV respectively. Convince yourself that there are well-defined linear operators

$$d \overset{\text{def}}{=} \sum_\nu \xi_\nu \otimes \frac{\partial}{\partial x_\nu} : \Lambda^k V \otimes S^m V \to \Lambda^{k+1} V \otimes S^{m-1} V,$$

$$\partial \overset{\text{def}}{=} \sum_\nu \frac{\partial}{\partial \xi_\nu} \otimes x_\nu : \Lambda^k V \otimes S^m V \to \Lambda^{k-1} V \otimes S^{m+1} V,$$

acting on decomposable tensors by the rules

$$d : \omega \otimes f \mapsto \sum_\nu \frac{\partial \omega}{\partial \xi_\nu} \otimes x_\nu \cdot f,$$

$$\partial : \omega \otimes f \mapsto \sum_\nu \xi_\nu \wedge \omega \otimes \frac{\partial f}{\partial x_\nu}.$$

Prove that neither operator depends on the choice of basis in V and that both operators have zero squares, $d^2 = 0 = \partial^2$. Verify that their *s-commutator* $d\partial + \partial d$ acts on $\Lambda^k V \otimes S^m V$ as a homothety $(k+m) \cdot \mathrm{Id}$. Describe the *homology spaces* $\ker d / \operatorname{im} d$ and $\ker \partial / \operatorname{im} \partial$.

[23] Note that the decomposition of a Grassmannian polynomial into a sum of decomposable monomials is highly nonunique.

[24] See Sect. 2.3.1 on p. 26 and Sect. 2.3.3 on p. 29.

Chapter 3
Symmetric Functions

3.1 Symmetric and Sign Alternating Polynomials

The symmetric group S_n acts on the polynomial ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ by permutations of variables:

$$gf(x_1, x_2, \dots, x_n) = f\left(x_{g^{-1}(1)}, x_{g^{-1}(2)}, \dots, x_{g^{-1}(n)}\right) \quad \forall\, g \in S_n. \tag{3.1}$$

A polynomial $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ is called *symmetric* if $gf = f$ for all $g \in S^n$, and *alternating* if $gf = \operatorname{sgn}(g) \cdot f$ for all $g \in S^n$. The symmetric polynomials clearly form a subring of $\mathbb{Z}[x_1, x_2, \dots, x_n]$, whereas the alternating polynomials form a module over this subring, since the product of symmetric and alternating polynomials is alternating.

In Example 1.1 on p. 6 we have seen that the polynomial ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$, considered as a $\mathbb{Z}$-module, is isomorphic to the nth tensor power $\mathbb{Z}[t]^{\otimes n}$ of the polynomial ring in one variable. The isomorphism

$$\varkappa : \mathbb{Z}[t]^{\otimes n} \xrightarrow{\sim} \mathbb{Z}[x_1, x_2, \dots, x_n], \quad t^{m_1} \otimes t^{m_2} \otimes \cdots \otimes t^{m_n} \mapsto x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}, \tag{3.2}$$

takes the multiplication of polynomials in $\mathbb{Z}[x_1, x_2, \dots, x_n]$ to the componentwise multiplication

$$(f_1 \otimes f_2 \otimes \cdots \otimes f_n) \cdot (g_1 \otimes g_2 \otimes \cdots \otimes g_n) = (f_1 g_1) \otimes (f_2 g_2) \otimes \cdots \otimes (f_n g_n).$$

Exercise 3.1 Verify that this multiplication equips $\mathbb{Z}[t]^{\otimes n}$ with the structure of a commutative ring with unit $1 \otimes 1 \otimes \cdots \otimes 1$.

The action of the symmetric group on $\mathbb{Z}[x_1, x_2, \dots, x_n]$ agrees with the action on $\mathbb{Z}[t]^{\otimes n}$ by permutations of tensor factors considered in Sect. 2.4 on p. 31. Therefore, the symmetric and alternating polynomials in $\mathbb{Z}[x_1, x_2, \dots, x_n]$ correspond to the symmetric and alternating tensors in $\mathbb{Z}[t]^{\otimes n}$. In particular, the standard monomial

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_3

bases of $\mathbb{Z}$-modules $\mathrm{Sym}^n(\mathbb{Z}[t])$ and $\mathrm{Alt}^n(\mathbb{Z}[t])$, defined in formulas (2.21) and (2.22) on p. 34, provide the $\mathbb{Z}$-modules of symmetric and alternating polynomials with some obvious bases over $\mathbb{Z}$, called the *monomial basis* of symmetric polynomials and the *determinantal basis* of alternating polynomials.

The first is formed by sums of monomials sharing the same S_n-orbit

$$m_\lambda \stackrel{\text{def}}{=} \left(\text{the sum of all monomials in the } S_n\text{-orbit of } x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}\right) \tag{3.3}$$

and is numbered by the Young diagrams $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ of length[1] at most n. The monomial $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ is the lexicographically highest[2] monomial in the orbit, because of the inequalities

$$\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n.$$

The polynomial m_λ is homogeneous of degree $\deg m_\lambda = |\lambda|$, the total number of cells in λ.

Exercise 3.2 Convince yourself that every symmetric polynomial can be uniquely written as a finite $\mathbb{Z}$-linear combination of the polynomials m_λ.

The determinantal basis of the alternating polynomials consists of the alternating sums of monomials forming one S_n-orbit:

$$\Delta_\nu = \sum_{g \in S_n} \mathrm{sgn}(g)\, x_{g(1)}^{\nu_1} x_{g(2)}^{\nu_2} \cdots x_{g(n)}^{\nu_n}. \tag{3.4}$$

It is numbered by the Young diagrams ν with *strictly decreasing* length of rows,

$$\nu_1 > \nu_2 > \cdots > \nu_n,$$

because the alternating property forces the exponents of all variables in every monomial to be distinct.[3] Note that all such Young diagrams ν contain the diagram

$$\delta \stackrel{\text{def}}{=} ((n-1), (n-2), \ldots, 1, 0),$$

the smallest Young diagram with n rows of nonnegative strictly decreasing lengths. The difference

$$\lambda = \nu - \delta = ((\nu_1 - n + 1),\, (\nu_2 - n + 2),\, \ldots,\, (\nu_{n-1} - 1),\, \nu_n)$$

[1]That is, consisting of at most n rows; see Example 1.3 in Algebra I for the terminology related to Young diagrams.

[2]Recall that the *lexicographic order* on $\mathbb{Z}^k$ assigns $(m_1, m_2, \ldots, m_k) > (n_1, n_2, \ldots, n_k)$ if the leftmost m_i such that $m_i \neq n_i$ is greater than n_i.

[3]The coefficient of every monomial changes sign under the transposition of any two variables.

has $\lambda_i = \nu_i - n + i$ and constitutes a Young diagram of length at most n with unconstrained lengths of rows. Sometimes it is convenient to number the determinantal alternating polynomials (3.4) by such unconstrained Young diagrams λ, and we will write $\Delta_{\lambda+\delta}$ instead of Δ_ν in such cases. The polynomial Δ_ν is called *determinantal*, because the right-hand side of (3.4) expands the determinant[4]

$$\Delta_\nu = \det(x_j^{\nu_i}) = \det \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix}. \tag{3.5}$$

For $\nu = \delta$, it becomes the *Vandermonde determinant*

$$\Delta_\delta = \det(x_j^{n-i}) = \det \begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}. \tag{3.6}$$

Since every alternating polynomial $f(x_1, x_2, \dots, x_n)$ vanishes for $x_i = x_j$, all the differences $(x_i - x_j)$ divide f in $\mathbb{Z}[x_1, x_2, \dots, x_n]$. This forces f to be divisible by the product $\prod_{i<j}(x_i - x_j)$, because all the differences $x_i - x_j$ are mutually nonassociated irreducible polynomials, and the ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ is factorial.

Exercise 3.3 Verify that $\Delta_\delta = \prod_{i<j}(x_i - x_j)$.

We conclude that multiplication by the Vandermonde determinant $f \mapsto f \cdot \Delta_\delta$ establishes a bijection between the symmetric and alternating polynomials. Note that this bijection is an isomorphism of modules over the ring of symmetric polynomials, and in particular, an isomorphism of $\mathbb{Z}$-modules. The preimage of the determinantal basis (3.5) under this isomorphism is called the *Schur basis* of the $\mathbb{Z}$-module of symmetric polynomials. We have the following proposition.

Proposition 3.1 (Schur Basis) *The determinantal Schur polynomials*

$$s_\lambda \stackrel{\text{def}}{=} \Delta_{\delta+\lambda}/\Delta_\delta,$$

where λ runs through the Young diagrams of length at most n, form a basis in the $\mathbb{Z}$-module of symmetric polynomials in n variables. □

[4]Recall that we use the notation $(f(i,j))$, where $f(i,j)$ is some function of i, j, for the matrix having $f(i,j)$ at the intersection of the ith row and jth column.

3.2 Elementary Symmetric Polynomials

The *elementary symmetric polynomials* $e_0, e_1, \ldots, e_n \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ are defined by the following equality in the ring of polynomials in t with coefficients in $\mathbb{Z}[x_1, x_2, \ldots, x_n]$:

$$E(t) = \prod_i (1 + x_i t) = \sum_{k=0}^{n} e_k(x) \cdot t^k. \tag{3.7}$$

Explicitly, $e_0 = 1$ and $e_k(x) = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$ is the sum of all *k-linear* monomials of degree k. These polynomials also appear in the *Viète formulas* expressing the coefficients of a monic polynomial

$$t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n = \prod_{i=1}^{n} (x - \alpha_i)$$

through the roots: $a_i = (-1)^i e_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

For every Young diagram $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we set

$$e_\lambda \stackrel{\text{def}}{=} e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k} = \prod_{i=1}^{k} e_{\lambda_i}$$

and call these polynomials *elementary symmetric* as well. Note that

$$e_\lambda = e_1^{m_1} e_2^{m_2} \cdots e_n^{m_n},$$

where $m_i = m_i(\lambda)$ is the number of rows of length i in the diagram λ. Thus, the polynomials e_λ are in bijection with the monomials in $e_1, e_2, \ldots, e_n$.

Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_m) = \lambda^t$ be a pair of transposed[5] Young diagrams. Then the lexicographically highest monomial of e_λ appears as the product of monomials $x_1 \cdots x_{\lambda_1}$ from e_{λ_1}, $x_1 \cdots x_{\lambda_2}$ from e_{λ_2}, etc., up to $x_1 \ldots x_{\lambda_m}$ from e_{λ_m}. Let us put x_1 in all cells of the first column of the Young diagram λ, x_2 in all cells of the second column, etc. Then the previous monomials appear in the rows of the filled diagram λ, and the product of these monomials equals $x_1^{\mu_1} x_2^{\mu_2} \cdots x_n^{\mu_n}$. Therefore, the elementary symmetric polynomial e_λ is expanded through the monomial basis (3.3) as

$$e_\lambda = m_{\lambda^t} + (\text{lexicographically lower terms}). \tag{3.8}$$

[5]That is, obtained from one another by reflection in the main diagonal.

Proposition 3.2 *The polynomials $e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_m}$, where λ runs through the Young diagrams with at most n columns, form a basis of the $\mathbb{Z}$-module of symmetric polynomials in n variables.*

Proof Write the basis vectors m_μ in the lexicographically increasing order of their indices μ, and the polynomials e_λ in the lexicographically increasing order of the transposed diagrams λ^t. Then the transition matrix from e_λ to m_μ is upper unitriangular by (3.8). We know from Example 8.17 of Algebra I that every such matrix is invertible.[6] Therefore, the polynomials e_λ also form a basis. □

Corollary 3.1 *The polynomials $e_1, e_2, \ldots, e_n$ are algebraically independent,[7] and the assignment $f(t_1, t_2, \ldots, t_n) \mapsto f(e_1, e_2, \ldots, e_n)$ establishes an isomorphism of the polynomial ring $\mathbb{Z}[t_1, t_2, \ldots, t_n]$ with the ring of symmetric polynomials in n variables. In other words, every symmetric polynomial in n variables is uniquely expressed as a polynomial in $e_1, e_2, \ldots, e_n$.* □

Corollary 3.2 *Every symmetric polynomial in the roots of a monic polynomial f can be rewritten as a polynomial in the coefficients of f.* □

3.3 Complete Symmetric Polynomials

The sum of all monomials of total degree k in the variables $x_1, x_2, \ldots, x_n$ is denoted by $h_k = h_k(x_1, x_2, \ldots, x_n)$ and called the *complete* symmetric polynomial of degree k. Equivalently, the polynomial h_k can be described as the coefficient of t^k in the following formal power series in t over the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$:

$$H(t) = \prod_i \frac{1}{1 - x_i t} = \prod_i \left(1 + x_i t + x_i^2 t^2 + x_i^3 t^3 + \cdots\right) = \sum_{k \geqslant 0} h_k(x) \cdot t^k. \tag{3.9}$$

Indeed, when we choose m_ith term in the ith geometric progression and multiply the chosen terms together, we get $x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} \cdot t^{m_1 + \cdots + m_n}$. Thus, the coefficient of t^k equals the sum of all monomials $x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$ with

$$m_1 + m_2 + \cdots + m_n = k.$$

Since the generating series for the elementary and complete symmetric polynomials are related by the equality $H(t)E(-t) = 1$, comparison of the coefficients of t^k on both sides leads to the following recurrence formulas:

$$(-1)^k h_k = e_k - e_{k-1} h_1 + e_{k-2} h_2 - \cdots + (-1)^{k-1} e_1 h_{k-1}, \tag{3.10}$$

$$(-1)^k e_k = h_k - h_{k-1} e_1 + h_{k-2} e_2 - \cdots + (-1)^{k-1} h_1 e_{k-1}. \tag{3.11}$$

[6] Over an arbitrary (even noncommutative) ring with unit.

[7] That is, $f(e_1, e_2, \ldots, e_n) \neq 0$ in $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ for every $f \in \mathbb{Z}[t_1, t_2, \ldots, t_n]$.

Proposition 3.3 *There exists a unique involutive automorphism ω of the ring of symmetric polynomials in n variables such that $\omega(e_k) = h_k$ and $\omega(h_k) = e_k$ for every $k = 1, 2, \dots, n$.*

Proof Since the ring of symmetric polynomials is $\mathbb{Z}[e_1, e_2, \dots, e_n]$, the assignment $\omega : e_k \mapsto h_k$ is uniquely extended to a ring endomorphism of the ring of symmetric polynomials. The recurrence formulas (3.10), (3.11) show that ω maps every h_k back to e_k for $1 \leqslant k \leqslant n$. Therefore, ω is an involutive automorphism. □

Corollary 3.3 *The polynomials $h_1, h_2, \dots, h_n$ are algebraically independent. Every symmetric polynomial in n variables can be uniquely written as a polynomial in $h_1, h_2, \dots, h_n$. In other words, the assignment $f(t_1, t_2, \dots, t_n) \mapsto f(h_1, h_2, \dots, h_n)$ establishes an isomorphism between the polynomial ring $\mathbb{Z}[t_1, t_2, \dots, t_n]$ and the ring of symmetric polynomials in n variables.* □

3.4 Newton's Sums of Powers

3.4.1 Generating Function for the p_k

The sum of kth powers of all the variables

$$p_k(x) \stackrel{\text{def}}{=} x_1^k + x_2^k + \cdots + x_n^k, \text{ where } k \geqslant 1, \tag{3.12}$$

is called the *Newton symmetric polynomial* of degree k. These polynomials appear as the coefficients of the logarithmic derivative

$$\begin{aligned}\frac{d}{dt} \log H(t) &= \frac{d}{dt} \log \prod_i \frac{1}{1 - x_i t} = -\sum_i \frac{d}{dt} \log(1 - x_i t) \\ &= \sum_i \frac{x_i}{1 - x_i t} = \sum_i \sum_{\alpha \geqslant 0} x_i^{\alpha+1} \cdot t^\alpha = \sum_{k \geqslant 1} p_k(x) \cdot t^{k-1}.\end{aligned}$$

The latter power series is denoted by $P(t)$. Since $H(t) = 1/E(-t)$, it follows that

$$P(t) = \frac{H'(t)}{H(t)} = \frac{E'(-t)}{E(-t)}.$$

Comparison of the coefficients of t^{k-1} on both sides of the equalities

$$H(t)P(t) = H'(t) \quad \text{and} \quad E(-t)P(t) = E'(-t)$$

leads to the recurrent *Newton formulas* expressing p_k in terms of h_k and e_k:

$$p_k = kh_k - h_{k-1}p_1 - h_{k-2}p_2 - \cdots - h_1 p_{k-1}, \tag{3.13}$$

$$(-1)^{k-1}p_k = ke_k - e_{k-1}p_1 + e_{k-2}p_2 - \cdots + (-1)^{k-1}e_1 p_{k-1}. \tag{3.14}$$

It follows from these formulas by induction on k that every polynomial p_k is an eigenvector of the involution ω from Proposition 3.3 with the eigenvalue $(-1)^{k-1}$,

$$\omega(p_k) = (-1)^{k-1}p_k. \tag{3.15}$$

Proposition 3.4 *The symmetric Newton polynomials $p_1, p_2, \dots, p_n$ are algebraically independent. Every symmetric polynomial in $\mathbb{Q}[x_1, x_2, \dots, x_n]$ can be uniquely written as a polynomial with rational coefficients in $p_1, p_2, \dots, p_n$. In other words, the assignment $f(t_1, t_2, \dots, t_n) \mapsto f(p_1, p_2, \dots, p_n)$ establishes an isomorphism between the polynomial ring $\mathbb{Q}[t_1, t_2, \dots, t_n]$ and the ring of symmetric polynomials in n variables with coefficients in $\mathbb{Q}$.*

Proof The formula (3.14) implies that for every $N \in \mathbb{N}$, the $\mathbb{Q}$-linear span of products $p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}$ in the vector space $\mathbb{Q}[x_1, x_2, \dots, x_n]_{\leqslant N}$ of polynomials of total degree at most N coincides with the $\mathbb{Q}$-linear span of products $e_1^{m_1}e_2^{m_2}\cdots e_n^{m_n}$. Since the polynomials $e_1^{m_1}e_2^{m_2}\cdots e_n^{m_n}$ are linearly independent and the total number of them coincides with the total number of polynomials $p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}$, the latter are linearly independent as well and form a basis of the vector space of symmetric polynomials with rational coefficients. □

3.4.2 Transition from e_k and h_k to p_k

For convenience in writing formulas, we associate with every Young diagram λ an *infinite* sequence of nonincreasing nonnegative integers $(\lambda_1, \lambda_2, \dots)$ that continues the sequence of actual row lengths to the right with zeros. For each $i \in \mathbb{N}$, we write $m_i = m_i(\lambda)$ for the number of rows of length i in λ. Recall that the *length* $\ell(\lambda)$ means the total number of nonzero elements in λ, and the *weight* $|\lambda| = \sum_i \lambda_i$ means the total number of cells in the corresponding Young diagram. We denote by $\varepsilon_\lambda = \pm 1$ the sign of the permutation of cyclic type[8] λ. Recall that the parity of such a permutation coincides with the parity of sums

$$\sum_{k\geqslant 1}(k-1)m_k \equiv |\lambda| + \sum_{k\geqslant 1} m_k \equiv \sum_{i=1}^{\ell(\lambda)}(\lambda_i - 1) \pmod 2.$$

[8] See Sect. 12.2.3 of Algebra I.

We write $z_\lambda \stackrel{\text{def}}{=} \prod_k (m_k! \cdot k^{m_k})$ for the total number of permutations commuting with a fixed permutation[9] of cyclic type λ. Thus, the total number of permutations of cyclic type λ is equal to $n!/z_\lambda$, where $n = |\lambda|$. Finally, we put

$$p_\lambda \stackrel{\text{def}}{=} p_{\lambda_1} p_{\lambda_2} p_{\lambda_3} \cdots = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots$$

and call these polynomials *Newton symmetric polynomials* as well. Note that the set of polynomials p_λ indexed by Young diagrams of length at most n coincides with the set of all monomials $p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$. Each polynomial p_λ is an eigenvector of the involution ω with eigenvalue ε_λ:

$$\omega(p_\lambda) = \varepsilon_\lambda \cdot p_\lambda. \tag{3.16}$$

Proposition 3.5 *The elementary and complete symmetric polynomials e_k, h_k are expanded as rational linear combinations of monomials p_λ by the formulas*

$$h_k = \sum_{|\lambda|=k} z_\lambda^{-1} p_\lambda, \tag{3.17}$$

$$e_k = \sum_{|\lambda|=k} \varepsilon_\lambda z_\lambda^{-1} p_\lambda, \tag{3.18}$$

where both summations run over all Young diagrams consisting of k cells.

Proof Formulas (3.17) and (3.18) are transferred one to the other by the involution ω. Thus, it is enough to prove only the first of them. Recall that

$$P(t) = \sum_{k \geqslant 1} p_k(x) \cdot t^{k-1} = \frac{d}{dt} \log H(t).$$

Therefore,

$$H(t) = e^{\int P(t)\,dt} = e^{\sum_{i \geqslant 1} p_i t^i / i} = \prod_{i \geqslant 1} e^{p_i t^i / i} = \prod_{i \geqslant 1} \sum_{m \geqslant 0} \frac{p_i^m}{i^m m!} t^{im}.$$

If we choose the m_ith summand within the ith factor in order to multiply the chosen terms together, then the monomial t^k appears if and only if $\sum_i i \cdot m_i = k$. Such sequences (m_i) are in bijection with the Young diagrams λ of weight k with m_i rows of length i for all $1 \leqslant i \leqslant k$. The product of summands corresponding to the Young diagram λ contributes p_λ / z_λ to the coefficient of t^k. □

[9] That is, the cardinality of the stabilizer of the permutation of cyclic type λ under the adjoint action of the symmetric group; see Example 12.16 of Algebra I.

Example 3.1 For $k = 3$, we get the expression $e_3 = p_3 - \frac{1}{2}p_1p_2 + \frac{1}{6}p_1^3$, which agrees with the multinomial formula

$$(x_1 + \cdots + x_n)^3 = \sum x_i^3 + 3\sum_{i\neq j} x_ix_j^2 + 6\sum_{i<j<k} x_ix_jx_k.$$

3.5 Giambelli's Formula

Giambelli's formula expresses the determinantal Schur polynomials s_λ from Proposition 3.1 on p. 59 in terms of the complete symmetric polynomials h_k. Write $e_k^{(p)}$ for the polynomial in $x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_n$ obtained from the elementary symmetric polynomial $e_k(x_1, x_2, \dots, x_n)$ by the substitution $x_p = 0$. We also put $e_k^{(p)} = 0$ for all $k > n-1$. For a fixed p, the generating function of the sequence of polynomials $e_k^{(p)}$, $k \geqslant 0$, is $E^{(p)}(t) = \sum_k e_k^{(p)}(x) \cdot t^k = \prod_{i\neq p}(1 + x_it)$. Therefore, $H(t)E^{(p)}(-t) = (1-x_pt)^{-1}$. Comparison of the coefficients of t^k on both sides leads to the relation $h_0 \cdot (-1)^k e_k^{(p)} + h_1 \cdot (-1)^{k-1}e_{k-1}^{(p)} + \cdots + h_k \cdot e_0^{(p)} = x_p^k$. Under our convention that $e_j^{(p)} = 0$ for all $j > n-1$, it can be written as

$$\begin{aligned} x_p^k &= h_{k-n+1} \cdot (-1)^{n-1}e_{n-1}^{(p)} + h_{k-n+2} \cdot (-1)^{n-2}e_{n-2}^{(p)} + \cdots + h_k \cdot e_0^{(p)} \\ &= \sum_{j=1}^{n} h_{k-n+j} \cdot (-1)^{n-j} e_j^{(p)}. \end{aligned} \tag{3.19}$$

Let us think of the right-hand side as the product of the row matrix of width n,

$$(h_{k-n+1},\ h_{k-n+2},\ \dots,\ h_k)\,, \tag{3.20}$$

and the column matrix of height n transposed to the row

$$\left((-1)^{n-1}e_{n-1}^{(p)},\ \dots,\ e_2^{(p)}, -e_1^{(p)},\ 1\right). \tag{3.21}$$

Fix an increasing sequence $\nu_1 > \nu_2 > \cdots > \nu_n$ of values for k and write the corresponding rows (3.20) as the $n \times n$ matrix

$$H_\nu = \left(h_{\nu_i-n+j}\right) = \begin{pmatrix} h_{\nu_1-n+1} & h_{\nu_1-n+2} & \cdots & h_{\nu_1} \\ h_{\nu_2-n+1} & h_{\nu_2-n+2} & \cdots & h_{\nu_2} \\ \vdots & \vdots & \cdots & \vdots \\ h_{\nu_n-n+1} & h_{\nu_n-n+2} & \cdots & h_{\nu_n} \end{pmatrix},$$

assuming that $h_0 = 1$ and $h_j = 0$ for $j < 0$. Similarly, write the columns (3.21) for $p = 1, 2, \dots, n$ as the $n \times n$ matrix

$$M = \left((-1)^{n-i} e_{n-i}^{(j)}\right) = \begin{pmatrix} (-1)^{n-1} e_{n-1}^{(1)} & (-1)^{n-1} e_{n-1}^{(2)} & \cdots & (-1)^{n-1} e_{n-1}^{(n)} \\ (-1)^{n-2} e_{n-2}^{(1)} & (-1)^{n-2} e_{n-2}^{(2)} & \cdots & (-1)^{n-2} e_{n-2}^{(n)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Formula (3.19) implies the matrix equality $D_\nu = H_\nu \cdot M$, where

$$D_\nu = (x_j^{\nu_i}) = \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix}$$

is the same matrix as in formula (3.5) on p. 59. Therefore,

$$\Delta_\nu = \det D_\nu = \det H_\nu \cdot \det M$$

for every Young diagram ν of length n with strictly decreasing lengths of rows. For $\nu = \delta = (n-1, \dots, 1, 0)$, the matrix H_δ becomes upper unitriangular, with $\det H_\delta = 1$. Hence, $\det M = \det D_\delta = \Delta_\delta$. This leads to the required expression for the Schur polynomials:

$$s_\lambda = \Delta_{\delta+\lambda} / \Delta_\delta = \det D_{\delta+\lambda} / \det M = \det H_{\delta+\lambda} = \det\left(h_{\lambda_i + j - i}\right). \tag{3.22}$$

In expanded form, this formula appears as follows:

$$s_\lambda = \det \begin{pmatrix} h_{\lambda_1} & h_{\lambda_1+1} & \ddots & h_{\lambda_1+n-1} \\ h_{\lambda_2-1} & h_{\lambda_2} & \ddots & \ddots \\ \ddots & \ddots & \ddots & h_{\lambda_{n-1}+1} \\ h_{\lambda_n-n+1} & \ddots & h_{\lambda_n-1} & h_{\lambda_n} \end{pmatrix}, \tag{3.23}$$

where $h_{\lambda_1}, h_{\lambda_2}, \dots, h_{\lambda_n}$ are on the main diagonal, and the indices of h are incremented sequentially by 1 from left to right in every row. Formula (3.23) is known as the *first Giambelli formula*. The second Giambelli formula expresses the Schur polynomials in terms of the elementary symmetric functions e_λ. However, we postpone its deduction until we know how the involution ω acts on the Schur polynomials.[10]

[10] See Corollary 4.3 on p. 94.

Example 3.2 For $n = 2$, the Giambelli formula gives the following expression for $s_{(2,1)}$ in $\mathbb{Z}[x_1, x_2]$:

$$s_{(2,1)} = \det \begin{pmatrix} h_2 & h_3 \\ 1 & h_1 \end{pmatrix} = h_1 h_2 - h_3 = e_1 e_2 - e_3 .$$

For $n = 3$, the expression of $s_{(2,1)}$ in $\mathbb{Z}[x_1, x_2, x_3]$ is given by the formula

$$s_{(2,1)} = s_{(2,1,0)} = \det \begin{pmatrix} h_2 & h_3 & h_4 \\ 1 & h_1 & h_2 \\ 0 & 0 & 1 \end{pmatrix} = \det \begin{pmatrix} h_2 & h_3 \\ 1 & h_1 \end{pmatrix},$$

which leads to the same result $s_{(2,1)} = h_1 h_2 - h_3$ as for $n = 2$.

Exercise 3.4 Convince yourself that the expansion of s_λ as a polynomial in h_k obtained for[11] $n = \ell(\lambda)$ remains unchanged for all $n > \ell(\lambda)$.

For the diagram $\lambda = (k)$, which consists of one row of length k, we get the equality $s_{(k)} = h_k$. It is obvious for $n = 1$ and holds for all n by Exercise 3.4. Can you deduce the identity $\Delta_{\delta+(n)} = h_k \cdot \Delta_\delta$ by the straightforward evaluation of the order-n Vandermonde-type determinant $\Delta_{\delta+(n)}$?

3.6 Pieri's Formula

Pieri's formula expands the product $s_\lambda \cdot h_k = s_\lambda \cdot s_{(k)}$ as a linear combination of polynomials s_μ. It requires a slight generalization of what was said in Sect. 3.1. Consider the ring of formal power series $\mathbb{Z}[\![x_1, x_2, \dots, x_n]\!] \simeq \mathbb{Z}[\![t]\!]^{\otimes n}$ and $\mathbb{Z}$-submodules of the symmetric and alternating power series[12] within this ring. Collecting the monomials sharing the same S_n-orbit allows us to expand every alternating power series $A \in \mathbb{Z}[\![x_1, x_2, \dots, x_n]\!]$ as

$$A = \sum_{\nu_1 > \nu_2 > \cdots > \nu_n} c_\nu \cdot \Delta_\nu , \tag{3.24}$$

where all the coefficients c_ν are integers, the summation is over all length-n Young diagrams $\nu = (\nu_1, \nu_2, \dots, \nu_n)$ with strictly decreasing lengths of rows, and the determinantal polynomials

$$\Delta_\nu = \sum_{g \in S_n} \operatorname{sgn}(g)\, x_{g(1)}^{\nu_1} x_{g(2)}^{\nu_2} \cdots x_{g(n)}^{\nu_n}$$

[11] Recall that we write $\ell(\lambda)$ for the number of rows in a Young diagram λ and call it the *length* of λ.

[12] The first form a ring, and the second form a module over this ring.

are exactly the same as in formula (3.5) on p. 59. The expansion (3.24) for the product of the alternating polynomial Δ_ν and the symmetric power series

$$H(x) = \prod_{i=1}^{n}(1-x_i)^{-1} = \prod_{i=1}^{n}\left(1 + x_i + x_i^2 + x_i^3 + \cdots\right) = \sum_{k\geqslant 0} h_k(x),$$

which generates the polynomials h_k, is described in the next lemma.

Lemma 3.1 *We have $\Delta_\nu \cdot H = \sum_\eta \Delta_\eta$, where $\eta = (\eta_1, \eta_2, \dots, \eta_n)$ runs through the Young diagrams of length n with*

$$\eta_1 \geqslant \nu_1 > \eta_2 \geqslant \nu_2 > \cdots > \eta_n \geqslant \nu_n.$$

Proof Given n power series in one variable $f_1(t), f_2(t), \dots, f_n(t) \in \mathbb{Z}[\![t]\!]$, write

$$f_1 \wedge f_2 \wedge \cdots \wedge f_n \overset{\text{def}}{=} \sum_{g\in S_n} \operatorname{sgn}(g)\cdot f_1\left(x_{g(1)}\right) f_2\left(x_{g(2)}\right)\cdots f_n\left(x_{g(n)}\right)$$

for the alternating power series mapped by the isomorphism

$$\mathbb{Z}[\![x_1, x_2, \dots, x_n]\!] \simeq \mathbb{Z}[\![t]\!]^{\otimes n}$$

to the complete polarization of the Grassmannian polynomial

$$n!\cdot f_1 \wedge f_2 \wedge \cdots \wedge f_n \in \Lambda^n \mathbb{Z}[\![t]\!].$$

The series $f_1 \wedge f_2 \wedge \cdots \wedge f_n \in \mathbb{Z}[\![x_1, x_2, \dots, x_n]\!]$ is an n-linear sign-alternating function of $f_1, f_2, \dots, f_n \in \mathbb{Z}[\![t]\!]$. In particular, $f_1 \wedge f_2 \wedge \cdots \wedge f_n$ is not changed under the replacement of any of the f_i by its sum with an arbitrary linear combination of the other f_ν.

Exercise 3.5 Convince yourself that $t^{\nu_1} \wedge t^{\nu_2} \wedge \cdots \wedge t^{\nu_n} = \Delta_\nu$.

Now we can write the product $\Delta_\nu \cdot H$ as

$$\Delta_\nu \cdot H = \sum_{g\in S_n} \operatorname{sgn}(g) \prod_{i=1}^{n} x_{g(i)}^{\nu_i}/(1 - x_{g(i)}) = f_1 \wedge f_2 \wedge \cdots \wedge f_n$$

for $f_i(t) = t^{\nu_i}/(1-t) = t^{\nu_i} + t^{\nu_i+1} + t^{\nu_i+2} + \cdots$. Subtraction of f_1 from all the f_i with $i > 1$ truncates the latter series to the polynomials of degree $\nu_1 - 1$, which we will denote by the same letters f_i. Subtraction of f_2 from all the f_i with $i > 2$ truncates them up to degree $\nu_2 - 1$. Then subtraction of f_3 truncates all f_i with $i > 3$ up to degree $\nu_3 - 1$, etc. Therefore, $\Delta_\nu \cdot H = f_1 \wedge f_2 \wedge \cdots \wedge f_n$, where $f_1 = \sum_{j\geqslant \nu_1} t^j$ and $f_i = t^{\nu_i} + t^{\nu_i+1} + \cdots + t^{\nu_{i-1}-1}$ for $2 \leqslant i \leqslant n$. This product is expanded into the sum of Grassmannian monomials $\sum_\eta t^{\eta_1} \wedge t^{\eta_2} \wedge \cdots \wedge t^{\eta_n} = \sum_\eta \Delta_\eta$, where the summation is over all $\eta_1 \geqslant \nu_1 > \eta_2 \geqslant \nu_2 > \eta_3 \geqslant \nu_3 > \cdots > \eta_n \geqslant \nu_n$. □

Corollary 3.4 (Pieri's Formula) *We have $s_\lambda \cdot h_k = \sum_\mu s_\mu$, where μ runs through the Young diagrams of length at most n obtained from λ by adding k cells in k different columns.*

Proof Let $\nu = \lambda + \delta$, $\eta = \mu + \delta$, where $\delta = (n-1, n-2, \dots, 1, 0)$ and λ, μ are Young diagrams with lengths of rows $\lambda_i = \nu_i - n + i$, $\mu_i = \eta_i - n + i$. In terms of λ, μ, the inequalities $\eta_i \geqslant \nu_i > \eta_{i+1}$ from Lemma 3.1 mean that $\mu_i \geqslant \lambda_i \geqslant \mu_{i+1}$. Thus, the equality of Lemma 3.1 can be written as $\Delta_{\delta+\lambda} \sum_{k \geqslant 0} h_k = \sum_\mu \Delta_{\delta+\mu}$, where the summation is over all Young diagrams μ such that $\mu_1 \geqslant \lambda_1 \geqslant \mu_2 \geqslant \lambda_2 \geqslant \cdots$. Dividing both sides by Δ_δ and looking at the homogeneous component of degree $|\lambda| + k$ in x gives Pieri's formula. □

Remark 3.1 If the diagram λ in Pieri's formula consists of $k < n$ rows, i.e., has $\lambda_m = 0$ for all $m > k$, where $k < n$, then some diagrams μ on the right-hand side have length $k + 1$, i.e., are one row higher than λ. For example, for $n = 2$, we get $s_{(2)} \cdot h_1 = s_{(2,1)} + s_{(3)}$, which gives another demonstration of the equality $s_{(2,1)} = h_2 h_1 - h_3$ from Example 3.2 on p. 67.

3.7 The Ring of Symmetric Functions

Many relations among symmetric polynomials do not depend on the number of variables as soon as the latter is large enough that all the polynomials involved in the relation are defined. For example, the relation $s_{(2,1)} = h_2 h_1 - h_3$ holds in all rings $\mathbb{Z}[x_1, x_2, \dots, x_n]$ with $n \geqslant 2$; the relation $6e_3 = 6p_3 - 3\, p_1 p_2 + p_1^3$ holds for $n \geqslant 3$; and so on. So it would be convenient to consider symmetric polynomials $m_\lambda(x)$, $s_\lambda(x)$, $e_\lambda(x)$, $h_\lambda(x)$, and $p_\lambda(x)$ without fixing the precise number of variables but assuming instead simply that this number is sufficiently large. This is formalized as follows. For all pairs of nonnegative integers $r > s$, write

$$\begin{aligned} \zeta_{sr} : \mathbb{Z}[x_1, x_2, \dots, x_r] &\twoheadrightarrow \mathbb{Z}[x_1, x_2, \dots, x_s], \\ f(x_1, x_2, \dots, x_r) &\mapsto f(x_1, x_2, \dots, x_s, 0, \dots, 0), \end{aligned} \tag{3.25}$$

for a surjective ring homomorphism[13] assigned by the substitution

$$x_{s+1} = x_{s+2} = \cdots = x_r = 0. \tag{3.26}$$

This substitution clearly preserves the symmetry and alternating properties of polynomials. Moreover, it takes the polynomials $m_\lambda(x)$, $s_\lambda(x)$, $e_\lambda(x)$, $h_\lambda(x)$, and $p_\lambda(x)$ either to zero or to the polynomial with exactly the same name.

[13]For $n = 0$, we put $\mathbb{Z}[x_1, x_2, \dots, x_n]$ equal to $\mathbb{Z}$.

A sequence of polynomials $f^{(n)} = f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, $n \geqslant 0$, $f^{(0)} \in \mathbb{Z}$, is called a *symmetric function* of degree d if for every n, the polynomial $f^{(n)} = f(x_1, x_2, \ldots, x_n)$ is symmetric and homogeneous of degree d, and

$$\zeta_{rs}\left(f^{(r)}\right) = f^{(s)}$$

for all $r > s$. We denote such a symmetric polynomial simply by f. When the number of variables on which f depends is specialized to some explicit value $n \in \mathbb{N}$, we will write either $f(x_1, x_2, \ldots, x_n)$ or $f^{(n)}$. Note that every $f^{(n)}$ uniquely determines all $f^{(k)}$ with $k < n$.

Fix a Young diagram λ of weight $|\lambda| = d$. The sequence of monomial symmetric polynomials $m_\lambda(x_1, x_2, \ldots, x_n)$, $n \geqslant 0$, is a symmetric function of degree d, denoted by m_λ. It has $m_\lambda^{(k)} = 0$ for $k < \ell(\lambda)$ and becomes nonzero starting from $m_\lambda(x_1, x_2, \ldots, x_{\ell(\lambda)})$. For example, $m_{(2,1)}$ has $m_\lambda^{(0)} = m_{(2,1)}(x_1) = 0$, and then

$$\begin{aligned} m_{(2,1)}(x_1, x_2) &= x_1^2 x_2 + x_1 x_2^2, \\ m_{(2,1)}(x_1, x_2, x_3) &= x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2, \\ &\cdots \end{aligned}$$

The other symmetric functions we met before, s_λ, e_λ, h_λ, and p_λ, are defined similarly. Note that $m_\lambda^{(k)} = s_\lambda^{(k)} = 0$ for all $k < \ell(\lambda)$, and $e_\lambda^{(k)} = 0$ for all $k < \ell(\lambda^t)$. Concerning these functions, we always follow the notation from Sect. 3.4.2 on p. 63, i.e., for a sequence q_i of symmetric functions $q_i = \left(q_i^{(n)}\right)$ numbered by positive integers $i \in \mathbb{N}$, we write

$$q_\lambda = q_{\lambda_1} q_{\lambda_2} q_{\lambda_3} \cdots = q_1^{m_1} q_2^{m_2} q_1^{m_3} \cdots = q^m$$

for the monomials constructed from the q_i and arranged either in nonincreasing order of i or in the standard collected form. The first are naturally numbered by the Young diagrams λ, thought of as infinite nonincreasing sequences λ_k such that $\lambda_k = 0$ for $k \gg 0$. The second are numbered by the sequences $m = (m_k)_{k \in \mathbb{N}}$ of nonnegative integers m_k with a finite number of nonzero elements. Each of the two presentations of a monomial uniquely determines the other: $m_k = m_k(\lambda)$ is the number of rows of length k in λ.

The symmetric functions of degree d form a free $\mathbb{Z}$-module, traditionally denoted by Λ_d. It should not be confused with the exterior power notation Λ^d. The four bases of Λ_d over $\mathbb{Z}$ are formed by the four systems of symmetric functions m_λ, s_λ, e_λ, h_λ, each numbered by all Young diagrams of weight $|\lambda| = d$, because those polynomials $m_\lambda^{(n)}$, $s_\lambda^{(n)}$, $e_\lambda^{(n)}$, $h_\lambda^{(n)}$ that are nonzero form a basis in $\Lambda_k \cap \mathbb{Z}[x_1, x_2, \ldots, x_n]$ for every n. For the same reason, the Newton symmetric functions p_λ form a basis over $\mathbb{Q}$ for the vector space $\mathbb{Q} \otimes \Lambda_d$ of symmetric functions with rational coefficients. Therefore, $\mathrm{rk}_\mathbb{Z} \Lambda_d = \dim_\mathbb{Q} \mathbb{Q} \otimes \Lambda_d$ is equal to the total number of Young diagrams of weight d. This number is denoted by $p(d)$ and called the *partition number* of $d \in \mathbb{N}$.

The product of two symmetric functions f_1, f_2 of degrees d_1, d_2 is the symmetric function $f_1 f_2$ formed by the series of symmetric polynomials $f_1^{(n)} f_2^{(n)}$ of degree $d_1 + d_2$. Therefore, the direct sum of $\mathbb{Z}$-modules

$$\Lambda \stackrel{\text{def}}{=} \bigoplus_{d \geqslant 0} \Lambda_d$$

is a graded commutative ring. It is called the *ring of symmetric functions*. All the polynomial relations among m_λ, s_λ, e_λ, h_λ proved above are valid in the ring of symmetric functions Λ, and moreover, the relations involving p_λ are true in the ring $\mathbb{Q} \otimes \Lambda$ of symmetric functions with rational coefficients.

Problems for Independent Solution to Chapter 3

Problem 3.1 The sum of the two complex roots of the polynomial

$$2\,x^3 - x^2 - 7\,x + \lambda$$

equals 1. Find λ.

Problem 3.2 Find all complex solutions of the system of polynomial equations

$$x_1 + x_2 + x_3 = x_1^2 + x_2^2 + x_3^2 = 0, \quad x_1^3 + x_2^3 + x_3^3 = 24.$$

Problem 3.3 Express the following symmetric functions as polynomials in the elementary symmetric functions e_i:

(a) $(x_1 + x_2)(x_2 + x_3)(x_3 + x_4)(x_1 + x_3)(x_2 + x_4)(x_1 + x_4)$,
(b) $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$,
(c) $\sum_{i \neq j} x_i^2 x_j$, **(d)** $\sum_{i \neq j \neq k \neq i} x_i(x_j + x_k)$.

Problem 3.4 (Discriminant) Let $f(x) = \prod(x - x_i)$ be a monic polynomial of degree n in the variable x with coefficients in the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$. The product

$$D_f = \Delta_\delta^2(x_1, x_2, \ldots, x_n) = \prod_{i<j}(x_i - x_j)^2$$

written as a polynomial in the coefficients $a_1, a_2, \ldots, a_n$ of the polynomial f is called the *discriminant* of f and denoted by $D(f)$. Show that $D(f)$ actually admits a unique expression as a polynomial in the coefficients of f, and write this expression for the trinomials **(a)** $f(x) = x^2 + px + q$, **(b)** $f(x) = x^3 + px + q$.

Problem 3.5 For a cubic trinomial $f(x) = x^3 + px + q \in \mathbb{R}[x]$, check that for $D_f < 0$, f has exactly one real root, and it is simple, whereas for $D_f > 0$, there are three distinct real roots. Show that in the latter case, the equation $f(x) = 0$ can be transformed by an appropriate substitution $x = \lambda t$, $\lambda \in \mathbb{R}$, into the form $4t^3 - 3t = a$ with $a \in \mathbb{R}$, $|a| \leqslant 1$, and solve the resulting equation in trigonometric functions of a.

Problem 3.6 Find all $\lambda \in \mathbb{C}$ such that the polynomial $x^4 - 4x + \lambda$ has a multiple root.

Problem 3.7 (Circulant) All the rows of a matrix $A \in \mathrm{Mat}_n(\mathbb{C})$ are the sequential cyclic permutations of the first row $(a_0, a_1, \dots, a_n) \in \mathbb{C}^n$ in the rightward direction. For example, for $n = 4$, this means that

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}.$$

Express $\det A$ in terms of the values of the polynomial

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

in the complex roots of unity of degree n .

Problem 3.8* Evaluate the discriminant of the nth cyclotomic polynomial[14] $\Phi_n(x)$. To begin with, consider $n = 3, 4, 5, 6, 7$.

Problem 3.9 Let $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ be a monic polynomial with roots $x_1, x_2, \dots, x_n$. Prove that every symmetric polynomial in $x_2, \dots, x_n$ can be expressed as a polynomial in x_1 and the coefficients $a_1, a_2, \dots, a_n$ of f.

Problem 3.10 Let $\zeta \in \mathbb{C}$ be a primitive mth root of unity. For $a \in \mathbb{C}$, multiply $\prod_{\nu=1}^{m}(a - \zeta^{\nu-1}x)$ out and collect like monomials. Show that for every $f \in \mathbb{C}[x]$, there exists $h \in \mathbb{C}[x]$ such that $\prod_{\nu=1}^{m} f(\zeta^{\nu-1}x) = h(x^m)$. Express the roots of h in terms of the roots of f.

Problem 3.11 Find the fourth-degree polynomial in $\mathbb{C}[x]$ whose roots are

(a) the squares of all roots of the polynomial $x^4 + 2x^3 - x + 3$,
(b) the cubes of all roots of the polynomial $x^4 - x - 1$.

[14]Recall that the *nth cyclotomic polynomial* $\Phi_n(x) = \prod(x - \zeta)$ is the monic polynomial of degree $\varphi(n)$ whose roots are the primitive nth roots of unity $\zeta \in \mathbb{C}$. (See Sect. 3.5.4 of Algebra I.)

Problem 3.12 Express $s_{(1^n)}$, where (1^n) means one column of n cells, as a polynomial in e_ν.

Problem 3.13 Express $s_{(n)}$, where (n) means one row of n cells, as a polynomial in h_ν.

Problem 3.14 Express the products $s_{(1)}^2$ and $s_{(1,1)} \cdot s_{(2)}$ as integer linear combinations of polynomials s_λ.

Problem 3.15 Let us set $h_0 = e_0 = 1$ and $h_k = e_k = 0$ for $k < 0$. Show that the matrices $\big(h_{i-j}\big)$ and $\big((-1)^{i-j} e_{i-j}\big)$ are inverse to each other, and deduce from this the relation $\det\big(h_{\lambda_i+j-i}\big) = \det\big(e_{\lambda_i^t+j-i}\big)$ in the complementary minors of these matrices.

Problem 3.16 Use Cramer's rule[15] and the recurrence formulas (3.10), (3.11) on p. 61 and (3.13), (3.14) on p. 63 to prove the equalities:

(a) $e_n = \det\big(h_{j-i+1}\big)$, $h_n = \det\big(e_{j-i+1}\big)$, where $1 \leqslant i, j \leqslant n$,

(b) $p_n = \det \begin{pmatrix} e_1 & 1 & 0 & \cdots & 0 \\ 2e_2 & e_1 & 1 & \ddots & \vdots \\ 3e_3 & e_2 & e_1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ ne_n & e_{n-1} & e_{n-2} & \cdots & e_1 \end{pmatrix}$, **(c)** $n!e_n = \det \begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \ddots & \vdots \\ p_3 & p_2 & p_1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & n-1 \\ p_n & p_{n-1} & p_{n-2} & \cdots & p_1 \end{pmatrix}$.

Problem 3.17 (The Second Giambelli Formula) Prove that

$$s_{\lambda^t} = \det \begin{pmatrix} e_{\lambda_1} & e_{\lambda_1+1} & \dots & e_{\lambda_1+n-1} \\ e_{\lambda_2-1} & e_{\lambda_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & e_{\lambda_{n-1}+1} \\ e_{\lambda_n-n+1} & \dots & e_{\lambda_n-1} & e_{\lambda_n} \end{pmatrix},$$

where the main diagonal is filled by $e_{\lambda_1}, e_{\lambda_2}, \dots, e_{\lambda_n}$ and the indices of e are incremented sequentially by 1 from left to right in each row.

[15] See Proposition 9.4 from Algebra I.

Chapter 4
Calculus of Arrays, Tableaux, and Diagrams

4.1 Arrays

4.1.1 Notation and Terminology

Fix two finite sets $I = \{1, 2, \dots, n\}$, $J = \{1, 2, \dots, m\}$ and consider a rectangular table with n columns and m rows numbered by the elements of I and J respectively in such a way that indices I increase horizontally from left to right, and indices j increase vertically from bottom to top. A collection of nonnegative integers $a(i,j)$ placed in the cells of such a table is called an *$I \times J$ array*, which we shall denote by a. We write $\mathcal{A} = \mathcal{A}_{IJ}$ for the set of all $I \times J$ arrays. The numbers $a_{i,j}$ should be thought of as numbers of small identical balls placed in the cells of the table. We will not use them in any computations similar to those made with matrix elements. Instead, we will deal with maps $\mathcal{A} \to \mathcal{A}$ acting on the arrays by moving balls among cells. In most applications, the balls will be equipped with pairs of properties numbered by the elements of the sets I, J. A collection of such balls is naturally organized in the array in accordance with the properties of the balls forming the collection. From this viewpoint, the operations acting on $\mathcal{A}$ are interpreted as changing some properties of some balls. The distribution of the balls between the properties provided by a given array a is coarsely described by two integer vectors,

$$w_I = (c_1, c_2, \dots, c_n) \in \mathbb{Z}^n_{\geqslant 0} \quad \text{with} \quad c_i = \sum_j a(i,j), \tag{4.1}$$

$$w_J = (r_1, r_2, \dots, r_m) \in \mathbb{Z}^m_{\geqslant 0} \quad \text{with} \quad r_j = \sum_i a(i,j), \tag{4.2}$$

called the *column weight* (or *I-weight*) and *row weight* (or *J-weight*) of a. The coordinates of these vectors are equal to the total numbers of balls in the columns and rows of a respectively.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_4

We consider four collections of maps $\mathcal{A} \to \mathcal{A}$ denoted by D_j, U_j with

$$1 \leqslant j \leqslant m - 1$$

and L_i, R_i with $1 \leqslant i \leqslant n - 1$. Applied to a given array $a \in \mathcal{A}$, such a map either leaves a fixed or moves exactly one ball of a to a neighboring cell in the down, up, left, or right direction in accordance with the notation of the operation. Operations D_j, U_j, which move balls within columns, are called *vertical*. Operations L_i, R_i are called *horizontal*.

4.1.2 Vertical Operations

For an array $a \in \mathcal{A}$ and fixed j in the range $1 \leqslant j \leqslant m - 1$, the operation D_j either does nothing with a or moves exactly one ball from the $(j + 1)$th row down to the jth row. To detect this ball or its absence, we should separate the balls of both rows into *free* and *coupled* balls by means of the following procedure. At the outset, all the balls of the jth row are considered free. We then look through the balls β of the $(j + 1)$th row going from left to right. If there is a free ball lying in the jth row at a column strictly to the left of β, then β is declared to be coupled with the rightmost such ball γ, which also changes its status from free to coupled. If there are no free balls strictly to the left of β in the jth row, the ball β is declared to be free. When all the balls β in the $(j + 1)$th row have been exhausted, all the remaining free balls of the jth row are said to be free. The resulting matching of the coupled balls is called a *stable matching* between the jth and $(j + 1)$th rows. Here is an example of stable matching (included in parentheses are the numbers of remaining free balls):

$$\begin{array}{ccccc} 2\,(2) & 2\,(0) & 4\,(1) & 3\,(0) & 3\,(0) \\ \\ 3\,(0) & 2\,(0) & 6\,(1) & 1\,(0) & 3\,(3). \end{array} \tag{4.3}$$

Note that for every stable matching, the rightmost free balls of the $(j + 1)$th row lie either strictly to the left or in the same column where the leftmost free balls of the jth row lie.

By definition, the operation D_j moves one of the rightmost free balls of the $(j + 1)$th row downward, or else does nothing if the $(j + 1)$th row has no free balls. Conversely, the operation U_j moves one of the leftmost free balls of the jth row upward, or does nothing if there are no free balls in the jth row. Note that all the vertical operations preserve the column weight w_I.

When an operation actually moves some ball in a, we say that this operation acts on *a effectively*. If D_j acts effectively on a, then the ball lowered by D_j becomes one of the leftmost free balls in the jth row of array $D_j a$. Therefore, $U_j D_j = a$ in this case. For the same reason, $D_jU_ja = a$ as soon as $U_ja \neq a$. We see that the set of vertical operations $U_j, D_j : \mathcal{A} \to \mathcal{A}$ possesses some properties of a transformation group. For example, if $b = D_{j_k} \cdots D_{j_2}D_{j_1}a$, where every D_ν acts effectively, then a is uniquely recovered from b as $a = U_{j_1}U_{j_2} \cdots U_{j_k}b$, and each U_ν in this chain acts effectively. In this situation, we say that the word $D_{j_k} \cdots D_{j_2}D_{j_1}$ is an *effective word*[1] of a.

4.1.3 Commutation Lemma

The horizontal operations L_i, R_i are defined in a completely symmetric way. Namely, write a^t for the array obtained from a by the reflection swapping I with J. The array a^t has $a^t(i,j) = a(j,i)$ and is called the *transpose* of a. We put

$$L_i(a) \stackrel{\text{def}}{=} \big(D_i(a^t)\big)^t \quad \text{and} \quad R_i(a) = \big(U_i(a^t)\big)^t .$$

Exercise 4.1 Give a direct explicit description of the horizontal operations, that is, explain how a stable matching between the ith and $(i+1)$th columns should be established, and what balls are moved by the operations R_i and L_i.

All the horizontal operations clearly preserve the row weight w_J.

Lemma 4.1 *Every horizontal operation preserves stable matchings between rows, meaning that all free balls remain free and all coupled pairs of balls remain coupled in the same pairs after the operation is applied. Similarly, every vertical operation preserves stable matchings between columns.*

Proof Let us fix a stable matching between the $(j+1)$th and jth rows in an array a, and verify that all operations L_i preserve this matching. It is clear when L_i does nothing with a. Let L_i move a ball β. If β lies neither in the $(j+1)$th nor in the jth row, then again there is nothing to prove.

Let β lie in the $(j+1)$th row, that is, in the cell $(i+1, j+1)$, as shown in Fig. 4.1. Then all balls in the cell (i,j) are coupled with some balls in the cell $(i+1, j+1)$, because otherwise, the ball β would be coupled with some free ball in the cell (i,j) under the stable matching between the ith and $(i+1)$th columns, and therefore could not be moved by L_i. Hence, if β is coupled with a ball γ in the row matching, then γ lies in a cell that is strictly to the left of (i,j). So β and γ remain coupled after β is moved to the cell $(i, j+1)$. If β is free, it certainly remains free after this movement. Thus, L_i has no effect on the row matching in this case.

Now let β lie in the jth row, that is, in the cell $(i+1, j)$, as shown in Fig. 4.2. Since β is among the topmost free balls of the column matching, all balls in the cell $(i+1, j+1)$ are coupled with some balls in the cell (i,j) in the column matching.

[1] Or just an *effective word* if a is clear from the context or inessential to the discussion.

Fig. 4.1 L_i acts on the $(j+1)$th row

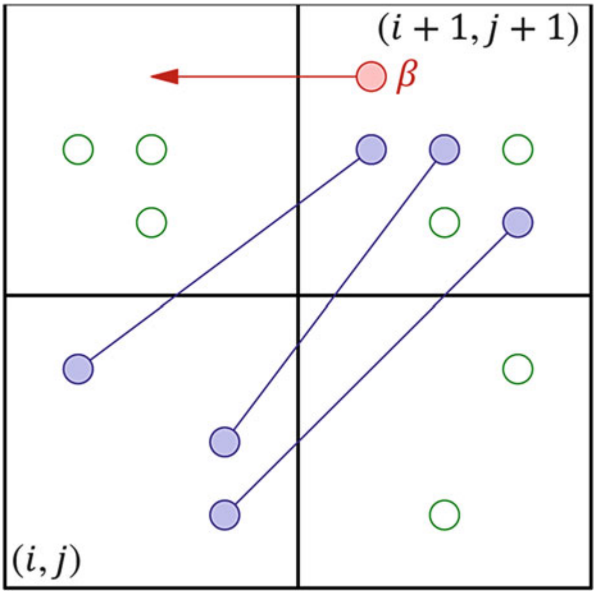
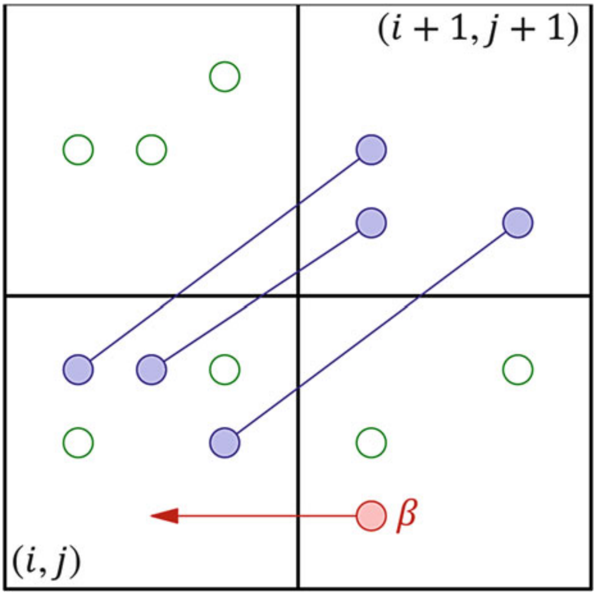


Fig. 4.2 L_i acts on the jth row



Therefore, in the row matching, all balls in the cell $(i+1, j+1)$ are coupled with some balls in the cell (i, j) as well. Hence, the ball β does not change its status under the movement into the left neighboring cell in this case as well.

Exercise 4.2 Use similar arguments to prove that all operations R_i also preserve the stable matching between the $(j+1)$th and jth rows.

The second statement of the lemma follows from the first by means of the transposition of a. □

Corollary 4.1 *Every horizontal operation L_i, R_i commutes with every vertical operation D_j, U_j.*

Proof Let us show, for example, that $D_jL_i = L_iD_j$ (all other cases are completely similar). Given an array a, it follows from Lemma 4.1 that the operation L_i either leaves both arrays a, D_ja unchanged or moves the same ball in a and in D_ja to the left. Similarly, the operation D_j either leaves both arrays a, L_ia unchanged or moves the same ball down in a and in L_ia. In all cases, the equality $D_jL_ia = L_iD_ja$ holds.[2] □

Corollary 4.2 *Let H be a word built from horizontal operations L_i, R_i. Then H acts effectively on an array a if and only if H acts effectively on all arrays obtained from a by means of vertical operations. Similarly, a word V built from vertical operations acts effectively on a if and only if V acts effectively on all arrays obtained from a by means of horizontal operations.*

Proof The second statement is obtained from the first by means of transposition. To verify the first, it is enough to check that for every array a and all i, j, the operation L_i acts effectively on a if and only if it acts effectively on D_ja and U_ja. This holds, because neither D_j nor U_j changes the stable matching between the $(i-1)$th and ith rows, by Lemma 4.1. □

4.2 Condensing

4.2.1 Condensed Arrays

An array a is called *D-dense*[3] if $D_ja = a$ for all j. The *U-dense*, *L-dense*, and *R-dense* arrays are defined similarly. Every array a can be condensed in any prescribed direction D, U, L, R by applying the respective operations D, U, L, R sufficiently many times. Usually, such a condensation of an array a can be realized in many different ways. For example, shown in Fig. 4.3 are two downward condensations of a random 3×2 array. Note that the both condensing words $D_2D_1^4D_2^3$ and $D_1^3D_2D_1$ lead to the same D-dense result:

[2]Note that if $i = j$ and both L_i, D_i act effectively, then L_iD_i and D_iL_i move one ball from the (i, i) cell to the $(i-1, i-1)$ cell in two different ways.

[3]Or *dense downward*.

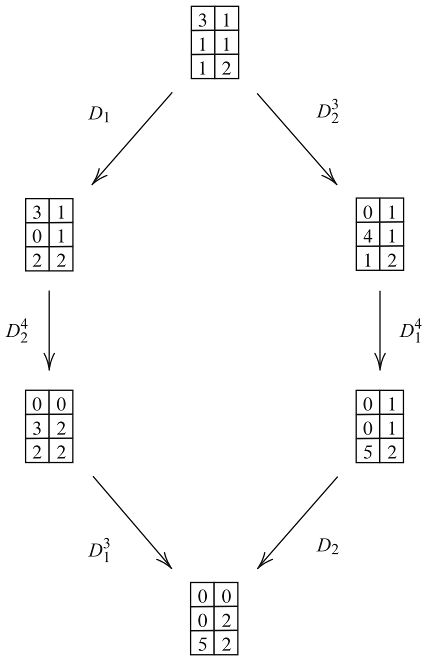


Fig. 4.3 Two downward condensations lead to the same result

We will prove this key property of condensing in Proposition 4.1 below, and now let us discuss an interaction between dense arrays and Young diagrams.

4.2.2 Bidense Arrays and Young Diagrams

Corollary 4.2 implies that both L- and R-density are preserved by the vertical operations. Similarly, the horizontal operations preserve D- and U-density. Therefore, every array can be made dense in two perpendicular directions simultaneously. We call such arrays *DL-dense*, *DR-dense*, etc. In what follows, we deal mostly with DL-dense arrays and call them *bidense*. All balls in a bidense array b are situated within cells of the main diagonal $i = j$, and the numbers of balls $b(i,i)$ decrease nonstrictly as i grows. Thus, the I- and J-weights of b coincide and form a Young diagram $\lambda = w_I(b) = w_J(b)$. We conclude that the bidense arrays are in bijection with the Young diagrams.[4] We write $\lambda(a)$ for the Young diagram corresponding to the bidense array obtained from an array a by means of DL-condensing, and call this Young diagram the *shape* of a.

[4]We follow Sect. 3.4.2 on p. 63 and think of a Young diagram as an infinite sequence of nonincreasing nonnegative integers tending to zero.

Proposition 4.1 *For every array a, the result of downward condensation of a does not depend on the choice of condensing word. The same holds for left, right, and upward condensing as well.*

Proof If a is L-dense, then every D-condensing of a preserves the column weight $w_I(a)$ and therefore leads to the bidense array corresponding to the Young diagram $\lambda = w_I(a)$. For an arbitrary array a, let $L = L_{i_1} L_{i_2} \ldots L_{i_k}$ be an effective word for a such that $a' = La$ is L-dense, and let $D = D_{j_1} D_{j_2} \ldots D_{j_k}$ be any word such that Da is D-dense. Since the action of L preserves D-density and the action of D preserves L-density, the array $LDa = DLa$ is bidense. As we have just seen, the downward condensation DLa of an L-dense array La does not depend on the choice of D. By Corollary 4.2, the action of L on Da is effective. Hence $Da = L^{-1}LDa = L^{-1}DLa$ does not depend on the choice of D. The left, right, and upward condensations are handled similarly. □

4.2.3 Young Tableaux

Let a be an arrow of height m and width n. Then the *line scanning* of a is the text consisting of m words over the alphabet $\{1, 2, \ldots, n\}$ written by the following rule. Interpret every ball of a as the letter of I marking the column in which the ball is placed; read the rows of a from left to right, row by row, from the bottom up; and record the words read in the column top down, aligning to the left. Thus, the bottom row of a gives the upper word of the column, the second row of a gives the next word, etc. For example,

$$\begin{array}{|c|c|c|c|c|}\hline 0&0&0&0&1\\\hline 0&0&1&1&0\\\hline 0&4&0&0&0\\\hline 3&1&0&0&1\\\hline\end{array} \rightsquigarrow \begin{array}{lllll} 1&1&1&2&5\\ 2&2&2&2&\\ 3&4&&&\\ 5&&&& \end{array}, \qquad \begin{array}{|c|c|c|c|c|}\hline 2&0&3&0&1\\\hline 0&2&1&1&0\\\hline 0&1&0&2&3\\\hline 1&1&2&0&1\\\hline\end{array} \rightsquigarrow \begin{array}{llllll} 1&2&3&3&5&\\ 2&4&4&5&5&5\\ 2&2&3&4&&\\ 1&1&3&3&3&5 \end{array}.$$

For every $j \in J$, the jth row of a is swept to the word

$$\underbrace{11\ldots1}_{a(1,j)}\underbrace{22\ldots2}_{a(2,j)}\ldots\ldots\ldots\underbrace{nn\ldots n}_{a(n,j)},$$

where the letters increase nonstrictly from left to right. The D-density of an array a means that every letter "i" of the jth row has a matching letter, which is strictly less than "i" and remains in the $(j-1)$th row, as happens in the lefthand example above. We conclude that a is D-dense if and only if the line scanning of a is a Young diagram filled by the numbers $1, 2, \ldots, n$ in such a way that they increase nonstrictly from left to right along the rows and increase strictly from top to bottom along the columns. Such a filled Young diagram λ is called a *Young tableau* of shape λ in the alphabet $I = \{1, 2, \ldots, n\}$. Note that an element of the alphabet may appear in a Young tableau several times or may not appear at all. To outline this circumstance, we say that this is a *semistandard* Young tableau. The name *standard Young tableau* is used for a Young tableau in which each number of I appears exactly once. This forces $n = |\lambda|$ and leads to strictly increasing numbers along the rows as well. Let us summarize this discussion by the following claim.

Proposition 4.2 *Line scanning assigns a bijection between the D-dense $m \times n$ arrays and the (semistandard) Young tableaux with at most m rows in the alphabet $I = \{1, 2, \ldots, n\}$.* □

4.2.4 Yamanouchi Words

The L-density of an arrow a can be treated as the D-density of the transposed arrow a^t. The transposed version of line scanning is called *column scanning*. It establishes a bijection between the L-dense $m \times n$ arrays and the Young tableaux with at most n columns over the alphabet $J = \{1, 2, \ldots, m\}$.

However, L-density can also be characterized in terms of line scanning. Namely, let us read the line scanning of an array a from right to left, word by word from top to bottom, and record the letters read in one line from left to right. Then the L-density of a means that every starting segment of the resulting long word contains no more twos than ones, no more threes than twos, no more fours than threes, etc. A word w over the alphabet I is called a *Yamanouchi word* if for every $i \in I$, the letter i appears in every starting segment of w at least as many times as the letter $i + 1$ does. For example, in the pair of line scans

$$
\begin{array}{lll}
1 & & \\
1 & 2 & \\
1 & 1 & 2 \\
3 & 3 &
\end{array}
\quad , \qquad
\begin{array}{llll}
1 & 1 & 1 & 1 \\
2 & 2 & 2 & \\
2 & 3 & 3 & \\
1 & 2 & &
\end{array}
\quad ,
$$

the first produces the Yamanouchi word 1 2 1 2 1 1 3 3, whereas the second produces the non-Yamanouchi word 1 1 1 1 2 2 2 3 3 2 2 1.

Exercise 4.3 Recover the arrays producing the above line scans and verify that the first of them is L-dense and the second is not.

Note that the rows of a line scanning are uniquely recovered from a Yamanouchi word: the leftmost nonstrictly increasing segment of the Yamanouchi word is the first word of the line scanning written from right to left; the next nonstrictly increasing segment of the Yamanouchi word is the second word of the line scanning; and so on.

Proposition 4.3 *Line scanning assigns a bijection between the set of L-dense $m \times n$ arrays and the set of Yamanouchi words over the alphabet $I = \{1, 2, \ldots, n\}$ and consisting of at most m nonstrictly increasing segments.* □

4.2.5 Fiber Product Theorem

Given two maps of sets $\varphi : X \to Z$ and $\psi : Y \to Z$, the disjoint union of the products of their fibers over all $z \in Z$ is denoted by

$$X \times_Z Y \stackrel{\text{def}}{=} \bigsqcup_{z \in Z} \varphi^{-1}(z) \times \psi^{-1}(z)$$

and is called the *fibered product* of X and Y over Z. The fiberwise projections $\pi_X : (x, y) \mapsto x$ and $\pi_Y : (x, y) \mapsto y$ fit into the commutative diagram

$$\begin{tikzcd} & X \times_Z Y \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] & \\ X \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\ & Z & \end{tikzcd} \tag{4.4}$$

called the *pullback diagram* or *Cartesian square*. It has the following universal property: for every commutative square

$$\begin{tikzcd} & M \arrow[dl, "\xi"'] \arrow[dr, "\eta"] & \\ X \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\ & Z & \end{tikzcd}$$

there exists a unique map $\alpha : M \to X \times_Z Y$ such that $\xi = \pi_X \circ \alpha$ and $\eta = \pi_Y \circ \alpha$.

Exercise 4.4 Verify this universal property and show that it uniquely determines the upper corner of the diagram (4.4) up to a unique isomorphism commuting with all the arrows of the pullback diagram.

Theorem 4.1 *Let $\mathcal{A}$, $\mathcal{L}$, $\mathcal{D}$, $\mathcal{B}$ denote the sets of all $m \times n$ arrays and all L-dense, D-dense, and bidense arrays respectively. The diagram*

$$\begin{tikzcd} & \mathcal{A} \arrow[dl, "L"'] \arrow[dr, "D"] & \\ \mathcal{L} \arrow[dr, "D"'] & & \mathcal{D} \arrow[dl, "L"] \\ & \mathcal{B} & \end{tikzcd}$$

in which the maps L, D send an array to its left and down condensations, is a Cartesian square.

Proof The maps L, D are well defined by Proposition 4.1 and commute by Corollary 4.1. We have to show that for every $b \in \mathcal{B}$, the map

$$\mathcal{A} \to \mathcal{L} \underset{\mathcal{B}}{\times} \mathcal{D}, \quad a \mapsto (La, Da),$$

establishes a bijection between the arrays a of shape $b = DLa = LDa$ and the pairs of arrays $(a_\ell, a_d) \in \mathcal{L} \times \mathcal{D}$ with the same shape $b = Da_\ell = La_b$. We begin with injectivity. Let two arrays a, a' have $La = La'$, $Da = Da'$. Write Λ for an effective word condensing the array $Da = Da'$ to the left. By Corollary 4.2, the word Λ effectively acts on both arrays a and a', and we have $\Lambda a = La = La' = \Lambda a'$. Hence, $a = \Lambda^{-1} La = \Lambda^{-1} La' = a'$. Now let us verify surjectivity. Given a pair $(a_\ell, a_d) \in \mathcal{L} \times \mathcal{D}$ with the same shape $b = Da_\ell = La_b$, consider a word Λ that effectively condenses a_d to La_d. The inverse word Λ^{-1} effectively acts on the array $La_d = Da_\ell$ and therefore on the array a_ℓ as well. Then the array $a = \Lambda^{-1} a_\ell$ has $La = a_\ell$ and $Da = D\Lambda^{-1} a_\ell = \Lambda^{-1} Da_\ell = \Lambda^{-1} La_d = a_d$, as required. □

Example 4.1 (Graphs of Maps and the Standard Young Tableaux) The graph of a map $a : I \to J$ can be viewed as an array with exactly one ball in every column. Theorem 4.1 bijectively parameterizes such arrays by the pairs (a_ℓ, a_d), where a_ℓ is L-dense, a_d is D-dense, $Da_\ell = La_d$, and $w_I(a_d) = (1, 1, \ldots, 1)$. By Sect. 4.2.3, every such a pair determines and is uniquely determined by the following data:

- the shape $\lambda(a) = \lambda(a_\ell) = \lambda(a_d) = DLa \in \mathcal{B}$, which is an arbitrary Young diagram λ of weight $|\lambda| = n$;
- the line scanning of a_d, which is an arbitrary standard[5] Young tableau of shape λ over the horizontal alphabet I;
- the column scanning of a_ℓ, which is an arbitrary semistandard Young tableau of shape λ over the vertical alphabet J.

[5] Recall that this means that every element of I appears in the tableau exactly once; see Sect. 4.2.3 on p. 81.

The total number of all (semistandard) Young tableaux of shape λ over an m-literal alphabet is denoted by $d_\lambda(m)$. The total number of all standard Young tableaux of shape λ over an alphabet of cardinality $|\lambda|$ is denoted just by d_λ. Since there are altogether m^n maps $I \to J$, we get the remarkable equality

$$\sum_\lambda d_\lambda \cdot d_\lambda(m) = m^n, \tag{4.5}$$

where the summation is over all Young diagrams of weight n, and we put $d_\lambda(m) = 0$ for all diagrams of length $\ell(\lambda) > m$.

Example 4.2 (RSK-Type Correspondence) For $J = I$, the construction from the previous example establishes a one-to-one correspondence between the symmetric group S_n, formed by the $n!$ bijections $I \xrightarrow{\sim} I$, and the pairs of standard Young tableaux of weight n. Hence,

$$\sum_\lambda d_\lambda^2 = n!, \tag{4.6}$$

where the summation is over all Young diagrams of weight n. Since the graphs of involutive permutations[6] are the self-conjugate arrays $a = a^t$, they correspond to the pairs of equal standard tableaux. Therefore,

$$\sum_\lambda d_\lambda = \left|\{\sigma \in S_n \mid \sigma^2 = 1\}\right|. \tag{4.7}$$

Remark 4.1 The standard version of the Robinson–Schensted–Knuth correspondence is described, e.g., in the textbook [Fu].[7] It also encodes the permutations $g \in S_n$ by the pairs of Young tableaux $P(g)$, $Q(g)$, the first of which, $P(g)$, coincides with that used in Example 4.2, i.e., with the row scan of the D-condensation of the graph a of g. The second tableau, $Q(g)$, in the standard RSK correspondence is the column scan of the L-condensation $D(a^*)$ of the array a^* obtained from a by central symmetry,[8] i.e., having $a^*(i,j) = a(n+1-i, n+1-j)$. A detailed comparison of Example 4.2 with the classical Robinson–Schensted–Knuth construction can be found in the remarkable paper [DK, §13].[9]

[6] That is, $\sigma \in S_n$ satisfying $\sigma^2 = 1$.

[7] W. Fulton. *Young Tableaux with Applications to Representation Theory and Geometry*. LMS Student Texts 35, CUP (1997).

[8] In combinatorics, the central symmetry $a \mapsto a^*$ is called the *Schützenberger involution*; see Problem 4.10 on p. 98.

[9] V. I. Danilov, G. A. Koshevoy. "Arrays and the Combinatorics of Young Tableaux." *Russian Math. Surveys* 60:2 (2005), 269–334.

4.3 Action of the Symmetric Group on DU-Sets

4.3.1 DU-Sets and DU-Orbits

A set of arrays $M \subset \mathcal{A}$ sent to itself by all vertical operations D, U, is called a *DU-set*. A map between DU-sets is called a *DU-homomorphism* if it commutes with all vertical operations D, U. A DU-set M is called a *DU-orbit* if the vertical operations act on M transitively. Every DU-set clearly splits into a disjoint union of DU-orbits, because of the next exercise.

Exercise 4.5 Show that unions, intersections, and differences of DU-sets are DU-sets as well.

Downward condensing establishes a bijection between DU-orbits and D-dense arrays. The DU-orbit O_{a_d} corresponding to an array $a_d \in \mathcal{D}$ is formed by all arrays obtained from a_d by means of effective U-words $U_{j_1} U_{j_2} \dots U_{j_k}$. We refer to a_d as the *lower end* of the orbit O_{a_d}. The DU-orbits O_λ of the bidense arrays λ are called *standard*. Theorem 4.1 implies that left condensation establishes a DU-isomorphism between an arbitrary DU-orbit O and the standard DU-orbit O_λ whose lower end is the bicondensation of the lower end of O. The diagram λ is called the *type* of the DU-orbit O. Note that the total number of DU-orbits of type λ in a given DU-set M is equal to the total number of D-dense arrays $a_d \in M$ with column weight $w_I(a_d) = \lambda$.

As an example, Fig. 4.4 shows the standard DU-orbit $O_{(2,1)}$ for $m = 3$. It consists of eight arrays, and its lower end is the bidense array $\begin{array}{|c|c|}\hline 0&0\\\hline 0&1\\\hline 2&0\\\hline\end{array}$ with row scan $\begin{array}{|c|c|}\hline 1&1\\\hline 2\\\cline{1-1}\end{array}$ of shape $\begin{array}{|c|c|}\hline &\\\hline \\\cline{1-1}\end{array}$.

4.3.2 Action of $S_m = \mathrm{Aut}(J)$

Write $\sigma_j \in S_n$, $1 \leqslant j \leqslant n-1$, for the standard generators swapping j with $j+1$, and let them act on an array a by the following rule. Assume that a stable matching between the jth and $(j+1)$th rows of a leaves s_j and s_{j+1} free balls respectively in those rows. If $s_j = s_{j+1}$, then σ_j does nothing with a. Otherwise,

$$\sigma_j a = D_j^{s_{j+1}-s_j} a = U_j^{s_j - s_{j+1}} a. \tag{4.8}$$

Equivalently, this action can be described as follows. Let us roll up the array a into a cylinder by gluing the right border of the nth column to the left border of the first, and proceed with the stable matching cyclically around the cylinder by coupling the rightmost free ball of the jth row with the leftmost free ball of the $(j+1)$th row, etc. The resulting cyclic matching leaves exactly $|s_{j+1} - s_j|$ free balls, all in the row that initially had more free balls. The action of σ_j moves all these balls vertically to the

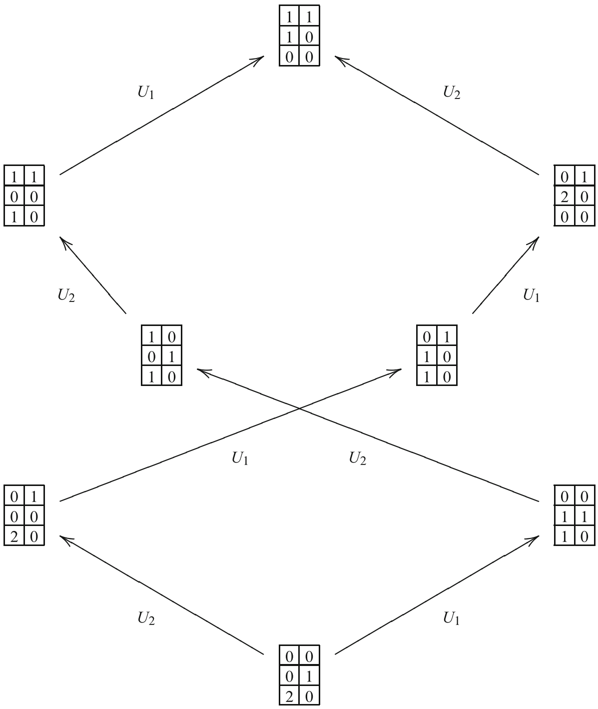


Fig. 4.4 Standard DU-orbit $O_{(2,1)}$

other row. In particular, the effect of σ_j on the row weight w_J consists in swapping the jth and $(j+1)$th coordinates.

By this construction, $\sigma_j^2 = \mathrm{Id}$, $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geqslant 2$, and all σ_j commute with the cyclic permutations of columns and all the horizontal operations L_i, R_i. Let us verify that the *triangle relation* $\sigma_j\sigma_{j+1}\sigma_j = \sigma_{j+1}\sigma_j\sigma_{j+1}$ holds as well for all j. We may assume that a consists of just three rows. Then the left condensation L and the cyclic permutation of columns C reduce a to just one column:

$$\begin{array}{|c|c|c|}\hline * & * & * \\ \hline * & * & * \\ \hline * & * & * \\ \hline\end{array} \xrightarrow{L} \begin{array}{|c|c|c|}\hline a & b & c \\ \hline d & e & 0 \\ \hline f & 0 & 0 \\ \hline\end{array} \xrightarrow{C} \begin{array}{|c|c|c|}\hline b & c & a \\ \hline e & 0 & d \\ \hline 0 & 0 & f \\ \hline\end{array} \xrightarrow{L} \begin{array}{|c|c|c|}\hline g & h & 0 \\ \hline k & 0 & 0 \\ \hline f & 0 & 0 \\ \hline\end{array} \xrightarrow{C} \begin{array}{|c|c|}\hline h & g \\ \hline 0 & k \\ \hline 0 & f \\ \hline\end{array} \xrightarrow{L} \begin{array}{|c|c|}\hline \ell & 0 \\ \hline k & 0 \\ \hline f & 0 \\ \hline\end{array}.$$

Since σ_1, σ_2 act on this column by the transpositions of elements, the required identity $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ clearly holds. Thus, the operations $a \mapsto \sigma_j a$ satisfy all the relations on the generators[10] σ_i in S_n. We conclude[11] that the action of the σ_j is correctly extended to the action of the whole symmetric group S_m on the set of arrays

[10] See Sect. 13.2 of Algebra I.

[11] See Sect. 13.1 of Algebra I.

with m rows. This action takes every DU-set to itself and permutes the coordinates of the row weights w_I.

4.4 Combinatorial Schur Polynomials

Let us interpret every ball in the jth row of an array a as the variable x_j and write

$$x^a \stackrel{\text{def}}{=} x_1^{w_1(a)} x_2^{w_2(a)} \cdots x_m^{w_m(a)}$$

for the product of all balls in a, where $(w_1(a), w_2(a), \ldots, w_m(a)) = w_J(a)$ means the J-weight of a. The sum of all monomials x^a taken over all arrays a from a given DU-set M is called the (*combinatorial*) *Schur polynomial* of the DU-set M and is denoted by

$$s_M(x) \stackrel{\text{def}}{=} \sum_{a \in M} x^a \in \mathbb{Z}[x_1, x_2, \ldots, x_m].$$

Since the symmetric group S_m acts on the monomials x^a by permutation of variables and this action takes M to itself, all the Schur polynomials are symmetric. In decomposing a DU-set M into a disjoint union of DU-orbits and combining all orbits isomorphic to a given standard orbit $\mathcal{O}_\lambda$, we expand every Schur polynomial s_M as a nonnegative integer linear combination of the *standard* Schur polynomials $s_\lambda(x)$, which have bidense lower ends and are numbered by the Young diagrams λ of length at most m. We will write this expansion as

$$s_M(x) = \sum_{\lambda \in \lambda(M)} c_M^\lambda \cdot s_\lambda(x), \tag{4.9}$$

where the summation runs over all shapes λ of arrays appearing in M, and the coefficient c_M^λ equals the total number of DU-orbits isomorphic to $\mathcal{O}_\lambda$ in M, i.e., to the number of D-dense arrays of J-weight λ in M. By Sect. 4.2.3, every standard DU-orbit $\mathcal{O}_\lambda$ is formed by the L-dense arrays of I-weight λ. Column scanning assigns a bijection between such the arrays and the (semistandard) Young tableaux of shape λ over the alphabet $\{x_1, x_2, \ldots, x_m\}$. Therefore, every standard Schur polynomial can be written as

$$s_\lambda(x) = \sum_\eta K_{\lambda,\eta} \cdot x^\eta = \sum_\eta K_{\lambda,\eta} \cdot x_1^{\eta_1} x_2^{\eta_2} \cdots x_m^{\eta_m}, \tag{4.10}$$

where $\eta \in \mathbb{Z}_{\geqslant 0}^m$ runs over vectors of dimension m with nonnegative integer coordinates, and the coefficient $K_{\lambda,\eta}$ equals the total number of (semistandard) Young tableaux of shape λ filled by η_1 ones, η_2 twos, η_3 threes, etc. We will say that such a Young tableau has *content* η. The sum $|\eta| \stackrel{\text{def}}{=} \sum \eta_i$ is called the *weight* of the content vector η.

For example, the standard DU-orbit shown in Fig. 4.4 on p. 87 produces the following standard Schur polynomial in $m = 3$ variables:

$$s_{(2,1)}(x_1, x_2, x_3) = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + 2\, x_1 x_2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2.$$

Exercise 4.6 Verify that for every Young diagram λ, the sequence of Schur polynomials

$$s_\lambda(x_1, x_2, \dots, x_m), \quad m \geqslant \ell(\lambda),$$

is a symmetric function in the sense of Sect. 3.7 on p. 69.

The numbers $K_{\lambda,\eta}$ of the (semistandard) Young tableaux of shape λ and content η are called *Kostka numbers*. Note that $K_{\lambda,(1^{|\lambda|})} = d_\lambda$ is the number of *standard* Young tableaux of shape λ. It follows from the definition that $K_{\lambda,\lambda} = 1$ for all λ, and $K_{\lambda,\eta} \neq 0$ only if the inequality

$$\lambda_1 + \lambda_2 + \cdots + \lambda_j \geqslant \eta_1 + \eta_2 + \cdots + \eta_j \tag{4.11}$$

holds for every $j = 1, 2, 3, \dots$. In this case, we say that the diagram λ *dominates* the vector η and write $\lambda \trianglerighteq \eta$.

Exercise 4.7 Show that the domination relation provides the set all Young diagrams[12] of weight[13] n with a partial order. Verify that this order is total for $n \leqslant 5$, and find a pair of incompatible Young diagrams of weight 6.

It follows from (4.10) that the transition matrix from the standard Schur polynomials s_λ to the monomial basis m_μ of the $\mathbb{Z}$-module of symmetric polynomials in $x_1, x_2, \dots, x_m$ is upper unitriangular, i.e.,

$$s_\lambda = \sum_{\mu \trianglelefteq \lambda} K_{\lambda,\mu} \cdot m_\mu. \tag{4.12}$$

Since such a matrix is invertible over $\mathbb{Z}$, we conclude that the combinatorial Schur polynomials s_λ also form a basis of the $\mathbb{Z}$-module of symmetric polynomials.

Example 4.3 (Complete and Elementary Symmetric Polynomials) The standard Schur polynomial $s_{(k)}(x)$, indexed by the one-row Young diagram

$$\lambda = (k,\, 0,\, \dots,\, 0) = \underbrace{\square\square \cdots \square\square}_{k}, \tag{4.13}$$

[12]Since every Young diagram $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_m)$ can be viewed as a vector in $\mathbb{Z}^m_{\geqslant 0}$, the domination relation $\lambda' \trianglerighteq \lambda''$ is well defined.

[13]Recall that the weight of a Young diagram λ is the total number of cells in λ.

is obtained from the DU-orbit of the array

$$\left.\begin{array}{c}\boxed{0}\\\boxed{0}\\\vdots\\\boxed{0}\\\boxed{k}\end{array}\right\} m \tag{4.14}$$

and coincides with the complete symmetric polynomial[14] $h_k(x_1, x_2, \ldots, x_m)$, the sum of all monomials of total degree k in the x_i. Indeed, for every content vector $\eta \in \mathbb{Z}^m_{\geqslant 0}$ of weight $|\eta| = \sum \eta_i = k$, there exists exactly one Young tableau of shape (4.13) and weight η. Equivalently, the DU-orbit of the array (4.14) is formed by all distributions of k balls between m cells.

Symmetrically, the standard Schur polynomial $s_{(1^k)}$, indexed by the one-column Young diagram

$$1^k = (1,\, 1,\, \ldots,\, 1) = \left.\begin{array}{c}\Box\\\Box\\\vdots\\\Box\\\Box\end{array}\right\} k,$$

is obtained from the DU-orbit of the array

$$\underbrace{\left.\begin{array}{ccc}\boxed{0}\boxed{0} & \cdots & \boxed{0}\boxed{0}\\ \vdots & \vdots & \vdots\\ \begin{array}{c}\boxed{0}\boxed{0}\\\boxed{0}\boxed{0}\\\boxed{0}\boxed{0}\end{array} & \cdots & \begin{array}{c}\boxed{0}\boxed{0}\\\boxed{0}\boxed{1}\\\boxed{1}\boxed{0}\end{array}\\ \vdots & \iddots & \vdots\\ \begin{array}{c}\boxed{0}\boxed{1}\\\boxed{1}\boxed{0}\end{array} & \cdots & \begin{array}{c}\boxed{0}\boxed{0}\\\boxed{0}\boxed{0}\end{array}\end{array}\right\} m}_{k} \tag{4.15}$$

and equals the elementary symmetric polynomial[15] $e_k(x_1, x_2, \ldots, x_m)$, the sum of all multilinear monomials of total degree k in the x_i. The reasons are similar, but now the fillings of the Young tableau must strictly increase. Equivalently, at most one ball is allowed in each row of every array in the DU-orbit of the array (4.15).

Example 4.4 (Cauchy and Schur Identities) Fix two collections of independent variables $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_m$ and interpret all the balls in the (i,j) cell of every $I \times J$ array a as the monomials $x_i y_j$. Then in the notation of Sect. 4.4, the

[14] See Sect. 3.3 on p. 61.

[15] See Sect. 3.2 on p. 60.

product of the balls in a equals $x^{a^t}y^a$. By Theorem 4.1 on p. 83, the sum of such monomials taken over all arrays a of a given shape $\lambda = \lambda(a)$ is equal to the product of Schur polynomials $s_\lambda(x) \cdot s_\lambda(y)$. Therefore, the sum of the monomials $x^{a^t}y^a$ taken over all $I \times J$ arrays a is equal to the sum $\sum_\lambda s_\lambda(x) \cdot s_\lambda(y)$ taken over all Young diagrams λ. At the same time, the same sum of monomials $x^{a^t}y^a$ appears on multiplying out the product of geometric progressions $\prod_{I\times J}\left(1 + x_iy_j + (x_iy_j)^2 + (x_iy_j)^3 + \cdots\right)$, because the choice of the summand $(x_iy_j)^{a(i,j)}$ in the (i,j)th factor contributes exactly the monomial $x^{a^t}y^a$ to the product. Thus, we get the *Cauchy's identity*

$$\sum_\lambda s_\lambda(x) \cdot s_\lambda(y) = \prod_{i,j} \frac{1}{1 - x_iy_j}. \tag{4.16}$$

Now let us take $I = J$, put $x_i = y_i$, and restrict ourselves to the symmetric arrays $a = a^t$. Write ξ_i instead of $x_i = y_i$ and replace every product $x^{a^t}y^a$ by its square root $\sqrt{x^{a^t}y^a} = \xi^a$. The sum of these ξ^a over all symmetric arrays $a = a^t$ of a given shape λ equals $s_\lambda(\xi)$. Therefore, $\sum_{a=a^t} \xi^a = \sum_\lambda s_\lambda(\xi)$. The same sum appears on multiplying out the product

$$\prod_k \left(1 + \xi_k + (\xi_k)^2 + (\xi_k)^3 + \cdots\right) \cdot \prod_{i<j} \left(1 + \xi_i\xi_j + (\xi_i\xi_j)^2 + (\xi_i\xi_j)^3 + \cdots\right).$$

Summing up the geometric progressions, we get the *Schur identity*

$$\sum_\lambda s_\lambda(\xi) = \prod_i \frac{1}{1-\xi_i} \cdot \prod_{i<j} \frac{1}{1-\xi_i\xi_j}. \tag{4.17}$$

4.5 The Littlewood–Richardson Rule

Given two DU-sets M, N, the product of their Schur polynomials $s_M(x) \cdot s_N(x)$ is the Schur polynomial of the DU-set consisting of all arrays ab, $a \in M$, $b \in N$, of size $(2n) \times m$, with the same vertical alphabet J but the doubled horizontal alphabet $I \sqcup I$. We write $M \otimes N$ for the set of all such arrays ab, obtained by writing the array $b \in N$ to the right of the array $a \in M$ for all possible choices of $a \in M$, $b \in N$, and call the set $M \otimes N$ the *tensor product* of DU-sets M, N. Thus,

$$s_M(x) \cdot s_N(x) = \Bigl(\sum_{a\in M} x^a\Bigr) \cdot \Bigl(\sum_{b\in N} x^b\Bigr) = \sum_{\substack{a\in M\\ b\in N}} x^{ab} = \sum_{c\in M\otimes N} x^c.$$

Since the standard Schur polynomials s_λ form a basis of the $\mathbb{Z}$-module of symmetric functions, the product $s_\lambda s_\mu$ can be expanded as

$$s_\lambda \cdot s_\mu = \sum_\nu c^\nu_{\lambda\mu} \cdot s_\nu. \tag{4.18}$$

Theorem 4.2 (The Littlewood–Richardson Rule) *In formula* (4.18)*, the summation is over all Young diagrams ν obtained by adding $|\mu|$ extra cells to the diagram λ. The coefficient $c^{\nu}_{\lambda\mu}$ in* (4.18) *equals the total number of fillings of the skew diagram $\nu \smallsetminus \lambda$ by μ_1 ones, μ_2 twos, μ_3 threes, etc., such that these numbers increase nonstrictly from left to right along the rows of $\nu \smallsetminus \lambda$, strictly increase from top to bottom along the columns of $\nu \smallsetminus \lambda$ (as in a Young tableau), and the word obtained by reading the skew tableau $\nu \smallsetminus \lambda$ from right to left row by row and top to bottom is a Yamanouchi word, i.e., in every starting segment of this word, the number of ones is not less than the number of twos, the number of twos is not less than the number of threes, etc.*

Exercise 4.8 Use the Littlewood–Richardson rule to compute the products $s_{(1)} \cdot s_{(1,1)}$ and $s_{(1,1)} \cdot s_{(1)}$ independently of each other. Also compute $s^2_{2,1}$.

Proof (of Theorem 4.2) For every ν, we have to compute a number of those DU-orbits in $O_\lambda \otimes O_\mu$ whose left condensation is the standard orbit O_ν. Let an array ab belong to such an orbit. Then both arrays a, b are L-dense and have $w_I(a){=}\lambda$, $w_I(b) = \mu$, because they are obtained from the bidense arrays λ, μ by means of some vertical operations. We claim that an action of every vertical condensing operation D_j on the "fat" array ab is reduced to the action of D_j either separately on a or separately on b. Indeed, if the rightmost free ball of a stable matching in the fat array ab lies in b, then this ball is certainly the rightmost free ball of a stable matching within b only, and $D_j(ab) = a(D_j b)$. If all the balls of b are coupled under the stable matching in the fat array ab, then $D_j(ab) = (D_j a)b$. Thus, in the D-condensation $a'b'$ of ab, the arrays a', b' are L-dense with $w_I(a') = \lambda$, $w_I(b'){=}\mu$, and the array a' is D-dense. Therefore, a' is bidense of shape λ. If the shape of the array $a'b' = \lambda b'$ is ν, the rows of the horizontal scan of b' coincide with the rows of the skew tableau $\nu \smallsetminus \lambda$, filled in accordance with the Littlewood–Richardson rule, because the Young tableau constraints assert that the fat array $a'b'$ is D-dense, whereas the Yamanouchi word constraint claims that b' is L-dense.[16] $\square$

Exercise 4.9 (Pieri's Formulas) Use the Littlewood–Richardson rule to prove the *Pieri's formulas*:

$$s_\lambda \cdot e_k = s_\lambda \cdot s_{(1^k)} = \sum_{\mu} s_\mu, \tag{4.19}$$

$$s_\lambda \cdot h_k = s_\lambda \cdot s_{(k)} = \sum_{\nu} s_\nu, \tag{4.20}$$

where μ, ν run through all the Young diagrams obtained by adding k extra cells to the diagram λ in such a way that all the new cells are in k different rows of μ and in k different columns of ν.

[16] See Sect. 4.2.4 on p. 82.

4.5.1 The Jacobi–Trudi Identity

Pieri's formula (4.20) and Corollary 3.4 on p. 69 imply that the determinantal Schur polynomials $\Delta_{\delta+\lambda}/\Delta_\delta$ introduced in Proposition 3.1 on p. 59 and the combinatorial Schur polynomials s_λ of the standard DU-orbits are actually the same symmetric polynomials. Indeed, Pieri's formulas allow us to express all the Schur polynomials in terms of the complete symmetric polynomials $h_k = s_{(k)}$. For example, it follows from (4.20) that

$$\begin{aligned}
s_{(2,2,1)} &= s_{(2,2)}h_1 - s_{(3,2)},\\
s_{(3,2)} &= s_{(3)}h_2 - s_{(5)} - s_{(4,1)} = h_3h_2 - h_5 - s_{(4,1)},\\
s_{(2,2)} &= s_{(2)}h_2 - s_{(3,1)} - s_{(4)} = h_2^2 - h_4 - s_{(3,1)},\\
s_{(4,1)} &= s_{(4)}h_1 - s_{(5)} = h_4h_1 - h_5,\\
s_{(3,1)} &= s_{(3)}h_1 - s_{(4)} = h_3h_1 - h_4.
\end{aligned}$$

Therefore, $s_{(2,2,1)} = -h_3h_2 + h_4h_1 + h_1(h_2^2 - h_1h_3)$.

Exercise 4.10 Check this by means of the Giambelli formula (3.23) on p. 66.

In the general case, let us leave on the right-hand side of (4.20) only the diagram ν of maximal length with the longest bottom row among such diagrams. Then s_ν turns out to be expressed in terms of h_k and s_η with either $\ell(\eta) < \ell(\nu)$ or $\ell(\eta) = \ell(\nu) = m$ but $\eta_m < \nu_m$. Induction on $\ell(\nu)$ and on the length of the bottom row in ν leads to the required expression for s_ν in terms of h_i.

Equivalence between the combinatorial and determinantal descriptions of the Schur polynomials is known as the *Jacobi–Trudi formula*.

4.5.2 Transition from e_λ and h_λ to s_λ

Recall that we write $m_i = m_i(\mu)$ for the number of length-i rows in the Young diagram μ and put

$$e_\mu = e_{\mu_1}e_{\mu_2}\cdots e_{\mu_r} = e_1^{m_1}e_2^{m_2}\cdots e_n^{m_n}, \tag{4.21}$$

$$h_\mu = h_{\mu_1}h_{\mu_2}\cdots h_{\mu_r} = h_1^{m_1}h_2^{m_2}\cdots h_n^{m_n}, \tag{4.22}$$

where $e_k(x) = s_{(1^k)}(x_1, x_2, \ldots, x_m)$, $h_k(x) = s_{(k)}(x_1, x_2, \ldots, x_m)$ for $k \in \mathbb{N}$ are the *elementary*[17] and *complete*[18] symmetric polynomials respectively. For an arbitrary

[17] See Sect. 3.2 on p. 60.

[18] See Sect. 3.3 on p. 61.

Young diagram η, the complete polynomial $h_\eta = s_{(\eta_1)}s_{(\eta_2)} \cdots s_{(\eta_r)}$ is the Schur polynomial of the DU-set $O_{(\eta_1)} \otimes O_{(\eta_2)} \otimes \cdots \otimes O_{(\eta_r)}$. The DU-orbits of shape ν in this DU-set are numbered by their lower ends, which are in bijection with the Young tableaux of shape ν and content η. Therefore,

$$h_\eta = \sum_\nu K_{\nu,\eta} \cdot s_\nu . \tag{4.23}$$

Similarly, $e_\eta = s_{(1^{\eta_1})}s_{(1^{\eta_2})} \cdots s_{(1^{\eta_r})}$ is the Schur polynomial of the DU-set

$$O_{(1^{\eta_1})} \otimes O_{(1^{\eta_2})} \otimes \cdots \otimes O_{(1^{\eta_r})} .$$

Every array a in this set has $|\eta|$ columns and can be considered a concatenation of subarrays $a_1a_2 \ldots a_r$ of widths $\eta_1, \eta_2, \ldots, \eta_r$ and the same height as a. Every column of a contains exactly one ball, and the J-coordinates of these balls strictly increase within every subarray a_i. The D-condensation of a preserves the latter property and leads to a D-dense array $a_1'a_2' \ldots a_r'$ such that the balls of every subarray a_i' are in different rows whose numbers increase from left to right. Therefore, every subarray a_i' contributes at most one ball to every component of the row weight $w_J(a_1'a_2' \ldots a_r')$. Let $w_J(a_1'a_2' \ldots a_r') = \nu$. If we fill every row ν_j in ν from left to right by the sequential indices i of those subarrays a_i' that contribute a ball to the jth coordinate of $w_J(a_1'a_2' \ldots a_r')$, then we get a Young tableau of content η and shape ν^t. The latter is the transpose of ν, because the D-density of the array $a_1'a_2' \ldots a_r'$ forces the numbers i to increase strictly along the rows and nonstrictly along the columns of ν. The construction also implies that every index i appears in exactly η_i different rows. We conclude that

$$e_\eta = \sum_\nu K_{\nu^t,\eta} \cdot s_\nu . \tag{4.24}$$

Proposition 4.4 *The involution $\omega : \Lambda \xrightarrow{\sim} \Lambda$ introduced in Proposition 3.3 on p. 62 acts on the Schur basis by the rule $\omega(s_\lambda) = s_{\lambda^t}$, i.e., transposes Young diagrams indexing the Schur polynomials.*

Proof Since the Schur polynomials s_λ form a basis of the $\mathbb{Z}$-module of symmetric functions Λ, the assignment $s_\lambda \mapsto s_{\lambda^t}$ provides Λ with a $\mathbb{Z}$-linear involution. It follows from formulas (4.23), (4.24) that this involution swaps e_k with h_k and therefore coincides with ω, which also swaps e_k with h_k. □

Corollary 4.3 (Second Giambelli Formula)

$$s_{\lambda^t} = \det \begin{pmatrix} e_{\lambda_1} & e_{\lambda_1+1} & \ddots & e_{\lambda_1+n-1} \\ e_{\lambda_2-1} & e_{\lambda_2} & \ddots & \ddots \\ \ddots & \ddots & \ddots & e_{\lambda_{n-1}+1} \\ e_{\lambda_n-n+1} & \ddots & e_{\lambda_n-1} & e_{\lambda_n} \end{pmatrix}, \tag{4.25}$$

where $e_{\lambda_1}, e_{\lambda_2}, \dots, e_{\lambda_n}$ are on the main diagonal and the indices of e are incremented by one from left to right along the rows.

Proof Apply the involution ω to the first Giambelli formula (3.23) on p. 66. □

4.6 The Inner Product on Λ

Let us equip the $\mathbb{Z}$-module of symmetric functions Λ with the Euclidean inner product $\langle *, * \rangle$ by declaring the Schur basis s_λ to be orthonormal,

$$\langle s_\lambda, s_\mu \rangle = \begin{cases} 1 & \text{for } \lambda = \mu, \\ 0 & \text{otherwise.} \end{cases}$$

Then Proposition 4.4 forces the involution ω to be orthogonal, and the formulas[19]

$$h_\lambda = \sum_{\mu \trianglerighteq \lambda} K_{\mu,\lambda} \cdot s_\mu, \quad s_\mu = \sum_{\lambda \trianglerighteq \mu} K_{\mu,\lambda} \cdot m_\lambda$$

show that $\langle h_\lambda, s_\mu \rangle = K_{\mu,\lambda} = \langle m_\lambda^\vee, s_\mu \rangle$, where $m_\lambda^\vee$ means the Euclidean dual[20] basis to the monomial basis m_λ. Therefore, $m_\lambda^\vee = h_\lambda$, i.e., the bases h_λ and m_λ are dual to each other,

$$\langle h_\lambda, m_\mu \rangle = \begin{cases} 1 & \text{for } \lambda = \mu, \\ 0 & \text{otherwise.} \end{cases} \tag{4.26}$$

Proposition 4.5 *The Newton polynomials p_λ form an orthogonal basis of the vector space of symmetric functions with rational coefficients $\mathbb{Q} \otimes \Lambda$, and*[21]

$$\langle p_\lambda, p_\lambda \rangle = z_\lambda = \prod_k (m_k! \cdot k^{m_k}) .$$

Proof Let us expand the geometric progressions on the right-hand side of Cauchy's identity[22] in terms of Newton power sums in the variables x and y:

$$\sum_\lambda s_\lambda(x)s_\lambda(y) = \prod_{i,j} \frac{1}{1 - x_i y_j} = \prod_j H(y_j) = \prod_j \exp\left(\int_0^{y_j} P(t)\, dt \right)$$

[19] See formula (4.23) and formula (4.12) on p. 89.

[20] See Sect. 10.3.1 of Algebra I.

[21] Compare with formulas (3.17)–(3.18) from Proposition 3.5 on p. 64.

[22] See formula (4.16) on p. 91.

$$
\begin{aligned}
&= \exp\left(\sum_j \sum_k \frac{1}{k} p_k(x) y_j^k\right) = \exp\left(\sum_k \frac{p_k(x)p_k(y)}{k}\right) \\
&= \prod_k \exp\left(\frac{p_k(x)p_k(y)}{k}\right) = \prod_k \sum_{\ell \geqslant 0} \frac{1}{\ell! \cdot k^\ell} \left(p_k(x)p_k(y)\right)^\ell \\
&= \sum_\lambda \frac{1}{z_\lambda} p_\lambda(x) p_\lambda(y)
\end{aligned}
$$

(the last equality holds for the same reason as in formula (3.17) on p. 64). Write

$$c_{\lambda\mu} = \left(s_\lambda, p_\mu \right)$$

for the elements of the transition matrix $C = C_{sp}$ from the Newton polynomials to the Schur basis. Then $p_\mu = \sum_\lambda s_\lambda \cdot c_{\lambda\mu}$. Substituting these expansions into the right-hand side of the above equality and comparing the coefficients in $s_\lambda(x)s_\eta(y)$ on both sides leads to the relations

$$\sum_\nu c_{\nu\lambda} c_{\nu\eta} = \begin{cases} z_\lambda & \text{for } \eta = \lambda, \\ 0 & \text{otherwise,} \end{cases}$$

i.e., the Gram matrix $\left(\left(p_\lambda, p_\mu \right)\right) = C^t \cdot C$ is diagonal with z_λ on the diagonal. $\square$

Problems for Independent Solution to Chapter 4

Problem 4.1 Verify that an array a is D-dense if and only if

$$
\begin{aligned}
a(1, j+1) + a(2, j+1) + \cdots + a(i, j+1) \\
\leqslant a(1, j) + a(2, j) + \cdots + a(i-1, j),
\end{aligned}
$$

for all $i \in I$, $j \in J$, and write similar inequalities expressing the L-, R-, and U-density of a.

Problem 4.2 Write the D-dense array with row scan

$$\begin{array}{|c|c|c|} \hline 1 & 4 & 6 \\ \hline 2 & 5 & 7 \\ \hline 3 & 8 & 9 \\ \hline \end{array},$$

and the L-dense array with column scan

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & 8 \\ \hline 6 & 7 & 9 \\ \hline \end{array}.$$

Compute the permutation $g \in S_9$ encoded by this pair of arrays under the RSK-type correspondence from Example 4.2 on p. 85.

Problem 4.3 Compute the permutation $g \in S_9$ mapped by the RSK-type correspondence from Example 4.2 on p. 85 to the following pairs of Young tableaux[23]:

(a) $\begin{ytableau} 1 & 2 & 3 & 6 & 7 & 8 & 9 \\ 4 \\ 5 \end{ytableau}$ and $\begin{ytableau} 1 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 \\ 3 \end{ytableau}$

(b) $\begin{ytableau} 1 & 3 & 5 & 6 \\ 2 & 4 & 9 \\ 7 & 8 \end{ytableau}$ and $\begin{ytableau} 1 & 3 & 5 & 7 \\ 2 & 4 & 8 \\ 6 & 9 \end{ytableau}$.

Problem 4.4 Show that for every DU-homomorphism of DU-orbits[24] $\varphi : O_1 \to O_2$, either φ is bijective or O_2 consists of just one point.

Problem 4.5 Write explicitly the Schur polynomials

(a) $s_{2,1}(x_1, x_2, x_3)$,
(b) $s_{3,1}(x_1, x_2, x_3)$,
(c) $s_{2,1,1}(x_1, x_2, x_3)$.

Problem 4.6 How many monomials are there in $s_{(2,1,1)}(x_1, x_2, x_3, x_4)$?

Problem 4.7 Express the determinant

$$\det \begin{pmatrix} x_1^6 & x_2^6 & x_3^6 & x_4^6 \\ x_1^3 & x_2^3 & x_3^3 & x_4^3 \\ x_1 & x_2 & x_3 & x_4 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

in terms of the elementary symmetric polynomials in x and the Vandermonde determinant $\Delta_\delta = \prod\limits_{i<j}(x_i - x_j)$.

Problem 4.8 (Domination) Given two Young diagrams λ, μ of the same weight $|\lambda| = |\mu| = n$, we write $\lambda \trianglerighteq \mu$ and say that λ *dominates* μ if

$$\lambda_1 + \lambda_2 + \cdots + \lambda_j \geqslant \mu_1 + \mu_2 + \cdots + \mu_j \quad \text{for all } j.$$

Let $\lambda \vartriangleright \mu$ be a minimal dominating diagram[25] for μ. Show that μ is obtained from λ by moving one cell the minimal possible distance in the southwesterly direction and that $\mu^t \vartriangleright \lambda^t$. Use this to prove the equivalence $\lambda \trianglerighteq \mu \iff \lambda^t \trianglelefteq \mu^t$ for every two $\trianglerighteq$-compatible Young diagrams.

Problem 4.9 Let us cut a Young diagram λ whose main diagonal consists of k cells into k Γ-shaped hooks[26] $\gamma_1, \gamma_2, \dots, \gamma_k$ with corners on the main diagonal of λ.

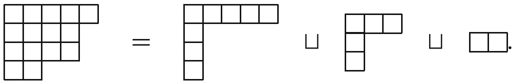
[23]Recall that the first tableau is the row scan of the D-condensation of the graph of $g : I \simeq J$, whereas the second is the column scan of the L-condensation of the same graph.

[24]That is, a map commuting with all the vertical operations D_j, U_j.

[25]That is, $\lambda \neq \mu$ and for every η, $\lambda \trianglerighteq \eta \trianglerighteq \mu$ forces either $\lambda = \eta$ or $\eta = \mu$.

[26]Formally, $\gamma_i = \left(\lambda_i - i + 1, 1^{\lambda_i^t - i}\right)$ for every $i = 1, 2, \dots, k$.

For example,



Compute the coefficient of s_λ in the expansion of the product $s_{\gamma_1} s_{\gamma_2} \cdots s_{\gamma_k}$ as a $\mathbb{Z}$-linear combination of the standard Schur polynomials s_λ.

Problem 4.10* (Schützenberger Involution) Show that rotation by 180° about the center of an $n \times m$ array does not change the shape[27] of the array, i.e., $\lambda(a) = \lambda(a^*)$, where $a^*(i,j) = a(n+1-i, m+1-j)$.

Problem 4.11* (Untangling Antichains) Given a poset[28] P, every totally ordered subset $C \subset P$ is called a *chain*, whereas every subset $A \subset P$ all of whose elements are mutually incompatible is called an *antichain*. A subset $K \subset M$ is called a *k-antichain* if K can be covered by k antichains. Write $\alpha_k(P)$ for the maximal cardinality among k-antichains in P. The sequence of differences

$$\delta_k(P) = \alpha_k(P) - \alpha_{k-1}(P)$$

is called the *shape* of the poset P. Given an array a, write $P(a)$ for the set of all balls in a equipped with the partial order $\beta > \gamma$, meaning that both the horizontal and vertical coordinates of β are greater than those of γ. Prove that for every array a, the shape of the poset $P(a)$ coincides with the shape of the array[29] $\lambda(a)$. Hint: prove that the vertical operations D_j, U_j do not decrease the differences δ_k (first prove this for δ_1, the cardinality of a maximal antichain, and then untangle every k-antichain into a disjoint union of k ordinary antichains).

---

[27]That is, the Young diagram encoding the DL-condensation of the array; see Sect. 4.2.2 on p. 80.

[28]See Sect. 1.4 of Algebra I.

[29]Note that this forces the shape of $P(a)$ to be a Young diagram, which is completely nonobvious from the definition of a poset's shape.

Chapter 5
Basic Notions of Representation Theory

5.1 Representations of a Set of Operators

5.1.1 Associative Envelope

Given a set R and a field $\Bbbk$, let us write $R \otimes \Bbbk$ for the vector space with basis R over $\Bbbk$. It is formed by the formal linear combinations $\sum x_r \cdot r$ of elements $r \in R$ with coefficients $x_r \in \Bbbk$, all but a finite number of which vanish. By definition, the *free associative* $\Bbbk$*-algebra* spanned by the set R is the tensor algebra $A_R \stackrel{\text{def}}{=} \mathsf{T}(R \otimes \Bbbk)$ of the vector space $R \otimes \Bbbk$.

Exercise 5.1 Verify that the tautological inclusion $\iota : R \hookrightarrow A_R$, mapping R to the distinguished basis of $R \otimes \Bbbk \subset \mathsf{T}(R \otimes \Bbbk)$, possesses the following universal property: for every associative $\Bbbk$-algebra B and map of sets $\varphi : A \to B$, there exists a unique homomorphism of $\Bbbk$-algebras $\widetilde{\varphi} : A_R \to B$ such that $\widetilde{\varphi}\iota = \varphi$. Prove that the algebra A_R together with the inclusion $\iota : R \hookrightarrow A_R$ is uniquely determined by this universal property up to a unique isomorphism commuting with ι.

For example, if $R = \{t\}$ consists of one element t, then the vector space

$$t \otimes \Bbbk = \Bbbk \cdot t$$

has dimension 1, and the free associative $\Bbbk$-algebra A_t is isomorphic to the polynomial algebra $\Bbbk[t]$ by mapping $t \otimes t \otimes \cdots \otimes t \in A_t$ to $t^n \in \Bbbk[t]$.

Given a vector space W over $\Bbbk$, a map of sets $\varrho : R \to \operatorname{End}_{\Bbbk}(W)$ is called a *linear representation* of the set R by endomorphisms of W. By Exercise 5.1, the linear representations of R in $\operatorname{End}_{\Bbbk}(W)$ are in bijection with the $\Bbbk$-algebra homomorphisms

$$\widetilde{\varrho} : A_R \to \operatorname{End}(W), \tag{5.1}$$

also called *linear representations* of A_R by endomorphisms of W. A vector space W equipped with a linear representation $\varrho : R \to \operatorname{End}_{\Bbbk}(W)$ or $\widetilde{\varrho} : A_R \to \operatorname{End}(W)$ is

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_5

called an R-*module* or A_R-*module*. This means that for every $f \in R$, the linear map $\varrho(f) : W \to W$ is given. Then an arbitrary tensor

$$f = \sum x_{f_1 f_2 \dots f_m} f_1 \otimes f_2 \otimes \cdots \otimes f_m \in A_R$$

with $f_\nu \in R$, $x_{f_1 f_2 \dots f_m} \in \Bbbk$, is represented by the linear operator

$$\widetilde{\varrho}(f) = \sum x_{f_1 f_2 \dots f_m} \varrho(f_1) \circ \varrho(f_2) \circ \cdots \circ \varrho(f_m) : W \to W.$$

In particular, the image of the algebra homomorphism (5.1) consists of all linear maps $W \to W$ obtained from the operators $\varrho(f), f \in R$, by compositions and finite linear combinations. All these maps form a $\Bbbk$-subalgebra in $\mathrm{End}_{\Bbbk}(W)$ called the *associative envelope* of the set of operators $\varrho(R) \subset \mathrm{End}(W)$. We write $\mathrm{Ass}\, X$ for the associative envelope of an arbitrary set of linear endomorphisms $X \subset \mathrm{End}\, W$. Thus, $\mathrm{Ass}(\varrho(R)) = \widetilde{\varrho}(A_R)$.

When the representation $\varrho : R \to \mathrm{End}\, W$ is clear from the context or inessential, we will write fw for the image of a vector $w \in W$ under the map $\widetilde{\varrho}(f) : W \to W$. Given a vector subspace $U \subset W$ and a set of tensors $F \subset A_R$, we put

$$FU \stackrel{\text{def}}{=} \{fu \mid f \in F,\ u \in U\}.$$

5.1.2 *Decomposability and (Semi)/Simplicity*

Let W be an R-module. A vector subspace $U \subset W$ is called R-*invariant* (or an R-*submodule*) if $RU \subset U$.

Exercise 5.2 (Factor Modules) Given an R-submodule U of an R-module W, verify that the quotient space $V = W/U$ inherits the R-module structure well defined by the assignment $f[w] \stackrel{\text{def}}{=} [fw]$ for all $f \in R$, $w \in W$, where $[w] = w + U$ means the congruence class of w modulo U.

A nonzero R-module W is called *simple* if it has no proper R-submodules except for the zero module. A representation $\varrho : R \to \mathrm{End}(W)$ producing a simple R-module W is called *irreducible*. An R-module is called *semisimple* if it is a direct sum of simple R-submodules. A representation producing such a module is called *completely reducible*. Note that direct sums of semisimple modules are semisimple. An R-module W and the corresponding representation $\varrho : R \to \mathrm{End}(W)$ are called *decomposable* if W splits into a direct sum of two nonzero R-submodules. Otherwise, W is called *indecomposable*. Note that every irreducible representation is completely reducible and indecomposable.

Exercise 5.3 Convince yourself that for every set of linear operators $X \subset \mathrm{End}\, W$ and vector subspaces $U_1, U_2 \subset W$, the conditions $XU_1 \subset U_2$ and $\mathrm{Ass}(X)U_1 \subset U_2$ are equivalent. Use this to show that (semi)simplicity or (in)decomposability of

W considered as an R-module implies the corresponding property of W as an A_R-module.

Example 5.1 (Representations of One Operator) Let the set R consist of a single element t. Then $A_R \simeq \Bbbk[t]$. To assign a representation

$$\varrho : R \to \operatorname{End} W$$

means to pick a linear operator $f = \varrho(t) : W \to W$. This provides W with the structure of a $\Bbbk[t]$-module. The corresponding homomorphism

$$\widetilde{\varrho} = \mathrm{ev}_f : \Bbbk[t] \to \operatorname{End}(W), \quad t \mapsto f, \tag{5.2}$$

takes a polynomial $F \in \Bbbk[t]$ to the linear map $F(f) : W \to W$ obtained by the substitution $t = f$ in the polynomial $F(t)$. If $\dim_\Bbbk W < \infty$, then the homomorphism (5.2) must have nonzero kernel $\ker \mathrm{ev}_f = (\mu_f)$, where μ_f is the monic polynomial of minimal degree such that $\mu_f(f) = 0$. Recall[1] that μ_f is called the *minimal polynomial* of f. The subalgebra $\operatorname{Ass}(f) = \operatorname{im} \widetilde{\varrho} \subset \operatorname{End} W$ consists of all linear operators on W represented as polynomials in f. It is isomorphic to the quotient algebra $\Bbbk[t]/(\mu_f)$. The elementary divisor theorem[2] implies that every $\Bbbk[t]$-module W of finite dimension over $\Bbbk$ is isomorphic to a direct sum of quotient modules

$$\frac{\Bbbk[t]}{(p_1^{m_1})} \oplus \frac{\Bbbk[t]}{(p_2^{m_2})} \oplus \cdots \oplus \frac{\Bbbk[t]}{(p_s^{m_s})}, \tag{5.3}$$

where all $p_i \in \Bbbk[t]$ are monic irreducible, and the operator f acts as multiplication by t. Two direct sums (5.3) are isomorphic if and only if they differ by a permutation of the summands. In particular, the quotient modules $\Bbbk[t]/(p^m)$ give a complete list of mutually nonisomorphic indecomposable $\Bbbk[t]$-modules. We have seen in Sect. 15.1.3 of Algebra I that the indecomposable module $\Bbbk[t]/(p^m)$ is simple if and only if $m = 1$. Thus the semisimple $\Bbbk[t]$-modules are exhausted by the sums (5.3) with all m_i equal to 1.

Example 5.2 (Commuting Operators) In Sect. 15.3.3 of Algebra I, we have seen that for every set $R \subset \operatorname{End}_\Bbbk W$ of pairwise commuting operators over an algebraically closed field $\Bbbk$ there exists an R-invariant subspace of dimension one in W. This means that every irreducible representation of every set of commuting operators over an algebraically closed field has to be of dimension one. Also, we have seen that every set of commuting diagonalizable linear operators (over an arbitrary field) can be simultaneously diagonalized in a common basis. Hence, every vector space W equipped with an action of a set R of commuting diagonalizable

[1] See Sect. 15.1.5 of Algebra I.

[2] See Algebra I, Theorem 14.4 in Sect. 14.3.1 and the discussion in Sect. 15.1.3.

operators splits into a direct sum of R-submodules of dimension one. In particular, W is completely reducible in this case.

Lemma 5.1 *Let W be an R-module (not necessarily of finite dimension over $\Bbbk$) linearly generated over $\Bbbk$ by a set $\mathcal{S}$ of simple R-submodules. Then for every proper R-submodule $U \subsetneq W$, there exists a complementary R-submodule $V \subset W$ such that $W = U \oplus V$ and V splits into a direct sum of submodules from $\mathcal{S}$. For $U = 0$, this means that W itself is such a direct sum. In particular, W is semisimple.*

Proof Since $U \neq W$ and W is spanned by submodules $S \in \mathcal{S}$, there exists $S \not\subset U$ in $\mathcal{S}$. Then the sum $U + S$ is a direct sum, because S is simple, and therefore $S \cap U \subsetneq S$ is zero. Write $\mathcal{S}'$ for the set of semisimple submodules $M \subset W$ decomposable into a direct sum of simple modules from $\mathcal{S}$ and such that the sum $U + M$ is a direct sum. Then $\mathcal{S}'$ is nonempty and partially ordered by the relation $M_1 < M_2$, meaning that $M_2 = M_1 \oplus M$ for some $M \in \mathcal{S}'$.

Exercise 5.4 Verify that the poset $\mathcal{S}'$ is complete.[3]

By Zorn's lemma,[4] there exists a maximal element V in $\mathcal{S}'$. We claim that $U \oplus V = W$. Indeed, otherwise, we could repeat the previous arguments for $U \oplus V$ in the role of U and find a simple submodule $S \subset W$ such that the sum $(U \oplus V) + S$ was a direct sum. Then $V \oplus S \in \mathcal{S}'$ would be strictly bigger than V. Everything just said works for $U = 0$ as well. □

Lemma 5.2 *Let W be an R-module such that every nonzero proper submodule of W contains a simple R-submodule.*[5] *Then W is semisimple if and only if every nonzero proper R-submodule $U \subsetneq W$ admits a complementary R-submodule $V \subset W$ such that $W = U \oplus V$.*

Proof Let every nonzero proper submodule $M \subset W$ have a complementary submodule. Write $\mathcal{S}$ for the set of all semisimple submodules $S \subseteq W$ partially ordered by the relation $S_1 < S_2$, meaning that $S_2 = S_1 \oplus S$ for some $S \in \mathcal{S}$. The poset $\mathcal{S}$ is nonempty and complete. We claim that (every) maximal element $M \in \mathcal{S}$ coincides with W. Indeed, otherwise, there would exist a nonzero submodule $V \subset W$ such that $W = M \oplus V$ and a simple submodule $S \subset V$. This would force $M \oplus S \in \mathcal{S}$ to be bigger than M. The converse implication follows from Theorem 5.1 applied to the set $\mathcal{S}$ of all simple submodules in W. □

Theorem 5.1 (Semisimplicity Criteria) *Let W be an R-module such that every R-submodule of W contains a finite-dimensional R-submodule. Then the following properties of W are equivalent:*

1. *W is semisimple.*
2. *W is linearly generated over $\Bbbk$ by simple R-submodules.*

---

[3]That is, every totally ordered subset of $\mathcal{S}'$ has an upper bound; see Sect. 1.4.3 of Algebra I.

[4]See Sect. 1.4.3 of Algebra I.

[5]This holds, for example, if the A_R-orbit of every vector $w \in W$ is finite-dimensional over $\Bbbk$. In this case, an A_R-invariant subspace of minimal dimension contained in the orbit has to be a simple A_R-module.

3. *For every nonzero proper R-submodule $U \subsetneq W$, there exists an R-submodule $V \subset W$ such that $W = U \oplus V$.* □

Proof For a finite-dimensional R-module U, every R-submodule $S \subset U$ of minimal nonzero dimension has to be simple. Thus, the assumption of Lemma 5.2 holds. Therefore, (3) ⇒ (1). Certainly, (1) ⇒ (2). Implication (2) ⇒ (3) follows from Lemma 5.1. □

5.1.3 Homomorphisms of Representations

Given two representations $\varrho_1 : R \to \mathrm{End}(W_1)$, $\varrho_2 : R \to \mathrm{End}(W_2)$ of a set R, a linear map $\varphi : W_1 \to W_2$ is called *R-linear* or a *homomorphism* of R-modules[6] if it commutes with all operators from R, that is, the diagram

$$\begin{tikzcd} W_1 \arrow[r, "\varphi"] & W_2 \\ W_1 \arrow[u, "\varrho_1(f)"] \arrow[r, "\varphi"] & W_2 \arrow[u, "\varrho_2(f)"'] \end{tikzcd}$$

is commutative for all $f \in R$. The set of all R-linear maps $\varphi : W_1 \to W_2$ is denoted by

$$\mathrm{Hom}_R(W_1, W_2) \stackrel{\text{def}}{=} \{\varphi : W_1 \to W_2 \mid \forall\, w \in W_1,\ \forall f \in R\ \varphi(fw) = f\varphi(w)\}.$$

Exercise 5.5 Check that **(a)** $\mathrm{Hom}_R(W_1, W_2) = \mathrm{Hom}_{A_R}(W_1, W_2)$ is a vector subspace in $\mathrm{Hom}_{\Bbbk}(W_1, W_2)$, **(b)** the composition of R-linear maps is R-linear, **(d)** the kernel and image of every R-linear map are R-submodules.

Lemma 5.3 (Schur's Lemma) *Every nonzero homomorphism of simple R-modules $\varphi : U \to W$ is an isomorphism. If the ground field $\Bbbk$ is algebraically closed, then the R-linear endomorphisms of a simple R-module U are exhausted by the scalar operators $\lambda \cdot \mathrm{Id}_U$ with $\lambda \in \Bbbk$.*

Proof Since $\ker\varphi \subset U$ is R-invariant, either $\ker\varphi = U$ or $\ker\varphi = 0$. In the first case, $\varphi = 0$. In the second, $\mathrm{im}\,\varphi \subset W$ is a nonzero R-submodule, and therefore $\mathrm{im}\,\varphi = W$. Hence, φ is bijective. If $\Bbbk$ is algebraically closed, then an R-linear endomorphism $\varphi : U \to U$ possesses an eigenvector, i.e., $\ker(\lambda \cdot \mathrm{Id}_U - \varphi) \neq 0$ for some $\lambda \in \Bbbk$. Since the map $\lambda \cdot \mathrm{Id}_U - \varphi$ also is R-linear, its kernel is a nonzero R-submodule in U. This forces $\ker(\lambda \cdot \mathrm{Id}_U - \varphi) = U$, i.e., $\varphi = \lambda \mathrm{Id}_U$. □

[6] Also called an *intertwining map* or a *homomorphism* of representations.

Corollary 5.1 *Let U, W be irreducible R-modules over an algebraically closed field. Then*

$$\dim \mathrm{Hom}_R(U, W) = \begin{cases} 0 & \text{if } U \not\simeq W, \\ 1 & \text{if } U \simeq W. \end{cases}$$

Proof If there is an R-linear isomorphism $\psi : U \xrightarrow{\sim} W$, then for every $\varphi \in \mathrm{Hom}(U, W)$, the equality $\psi^{-1}\varphi = \lambda \cdot \mathrm{Id}_U$ holds for some $\lambda \in \Bbbk$ by Schur's lemma. Hence $\varphi = \lambda\psi$. □

Corollary 5.2 *A quotient module of a semisimple R-module is semisimple.*

Proof Let $\pi : W \twoheadrightarrow U$ be an R-linear surjection. Then for every simple R-submodule $S \subset W$, its image $\pi(S) \subset U$ is either zero or simple. Thus if W is spanned by simple submodules, then so is U. □

Proposition 5.1 *Under the assumptions of Theorem 5.1 on p. 102, an R-module W is semisimple if and only if for every submodule $U \subset W$, there exists an R-linear endomorphism $\pi_U \in \mathrm{End}_R(W)$ such that $\pi_U^2 = \pi_U$ and $\mathrm{im}\,\pi_U = U$.*

Proof We have seen in Example 15.3 of Algebra I that every linear endomorphism $\pi : V \to V$ satisfying the relation $\pi^2 = \pi$ projects V onto $\mathrm{im}\,\pi$ along $\ker\pi$, i.e., $V = \ker\pi \oplus \mathrm{im}\,\pi$ and $\pi(u) = u$ for all $u \in \mathrm{im}\,\pi$. Since π_U is R-linear, both $\ker\pi_U$ and $\mathrm{im}\,\pi_U$ are R-submodules in W by Exercise 5.5. Thus, the existence of π_U is equivalent to condition (3) of Theorem 5.1. □

Corollary 5.3 *A submodule of a semisimple R-module is semisimple.*

Proof Let W be a semisimple R-module, and $L \subsetneq W$ an R-submodule. Then for every R-submodule $U \subset L$, there exists an R-linear projector $W \twoheadrightarrow U$. Its restriction to L gives the required projector $L \twoheadrightarrow U$. □

5.2 Representations of Associative Algebras

5.2.1 Double Centralizer Theorem

Let A be an associative algebra over an arbitrary field $\Bbbk$, and let V be a vector space over $\Bbbk$. A homomorphism of $\Bbbk$-algebras $\varrho : A \to \mathrm{End}\,V$ is called a *linear representation* of the algebra A by endomorphisms of V. In this case, the vector space V is called an *A-module*. All notions related to linear representations of sets make sense for A-modules as well. In particular, given two A-modules U, W, we write

$$\mathrm{Hom}_A(U, W) \stackrel{\text{def}}{=} \{\varphi : U \to W \mid \forall f \in A,\ \forall u \in U\ \varphi(fu) = f\varphi(u)\}$$

for the space of *A-linear* maps $\varphi : U \to W$. For $U = W$, the A-linear endomorphisms of W form an associative $\Bbbk$-subalgebra $\mathrm{End}_A(W) \subset \mathrm{End}_{\Bbbk}(W)$ in the algebra of all linear endomorphisms of W. The subalgebra $\mathrm{End}_A(W)$ is often called the *centralizer* of A in $\mathrm{End}_{\Bbbk}(W)$.

If W splits into a direct sum of A-modules $W = V_1 \oplus V_2 \oplus \cdots \oplus V_n$, we write $\iota_\nu : V_\nu \hookrightarrow W$ for the inclusion of the νth summand in W and $\pi_\mu : W \twoheadrightarrow V_\mu$ for the projections of W onto the μth summand.

Exercise 5.6 Verify the relations $\sum_\nu \iota_\nu \pi_\nu = \mathrm{Id}_W$, $\pi_\nu \iota_\nu = \mathrm{Id}_{V_\nu}$ for all ν, $\pi_\nu \iota_\mu = 0$ and $\iota_\mu \pi_\nu = 0$ for all $\mu \neq \nu$.

For every $\varphi \in \mathrm{End}(W)$, we put $\varphi_{\mu\nu} \stackrel{\text{def}}{=} \pi_\mu \circ \varphi \circ \iota_\nu$ and arrange the maps

$$\varphi_{\mu\nu} : V_\nu \to V_\mu$$

into the square matrix $\left(\varphi_{\mu\nu}\right)$. Note that φ is uniquely recovered from this matrix by the formula

$$\varphi = \mathrm{Id}_W \circ \varphi \circ \mathrm{Id}_W = \left(\sum_\mu \iota_\mu \pi_\mu\right) \circ \varphi \circ \left(\sum_\nu \iota_\nu \pi_\nu\right) = \sum_{\mu,\nu} \iota_\mu \varphi_{\mu\nu} \pi_\nu,$$

and $\varphi \in \mathrm{End}_A(W)$ if and only if all $\varphi_{\mu\nu}$ are in $\mathrm{Hom}_A(V_\nu, V_\mu)$. Therefore, there is an isomorphism of vector spaces

$$\mathrm{End}_A(W) \xrightarrow{\sim} \bigoplus_{\mu,\nu} \mathrm{Hom}_A(V_\nu, V_\mu), \quad \varphi \mapsto \left(\varphi_{\mu\nu}\right). \tag{5.4}$$

Exercise 5.7 Verify that isomorphism (5.4) takes the composition of endomorphisms to the multiplication of matrices.

In particular, if all $V_\nu = V$ are copies of the same A-module V, then the isomorphism (5.4) becomes an isomorphism of $\Bbbk$-algebras

$$\mathrm{End}_A\left(V^{\oplus n}\right) \simeq \mathrm{Mat}_n\left(\mathrm{End}_A(V)\right). \tag{5.5}$$

Theorem 5.2 (Double Centralizer Theorem) *Let V be a finite-dimensional vector space over $\Bbbk$, let $A \subset \mathrm{End}(V)$ be an associative $\Bbbk$-subalgebra, and let $B = \mathrm{End}_A(V)$. If V is a semisimple A-module, then $\mathrm{End}_B(V) = A$.*

Proof The inclusion $A \subset \mathrm{End}_B(V)$ follows from the definition of centralizer. To establish the opposite inclusion, we fix some basis $e_1, e_2, \ldots, e_n$ of V over $\Bbbk$ and for every $\varphi \in \mathrm{End}_B(V)$, indicate an element $a \in A$ such that $\varphi e_i = a e_i$ for all i. This forces $\varphi = a$. Write $W = V^{\oplus n}$ for the direct sum of n copies of V and consider the *diagonal representation* of $\mathrm{End}_{\Bbbk}(V)$ in W, which takes $f \in \mathrm{End}_{\Bbbk}(V)$ to the linear map

$$\widetilde{f} : W \to W, \quad (v_1, v_2, \ldots, v_n) \mapsto (fv_1, fv_2, \ldots, fv_n).$$

In terms of the isomorphism (5.5), the endomorphism $\widetilde{f}$ is represented by the constant diagonal matrix fE. Restricting the diagonal representation to the subalgebras $A, B, \mathrm{End}_B(V) \subset \mathrm{End}_{\Bbbk}(V)$ provides W with module structures over these three subalgebras. Consider the vector $e = (e_1, e_2, \dots, e_n) \in W$. We have to show that $\widetilde{\varphi}e \in Ae$ for every $\varphi \in \mathrm{End}_B(V)$. Since W is a semisimple A-module, there exists an A-linear projector $\pi : W \twoheadrightarrow Ae$ that acts identically on the A-submodule $Ae \subset W$. If π commutes with $\widetilde{\varphi}$, then $\widetilde{\varphi}(e) = \widetilde{\varphi}(\pi e) = \pi(\widetilde{\varphi}e) \in Ae$, as required. Thus, it is enough to verify that $\pi\widetilde{\varphi} = \widetilde{\varphi}\pi$. Let $\left(\pi_{\mu\nu}\right) \in \mathrm{Mat}_n\left(\mathrm{End}_{\Bbbk}(V)\right)$ be the matrix of π. This is an $n \times n$ matrix with elements $\pi_{ij} \in \mathrm{End}_A(V) = B$. The endomorphism $\widetilde{\varphi}$ has the constant diagonal matrix φE, whose diagonal element $\varphi \in \mathrm{End}_B(V)$ commutes with all $\pi_{\mu\nu}$. Hence, the matrices of π and $\widetilde{\varphi}$ commute. □

Corollary 5.4 (Burnside's Theorem) *Let V be a finite-dimensional vector space over an algebraically closed field $\Bbbk$, and $R \subset \mathrm{End}_{\Bbbk}(V)$ a set of operators. If V is simple as an R-module, then the associative envelope $\mathrm{Ass}(R)$ is equal to $\mathrm{End}_{\Bbbk}(V)$. In particular, every finite-dimensional irreducible representation $A \to \mathrm{End}_{\Bbbk}(V)$ of an associative $\Bbbk$-algebra A is surjective.*

Proof By Schur's lemma,[7] $\mathrm{End}_{\mathrm{Ass}(R)}(V) = \Bbbk$. Therefore, $\mathrm{End}_{\Bbbk}(V) = \mathrm{Ass}(R)$ by Theorem 5.2. □

Exercise 5.8 Prove that over every field $\Bbbk$, the equality $\mathrm{Ass}(R) = \mathrm{End}_{\Bbbk}(V)$ forces V to be a simple R-module.

5.2.2 Digression: Modules Over Noncommutative Rings

Modules over associative algebras are particular examples of modules over rings. Let R be a ring, not necessarily commutative. An abelian group M is called a *left R-module* if M is equipped with a *left action* of R, that is, with a map

$$R \times M \to M\,, \quad (\lambda, a) \mapsto \lambda a\,,$$

such that

$$\lambda(\mu a) = (\lambda\mu)a \quad \forall\, a \in M,\ \forall\, \lambda, \mu \in K, \tag{5.6}$$

$$(\lambda + \mu)a = \lambda a + \mu a \quad \forall\, a \in M,\ \forall\, \lambda, \mu \in K, \tag{5.7}$$

$$\lambda(a + b) = \lambda a + \lambda b \quad \forall\, \lambda \in K,\ \forall\, a, b \in K. \tag{5.8}$$

Symmetrically, a *right action* of R on M is a map

$$M \times R \to M\,, \quad (a, \lambda) \mapsto a\lambda\,,$$

[7] See Lemma 5.3 on p. 103.

such that

$$(a\mu)\lambda = a(\mu\lambda) \quad \forall\, a \in M,\ \forall\, \lambda, \mu \in K, \tag{5.6$'$}$$

$$a(\lambda + \mu) = a\lambda + a\mu \quad \forall\, a \in M,\ \forall\, \lambda, \mu \in K, \tag{5.7$'$}$$

$$(a + b)\lambda = a\lambda + b\lambda \quad \forall\, \lambda \in K,\ \forall\, a, b \in K, \tag{5.8$'$}$$

and an abelian group equipped with a right action of R is called a *right R-module*. The last two properties (5.7), (5.8) and (5.7′), (5.8′) of left and right actions mean the same, namely, that the action of R on M is distributive with respect to the additions in both R and M. The left action differs from the right only in the first property, which says that the multiplication of a vector $a \in M$ by $\mu \in R$ followed by the multiplication of the result by $\lambda \in R$ coincides with the multiplication of a by $\lambda\mu$ in the left action, and by $\mu\lambda$ in the right. In other words, the right action of R is the same as the left action of the *opposite ring* R^{opp}, which coincides with R as a set but has the reversed order of operands in the products, i.e., the product $\lambda\mu$ in R^{opp} is defined to be the product $\mu\lambda$ in R. Thus, for a commutative ring R, there is no difference between the left and right R-module structures.

If a ring R has a unit element $1 \in R$ and a left (respectively, right) action of R on M satisfies the extra property $1 \cdot a = a$ (respectively, $a \cdot 1 = a$) for all $a \in M$, then the R-module M is called a *unital* module. For example, the unital modules over a field $\Bbbk$ are exactly the vector spaces over $\Bbbk$. A linear representation of an associative $\Bbbk$-algebra A with unit $\varrho : A \to \operatorname{End}_{\Bbbk}(W)$ provides W with the structure of a left unital module over A with the action $aw \overset{\text{def}}{=} \varrho(a)w$. Conversely, every left unital A-module W is a vector space over $\Bbbk = \Bbbk \cdot 1 \subset A$, and the map $A \to \operatorname{End}_{\Bbbk}(W)$ sending an element $a \in A$ to the linear endomorphism $w \mapsto aw$ assigns a linear representation of A in W. Thus, the abstract algebraic notion of (left unital) module over a ring agrees with that used above. In what follows, a module over an associative $\Bbbk$-algebra A always means a left unital A-module by default.

5.3 Isotypic Components

Let us fix an associative $\Bbbk$-algebra A and a simple A-module U. For every A-module W, the tensor product of vector spaces $\operatorname{Hom}_A(U, W) \otimes U$ admits the natural action of A by the rule $a(\varphi \otimes u) \overset{\text{def}}{=} \varphi \otimes (au)$ for all $a \in A$, $\varphi \in \operatorname{Hom}_A(U, W)$, $u \in U$. There is also the canonical A-linear *contraction map*

$$c_{UW} : \operatorname{Hom}_A(U, W) \otimes U \to W, \quad \varphi \otimes u \mapsto \varphi(u). \tag{5.9}$$

The image of this map is denoted by $W_U \subset W$ and called the *U-isotypic component* of W. It coincides with the $\Bbbk$-linear span of all simple submodules of W isomorphic to U. Indeed, since all nonzero A-linear maps $\psi : U \to W$ map U isomorphically onto some simple submodule $\psi(U) \subset W$, every vector of the form $\sum \psi_i(u_i) \in W$,

$u_i \in U$, $\psi_i \in \mathrm{Hom}_A(U, W)$, lies in the linear span of such simple submodules. Conversely, if vectors $v_i \in \mathrm{im}\,\psi_i$ belong to the images of some A-liner inclusions $\psi_i : U \hookrightarrow W$, then $\sum v_i = c_{UW}\left(\sum \psi_i \otimes \psi_i^{-1} v_i\right)$.

Proposition 5.2 *For every A-linear map $\varphi : V \to W$, the image of the U-isotypic component $V_U \subset V$ belongs to the U-isotypic component $W_U \subset W$. In particular, $V_U = V \cap W_U$ for every A submodule $V \subset W$.*

Proof Every vector of the form $\sum \psi_i(u_i)$, $\psi_i \in \mathrm{Hom}_A(U, V)$, $u_i \in U$, is mapped to $\sum \varphi\psi_i(v)$, where $\varphi\psi_i \in \mathrm{Hom}_A(U, W)$, $u_i \in U$. □

Proposition 5.3 *Over an algebraically closed ground field $\Bbbk$, the contraction map (5.9) is injective and therefore establishes the canonical isomorphism*

$$c_{UW} : \mathrm{Hom}_A(U, W) \otimes U \xrightarrow{\sim} W_U .$$

Proof Since W_U is linearly spanned by simple submodules isomorphic to U, it follows from Lemma 5.1 applied to the set $\mathcal{S}$ of these submodules that W_U splits into a direct sum

$$W_U = V_1 \oplus V_2 \oplus \cdots \oplus V_s, \text{ where } V_i \simeq U \text{ for all } i. \tag{5.10}$$

Fix some A-linear inclusions $\psi_i : U \hookrightarrow W$ with $\psi_i(U) = V_i$. Then

$$\mathrm{Hom}_A(U, W) \simeq \mathrm{Hom}_A(U, W_U) \simeq \bigoplus_i \mathrm{Hom}_A(U, V_i).$$

By Corollary 5.1, the space $\mathrm{Hom}_A(U, V_i) \simeq \Bbbk \cdot \psi_i$ has dimension 1 and basis ψ_i. Therefore, every element of $\mathrm{Hom}_A(U, W) \otimes U$ is uniquely represented as $\sum \psi_i \otimes u_i$ with $u_i \in U$. If $c_{UW}\left(\sum \psi_i \otimes u_i\right) = \sum \psi_i(u_i) = 0$, then every vector $\psi_i(u_i)$ vanishes, because all these vectors lie in different components of the direct sum (5.10). Since all ψ_i are injective, all u_i are equal to 0. □

Proposition 5.4 (Isotypic Decomposition) *Let $W = \bigoplus_i V_i$, where all V_i are simple A-modules. Then the sum of all the V_i that are isomorphic to U coincides with the U-isotypic component $W_U \subset W$. In particular, this sum does not depend on the choice of decomposition $W = \bigoplus_i V_i$, and therefore, every semisimple A-module W admits the unique direct sum decomposition*

$$W = \bigoplus_{[U]} W_U, \tag{5.11}$$

where the summation is over all isomorphism classes $[U]$ of simple A-modules U such that $\mathrm{Hom}_A(U, W) \neq 0$.

Proof Since $\mathrm{Hom}_A(U, W) = \bigoplus_i \mathrm{Hom}_A(U, V_i)$ and $\mathrm{Hom}_A(U, V_j) = 0$ for all $V_j \not\simeq U$, the image of the canonical contraction (5.9) is contained in the sum of the V_i that are isomorphic to U. □

Definition 5.1 Let W be a semisimple module over an associative algebra A. The decomposition (5.11) is called the *isotypic decomposition*. For every class $[U]$ of isomorphic simple A-modules, the projection $W \twoheadrightarrow W_U$ along all the other isotypic components is called the *U-isotypic projection*, and the number

$$m_U \stackrel{\text{def}}{=} \frac{\dim W_U}{\dim U} \tag{5.12}$$

is called the *multiplicity* of U in W. By Proposition 5.4, for every decomposition $W = \bigoplus_i V_i$ into a direct sum of simple A-submodules $V_i \subset W$, the multiplicity m_U equals the number of summands V_i isomorphic to U.

Corollary 5.5 *For every pair of finite-dimensional semisimple A-modules V, W over an algebraically closed field $\Bbbk$, one has*

$$\dim \mathrm{Hom}_A(V, W) = \sum_{[U]} m_U(U) \cdot m_U(W) = \dim \mathrm{Hom}_A(W, V),$$

where the summation is over all isomorphism classes $[U]$ of simple A-modules U.

Proof Let $V = \oplus V_i$, $W = \oplus W_j$, where all V_i, W_j are simple. By Schur's lemma, the space $\mathrm{Hom}_A(V_i, W_j)$ is zero for $V_i \not\simeq W_j$ and has dimension 1 for $V_i \simeq W_j$. Therefore, the space $\mathrm{Hom}_A(V, W) = \oplus_{ij} \mathrm{Hom}_A(V_i, W_j)$ has dimension $\sum_U m_U(U) \cdot m_U(W)$. The same holds for the space $\mathrm{Hom}_A(W, V)$ as well. □

5.4 Representations of Groups

5.4.1 Direct Sums and Tensor Constructions

An action of a group G on a vector space V by linear automorphisms of V, that is, a group homomorphism $\varrho : G \to \mathrm{GL}(V)$, is called a *linear representation* of G in V. We say in this case that V is a *G-module*. For G-modules U, W, the direct sum $U \oplus W$, tensor product $U \otimes W$, symmetric powers $S^n U$, and exterior powers $\Lambda^n U$ inherit natural structures of G-modules with the action of $g \in G$ by the rules

$$g(u + w) \stackrel{\text{def}}{=} gu + gw, \quad g(u \otimes w) \stackrel{\text{def}}{=} (gu) \otimes (gw),$$
$$g(u_1 \cdot u_2) \stackrel{\text{def}}{=} (gu_1) \cdot (gu_2), \quad g(u_1 \wedge u_2) \stackrel{\text{def}}{=} (gu_1) \wedge (gu_2).$$

For every G-submodule $V \subset W$, the quotient space W/V is a G-module with the action $g[v] \stackrel{\text{def}}{=} [gv]$.

Exercise 5.9 Verify that the above formulas give well-defined group homomorphisms from G to $\mathrm{GL}(U \oplus W)$, $\mathrm{GL}(U \otimes W)$, $\mathrm{GL}(\Lambda U)$, $\mathrm{GL}(SU)$, and $\mathrm{GL}(W/V)$ respectively.

Given a linear representation $\varrho : G \to \mathrm{GL}(V)$ of a group G, the *dual representation*

$$\varrho^* : G \to \mathrm{GL}(V^*)$$

is defined by the requirement that the action of G leave invariant the contraction between vectors and covectors, i.e., that the equality $\langle\, \varrho^*(g)\xi,\, \varrho(g)v\,\rangle = \langle\, \xi,\, v\,\rangle$ holds for all $g \in G$, $\xi \in V^*$, $v \in V$. Since all the operators $\varrho(g)$ are invertible, this condition means that

$$\langle\, \varrho^*(g)\xi,\, v\,\rangle = \left\langle \xi,\, \varrho\left(g^{-1}\right) v\right\rangle.$$

Therefore, the operator $\varrho^*(g) = \varrho\left(g^{-1}\right)^*$ is dual[8] to the operator $\varrho(g)^{-1}$ for every $g \in G$. In particular, the matrices of operators $\varrho^*(g)$, $\varrho(g)$ in every pair of dual bases of V and V^* are inverse transposes of each other.

Exercise 5.10 Verify that $\varrho^* : G \to \mathrm{GL}(V^*)$, $g \mapsto \varrho\left(g^{-1}\right)^*$, is a group homomorphism.

For every pair of representations $\varrho : G \to \mathrm{GL}(U)$, $\lambda : G \to \mathrm{GL}(W)$, the representation $\varrho^* \otimes \lambda$ provides the space $U^* \otimes V \simeq \mathrm{Hom}(U, V)$ of linear maps $\varphi : U \to V$ with the action G by the conjugations

$$g : \varphi \mapsto g\varphi g^{-1}. \tag{5.13}$$

Exercise 5.11 Check this.

Thus, the space of G-linear maps

$$\mathrm{Hom}_G(U, V) = \{\varphi : U \to V \mid \forall\, g \in G\;\, g\varphi = \varphi g\}$$

is exactly the space of G-invariant vectors in the representation (5.13).

Lemma 5.4 *Let G be a finite group of order $|G| = n$. Assume that* $\mathrm{char}\,\Bbbk \nmid n$*, and that the polynomial $t^n - 1$ completely splits over $\Bbbk$ into a product of n linear factors. Then in every (not necessarily finite-dimensional) G-module V, all elements of G are represented by operators that are diagonalizable over $\Bbbk$.*

Proof Since $g^{|G|} = e$ for all $g \in G$, every operator $g \in G$ in a linear representation of G is annihilated by the polynomial $f(t) = t^n - 1$. By our assumption, f is a product

[8]That is, it takes every $\xi : V \to \Bbbk$ to the composition $\xi \circ g^{-1} : v \mapsto \xi\left(g^{-1}v\right)$; see Sect. 7.3 of Algebra I.

of n linear factors, which are all distinct, because $f' = nt^{n-1} \neq 0$ is coprime to f. We know from Sect. 15.2.6 of Algebra I that this forces g to be diagonalizable on every finite-dimensional g-invariant subspace. Since the G-orbit of every vector v spans a finite-dimensional g-invariant subspace containing v, the whole space is linearly generated by the eigenvectors of g. Hence, g is diagonalizable. □

Exercise 5.12 Convince yourself that a linear operator g on a vector space V (not necessarily finite-dimensional) is diagonalizable if and only if V is linearly spanned by the eigenvectors of g.

5.4.2 Representations of Finite Abelian Groups

Everywhere in this section we assume that G is a finite abelian group and that a ground field $\Bbbk$ is algebraically closed with $\operatorname{char}(\Bbbk) \nmid |G|$.

It follows from Lemma 5.4 and Example 5.2 on p. 101 that every linear representation of G is a direct sum of simple G-modules of dimension one. Since every linear operator on a one-dimensional space is a scalar homothety $v \mapsto \lambda v$, every simple G-module V provides G with a multiplicative homomorphism $\chi_V : G \to \Bbbk^*$ mapping $g \in G$ to the coefficient of the homothety by which g acts on V, i.e.,

$$gv = \chi_V(g) \cdot v$$

for all $g \in G$, $v \in V$. Conversely, every multiplicative homomorphism $\chi : G \to \Bbbk^*$ allows us to construct a simple G-module V_χ of dimension one on which every $g \in G$ acts as $g : v \mapsto \chi(g) \cdot v$.

Exercise 5.13 Verify that $V_\chi \simeq V_\psi$ as G-modules if and only if $\chi = \psi$ as maps $G \to \Bbbk^*$.

Multiplicative homomorphisms $G \to \Bbbk^*$ are called *multiplicative characters* of G. Therefore, the isomorphism classes of irreducible representations of G are bijectively numbered by the multiplicative characters of G.

Since $\chi^{|G|}(g) = \chi\left(g^{|G|}\right) = \chi(e) = 1$ for every $g \in G$, every multiplicative character of G takes values in the finite group $\boldsymbol{\mu}_{|G|}(\Bbbk) \subset \Bbbk^*$ of $|G|$th roots of unity in $\Bbbk$. All the multiplicative characters form an abelian multiplicative subgroup in the $\Bbbk$-algebra $\Bbbk^G$ of all functions $G \to \Bbbk$. This group is denoted by $G^\wedge$ and called the *Pontryagin dual* to G. The identity element of $G^\wedge$ is the *trivial character* $\chi = 1$, corresponding to the *trivial representation* in which every $g \in G$ acts by the identity map.

Exercise 5.14 Verify that $\chi_{U \otimes W} = \chi_U \chi_W$ and $\chi_{U^*} = \chi_U^{-1}$ for every pair of simple G-modules U, W.

Consider the action of G on the space $\Bbbk^G$ of all functions $f : G \to \Bbbk$ by the rule $g : f(x) \mapsto f(gx)$. The χ-isotypic component of this representation consists of all functions $f : G \to \Bbbk$ such that $f(gx) = \chi(g)f(x)$ for all $x, g \in G$. For $x = e$, this forces $f(g) = \chi(g) \cdot f(e)$ for all $g \in G$. Therefore, every function f lying in the isotypic component $\Bbbk_\chi^G$ is proportional to the character χ. We conclude that $\dim \Bbbk_\chi^G = 1$ for every $\chi \in G^\wedge$, and the isotypic decomposition of $\Bbbk^G$ looks like

$$\Bbbk^G = \bigoplus_{\chi \in G^\wedge} \Bbbk \cdot \chi.$$

In particular, $|G^\wedge| = |G|$, and the multiplicative characters form a basis of the space $\Bbbk^G$.

Exercise 5.15 Prove that for every (not necessarily algebraically closed) field $\Bbbk$ and (not necessarily abelian) group G, an arbitrary set of distinct multiplicative homomorphisms $G \to \Bbbk^*$ is linearly independent in $\Bbbk^G$.

Theorem 5.3 (Pontryagin Duality) *For every finite abelian group G and $g \in G$, the evaluation map*

$$\mathrm{ev}_g : G^\wedge \to \Bbbk, \quad \chi \mapsto \chi(g),$$

is a multiplicative character of the Pontryagin dual group $G^\wedge$. The map

$$G \to G^{\wedge\wedge}, \quad g \mapsto \mathrm{ev}_g, \tag{5.14}$$

is a group isomorphism.

Proof The first statement holds because

$$\mathrm{ev}_g(\chi_1\chi_2) = \chi_1(g) \cdot \chi_2(g) = \mathrm{ev}_g(\chi_1) \cdot \mathrm{ev}_g(\chi_2).$$

Since $\mathrm{ev}_{g_1g_2}(\chi) = \chi(g_1g_2) = \chi(g_1) \cdot \chi(g_2) = \mathrm{ev}_{g_1}(\chi)\, \mathrm{ev}_{g_2}(\chi)$, the map (5.14) is a group homomorphism. If $g \in G$ lies in the kernel of (5.14), then $\chi(g) = 1$ for all $\chi \in G^\wedge$. Hence, g acts trivially in every representation of G. In particular, $f(gx) = f(x)$ for all functions $f : G \to \Bbbk$. This forces $xg = x$ for every $x \in G$, and therefore $g = e$. Since $|G^{\wedge\wedge}| = |G|$, the monomorphism (5.14) is bijective. $\square$

Remark 5.1 Pontryagin duality actually holds in all locally compact topological abelian groups G, such as $\mathbb{Z}$, $\mathrm{SU}_1 = S^1$, $\mathbb{R}$. Finite abelian groups are just the simplest examples of such groups. A good presentation of the general theory can be found in [Mo].[9]

[9] S.A. Morris, *Pontryagin Duality and the Structure of Locally Compact Abelian Groups,* London Math. Society Lecture Notes 29, Cambridge University Press (1977).

5.4.3 Reynolds Operator

Let G be an arbitrary group, not necessarily abelian, and V a linear representation of G. The vectors $v \in V$ left fixed by all linear transformations from G form a G-submodule in V, called the submodule of *G-invariants* and denoted by

$$V^G \stackrel{\text{def}}{=} \{\, v \in V \mid \forall\, g \in G\ gv = v \,\}.$$

If G is finite and $\operatorname{char} \Bbbk \nmid |G|$, then for every linear representation V of G, there exists a G-linear projector

$$V \twoheadrightarrow V^G, \quad v \mapsto v^\natural,$$

called the *Reynolds operator*. It sends a vector $v \in V$ to the barycenter[10] of the G-orbit of v in the affine space $\mathbb{A}(V)$,

$$v^\natural \stackrel{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} gv. \tag{5.15}$$

Exercise 5.16 Check by a direct computation that the Reynolds operator commutes with all $g \in G$ and projects V onto V^G for $\operatorname{char} \Bbbk \nmid |G|$.

Exercise 5.17 Give an example of an indecomposable representation V of a finite group G over a finite field $\Bbbk$ with a proper nonzero G-invariant submodule V^G.

Theorem 5.4 *Every linear representation V of a finite group G over a field $\Bbbk$ with* $\operatorname{char} \Bbbk \nmid |G|$ *is completely reducible.*[11]

Proof By Proposition 5.1 on p. 104, it is enough to show that every G-submodule $U \subset V$ admits a G-linear projector $\pi_U : V \twoheadrightarrow U$. Recall[12] that G acts on $\operatorname{Hom}_{\Bbbk}(V, U)$ as $g : \varphi \mapsto g\varphi g^{-1}$ and that G-linear maps $V \to U$ are exactly the invariants of this action. Take an arbitrary $\Bbbk$-linear projector $\pi : V \twoheadrightarrow U$ and put

$$\pi_U \stackrel{\text{def}}{=} \pi^\natural = |G|^{-1} \sum_g g\pi g^{-1} \in \operatorname{Hom}_G(V, U).$$

Then $\operatorname{im} \pi^\natural \subset U$, since $g\pi g^{-1} U \subset U$ for all $g \in G$, and every vector $u \in U$ is fixed by $\pi^\natural$, because $g^{-1}U \subset U$ and $\pi|_U = \mathrm{Id}_U$ force $g\pi g^{-1} u = gg^{-1} u = u$ for all $g \in G$. Thus, π_U projects V onto U. $\square$

[10] See Sect. 6.5.3 of Algebra I. Note that for $\operatorname{char}(\Bbbk) \mid |G|$, the sum of unit masses vanishes and the barycenter is not well defined.

[11] That is, splits as a direct sum of irreducible representations; see Sect. 5.1.2 on p. 100.

[12] See formula (5.13) on p. 110.

5.5 Group Algebras

Associated with every group G and commutative ring K is an associative K-algebra $K[G]$ called the *group algebra* of G with coefficients in K. As a K-module, $K[G] \overset{\text{def}}{=} K \otimes G$ is free with basis G, i.e., it consists of linear combinations $\sum_{g\in G} c_g\, g$ with coefficients $c_g \in K$, all but a finite number of which vanish. These linear combinations are multiplied by the standard distributivity rules under the assumption that the constants from K commute with the group elements and are multiplied within K, whereas the group elements are composed within G, i.e.,

$$\Big(\sum_g a_g g\Big)\Big(\sum_h b_h h\Big) = \sum_{g,h} a_g b_h gh = \sum_f c_f f, \tag{5.16}$$

where

$$c_f = \sum_{gh=f} a_g b_h = \sum_t a_{ft^{-1}} b_t = \sum_s a_s b_{s^{-1}f}.$$

The group G is embedded into $K[G]$ as a multiplicative subgroup. Every linear representation $\varrho : G \to \mathrm{GL}(V)$ over a field $\Bbbk$ can be uniquely extended by linearity to a representation of the group algebra $\varrho : \Bbbk[G] \to \mathrm{End}(V)$ whose image is simultaneously the linear span and associative envelope of $\varrho(G) \subset \mathrm{End}(V)$.

Exercise 5.18 Verify that the assignment $m \mapsto t^m$ establishes the isomorphisms

$$\Bbbk[\mathbb{Z}] \xrightarrow{\sim} \Bbbk[t, t^{-1}] \quad \text{and} \quad \Bbbk[\mathbb{Z}/(n)] \xrightarrow{\sim} \Bbbk[t]/(t^n - 1).$$

Example 5.3 (Reynolds Operator) The Reynolds operator from Sect. 5.4.3 can be treated as an element of the group algebra $\mathbb{Q}[G]$,

$$\pi_{\mathbb{1}} \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g\in G} g \in \mathbb{Q}[G]. \tag{5.17}$$

Every linear representation of G extended to the representation $\varrho : \mathbb{Q}[G] \to \mathrm{End}(V)$ maps $\pi_{\mathbb{1}}$ to a G-linear projector on the submodule of G-invariants

$$\varrho(\pi_{\mathbb{1}}) : V \twoheadrightarrow V^G, \quad v \mapsto v^\natural.$$

Note that it lies in the $\mathbb{Q}$-linear span of $\varrho(G)$ but not in $\varrho(G)$.

Exercise 5.19 Verify that $\pi_{\mathbb{1}} \in Z(\mathbb{Q}[G])$ lies in the center[13] of the group algebra.

[13]Recall that the *center* of a ring R consists of the elements of R commuting with every element of R, $Z(R) \overset{\text{def}}{=} \{c \in R \mid \forall\, r \in R\ cr = rc\}$.

5.5.1 Center of a Group Algebra

Recall that the *conjugacy classes* of a group G are the orbits of the adjoint action[14] of G on itself. Thus, the conjugacy class of an element $h \in G$ consists of all elements ghg^{-1}, $g \in G$, conjugate to h. We write $\mathrm{Cl}(G)$ for the set of conjugacy classes. The center of the group algebra

$$Z(\Bbbk[G]) \stackrel{\text{def}}{=} \{z \in \Bbbk[G] \mid \forall\, x \in \Bbbk[G]\ zx = xz\} = \{z \in \Bbbk[G] \mid \forall\, g \in G\ gzg^{-1} = z\}$$

consists of the linear combinations $z = \sum_h z_h h \in \Bbbk[G]$ whose coefficients z_h are constant on every conjugacy class, i.e., $z_{ghg^{-1}} = z_h$ for all $g \in G$. In particular, for a finite group G, the sums

$$z_C = \sum_{h \in C} h, \tag{5.18}$$

numbered by the conjugacy classes $C \in \mathrm{Cl}(G)$, form a basis of the vector space $Z(\Bbbk[G])$ over $\Bbbk$. Thus,

$$\dim_{\Bbbk} Z(\Bbbk[G]) = |\,\mathrm{Cl}(G)|.$$

We call this quantity the *class number* of G.

Every linear representation $\Bbbk[G] \to \mathrm{End}(V)$ maps the center $Z(\Bbbk[G])$ inside the subalgebra $\mathrm{End}_G(V)$ of G-linear endomorphisms of V. In particular, over an algebraically closed field $\Bbbk$, every central element of $\Bbbk[G]$ acts by a scalar homothety in every linear representation of G.

5.5.2 Isotypic Decomposition of a Finite Group Algebra

Everywhere in this section we assume that G is a finite group and that $\operatorname{char} \Bbbk \nmid |G|$. Let us fix some set $\mathrm{Irr}(G)$ of irreducible representations of G over $\Bbbk$ such that every simple G-module is isomorphic to exactly one element of $\mathrm{Irr}(G)$. Representations from $\mathrm{Irr}(G)$ will be denoted by $\lambda : G \to \mathrm{GL}(U_\lambda)$, and we will write $\lambda \in \mathrm{Irr}(G)$ to outline that the representation λ is irreducible. It follows from Theorem 5.4 and Proposition 5.4 on p. 108 that every finite-dimensional G-module V has the unique *isotypic decomposition*

$$V = \bigoplus_{\lambda \in \mathrm{Irr}(G)} V_\lambda, \tag{5.19}$$

[14] See Example 12.14 in Algebra I.

where $V_\lambda \in V$ is the linear span of all simple G-submodules of V isomorphic to $U_\lambda \in \mathrm{Irr}(G)$, or equivalently, the image of the contraction map

$$c : \mathrm{Hom}_G(U_\lambda, V) \otimes U_\lambda \to V, \quad \varphi \otimes u \mapsto \varphi(u). \tag{5.20}$$

Recall[15] that we write $m_\lambda(V) = \dim V_\lambda / \dim U_\lambda$ for the *multiplicity* of $\lambda \in \mathrm{Irr}(G)$ in V, which equals the number of summands isomorphic to U_λ in any decomposition of V into a direct sum of simple G-modules.

There is the *left regular representation* of G in $\Bbbk[G]$ defined by the prescription

$$g : x \mapsto gx \quad \text{for} \quad g \in G, x \in \Bbbk[G].$$

This is the $\Bbbk$-linear extension of the left regular action[16] of G on the basis G of $\Bbbk[G]$. For $\lambda \in \mathrm{Irr}(G)$, let $I_\lambda \subset \Bbbk[G]$ be the λ-isotypic component of the left regular representation. Thus,

$$\Bbbk[G] = \bigoplus_{\substack{\lambda \in \mathrm{Irr}(G) \\ m_\lambda(\Bbbk[G]) \neq 0}} I_\lambda \tag{5.21}$$

as a left $\Bbbk[G]$-module. We will see in Corollary 5.6 that $I_\lambda \neq 0$ for every irreducible representation λ of G, i.e., the summation in (5.21) actually goes over all $\lambda \in \mathrm{Irr}(G)$. But now let us analyze the decomposition (5.21) without this assumption.

Since every I_λ in (5.21) is a G-submodule, it follows that $gI_\lambda \subset I_\lambda$ for all $g \in G$. This forces every I_λ to be a left ideal of the algebra $\Bbbk[G]$. For every $h \in G$, the right multiplication by h, $x \mapsto xh$, obviously commutes with the left multiplication by an element $g \in G$, i.e., it assigns a G-linear endomorphism of the left regular representation. Thus by Proposition 5.2 on p. 108, the right multiplication by an element $h \in G$ takes every isotypic component I_λ to itself. Therefore, every I_λ is a two-sided ideal in $\Bbbk[G]$. Since $I_\lambda \cap I_\varrho = 0$ for $\lambda \neq \varrho$, and both I_λ and I_ϱ are two-sided ideals,

$$I_\lambda \cdot I_\varrho \subset I_\lambda \cap I_\varrho = 0 \quad \text{for} \quad \lambda \neq \varrho. \tag{5.22}$$

Let $\pi_\lambda : \Bbbk[G] \twoheadrightarrow I_\lambda$ be the λ-isotypic projection. Since for all $x \in \Bbbk[G]$, we have $\pi_\lambda(x) = \pi_\lambda(x \cdot e) = x \cdot \pi_\lambda(e)$, this projection coincides with the right multiplication by the element $e_\lambda = \pi_\lambda(e) \in I_\lambda$. Therefore, $I_\lambda = \Bbbk[G] \cdot e_\lambda$ is the principal left ideal generated by e_λ, and $e_\lambda \cdot e_\lambda = \pi_\lambda(e_\lambda) = e_\lambda$, whereas $e_\lambda \cdot e_\varrho = 0$ for $\lambda \neq \varrho$.

Definition 5.2 The elements e_λ are called *irreducible idempotents*, and the equality $e = \sum_{\lambda \in \mathrm{Irr}(G)} e_\lambda$ will be referred to as the *decomposition of the identity* into a sum of irreducible idempotents.

---

[15]See Definition 5.1 on p. 109.

[16]See Example 12.13 of Algebra I.

Lemma 5.5 *Let* $\varrho : \Bbbk[G] \to \mathrm{End}(V)$ *be a linear representation. If* $m_\lambda(V) = 0$*, then* $\rho(I_\lambda) = 0$.

Proof For every $v \in V$, the assignment $xe_\lambda \mapsto \varrho(xe_\lambda)v$ gives a well-defined G-linear map $I_\lambda \to V$. By Proposition 5.2, the image of this map is contained in the λ-isotypic component of V, which is zero by the assumption of the lemma. □

Corollary 5.6 *The multiplicity* $m_\lambda(\Bbbk[G]) \neq 0$ *for every irreducible* G*-module* λ*, that is,* $\Bbbk[G] = \oplus_{\lambda \in \mathrm{Irr}(G)} I_\lambda$.

Proof If there exists an irreducible G-module W that does not appear in (5.22), then $m_\lambda(W) = 0$ for all λ from (5.22). It follows from Lemma 5.5 that $\Bbbk[G]$ acts by zero on W, i.e., $W = 0$. □

Proposition 5.5 *Every linear representation* $\varrho : \Bbbk[G] \to \mathrm{End}(V)$ *maps every irreducible idempotent* e_λ*,* $\lambda \in \mathrm{Irr}(G)$*, to the* λ*-isotypic projector* $\pi_\lambda : V \twoheadrightarrow V_\lambda$.

Proof By Lemma 5.5, the left multiplication by e_λ annihilates all ideals I_ϱ with $\varrho \neq \lambda$. This forces e_λ to act by zero in every irreducible representation $\varrho \neq \lambda$. By Schur's lemma, the action of e_λ in the irreducible representation U_λ is either zero or invertible. In the first case, e_λ annihilates the whole of $\Bbbk[G]$, which is impossible, because $e_\lambda \cdot e = e_\lambda \neq 0$. Hence, e_λ acts by the invertible automorphism in the irreducible representation $\lambda : \Bbbk[G] \to \mathrm{End}(U_\lambda)$. Since $\lambda(e_\lambda)$ is a projector and $\ker \lambda(e_\lambda) = 0$, we conclude that $\lambda(e_\lambda) = \mathrm{Id}_{U_\lambda}$. Now we decompose V into a sum of irreducible G-modules and see that e_λ acts identically on each summand U_λ and annihilates all other summands. □

Corollary 5.7 *The irreducible idempotents* e_λ *belong to* $Z(\Bbbk[G])$ *and are linearly independent over* $\Bbbk$*. In particular,* $|\,\mathrm{Irr}(G)| \leqslant |\,\mathrm{Cl}(G)|$.

Proof Applying Proposition 5.5 to the left regular representation shows that left multiplication by e_λ acts identically on I_λ and annihilates all I_ϱ with $\varrho \neq \lambda$. Thus,

$$e_\lambda \sum_\varrho x_\varrho e_\varrho = x_\lambda e_\lambda = \Big(\sum_\varrho x_\varrho e_\varrho\Big) e_\lambda$$

for every $x = \sum x_\varrho e_\varrho \in \Bbbk[G]$. Hence, all e_λ are in $Z(\Bbbk[G])$. Since all e_λ belong to different components of the isotypic decomposition (5.21), they are linearly independent. □

Theorem 5.5 (Maschke's Theorem) *Let* G *be a finite group and* $\Bbbk$ *an algebraically closed field with* $\mathrm{char}\,\Bbbk \nmid |G|$*. Then an isomorphism of* $\Bbbk$*-algebras is given by the map*

$$\mathfrak{r} : \Bbbk[G] \to \bigoplus_{\lambda \in \mathrm{Irr}(G)} \mathrm{End}_\Bbbk(U_\lambda) \tag{5.23}$$

that takes an element $f \in \Bbbk[G]$ *to the family of linear endomorphisms representing* f *in all simple* G*-modules from* $\mathrm{Irr}(G)$. *The restriction of* (5.23) *to the isotypic ideal* $I_\lambda \subset \Bbbk[G]$ *establishes an isomorphism* $\mathfrak{r}\,|_{I_\lambda} : I_\lambda \xrightarrow{\sim} \mathrm{End}_\Bbbk(U_\lambda)$.

Proof Let us first show that $\mathfrak{r}$ is injective. If $h \in \Bbbk[G]$ acts by the zero operator in all irreducible representations, then h is zero in every finite-dimensional representation, because every such representation splits into a direct sum of irreducible representations. In particular, left multiplication by h in $\Bbbk[G]$ is the zero map. Therefore, $h = h \cdot e = 0$. Now let us prove the last statement of the proposition. By Lemma 5.5, every irreducible representation $\lambda : \Bbbk[G] \to \mathrm{End}(U_\lambda)$ annihilates all the direct summands of the isotypic decomposition (5.21) except for I_λ. Therefore,

$$\mathfrak{r}(I_\lambda) = \lambda(I_\lambda) = \lambda(\Bbbk[G]) \subset \mathrm{End}_\Bbbk(U_\lambda).$$

By Burnside's theorem,[17] $\lambda(\Bbbk[G]) = \mathrm{End}_\Bbbk(U_\lambda)$. Hence, $\mathfrak{r}(I_\lambda) = \mathrm{End}(U_\lambda)$. Since $\mathfrak{r}$ is injective, it maps I_λ to $\mathrm{End}_\Bbbk(U_\lambda)$ isomorphically. In particular,

$$m_\lambda(\Bbbk[G]) = \frac{\dim(I_\lambda)}{\dim(U_\lambda)} = \frac{\dim \mathrm{End}(U_\lambda)}{\dim U_\lambda} = \dim U_\lambda$$

for all $\lambda \in \mathrm{Irr}(G)$. Finally, let us check that $\mathfrak{r}$ is surjective. By the last statement of the proposition, for every element

$$\varphi = \sum_\lambda \varphi_\lambda \in \bigoplus_{\lambda \in \mathrm{Irr}(G)} \mathrm{End}_\Bbbk(U_\lambda), \text{ where } \varphi_\lambda \in \mathrm{End}_\Bbbk(U_\lambda),$$

there exists some $f_\lambda \in I_\lambda$ such that $\lambda(f_\lambda) = \varphi_\lambda$ for every λ. Then for every $\varrho \in \mathrm{Irr}(G)$, we have

$$\varrho\Big(\sum_\lambda f_\lambda\Big) = \sum_\lambda \varrho\,(f_\lambda) = \varphi_\varrho,$$

because $\varrho(f_\lambda) = 0$ for $\lambda \neq \varrho$. Thus, $\mathfrak{r}\big(\sum f_\lambda\big) = \varphi$. □

Corollary 5.8 *Under the assumptions of Theorem 5.5,* $m_\lambda(\Bbbk[G]) = \dim U_\lambda$ *for every* $\lambda \in \mathrm{Irr}(G)$*, and*

$$\sum_{\lambda \in \mathrm{Irr}(G)} \dim^2 U_\lambda = |G|. \tag{5.24}$$

Moreover, $|\,\mathrm{Irr}(G)| = |\,\mathrm{Cl}(G)|$*, and the irreducible idempotents* e_λ *form a basis of* $Z(\Bbbk[G])$.

---

[17] See Corollary 5.4 on p. 106.

Proof The equality $m_\lambda(\Bbbk[G]) = \dim U_\lambda$ was established in the proof of (5.23). Comparing the dimensions of both sides in (5.23) gives (5.24):

$$|G| = \dim \Bbbk[G] = \sum_{\lambda \in \operatorname{Irr}(G)} \dim \operatorname{End}(U_\lambda) = \sum_{\lambda \in \operatorname{Irr}(G)} \dim^2 U_\lambda .$$

Since the center $Z(\operatorname{End}_\Bbbk(V)) = \Bbbk \cdot \operatorname{Id}_V$ is formed by the one-dimensional space of scalar matrices, it follows that

$$\begin{aligned} \dim Z\Big(\prod_{\lambda \in \operatorname{Irr}(G)} \operatorname{End}(U_\lambda)\Big) &= \dim \prod_{\lambda \in \operatorname{Irr}(G)} Z\big(\operatorname{End}(U_\lambda)\big) \\ &= \dim \bigoplus_{\lambda \in \operatorname{Irr}(G)} \Bbbk \cdot \operatorname{Id}_{U_\lambda} = |\operatorname{Irr}(G)|. \end{aligned}$$

At the same time, $\dim Z(\Bbbk[G]) = |\operatorname{Cl}(G)|$ by Sect. 5.5.1 on p. 115. Thus,

$$|\operatorname{Irr}(G)| = |\operatorname{Cl}(G)|.$$

It follows from Proposition 5.5 that

$$\mathfrak{r}(e_\lambda) = (0, \dots, 0, \operatorname{Id}_{U_\lambda}, , 0, \dots, 0) \in \bigoplus_{\varrho \in \operatorname{Irr}(G)} \operatorname{End}_\Bbbk(U_\varrho).$$

Since the right-hand-side elements form a basis of $Z\big(\bigoplus_{\varrho \in \operatorname{Irr}(G)} \operatorname{End}(U_\varrho)\big)$, the irreducible idempotents form a basis in $Z(\Bbbk[G])$. □

Example 5.4 In accordance with Sect. 5.4.2, the abelian group $G = \mathbb{Z}/(3)$ has three irreducible representations of dimension 1 over $\Bbbk = \mathbb{C}$. The generator $g = [1]$ acts in these representations as multiplication by 1, ω, and ω^2 respectively, where $\omega = \big(-1 + i\sqrt{3}\big)/2 \in \mathbb{C}$ is a primitive cube root of unity. This agrees with Corollary 5.8 and the isotypic decomposition

$$\mathbb{C}[G] \simeq \frac{\mathbb{C}[g]}{(g^3-1)} \simeq \frac{\mathbb{C}[g]}{(g-1)} \oplus \frac{\mathbb{C}[g]}{(g-\omega)} \oplus \frac{\mathbb{C}[g]}{(g-\omega^2)} \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}.$$

For $\Bbbk = \mathbb{R}$, there exists just one irreducible representation in dimension 1, the trivial representation, because there is only one multiplicative character $G \to \mathbb{R}^*$. However, there is a 2-dimensional irreducible representation, in which g acts as rotation by 120°. Since

$$\mathbb{R}[G] \simeq \frac{\mathbb{R}[g]}{(g^3-1)} \simeq \frac{\mathbb{C}[g]}{(g-1)} \oplus \frac{\mathbb{R}[g]}{(g^2+g+1)} \simeq \mathbb{R} \oplus \mathbb{R}^2,$$

where the summands are exactly the two irreducible G-modules just described, the group G has no other irreducible representations over $\mathbb{R}$. Thus, the inequality $|\operatorname{Irr}(G)| \leqslant |Z(G)|$ from Corollary 5.7 is strict in this case.

Example 5.5 (Toy Representations of Symmetric Groups) Every symmetric group S_n has two nonisomorphic representations of dimension one: the *trivial* representation, in which all $g \in S_n$ act identically, and the *sign* representation, in which each $g \in S_n$ acts as multiplication by the sign $\operatorname{sgn}(g)$. The isotypic projections onto the symmetric and sign components of an arbitrary S_n-module are given by the symmetrization and alternation operators

$$\operatorname{sym}_n = \frac{1}{n!}\sum_{g\in S_n} g \quad \text{and} \quad \operatorname{alt}_n = \frac{1}{n!}\sum_{g\in S_n} \operatorname{sgn}(g)\, g.$$

Exercise 5.20 Verify this.

The representation of S_n in $\Bbbk^n$ by the permutations of the standard basis vectors e_i is called the *tautological* representation. It contains the trivial S_n-submodule of dimension 1 spanned by the sum $e = \sum e_i$. The induced $(n-1)$-dimensional representation of S_n in the quotient space $\Bbbk^n/\Bbbk \cdot e$ is called *simplicial*,[18] because for $\Bbbk = \mathbb{R}$, its image coincides with the complete group of the regular simplex of dimension $(n-1)$, the convex hull of the classes $e_i \pmod e$ in the affine space $\mathbb{A}(\mathbb{R}^n/\mathbb{R}\cdot e)$.

Exercise 5.21 Show that the S_n-orbit of every nonzero vector $v \in \Bbbk^n/\Bbbk \cdot e$ linearly spans the whole space and that therefore, the simplicial representation is irreducible.

The simplest nonabelian symmetric group, S_3, has three conjugacy classes.[19] Hence, the irreducible representations of S_3 are exhausted by the trivial and sign representations of dimension one and the two-dimensional simplicial representation U_Δ by the group of the triangle. This agrees with the second equality of Corollary 5.8, $1^2 + 1^2 + 2^2 = 6$. The Δ-isotypic projector equals[20]

$$e_\Delta \overset{\text{def}}{=} 1 - \operatorname{sym}_3 - \operatorname{alt}_3 = 1 - \frac{1}{6}\sum_{g\in S_3}(1+\operatorname{sgn}(g))g = 1 - \frac{1}{3}\left(1+\tau+\tau^2\right),$$

where $\tau = |123\rangle \in S_3$ means a cycle of length 3.

Exercise 5.22 By the direct computations in the group algebra $\mathbb{Q}[S_3]$, verify that e_Δ lies in the center $Z\big(\mathbb{Q}[S_3]\big)$, is idempotent, annihilates both the trivial and sign isotypic components, and acts identically on U_Δ.

---

[18] For $n = 2$, the simplicial and sign representations coincide.

[19] Recall that the conjugacy classes in S_n are in bijection with the cyclic types of permutations, i.e., are numbered by the Young diagrams of weight n; see Sect. 12.2.3 of Algebra I.

[20] Compare with Example 2.3 on p. 33.

The next symmetric group, S_4, has five conjugacy classes. Besides the trivial and sign representations of dimension 1 and the simplicial representation of dimension 3, the group S_4 has one more 3-dimensional representation, by the proper group of the cube.[21]

Exercise 5.23 Show that the 3-dimensional representations of S_4 by the complete group of the regular tetrahedron and the proper group of the cube are nonisomorphic and obtained from each other by taking the tensor product with the sign representation. Deduce from this that the representation by the proper group of the cube is irreducible.

Also, there is the two-dimensional irreducible representation of S_4 by the group of the triangle obtained by composing the quotient map[22] $S_4 \twoheadrightarrow S_3 \simeq S_4/V_4$ with the triangle representation of S_3. The equality $2 \cdot 1^2 + 2 \cdot 3^2 + 2^2 = 24$ confirms once more that we have enumerated all the irreducible representations of S_4.

5.6 Schur Representations of General Linear Groups

Everywhere in this section we consider a fixed vector space V of dimension $d < \infty$ over an arbitrary field $\Bbbk$ of characteristic zero. For every $n \in \mathbb{N}$, the symmetric group S_n acts on $V^{\otimes n}$ by the permutations of factors in the decomposable tensors. The isotypic decomposition

$$V^{\otimes n} = \bigoplus_{\lambda \in \mathrm{Irr}(S_n)} W_\lambda \tag{5.25}$$

of this representation is called the decomposition by *symmetry types of tensors*, and the tensors lying in W_λ are referred to as having symmetry type λ.

Example 5.6 (Quadratic and Cubic Tensors Revisited) The decomposition

$$V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$$

from Example 2.2 on p. 32 is the isotypic decomposition with respect to the action of $S_2 \simeq \mathbb{Z}/(2)$. This action is trivial in the first summand and sign alternating in the second. The decomposition from Example 2.3 on p. 33,

$$V^{\otimes 3} = \mathrm{Sym}^3(V) \oplus \mathrm{Alt}^3(V) \oplus W_\Delta, \tag{5.26}$$

is the isotypic decomposition with respect to the action of S_3. The three symmetry types appearing here are called *symmetric*, *sign alternating*, and *Lie*. The S_3-linear

[21] See Example 12.11 of Algebra I.

[22] See Example 12.10 of Algebra I.

projectors on the components are provided by the operators sym_3, alt_3, and π_Δ from Example 5.5. Thus, a tensor $t \in V^{\otimes 3}$ is of Lie type if and only if it is annihilated by averaging over the action of a 3-cycle: $t + \tau t + \tau^2 t = 0$, $\tau = |123\rangle \in S_3$.

5.6.1 *Action of* GL(V) × S_n *on* $V^{\otimes n}$

For every $n \in \mathbb{N}$, the linear representation of the general linear group $\mathrm{GL}(V)$ in the space $V^{\otimes n}$ is given by the group homomorphism

$$\tau_n : \mathrm{GL}(V) \to \mathrm{GL}\left(V^{\otimes n}\right), \quad f \mapsto f^{\otimes n},$$

where the operator $f \in \mathrm{GL}(V)$ acts on decomposable tensors by the rule

$$f^{\otimes n} : v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto f v_1 \otimes f v_2 \otimes \cdots \otimes f v_n. \tag{5.27}$$

In the sense of Sect. 5.4 on p. 109, τ_n is the nth tensor power of the tautological representation of $\mathrm{GL}(V)$ in V provided by the identity homomorphism

$$\tau_1 = \mathrm{Id}_{\mathrm{GL}(V)} : \mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}(V).$$

Since the action (5.27) certainly commutes with the action of the symmetric group S_n, the space $V^{\otimes n}$ is a $\mathrm{GL}(V) \times S_n$-module. An element $f \times g \in \mathrm{GL}(V) \times S_n$ acts on decomposable tensors as

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto f\left(v_{g(1)}\right) \otimes f\left(v_{g(2)}\right) \otimes \cdots \otimes f\left(v_{g(n)}\right).$$

Since the operator $f^{\otimes n}$ is S_n-linear for every $g \in \mathrm{GL}(V)$, the action of $\mathrm{GL}(V)$ maps every component of the S_n-isotypic decomposition $V^{\otimes n} = \bigoplus_{\lambda \in \mathrm{Irr}(S_n)} W_\lambda$ to itself, i.e., it preserves the symmetry type of tensors. Thus, every S_n-isotypic component W_λ is a $\mathrm{GL}(V) \times S_n$-module as well.

Let U_λ be an irreducible S_n-module. The tensor product $\mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right) \otimes U_\lambda$ possesses a $\mathrm{GL}(V) \times S_n$-module structure provided by the action

$$f \times g : \varphi \otimes u \mapsto (f^{\otimes n} \circ \varphi) \otimes (gu).$$

By Proposition 5.3 on p. 108, the contraction map $\varphi \otimes u \mapsto \varphi(u)$ establishes an isomorphism[23]

$$c : \mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right) \otimes U_\lambda \xrightarrow{\sim} W_\lambda, \tag{5.28}$$

[23] Although Proposition 5.3 was proved under the assumption that the ground field $\Bbbk$ is algebraically closed, for S_n-modules it holds over the field $\mathbb{Q}$ as well, because every complex irreducible representation of S_n is actually defined over $\mathbb{Q}$, as we will see in Chap. 7.

which is certainly both $\mathrm{GL}(V)$- and S_n-linear. The space

$$\mathbb{S}^\lambda V \stackrel{\text{def}}{=} \mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right) \tag{5.29}$$

provided with the action of $\mathrm{GL}(V)$ by the rule $f : \varphi \mapsto f^{\otimes n} \circ \varphi$ is called the *Schur representation* of $\mathrm{GL}(V)$.

Lemma 5.6 *The linear span of the operators $f^{\otimes n}$, $f \in \mathrm{GL}(V)$, coincides with the centralizer $\mathrm{End}_{S_n}\left(V^{\otimes n}\right)$ of the action of S_n on $V^{\otimes n}$.*

Proof The chain of canonical isomorphisms

$$\mathrm{End}(V^{\otimes n}) \simeq V^{\otimes n *} \otimes V^{\otimes n} \simeq V^{* \otimes n} \otimes V^{\otimes n} \simeq \left(V^* \otimes V\right)^{\otimes n} \simeq \mathrm{End}(V)^{\otimes n}$$

identifies the centralizer $\mathrm{End}_{S_n}\left(V^{\otimes n}\right) \subset \mathrm{End}\left(V^{\otimes n}\right)$ with the space of symmetric tensors

$$\mathrm{Sym}^n\left(\mathrm{End}(V)\right) \subset \mathrm{End}(V)^{\otimes n}.$$

The latter space is linearly generated over $\Bbbk$ by the proper nth powers $f^{\otimes n}$ of $f \in \mathrm{GL}(V)$, because of the following general claims.

Exercise 5.24 (Aronhold's Principle) Let W be a finite-dimensional vector space over a field of zero characteristic. Prove that the subspace of symmetric tensors

$$\mathrm{Sym}^n(W) \subset W^{\otimes n}$$

is linearly generated by the proper nth tensor powers $w^{\otimes n} = w \otimes w \otimes \cdots \otimes w$.

Exercise 5.25 (Enhanced Aronhold's Principle) Under the assumption of Exercise 5.24, let $F \in SW^*$ be a nonzero polynomial on W. Show that $\mathrm{Sym}^n(W)$ is linearly spanned by the $w^{\otimes n}$ with $F(w) \neq 0$.

The enhanced Aronhold's principle applied to $W = \mathrm{End}(V)$ and $F = \det$ proves the lemma. □

Proposition 5.6 *All the Schur representations*

$$\mathbb{S}^\lambda V = \mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right)$$

of $\mathrm{GL}(V)$ *are irreducible.*

Proof The isomorphism $\mathbb{S}^\lambda V \otimes U_\lambda \xrightarrow{\sim} W_\lambda$ from (5.28) transfers the action of S_n on W_λ to the action $g : \varphi \otimes u \mapsto \varphi \otimes (gu)$. Every linear operator $F \in \mathrm{End}(\mathbb{S}^\lambda V)$ acts on the space $W_\lambda = \mathbb{S}^\lambda V \otimes U_\lambda$ by the rule $F : \varphi \otimes u \mapsto F(\varphi) \otimes u$, and this action clearly commutes with the action of S_n. By Lemma 5.6, all linear operators $F \in \mathrm{End}(\mathbb{S}^\lambda V)$ belong to the linear span of the operators $\varphi \otimes u \mapsto \left(f^{\otimes n} \circ \varphi\right) \otimes u$ with $f \in \mathrm{GL}(V)$. Therefore, the image of the Schur representation $\mathrm{GL}(V) \to \mathrm{GL}\left(\mathbb{S}^\lambda V\right)$ linearly generates the whole algebra $\mathrm{End}\left(\mathbb{S}^\lambda V\right)$. By Exercise 5.8 on p. 106, this forces the Schur representation to be irreducible. □

5.6.2 The Schur–Weyl Correspondence

The correspondence $U_\lambda \leftrightarrow \mathbb{S}^\lambda V$, between the irreducible representations U_λ of the symmetric groups S_n and the Schur representations $\mathbb{S}^\lambda V$ of the general linear group[24] $\mathrm{GL}(V)$, is known as the *Schur–Weyl correspondence*. For example, the trivial representation of S_n corresponds to the irreducible representation of $\mathrm{GL}(V)$ in the space $\mathrm{Sym}^n V \simeq S^n V$ of symmetric tensors, whereas the sign representation corresponds to the irreducible representation of $\mathrm{GL}(V)$ in the space $\mathrm{Alt}^n V \simeq \Lambda^n V$. One can show that all nonzero $\mathrm{GL}(V)$-modules $\mathbb{S}^\lambda V$ are nonisomorphic for different λ, and every finite-dimensional irreducible representation $\varrho : \mathrm{GL}(V) \to \mathrm{GL}(W)$ such that all matrix elements of $\varrho(f)$ are rational functions of the matrix elements of f is isomorphic to some Schur module $\mathbb{S}^\lambda V$ tensored by an appropriate one-dimensional representation $\det^m : \mathrm{GL}(V) \to \mathrm{GL}_1(\Bbbk)$, in which every $f \in \mathrm{GL}(V)$ acts by multiplication by $\det^m(f)$. For the proofs and generalizations to other linear groups, see [Fu, FH].[25]

Problems for Independent Solution to Chapter 5

Problem 5.1 Construct a reducible indecomposable representation of dimension two for the additive group $\mathbb{Z}$.

Problem 5.2 Show that every finite-dimensional associative algebra with unit and without zero divisors is a division algebra.[26]

Problem 5.3 Let A be an associative $\Bbbk$-algebra with unit and $\varphi : A \to A$ an endomorphism of A considered as a left A-module.[27] Show that there exists $a_\varphi \in A$ such that $\varphi(x) = xa_\varphi$ for all $x \in A$.

Problem 5.4 Describe all associative $\mathbb{R}$-subalgebras with unit of dimension at least 32 in the matrix algebra $\mathrm{Mat}_{6\times 6}(\mathbb{R})$.

Problem 5.5 (Artinian Algebras) An associative algebra A is called *left Artinian* if for every descending chain of left ideals $L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots$, there exists $n \in \mathbb{N}$ such that $L_i = L_n$ for all $i \geqslant n$. Prove that: **(a)** Every finite-dimensional algebra is left Artinian. **(b)** Every nonzero left ideal in A contains a minimal

---

[24] Note that the weight n of the Young diagram λ knows nothing about the dimension d of V. However, some $\mathbb{S}^\lambda V$ may turn out to be zero, as happens, say, with the exterior powers $\Lambda^n V$ for $n > \dim V$.

[25] W. Fulton, *Young Tableaux: With Applications to Representation Theory and Geometry*, Cambridge University Press (1997). W. Fulton and J. Harris. *Representation Theory. A First Course.* Graduate Texts in Mathematics, Springer (1997).

[26] That is, for every $a \neq 0$, there exists a^{-1} such that $aa^{-1} = a^{-1}a = 1$. Equivalently, A satisfies all the axioms of a field except for the commutativity of multiplication (see Definition 2.1 from Algebra I).

[27] That is, $\varphi(ax) = a\varphi(x)$ for all $a, x \in A$.

(with respect to inclusions) nonzero left ideal, which automatically is a simple A-submodule of the left regular representation $a : x \mapsto ax$ of A in A.

Problem 5.6 (Semisimple Algebras) An associative algebra A with unit is called *semisimple* if the left regular representation $A \mapsto \mathrm{End}_{\Bbbk} A$, which takes $a \in A$ to the left multiplication map $x \mapsto ax$, is completely reducible. Let A be a semisimple $\Bbbk$-algebra of finite dimension as a vector space over $\Bbbk$. Show that:

(a) All A-modules are semisimple.
(b) $A = L_1 \oplus L_2 \oplus \cdots \oplus L_s$ as a left A-module, where every $L_i \subset A$ is a minimal nonzero left ideal in A, and $L_iL_j = 0$ if L_i and L_j are not isomorphic as left A-modules.
(c) Every simple A-module is isomorphic to some ideal L_i from the previous decomposition.
(d) For every simple A-module $\lambda : A \to \mathrm{End}\, U_\lambda$, the λ-isotypic component in the left regular representation of A is nonzero, forms a two-sided ideal $I_\lambda \subset A$, and coincides with the direct sum of those ideals L_i in (b) that are isomorphic to U_λ as A-modules.
(e) Every $I_\lambda \subset A$ is a semisimple $\Bbbk$-algebra with unit.[28]
(f) The unit elements $e_\lambda \in I_\lambda$ satisfy the following relations: $\sum_\lambda e_\lambda = 1$ is the unit of A, and

$$e_\lambda e_\mu = \begin{cases} e_\lambda & \text{for} \quad \lambda = \mu, \\ 0 & \text{otherwise.} \end{cases}$$

(g) The isotypic decomposition of the left regular representation $A \simeq \prod_{\lambda \in \mathrm{Irr}(A)} I_\lambda$ is an isomorphism of $\Bbbk$-algebras with unit.
(h) Every I_λ possesses a unique, up to isomorphism, simple I_λ-module, i.e.,

$$|\,\mathrm{Irr}(I_\lambda)| = 1.$$

Problem 5.7 (Simple Algebras) An associative semisimple $\Bbbk$-algebra A is called *simple* if $|\,\mathrm{Irr}(A)| = 1$. Deduce from the previous problem that every finite-dimensional semisimple algebra is a direct sum of simple algebras. For every finite-dimensional simple $\Bbbk$-algebra A, prove that:

(a) All minimal nonzero left ideals in A are isomorphic as A-modules, and for every two such ideals $L', L'' \subset A$, there exists an element $a \in A$ such that $L'a = L''$.
(b) $LA = A$ for every nonzero minimal left ideal $L \subset A$.
(c) There are no nonzero proper two-sided ideals in A.
(d) For the simple A-module U, the algebra $D = \mathrm{End}_A(U)$ is a division algebra.
(e) $A \simeq \mathrm{End}_D(U)$.

[28]The unit elements $e_\lambda \in I_\lambda$ are called *irreducible idempotents* of A.

Problem 5.8 Prove that following conditions on a finite-dimensional $\Bbbk$-algebra A with unit are equivalent: **(a)** A is simple, **(b)** A has no proper nonzero two-sided ideals, **(c)** $A = \mathrm{End}_D(U)$, where $D \supset \Bbbk$ is a division algebra and U a finite-dimensional vector space over D.

Problem 5.9 Prove that every finite-dimensional simple algebra A over an algebraically closed field $\Bbbk$ is isomorphic to $\mathrm{End}_{\Bbbk}(V)$ for an appropriate finite-dimensional vector space V over $\Bbbk$, and every nonzero irreducible representation of A is isomorphic to the tautological linear representation of A in V.

Problem 5.10 (Nilpotent Algebras and Radicals) An associative $\Bbbk$-algebra A is called *nilpotent* if for every $a \in A$, there exists $n \in \mathbb{N}$ such that $a^n = 0$. Prove that:

(a) All subalgebras and quotient algebras of a nilpotent algebra are nilpotent.
(b) If $I \subset A$ is a nilpotent two-sided ideal such that the quotient algebra A/I is nilpotent, then A is nilpotent.
(c) For every nilpotent algebra A, there exists $m \in \mathbb{N}$ such that $a^m = 0$ simultaneously for all $a \in A$.
(d) For every associative algebra A, the sum $I + J = \{x + y \mid x \in I, y \in J\}$ of two nilpotent two-sided ideals $I, J \subset A$ is a nilpotent two-sided ideal, and therefore, there exists a unique maximal proper nilpotent two-sided ideal containing all nilpotent two-sided ideals of A. (This ideal is called the *radical* of A and denoted by $\mathrm{rad}(A)$.)

Problem 5.11 (Trace Form) Let A be a finite-dimensional associative $\Bbbk$-algebra. For $a, b \in A$ write

$$(a, b) \stackrel{\text{def}}{=} \mathrm{tr}(ab) \in \Bbbk \tag{5.30}$$

for the trace of the multiplication map $A \to A$, $x \mapsto abx$. Prove that:

(a) (x, y) is a symmetric bilinear form $A \times A \to \Bbbk$, and $(ax, y) = (x, ya)$ for all $a, x, y \in A$.
(b) For every left ideal $L \subset A$, the orthogonal complement $L^{\perp} \subset A$ is a right ideal, and the orthogonal $R^{\perp}$ of every right ideal $R \subset A$ is a left ideal in A.
(c) If $\mathrm{char}\,\Bbbk = 0$, then $a \in A$ is nilpotent if and only if $(a, a^n) = 0$ for all $n \in \mathbb{N}$.

Problem 5.12 Let A be a finite-dimensional associative algebra with unit over a field $\Bbbk$ of characteristic zero. Prove that the following conditions are equivalent: **(a)** A is semisimple, **(b)** $\mathrm{rad}(A) = 0$, **(c)** the trace form (5.30) is nondegenerate.

Problem 5.13 Let char $\Bbbk \nmid |G|$. Under the notations of Sect. 5.5.2, prove that:

(a) Every I_λ is a minimal two-sided ideal in $\Bbbk[G]$ with respect to inclusions.
(b) Every two-sided ideal in $\Bbbk[G]$ is a direct sum of some ideals I_λ.
(c) Every linear representation $\Bbbk[G] \to \mathrm{End}(V)$ sends each irreducible idempotent e_λ to a G-linear projector onto the λ-isotypic component of V.

Problem 5.14 (Characters of Linear Representations) Let $\varrho : G \to \mathrm{End}(V)$ be a finite-dimensional linear representation of a finite group G over an arbitrary field $\Bbbk$. The function

$$\chi_V : G \to \Bbbk, \quad g \mapsto \operatorname{tr} \varrho(g),$$

is called the *character* of this representation. Prove that:

(a) The character of a representation takes a constant value on every conjugacy class of G, i.e., assigns a well-defined function $\chi_V : \mathrm{Cl}(G) \to \Bbbk$.
(b) If G acts on the coordinate vector space $V = \Bbbk^n$ by some permutations of the standard basis vectors, then $\chi_V(g)$ equals the number of fixed points of the permutation g.
(c) The characters of the symmetric and exterior squares of a representation V are expressed in terms of χ_V as

$$\chi_{S^2V}(g) = \left(\chi_V^2(g) + \chi_V(g^2)\right)/2,$$
$$\chi_{\Lambda^2V}(g) = \left(\chi_V^2(g) - \chi_V(g^2)\right)/2.$$

Problem 5.15 Compute the characters of the five irreducible representations of S_4 described in Example 5.5.

Problem 5.16 Let $\varrho : G \to \mathrm{SL}(V)$ be a linear representation of a group G by volume-preserving linear automorphisms of a d-dimensional vector space V. For all $0 \leqslant k \leqslant d$, construct an isomorphism of the representations $\Lambda^k\varrho \simeq \Lambda^{d-k}\varrho$.

Problem 5.17 (Molin's Formula) Given a finite-dimensional linear representation of a finite group $\varrho : G \to \mathrm{GL}(V)$ over an algebraically closed field $\Bbbk$ of characteristic zero, write

$$d_m = \dim_\Bbbk \{f \in S^mV^* \mid \forall\, g \in G,\ \forall\, v \in V,\ f(\varrho(g)v) = f(v)\}$$

for the dimension of the space of G-invariant homogeneous polynomials of degree m on V. Prove that

$$\sum_{m\geqslant 0} d_m t^m = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1 - t\,\varrho(g))}.$$

Problem 5.18 (Representations of D_3) Use the presentation of D_3 by generators σ, τ and relations $\sigma^2 = \tau^3 = e$, $\sigma\tau\sigma = \tau^{-1}$ to show that the eigenvalues of s and τ

in every linear representation are exhausted, respectively, by the square and cube roots of unity, and that σ sends every eigenvector of τ to an eigenvector with the inverse eigenvalue. Deduce from this[29] that the irreducible representations of $D_3 = S_3$ over $\mathbb{C}$ are exhausted by the trivial and sign representations of dimension 1 and by the triangle representation U_Δ of dimension 2. Show that $S^{n+6}U_\Delta \simeq S^n U_\Delta \oplus \Bbbk[D_3]$, where $\Bbbk[D_3]$ means the left regular representation. Find the multiplicity of every simple D_3-module in $S^n U_\Delta$ for all $n \in \mathbb{N}$.

Problem 5.19* (Schur Reciprocity) Under the notation of the previous problem, prove that for all $k, m \in \mathbb{N}$, there is an isomorphism of D_3-modules

$$S^k\left(S^m U_\Delta\right) \simeq S^m\left(S^k U_\Delta\right).$$

Problem 5.20 Enumerate all irreducible representations of the dihedral group D_n and compute their characters.

Problem 5.21 Let $G \simeq S_4$ be the proper group of the cube in $\mathbb{R}^3$. Write $\mathbb{C}^V$, $\mathbb{C}^E$, $\mathbb{C}^F$ for the spaces of complex-valued functions on the respective sets of vertices, edges, and faces of the cube.

(a) Find the multiplicity of every simple S_4-module in the natural representations of G in $\mathbb{C}^V$, $\mathbb{C}^E$, $\mathbb{C}^F$ by the rule $g : f \mapsto f \circ g^{-1}$.

(b) Let the map $s : \mathbb{C}^V \to \mathbb{C}^F$ send a function f to the function sf whose value on a face equals the sum of the values of f on the edges bounding the face. Find the dimensions[30] of $\ker s$ and $\operatorname{im} s$ and indicate some bases in these two spaces.

Problem 5.22 The faces of the cube are marked by $1, 2, 3, 4, 5, 6$, as on a die. Once per second, every mark is changed to the arithmetic mean of the marks on the four neighboring faces. To an accuracy within $\pm 10^{-2}$, evaluate the marking numbers after 2017 s. Does the answer change if the initial marks $1, 2, 3, 4, 5, 6$ are placed differently?

Problem 5.23 Solve Problem 5.21 for the proper group of the dodecahedron.

Problem 5.24* Describe all finite subgroups of $\mathrm{SO}_3(\mathbb{R})$ up to conjugation.

Problem 5.25 (Invariant Inner Product) Show that every finite-dimensional representation of a finite group G over $\mathbb{R}$ (respectively over $\mathbb{C}$) admits a G-*invariant* Euclidean (respectively Hermitian) inner product (v, w), meaning that $(gv, gw) = (v, w)$ for all $g \in G$.

Problem 5.26 Assume that a G-invariant Hermitian structure and orthonormal basis are fixed in every finite-dimensional complex G-module. Write all operators $g \in G$ in terms of unitary matrices in these bases. Consider the matrix elements of

[29] Without any reference to Corollary 5.8 and Example 5.5.

[30] Hint: use the G-linearity of s, isotypic decompositions from (a), and Schur's lemma.

these matrices as functions $G \to \mathbb{C}$. Prove that every two matrix elements from different irreducible representations are orthogonal with respect to the standard Hermitian structure on $\mathbb{C}^G$ provided by the inner product

$$(f_1, f_2) = |G|^{-1} \sum_{g \in G} f_1(g) \cdot \overline{f_2(g)},$$

and compute the inner products of matrix elements of the same irreducible representation.[31]

[31]Hint: for every $\Bbbk$-linear map between irreducible representations $\varphi : U_\lambda \to U_\varrho$, the average

$$|G|^{-1} \sum_{g \in G} g\varphi g^{-1} = |G|^{-1} \sum_{g \in G} g\varphi \overline{g}^t$$

is G-linear, and therefore, either zero (for $\lambda \neq \varrho$) or a scalar homothety (for $\lambda = \varrho$); apply this to $\varphi = E_{ij}$ and use the trace to evaluate the coefficient of the homothety.

Chapter 6
Representations of Finite Groups in Greater Detail

Everywhere in this section, we write by default G for an arbitrary finite group and $\Bbbk$ for an algebraically closed field such that $\operatorname{char}(\Bbbk) \nmid |G|$.

6.1 Orthogonal Decomposition of a Group Algebra

6.1.1 Invariant Scalar Product and Plancherel's Formula

For a vector space V of finite dimension over $\Bbbk$, the algebra $\operatorname{End}_{\Bbbk}(V)$ possesses the canonical inner product

$$\operatorname{End}(V) \times \operatorname{End}(V) \to \Bbbk\,, \quad (A, B) \stackrel{\text{def}}{=} \operatorname{tr}(AB) \tag{6.1}$$

provided by complete contraction.

Exercise 6.1 Check that for every pair of decomposable operators $A = a \otimes \alpha$, $B = b \otimes \beta$ from $\operatorname{End}(V) \simeq V \otimes V^*$, one has $\operatorname{tr}(AB) = \alpha(b) \cdot \beta(a)$. Deduce from this that $\operatorname{tr}(AB)$ is symmetric and nondegenerate.

Write $L : \Bbbk[G] \hookrightarrow \operatorname{End}(\Bbbk[G])$, $x \mapsto L_x$, for the left regular representation, which sends $x \in \Bbbk[G]$ to the left multiplication $L_x : z \mapsto xz$. Note that it is injective, because $L_x(e) = x \neq 0$ for $x \neq 0$. The restriction of the inner product (6.1) written for $V = \Bbbk[G]$ to the subspace $L(\Bbbk[G]) \subset \operatorname{End}_{\Bbbk}(\Bbbk[G])$ provides the group algebra $\Bbbk[G]$ with the symmetric bilinear form

$$(f, g) \stackrel{\text{def}}{=} \operatorname{tr}\left(L_f L_g\right) = \operatorname{tr}\left(L_{fg}\right)\,. \tag{6.2}$$

Since multiplication by the identity element e has trace $|G|$, and multiplication by every nonidentity element $g \in G$ is traceless, the Gram matrix of (6.2) in the

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_6

standard basis formed by group elements is

$$(g,h) = \begin{cases} |G| & \text{for } h = g^{-1}\,, \\ 0 & \text{for } h \neq g^{-1}. \end{cases} \tag{6.3}$$

Therefore, the symmetric form (6.2) is nondegenerate.[1] For the standard basis consisting of all $g \in G$, the dual basis is formed by the normalized inverse group elements

$$g^{\vee} \stackrel{\text{def}}{=} g^{-1}/|G|\,. \tag{6.4}$$

Therefore, every element of the group algebra $x \in \Bbbk[G]$ is expanded through the standard basis $G \subset \Bbbk[G]$ as

$$x = \frac{1}{|G|}\sum_{g\in G}(g^{-1},x)\cdot g. \tag{6.5}$$

Exercise 6.2 For every $g \in G$, verify that the left and right multiplications by g, which map $x \mapsto gx$ and $x \mapsto xg$ respectively, are adjoint linear endomorphisms of $\Bbbk[G]$ with respect to the inner product (6.2). Use this to prove that the orthogonal complement to every left ideal in $\Bbbk[G]$ is a right ideal, and conversely, the orthogonal complement of every right ideal is a left ideal.

It follows from the exercise that the orthogonal complement of every two-sided ideal $I \subset \Bbbk[G]$ is a two-sided ideal as well. Therefore, the isotypic decomposition of the left regular representation

$$\Bbbk[G] = \bigoplus_{\lambda\in\mathrm{Irr}(G)} I_{\lambda} \tag{6.6}$$

is an orthogonal decomposition. The isomorphism provided by Maschke's theorem,[2]

$$\mathfrak{r}:\ \Bbbk[G] \xrightarrow{\sim} \prod_{\lambda\in\mathrm{Irr}(G)} \mathrm{End}(U_{\lambda})\,,$$

allows us to evaluate the inner product (6.2) in terms of the traces of group elements taken in the irreducible representations.

[1] Note that this fails if $\operatorname{char}\Bbbk \mid |G|$.

[2] See Theorem 5.5 on p. 117.

Proposition 6.1 (Plancherel's Formula) *For all $f, g \in \Bbbk[G]$,*

$$(f, g) = \sum_{\lambda \in \mathrm{Irr}(G)} \dim(U_\lambda) \cdot \mathrm{tr}\big(\lambda(fg)\big)\,.$$

Proof The trace of left multiplication by fg in the algebra $\oplus_{\lambda \in \mathrm{Irr}(G)} \mathrm{End}(U_\lambda)$ equals the sum of the traces of left multiplications by $\lambda(fg)$ in the algebras $\mathrm{End}(U_\lambda)$ for all irreducible representations $\lambda \in \mathrm{Irr}(G)$. It remains to note that the trace of left multiplication by a matrix M: $X \mapsto MX$ in $\mathrm{Mat}_n(\Bbbk)$ equals $n \cdot \mathrm{tr}(M)$, because every standard basis matrix E_{ij} appears in the expansion of ME_{ij} with the coefficient m_{ii}. □

6.1.2 *Irreducible Idempotents*

It follows from Sect. 5.5.2 on p. 115 that the irreducible idempotents

$$e_\lambda = \pi_\lambda(e) = \mathfrak{r}^{-1}\left(0 \,\dots\, ,0,\, \mathrm{Id}_{U_\lambda}\, ,0,\, \dots\, 0\right) \in I_\lambda \subset \Bbbk[G] \tag{6.7}$$

form an orthogonal basis of the center $Z(\Bbbk[G])$ and satisfy the relations

$$e_\lambda e_\varrho = \begin{cases} e_\lambda & \text{for } \varrho = \lambda\,, \\ 0 & \text{for } \varrho \neq \lambda\,. \end{cases} \tag{6.8}$$

Since the trace of multiplication by the identity in the algebra $\mathrm{End}_\Bbbk(U_\lambda)$ equals $\dim^2 U_\lambda$, the following *orthogonality relations* hold:

$$(e_\lambda, e_\varrho) = \begin{cases} \dim^2 U_\lambda & \text{for } \varrho = \lambda\,, \\ 0 & \text{for } \varrho \neq \lambda\,. \end{cases} \tag{6.9}$$

Note that the basic idempotents e_λ are uniquely characterized as the orthogonal projections of unity $e \in \Bbbk[G]$ on the isotypic ideals I_λ.

Proposition 6.2 *For every $\lambda \in \mathrm{Irr}(G)$, the linear expansion of e_λ through the group elements is*

$$e_\lambda = \frac{\dim U_\lambda}{|G|} \sum_{g \in G} \mathrm{tr}\left(\lambda(g^{-1})\right) \cdot g\,. \tag{6.10}$$

In particular, every linear representation $\Bbbk[G] \to \mathrm{End}(V)$ maps the right-hand side of this equality to the λ-isotypic projector $\pi_\lambda : V \twoheadrightarrow V_\lambda$.

Proof By formula (6.5), $e_\lambda = |G|^{-1} \sum_{\mu \in \mathrm{Irr}(G)} (g^{-1}, e_\lambda) \cdot g$. By the Plancherel formula,[3]

$$(g^{-1}, e_\lambda) = \sum_{\mu \in \mathrm{Irr}(G)} \dim\left(U_\mu\right) \cdot \mathrm{tr}\left(\mu(g^{-1} e_\lambda)\right) = \dim\left(U_\lambda\right) \cdot \mathrm{tr}\left(\lambda(g^{-1})\right) .$$

The sum is reduced to one summand, because left multiplication by e_λ annihilates all simple G-modules U_μ with $\mu \neq \lambda$, and acts on U_λ as the identity endomorphism. □

6.2 Characters

6.2.1 Definition, Properties, and Examples of Computation

Associated with every finite-dimensional linear representation $\varrho : \Bbbk[G] \to \mathrm{End}(V)$ is the $\Bbbk$-linear form

$$\chi_\varrho : \Bbbk[G] \to \Bbbk\,, \quad x \mapsto \mathrm{tr}\,\varrho(x)\,, \tag{6.11}$$

called the *character*[4] of ϱ. When ϱ is clear from the reference to V, we will also write χ_V instead of χ_ϱ. Since the trace of a linear map is unchanged under conjugations of the map, the character of every linear representation takes a constant value on every conjugacy class of G. For the same reason, the characters of isomorphic G-modules coincide. In terms of characters, formula (6.10) for the λ-isotypic projector can be rewritten as

$$e_\lambda = \frac{\dim U_\lambda}{|G|} \sum_{g \in G} \chi_\lambda\left(g^{-1}\right) \cdot g\,. \tag{6.12}$$

Example 6.1 (Characters of Permutation Representations) Let a group G act on $\Bbbk^n$ by permutations of the standard basis vectors. Then the character of this action takes an element $g \in G$ to the number of fixed points of the permutation provided by g. In particular, the values of the character of the left regular representation are

$$\chi_L(g) = \begin{cases} |G| & \text{for } g = e\,, \\ 0 & \text{for } g \neq e\,. \end{cases}$$

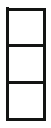
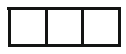
---

[3] See Proposition 6.1 on p. 133.

[4] Do not confuse these *additive* characters of arbitrary groups with the *multiplicative* characters of abelian groups considered in Sect. 5.4.2 on p. 111.

For a Young diagram λ, write $C_\lambda \subset S_n$ for the conjugacy class consisting of all permutations of the cyclic type λ. Then the character of the tautological representation of S_n in $\Bbbk^n$ equals $m_1(\lambda)$, the number of length-one rows in λ. Since the tautological representation is a direct sum of the simplicial and trivial representations, and the latter has the constant character equal to 1 for all g, the value of the simplicial character on the class $C_\lambda \subset S_n$ is $\chi_\Delta(C_\lambda) = m_1(\lambda) - 1$.

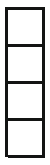
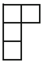
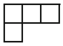
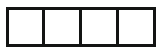
Exercise 6.3 Verify the following table of irreducible characters of S_3,

conjugacy class			
its cardinality	1	3	2
values of character:			
trivial	1	1	1
sign	1	-1	1
triangular	2	0	-1

(6.13)

and convince yourself that the isotypic projectors e_λ obtained from this table by formula (6.12) agree with those described in Example 5.5 on p. 120.

Example 6.2 (Irreducible Characters of S_4) If a representation admits an explicit geometric description, its character usually can be computed by straightforward summation of the eigenvalues of rotations and reflections representing the group elements. For example, the five irreducible representations of S_4 from Example 5.5 on p. 120 take the following values on the conjugacy classes in S_4:

conjugacy class					
its cardinality	1	6	3	8	6
values of character:					
trivial	1	1	1	1	1
sign	1	-1	1	1	-1
tetrahedral	3	1	-1	0	-1
cubic	3	-1	-1	0	1
triangular	2	0	2	-1	0

(6.14)

The fourth row of this table was computed as follows. The trace of the identity equals the dimension of the representation. Since a lone transposition and a pair of disjoint transpositions act as rotations by 180° about some lines, their eigenvalues are $1, -1, -1$, and the trace equals -1. A 3-cycle and 4-cycle act as rotations by 120° and 90° respectively, and their eigenvalues are $1, \omega, \omega^2$ and $1, i, -i$, where $\omega, i \in \Bbbk$ are respectively a third and a fourth root of unity. The traces are 0 and 1.

Exercise 6.4 Verify the third and fifth rows of the table.

Lemma 6.1 *For every linear representations V, W of a finite group G with characters χ_U, χ_V, one has*

$$\chi_{V\oplus W}(g) = \chi_V(g) + \chi_W(g)\,, \tag{6.15}$$

$$\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g)\,, \tag{6.16}$$

$$\chi_{V^*}(g) = \chi_V(g^{-1})\,, \tag{6.17}$$

$$\chi_{\mathrm{Hom}(V,W)}(g) = \chi_V(g^{-1})\chi_W(g)\,. \tag{6.18}$$

Proof Since every operator g in a finite group of linear operators is diagonalizable over an algebraically closed field of characteristic zero, there exist bases

$$v_1, v_2, \dots, v_n \in V \quad \text{and} \quad w_1, w_2, \dots, w_m \in W$$

consisting of eigenvectors of g. Write α_i and β_j for the eigenvalues of v_i and w_j. The disjoint union of these eigenvalues is the set of eigenvalues for the representation g in $V \oplus W$. This proves the first formula (6.15). The mn eigenvalues of g in the representation $V \otimes W$ are $\alpha_i\beta_j$. This leads to (6.16). Formula (6.17) holds, because the diagonal matrices of g in the dual eigenbases of the dual representations are inverse to each other.[5] The last formula follows from (6.16) and (6.17). □

Exercise 6.5 Verify that the generating power series for the characters of symmetric and exterior powers of a linear representation $\varrho : G \to \mathrm{GL}(V)$ are

$$\sum_{\nu\geqslant 0} \chi_{\Lambda^\nu V}(g)\, t^\nu = \det(1 + t\,\varrho(g)) \quad \text{and} \quad \sum_{\nu\geqslant 0} \chi_{S^\nu V}(g)\, t^\nu = \frac{1}{\det(1 - t\,\varrho(g))}\,.$$

Corollary 6.1 *The character of an arbitrary linear representation V is a linear combination of the irreducible characters χ_λ, $\lambda \in \mathrm{Irr}(G)$ with nonnegative integer coefficients:*

$$\chi_V = \sum_{\lambda\in\mathrm{Irr}(G)} m_\lambda(V)\cdot\chi_\lambda\,, \tag{6.19}$$

where $m_\lambda(V) = \dim V_\lambda / \dim U_\lambda$ is the multiplicity[6] *of the simple G-module U_λ in V.* □

[5] See Sect. 5.4 on p. 109.

[6] See Definition 5.1 on p. 109.

6.2.2 *The Fourier Transform*

Since every covector is uniquely determined by its values on a basis, the vector space $\Bbbk[G]^*$ dual to the group algebra $\Bbbk[G]$ is naturally isomorphic[7] to the space $\Bbbk^G$ of all functions $G \to \Bbbk$ on the basis G of $\Bbbk[G]$. The isomorphism maps a function $\varphi : G \to \Bbbk$ to the linear form evaluated as $\varphi(\sum x_g \cdot g) = \sum x_g \varphi(g)$. At the same time, associated with the inner product on $\Bbbk[G]$ is the isomorphism[8]

$$\Bbbk[G] \xrightarrow{\sim} \Bbbk[G]^*, \quad f \mapsto (f, *), \tag{6.20}$$

which maps a vector to the inner multiplication by this vector. The inverse map sends the basis of $\Bbbk[G]^*$ dual to the basis G of $\Bbbk[G]$ to the basis consisting of elements[9] $g^\vee = g^{-1}/|G|$ for all $g \in G$. The composition of $\Bbbk$-linear isomorphisms

$$\Bbbk^G \xrightarrow{\sim} \Bbbk[G]^* \xrightarrow{\sim} \Bbbk[G]$$

is called the *Fourier transform*. We denote it by

$$\Phi : \Bbbk^G \xrightarrow{\sim} \Bbbk[G], \quad \varphi \mapsto \widehat{\varphi} \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} \varphi\left(g^{-1}\right) \cdot g\,. \tag{6.21}$$

It maps the irreducible characters $\chi_\lambda \in \Bbbk^G$, $\lambda \in \mathrm{Irr}(G)$, to rational multiples of the irreducible idempotents

$$\widehat{\chi}_\lambda = \frac{1}{\dim U_\lambda} \cdot e_\lambda\,. \tag{6.22}$$

Exercise 6.6 Describe the binary operation on $\Bbbk[G]$ corresponding to the (commutative) multiplication of functions in $\Bbbk^G$, and the binary operation on $\Bbbk^G$ corresponding to the (noncommutative) multiplication in $\Bbbk[G]$ under the Fourier transform.

Let us transfer the inner product (6.2) from the group algebra $\Bbbk[G]$ to the space of functions $\Bbbk^G$ by means of the isomorphism (6.21), that is, put

$$(\varphi, \psi) \overset{\text{def}}{=} (\widehat{\varphi}, \widehat{\psi}) = \frac{1}{|G|^2} \sum_{g,h \in G} \varphi\left(g^{-1}\right) \psi\left(h^{-1}\right) (g, h) = \frac{1}{|G|} \sum_{g \in G} \varphi\left(g^{-1}\right) \psi\left(g\right) \tag{6.23}$$

for every two functions $\varphi, \psi : G \to \Bbbk$. The next claims follow immediately from the formulas (6.22), (6.9), and they completely reduce the structural analysis of linear representations to formal algebraic manipulations with their characters.

---

[7] See Lemma 7.1 in Sect. 7.1.1 of Algebra I.

[8] See Sects. 10.3.1 and 16.1.1 of Algebra I.

[9] See formula (6.4) on p. 132.

Corollary 6.2 *The irreducible characters form an orthonormal basis in the subspace* $\Bbbk^{\mathrm{Cl}(G)} \subset \Bbbk^G$ *of functions* $G \to \Bbbk$ *taking constant values on the conjugacy classes.* □

Corollary 6.3 $\dim \mathrm{Hom}_G(V, W) = (\chi_V, \chi_W)$ *for every pair of finite-dimensional* G*-modules* V, W.

Proof Both sides are equal to $\sum_{\lambda \in \mathrm{Irr}(G)} m_\lambda(V) m_\lambda(W)$, where $m_\lambda(M)$ means the multiplicity of the irreducible representation λ in a given G-module M. For the left-hand side, this follows from Corollary 5.5 on p. 109, and for the right-hand side, from Corollary 6.1 on p. 136 and the previous corollary. □

Corollary 6.4 *The multiplicity of a simple* G*-module* U_λ *in an arbitrary* G*-module* V *can be computed by the formula* $m_\lambda(V) = (\chi_\lambda, \chi_V)$.

Proof Take the inner product of the character χ_λ with both sides of formula (6.19) on p. 136, and use the orthonormality of irreducible characters. □

Corollary 6.5 *A linear representation* V *is irreducible if and only if* $(\chi_V, \chi_V) = 1$.

Proof It follows from Corollary 6.1 and the orthonormality of irreducible characters that

$$(\chi_V, \chi_V) = \sum_{\lambda \in \mathrm{Irr}(G)} m_\lambda^2(V) \,,$$

where all the multiplicities $m_\lambda(V)$ are nonnegative integers. This sum equals one if and only if it is exhausted by exactly one summand equal to one. □

Exercise 6.7 Enumerate all irreducible representations and compute their characters for the following groups: **(a)** D_n, **(b)** A_4, **(c)** A_5, **(d)** S_5.

Remark 6.1 (Inner Product of Complex Characters) Since the eigenvalues of all operators from a finite group G of order $|G| = n$ are nth roots of unity, for $\Bbbk = \mathbb{C}$, they all lie on the unit circle $\mathrm{U}_1 \subset \mathbb{C}$. This forces the inverse eigenvalues of the inverse operators $g, g^{-1} \in G$ to be complex conjugate to each other, because $\lambda^{-1} = \overline{\lambda}$ for all $\lambda \in \mathrm{U}_1$. Therefore, $\chi\left(g^{-1}\right) = \overline{\chi(g)}$ for all characters χ of G. Hence, the inner product of complex characters is proportional to the standard Hermitian inner product of functions[10] $G \to \mathbb{C}$,

$$(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)} \cdot \chi_2(g) \,.$$

Remark 6.2 (Inner Product of Characters of the Symmetric Group) Since every two inverse permutations $g,\ g^{-1} \in S_n$ are of the same cyclic type, they are conjugate

[10] See Examples 18.3, 18.4 of Algebra I.

in S_n. Therefore, $\chi\left(g^{-1}\right) = \chi(g)$ for all characters χ of the symmetric group S_n. Hence, the inner product of characters of S_n is proportional to the standard Euclidean inner product of functions[11]:

$$(\chi_1, \chi_2) = \frac{1}{n!} \sum_{g \in S_n} \chi_1(g) \cdot \chi_2(g) .$$

In particular, it is positive anisotropic over $\mathbb{Q}$ and $\mathbb{R}$.

Example 6.3 (Exterior Powers of the Simplicial Representation) Write $\mathbb{1}$, Δ, and τ for the trivial, simplicial, and tautological representations of S_n over $\mathbb{Q}$. Since $\tau = \Delta \oplus \mathbb{1}$, the mth exterior power is given by

$$\Lambda^m \tau = \Lambda^m \Delta \oplus \Lambda^{m-1} \Delta .$$

Exercise 6.8 Check that $\Lambda^k(U \oplus W) \simeq \bigoplus_{\alpha+\beta=k} \Lambda^\alpha U \otimes \Lambda^\beta W$.

We are going to show that $(\chi_{\Lambda^m \tau}, \chi_{\Lambda^m \tau}) = 2$ for all $1 \leqslant m \leqslant (n-1)$. This forces the representations $\Lambda^m \Delta$ to be irreducible for all $0 \leqslant m \leqslant n$. The trace of a permutation $\sigma \in S_n$ computed in the standard basis $e_I = e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_m}$ of $\Lambda^m(\mathbb{k}^n)$ equals the sum of signs $\operatorname{sgn} \sigma|_I$ of the permutations induced by σ on all cardinality-m subsets $I \subset \{1, 2, \dots, n\}$ such that $\sigma(I) \subset I$. Therefore,

$$\begin{aligned}
(\chi_{\Lambda^k \tau}, \chi_{\Lambda^k \tau}) &= \frac{1}{n!} \sum_{\sigma \in S_n} \Big(\sum_{I: \sigma(I) \subset I} \operatorname{sgn}(\sigma|_I) \Big) \cdot \Big(\sum_{J: \sigma(J) \subset J} \operatorname{sgn}(\sigma|_J) \Big) \\
&= \frac{1}{n!} \sum_{\sigma \in S_n} \sum_{\substack{I,J: \sigma(I) \subset I \\ \sigma(J) \subset J}} \operatorname{sgn}(\sigma|_I) \cdot \operatorname{sgn}(\sigma|_J) \\
&= \frac{1}{n!} \sum_{I,J} \sum_{\substack{\sigma: \sigma(I) \subset I \\ \sigma(J) \subset J}} \operatorname{sgn}(\sigma|_I) \cdot \operatorname{sgn}(\sigma|_J) .
\end{aligned}$$

The permutations σ such that $\sigma(I) \subset I$ and $\sigma(J) \subset J$ form a direct product of four symmetric groups $S_k \times S_{m-k} \times S_{m-k} \times S_{n-2m+k}$, where $k = k(I, J) = |I \cap J|$ and the factors independently permute the elements within the sets

$$I \cap J, I \smallsetminus (I \cap J), J \smallsetminus (I \cap J), \{1, 2, \dots, n\} \smallsetminus (I \cup J) .$$

Since

$$\begin{aligned}
\operatorname{sgn}(\sigma|_I) \cdot \operatorname{sgn}(s|_J) &= \operatorname{sgn}(\sigma|_{I \cap J})^2 \cdot \operatorname{sgn}(\sigma|_{I \smallsetminus (I \cap J)}) \cdot \operatorname{sgn}(\sigma|_{J \smallsetminus (I \cap J)}) \\
&= \operatorname{sgn}(\sigma|_{I \smallsetminus (I \cap J)}) \cdot \operatorname{sgn}(\sigma|_{J \smallsetminus (I \cap J)}) ,
\end{aligned}$$

[11] See Examples 10.1, 10.2 of Algebra I.

the previous sum can be written as

$$\frac{1}{n!}\sum_{I,J} k!\cdot(n-2m+k)!\cdot\Big(\sum_{g\in S_{m-k}}\operatorname{sgn}(g)\Big)\cdot\Big(\sum_{h\in S_{m-k}}\operatorname{sgn}(h)\Big)\,. \tag{6.24}$$

The last two sums are equal to 1 for $k = m, m-1$ and vanish for all other values of k, m. If $k = m$, then $I = J$, and the corresponding part of (6.24) looks like

$$\frac{1}{n!}\sum_{I} m!\cdot(n-m)!\,.$$

It consists of $\binom{n}{m}$ coinciding summands $\binom{m}{n}^{-1}$ and equals 1. If $k = m-1$, then we have $|I\cap J| = (m-1)$, and the corresponding part of (6.24) looks like

$$\frac{1}{n!}\sum_{I\cap J}\sum_{\substack{i\neq j\\ i,j\notin I\cap J}}(m-1)!\cdot(n-m-1)!\,.$$

It consists of $\binom{n}{m-1}\cdot(n-m+1)(n-m)$ coinciding summands of the form

$$\frac{(m-1)!\cdot(n-m-1)!}{n!} = \binom{n}{m-1}^{-1}\cdot\frac{1}{(n-m+1)(n-m)}\,,$$

i.e., it equals 1 as well.

6.2.3 *Ring of Representations*

The $\mathbb{Z}$-linear combinations of complex irreducible characters of a finite group G form a commutative subring with unit in the algebra $\mathbb{C}^G$ of all functions $G\to\mathbb{C}$. It is called the *representation ring* of the group G and is denoted by

$$\operatorname{Rep}(G) \stackrel{\text{def}}{=} \bigoplus_{\lambda\in\operatorname{Irr}(G)}\mathbb{Z}\cdot\chi_\lambda \subset \mathbb{C}^G\,.$$

The terminology is justified by the fact that the linear combinations of irreducible characters with nonnegative integer coefficients are in bijection with the finite-dimensional linear representations of G over $\mathbb{C}$. Under this bijection, addition and multiplication of characters in $\mathbb{C}^G$ correspond to direct sums and tensor products of the representations. Integer linear combinations containing some irreducible characters with negative coefficients are called *virtual representations*.

6.3 Induced and Coinduced Representations

6.3.1 Restricted and Induced Modules Over Associative Algebras

Let $A \subset B$ be associative $\Bbbk$-algebras with a common unit element. Every linear representation of B in a vector space W can be considered a representation of the subalgebra $A \subset B$. The space W considered as an A-module is called the *restriction* of the B-module W on A, and is denoted by $\operatorname{res} W$, or $\operatorname{res}_A^B W$ when the precise reference to A, B is essential. We already met this construction in Sect. 18.1 of Algebra I, when we considered the realification of a complex vector space. In this case, $\Bbbk = A = \mathbb{R}$, $B = \mathbb{C}$, and every vector space W of dimension n over $\mathbb{C}$ produces the vector space $W_{\mathbb{R}} = \operatorname{res}_{\mathbb{R}}^{\mathbb{C}} W$ of dimension $2n$ over $\mathbb{R}$.

Conversely, associated with every A-module V is the *induced* B-module, denoted by $\operatorname{ind}_A^B V = B \otimes_A V$ and defined as the quotient space of the tensor product of vector spaces $B \otimes V$ by the subspace spanned by the differences $ba \otimes v - b \otimes av$ for all $b \in B$, $a \in A$, $v \in V$. Thus, $ba \otimes_A v = b \otimes_A av$ in $B \otimes_A V$. For this reason, the space $B \otimes_A V$ is also called the *tensor product over* A. Elements $b \in B$ act on $B \otimes_A V$ by the rule

$$b(b' \otimes v) \stackrel{\text{def}}{=} (bb') \otimes v \,.$$

We met this construction as well in Sect. 18.2 of Algebra I, when we studied the complexification of a real vector space. Indeed, for $\Bbbk = A = \mathbb{R}$, $B = \mathbb{C}$, and a vector space V of dimension n over $\mathbb{R}$, the induced complex vector space $\mathbb{C} \otimes V$ is exactly the complexification of V.

Proposition 6.3 *The map $\tau_A^B : V \to B \otimes_A V$, $v \mapsto 1 \otimes_A v$, is A-linear and possesses the following universal property: for every B-module W and A-linear map $\varphi : V \to W$, there exists a unique B-linear homomorphism $\psi : B \otimes_A V \to W$ such that $\psi \circ \tau_A^B = \varphi$. In other words, for every A-module V and B-module W, there exists the canonical isomorphism*

$$\operatorname{Hom}_B(\operatorname{ind} V, W) \xrightarrow{\sim} \operatorname{Hom}_A(V, \operatorname{res} W) \,, \quad \psi \mapsto \psi \circ \tau_A^B \,. \tag{6.25}$$

Proof Let $\psi : B \otimes_A U \to V$ be a B-linear map. Then the composition

$$\varphi = \psi \circ \tau_A^B : V \to W \,, \quad v \mapsto \psi(1 \otimes_A u)$$

is A-linear, because $\varphi(av) = \psi(1 \otimes_A av) = \psi(a \otimes_A v) = a\psi(1 \otimes_A v) = a\varphi(v)$. Thus, the map (6.25) is well defined. For every A-linear map $\varphi : V \to W$, there exists at most one B-linear map $\psi : B \otimes_A V \to W$ such that $\varphi = \psi \circ \tau_A^B$, because it must act on the decomposable tensors by the rule $b \otimes v \mapsto b\varphi(v)$. Since $b\varphi(v)$ is bilinear in b, v, this rule actually assigns a well-defined map $B \otimes V \to W$, which is obviously B-linear and annihilates all differences $ba \otimes v - b \otimes av$, because φ is A-linear and $ba\varphi(v) - b\varphi(av) = 0$. Hence, ψ is factorized through the map $B \otimes_A V \to W$. □

Exercise 6.9 Check that the universal property from Proposition 6.3 determines the B-module $B \otimes_A V$ and the A-linear map τ_A^B uniquely up to a unique isomorphism of B-modules commuting with τ_A^B.

Exercise 6.10 Verify that both restriction and induction commute with direct sums.

6.3.2 Induced Representations of Groups

Let $B = \Bbbk[G]$, $A = \Bbbk[H]$ be the group algebras of a finite group G and subgroup $H \subset G$. Then every linear representation $\varrho : G \to \mathrm{GL}(W)$ can be restricted to the representation

$$\operatorname{res}\varrho \overset{\text{def}}{=} \varrho|_H : H \to \mathrm{GL}(W)$$

of H, and this agrees with the restriction of $\Bbbk[G]$-modules to $\Bbbk[H]$-modules. Conversely, every linear representation $\lambda : H \to \mathrm{GL}(V)$ provides G with the *induced representation*

$$\operatorname{ind}\lambda : G \to \mathrm{GL}\big(\Bbbk[G] \otimes_{k[H]} V\big) \tag{6.26}$$

such that $\mathrm{Hom}_G(\operatorname{ind} V, W) \simeq \mathrm{Hom}_H(V, \operatorname{res} W)$. We write res_H^G and ind_H^G for the restriction and induction if the precise reference to $H \subset G$ is required. In terms of characters, restriction and induction assign the homomorphisms of the representation rings

$$\mathrm{Rep}(H) \underset{\text{res}}{\overset{\text{ind}}{\rightleftarrows}} \mathrm{Rep}(G) \quad ,$$

which are adjoint to each other with respect to the scalar product of characters,[12] i.e.,

$$(\chi_{\operatorname{ind} V}, \chi_W)_{\Bbbk^G} = (\chi_V, \chi_{\operatorname{res} W})_{\Bbbk^H}\,,$$

where the left- and right-hand-side scalar products are taken within the spaces of functions $G \to \Bbbk$ and $H \to \Bbbk$ respectively. It follows from this formula that for every two *irreducible* representations

$$\mu : G \to \mathrm{GL}(U_\mu) \quad \text{and} \quad \nu : H \to \mathrm{GL}(U_\nu)\,,$$

[12]See formula (6.23) on p. 137.

the multiplicity of μ in the representation induced by ν equals the multiplicity of ν in the restricted representation μ,

$$m_\mu\,(\operatorname{ind}\nu) = m_\nu\,(\operatorname{res}\mu)\ . \tag{6.27}$$

This equality is known as *Frobenius reciprocity*.

Proposition 6.4 (Transitivity of Induction) *For every tower of subgroups* $K \subset H \subset G$ *and every linear representation* $\varrho : K \to \mathrm{GL}(U)$*, there is the canonical isomorphism of* G*-modules* $\operatorname{ind}_H^G \operatorname{ind}_K^H U \simeq \operatorname{ind}_H^G U$.

Proof Since for every G-module W there are the canonical isomorphisms

$$\operatorname{Hom}_K(U, W) \simeq \operatorname{Hom}_H\left(\operatorname{ind}_K^H U, W\right) \simeq \operatorname{Hom}_G\left(\operatorname{ind}_H^G \operatorname{ind}_K^H U, W\right)\ ,$$
$$\psi \mapsto \psi \circ \tau_K^H \circ \tau_H^G\,,$$

the map $\tau_K^H \circ \tau_H^G : U \to \operatorname{ind}_H^G \operatorname{ind}_K^H U$ possesses the universal property from Proposition 6.3. By Exercise 6.9, there exists a unique isomorphism

$$\operatorname{ind}_H^G \operatorname{ind}_K^H U \simeq \operatorname{ind}_H^G U$$

whose composition with $\tau_K^H \circ \tau_H^G$ is the universal map $\tau_K^G : U \to \operatorname{ind}_K^G U$. $\square$

6.3.3 The Structure of Induced Representations

The tensor product of vector spaces

$$\Bbbk[G] \otimes V = \bigoplus_{g \in G} (\Bbbk \cdot g) \otimes V$$

is a direct sum of $|G|$ copies of the vector space V indexed by the elements $g \in G$. Factorization by the relations $(gh) \otimes v = g \otimes (vu)$ identifies all the direct summands whose indices belong to the same coset gH by gluing together the elements $gh \otimes v$ and $g \otimes hv$. Hence, as a vector space over $\Bbbk$, the tensor product $\Bbbk[G] \otimes_{\Bbbk[H]} V$ is a direct sum of $r = [G : H]$ copies of V indexed by some fixed representatives $g_1, g_2, \ldots, g_r$ of all the left cosets of the subgroup H in G,

$$\Bbbk[G] \underset{\Bbbk[H]}{\oplus} V \simeq g_1 V \oplus g_2 V \oplus g_3 V \oplus\ \cdots\ \oplus g_r V\,. \tag{6.28}$$

Every summand $g_\nu V$ in this sum is a copy of V, and the element g_ν tells that this copy corresponds to the left coset $g_\nu H$. For a vector $v \in V$, we write $g_\nu v$ for the copy of v belonging to the summand $g_\nu V$. Every vector $w \in \Bbbk[G] \otimes_{k[H]} V$ has a unique expansion of the form

$$w = \sum_{\nu=1}^{r} g_\nu v_\nu \,, \text{ where } v_\nu \in V \,.$$

An element $g \in G$ acts on the sum (6.28) as follows. For every $\nu = 1, 2, \dots, r$, there exist unique $h = h(g, \nu) \in H$ and $\mu = \mu(g, \nu) \in \{1, 2, \dots, r\}$ such that $gg_\nu = g_\mu h$. Then for every ν, the element g maps the summand $g_\nu V$ isomorphically onto the summand $g_\mu V$ by the rule $g : g_\nu v \mapsto g_\mu hv$ for all $v \in V$, where $hv \in V$ means the action of the automorphism $h = h(g, \nu) \in H$ on the vector $v \in V$ provided by the initial representation $H \to \mathrm{GL}(V)$.

Example 6.4 Let $G = S_3$, and let $H \subset S_3$ be the subgroup of order 2 generated by the transposition $\sigma = |12\rangle$. Then the elements of G/H can be represented by e, τ, τ^2, where $\tau = |123\rangle$ is a 3-cycle. The representation $W = \operatorname{ind} \mathbb{1}$ induced by the trivial H-module of dimension one has dimension 3 and basis e, τ, τ^2. The generators $\sigma, \tau \in S_3$ are represented by the linear operators with matrices

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

in this basis. Therefore, W is isomorphic to the tautological S_3-module, which is the direct sum of trivial and triangular irreducible representations of S_3. The representation $W' = \operatorname{ind} \operatorname{sgn}$ induced by the 1-dimensional sign representation of H has the same basis e, τ, τ^2, but now σ, τ are represented by the linear operators with matrices

$$\sigma = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} .$$

This representation is a direct sum of the sign representation in the linear span of the vector $e + \tau + \tau^2$ and the triangle representation in the orthogonal 2-plane. The representation of S_3 induced by the 2-dimensional regular representation of H in $\Bbbk[H] \simeq \Bbbk[\sigma]/(\sigma^2 - 1)$ is the 6-dimensional regular representation of S_3 in $\Bbbk[S_3] = e \cdot \Bbbk[H] \oplus \tau \cdot \Bbbk[H] \oplus \tau^2 \cdot \Bbbk[H]$.

Exercise 6.11 Verify that the regular representation of a subgroup always induces the regular representation of the ambient group.

Proposition 6.5 *If a group G has an abelian subgroup $H \subset G$, then every simple G-module has dimension at most*[13] $[G : H]$.

Proof Let U be an irreducible representation of G, and $L \subset \operatorname{res} U$ an H-submodule of dimension 1. By Frobenius reciprocity, U has positive multiplicity in $\operatorname{ind} L$. Hence, $\dim U \leqslant \dim \operatorname{ind} L = [G : H]$. □

Proposition 6.6 *Assume that the intersection of a conjugacy class $C \subset G$ with a subgroup $H \subset G$ splits into m distinct classes with respect to conjugation by the elements of H:*

$$C \cap H = D_1 \sqcup D_2 \sqcup \cdots \sqcup D_m .$$

Then for every representation $H \to \mathrm{GL}(V)$, the character of the induced representation of G takes on the class C, the value

$$\chi_{\operatorname{ind} V}(C) = [G : H] \cdot \sum_{i=1}^{m} \chi_V(D_i) \cdot \frac{|D_i|}{|C|} .$$

In particular, for the trivial 1*-dimensional representation* $\mathbb{1}$ *of H,*

$$\chi_{\operatorname{ind} \mathbb{1}}(C) = [G : H] \cdot \frac{|C \cap H|}{|C|} . \tag{6.29}$$

Proof For every $g \in C$, the summands $g_\nu V$ in the decomposition (6.28) are permuted under the action of g, and a nonzero contribution to the value $\chi_{\operatorname{ind} V}(g)$ is made only by those summands $g_\nu V$ that are mapped to itself by g. The inclusion $g(g_\nu V) \subset g_\nu V$ means that $g g_\nu = g_\nu h$ for some $h = g_\nu^{-1} g g_\nu \in H$. In this case, g acts on $g_\nu V$ by the linear operator representing h in $\mathrm{GL}(V)$ whose trace equals $\chi_V(h) = \chi_V(g_\nu^{-1} g g_\nu)$. Therefore,

$$\chi_{\operatorname{ind} V}(g) = \sum_{\substack{\nu: \\ g_\nu^{-1} g g_\nu \in H}} \chi_V(g_\nu^{-1} g g_\nu) = \frac{1}{|H|} \sum_{\substack{s \in G: \\ s^{-1} g s \in H}} \chi_V(s^{-1} g s) = \frac{1}{|H|} \sum_{i=1}^{m} \sum_{\substack{s \in G: \\ s^{-1} g s \in D_i}} \chi_V(D_i) .$$

(In the second equality, we replace every summand by $|H|$ coinciding summands obtained by writing arbitrary elements $s \in g_\nu H$ instead of g_ν. In the third equality, we collect all the summands with $s^{-1} g s$ lying in the same class D_i.) By the orbit length formula,[14] every product $s^{-1} g s \in D_i$ is obtained from $|G|/|C|$ distinct

[13] In Theorem 10.2 on p. 233 we will see that for every normal abelian subgroup $H \lhd G$, the dimension of every irreducible G-module divides the index $[G : H]$.

[14] See Proposition 12.2 in Sect. 12.5.2 of Algebra I.

elements $s \in G$, and altogether, there are $|D_i|$ such distinct products. Therefore,

$$\chi_{\operatorname{ind} V}(g) = \frac{1}{|H|} \sum_{i=1}^{m} \chi_V(D_i) \cdot |D_i| \cdot |G|/|C| \,,$$

as required. □

Exercise 6.12 (Projection Formula) For every G-module W and H-module V, construct the canonical isomorphism of G-modules $\operatorname{ind}\big((\operatorname{res} W) \otimes V\big) \simeq W \otimes \operatorname{ind} V$, where both tensor products mean the tensor products of the group representations.[15]

6.3.4 *Coinduced Representations*

In the representation theory of associative $\Bbbk$-algebras, besides the induced module $B \otimes_A V$, there is another B-module naturally associated with a representation of a subalgebra $A \subset B$ in a vector space V, namely, the *coinduced module*

$$\operatorname{coind} V \stackrel{\text{def}}{=} \operatorname{Hom}_A(B, V) \,. \tag{6.30}$$

The algebra B acts on $\operatorname{Hom}_A(B, V)$ from the *left* by means of the *right* regular action on itself, that is, given a map $\psi : B \to V$, the map $b\psi : B \to V$ is defined by $b\psi(x) \stackrel{\text{def}}{=} \psi(xb)$ for all $x \in B$.

Exercise 6.13 Check that $b\psi$ is A-linear for A-linear ψ, and that

$$(b_1 b_2)\, \psi = b_1(b_2\psi) \,.$$

The coinduced module has the universal property dual to that from Proposition 6.3. Namely, there exists the canonical A-linear map

$$\tau_B^A : \operatorname{Hom}_A(B, V) \to V \,, \quad \varphi \mapsto \varphi(1) \,,$$

and for every B-module W and A-linear map $\varphi : W \to V$, there exists a unique homomorphism of B-modules $\psi : W \to \operatorname{Hom}_A(B, V)$ such that $\tau_B^A \circ \psi = \varphi$. Equivalently, for every A-module V and B-module W, an isomorphism of vector spaces

$$\begin{gathered} \operatorname{Hom}_B(W, \operatorname{coind} V) \xrightarrow{\sim} \operatorname{Hom}_A(\operatorname{res} W, V) \,, \\ \psi \mapsto \tau_B^A \circ \psi \,, \end{gathered} \tag{6.31}$$

[15] See Sect. 5.4 on p. 109.

is given by sending a B-linear map $\psi : W \to \mathrm{Hom}_A(B, V)$, $w \mapsto \psi_w$, to the A-linear map $\tau_B^A \circ \psi : W \to V\,,\quad w \mapsto \psi_w(1)$. The inverse isomorphism takes an A-linear map $\varphi : W \to V$ to the B-linear map

$$\psi : W \to \mathrm{Hom}_A(B, V)\,, \quad w \mapsto \psi_w\,,$$

where $\psi_w : B \to V\,, \quad b \mapsto \varphi(bw)$.

Exercise 6.14 Verify that both maps are well defined and inverse to each other.

When $A = \Bbbk[H]\,,\ B = \Bbbk[G]$ are the group algebras of a finite group G and a subgroup $H \subset G$, the Fourier transform[16] leads to the isomorphism of vector spaces

$$\Phi \otimes \mathrm{Id}_V : \mathrm{Hom}(\Bbbk[G], V) \xrightarrow{\sim} \Bbbk[G] \otimes V\,, \tag{6.32}$$

mapping a rank-one operator $\xi \otimes v \in \Bbbk[G]^* \otimes V$ to the tensor

$$\widehat{\xi} \otimes v = \frac{1}{|G|} \sum_{g \in G} \xi(g^{-1}) \cdot g \otimes v = \frac{1}{|G|} \sum_{h \in G} h^{-1} \otimes (\xi(h) \cdot v)\ ,$$

where in the second equality we change the summation index by $h = g^{-1}$. Since $\xi(h) \cdot v$ is nothing but the value of the operator $\xi \otimes v : \Bbbk[G] \to V$ at $h \in \Bbbk[G]$, the transformation (6.32) sends an arbitrary linear map $\varphi : \Bbbk[G] \to V$ to the tensor

$$\widehat{\varphi} \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} g^{-1} \otimes \varphi(g)\,,$$

called the *Fourier transform* of the operator φ. The Fourier transform is G-linear, because for every $s \in G$,

$$\begin{aligned} \widehat{s\varphi} &= \frac{1}{|G|} \sum_{g \in G} g^{-1} \otimes s\varphi(g) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \otimes \varphi(gs) \\ &= \frac{1}{|G|} \sum_{g \in G} sg^{-1} \otimes \varphi(g) = s\widehat{\varphi}\,. \end{aligned}$$

The Fourier transform (6.32) followed by the quotient map

$$\Bbbk[G] \otimes V \twoheadrightarrow \Bbbk[G] \otimes_{\Bbbk[H]} V$$

establishes a G-linear isomorphism between the subspace

$$\mathrm{Hom}_H(\Bbbk[G], V) \subset \mathrm{Hom}(\Bbbk[G], V)$$

and $\Bbbk[G] \otimes_{\Bbbk[H]} V$.

[16]See formula (6.21) on p. 137.

Exercise 6.15 Verify the last statement.

Thus, the induced and coinduced representations of a finite group are canonically isomorphic by means of the Fourier transform.

Exercise 6.16 Convince yourself that everything said in this section makes sense and remains true for finite-dimensional representations of every (not necessarily finite) group G and subgroup $H \subset G$ such that $[G : H] < \infty$.

Problems for Independent Solution to Chapter 6

Problem 6.1 Let U, U', and V be the trivial, sign, and simplicial representations of S_5 respectively. Use the isomorphism[17] $\mathrm{PGL}_2(\mathbb{F}_5) \xrightarrow{\sim} S_5$ to construct a representation of S_5 in the space W of all functions $\mathbb{P}_1(\mathbb{F}_5) \to \mathbb{C}$ with a zero sum of values. Compute the characters of the representations U, U', V, $V \otimes U'$, $\Lambda^2 V$, $S^2 V$, W, $W \otimes U'$, $W \otimes V$, $S^2 W$, and $\Lambda^2 W$. Indicate which of these representations are irreducible.

Problem 6.2 Describe the isotypic decompositions of the restrictions of all irreducible representations of S_4 on the subgroups **(a)** $S_3 = \mathrm{Stab}_{S_4}(4)$, **(b)** A_4.

Problem 6.3 The same question for the restrictions of simple S_5-modules to the subgroups **(a)** $S_4 = \mathrm{Stab}_{S_5}(5)$, **(b)** A_5.

Problem 6.4 Let G be a finite group, and $\varrho : \mathbb{C}[G] \to \mathrm{GL}(V)$ an injective complex representation of dimension $\dim V \geqslant 2$. Prove that the character χ_ϱ takes the value $\dim V$ on exactly one conjugacy class of G.

Problem 6.5 Let the character of an irreducible complex representation V of a finite group take a nonzero value on a conjugacy class K such that $|K|$ and $\dim V$ are coprime. Prove that all elements of K act on V by scalar homotheties.

Problem 6.6 Describe the isotypic decomposition of the complex representation of S_4 induced by **(a)** the 1-dimensional representation of a 4-cycle by multiplication by $i \in \mathbb{C}$, **(b)** the 1-dimensional representation of a 3-cycle by multiplication by $e^{2\pi i/3} \in \mathbb{C}$, **(c)** the triangular representation of $S_3 = \mathrm{Stab}_{S_4}(4) \subset S_4$.

Problem 6.7 Describe the isotypic decomposition of the complex representation of S_5 induced by **(a)** the 1-dimensional representation of a 5-cycle by multiplication by $e^{2\pi i/5} \in \mathbb{C}$, **(b)** both 3-dimensional representations of $A_5 \subset S_5$ by the rotations of the dodecahedron.[18]

[17] See the comments to Exercise 6.7.

[18] See Exercise 6.7 on p. 138 about the dodecahedral representations, and Example 12.12 in Sect. 12.4 of Algebra I for more details about the isomorphism between A_5 and the proper dodecahedral group.

Problem 6.8 Write $R(G) \subset \mathbb{C}^G$ for the representation ring[19] of a finite group G. Establish an isomorphism of additive abelian groups

$$R(G_1 \times G_2) \simeq R(G_1) \otimes R(G_2).$$

Problem 6.9 Are the representation rings $R(Q_8)$ and $R(D_4)$ isomorphic?[20]

Problem 6.10 (Affine Group of a Line) Write A for the group of affine automorphisms $x \mapsto ax + b$ of the line $\mathbb{A}^1 = \mathbb{A}(\mathbb{F}_p)$ over the field $\mathbb{F}_p = \mathbb{Z}/(p)$.

(a) Show that $A = \mathbb{F}_p \rtimes \mathbb{F}_p^*$, where $\mathbb{F}_p \subset A$ is the additive group of parallel displacements, and is $\mathbb{F}_p^* \subset A$ the multiplicative group of dilatations with respect to the origin $0 \in \mathbb{A}^1$. Enumerate the conjugacy classes of A.
(b) Calculate the character of the representation of A in the space V of functions $\mathbb{A}^1 \to \mathbb{C}$ with zero sum of values, and show that V is irreducible.
(c) Check that the previous representation V is induced by the 1-dimensional representation $\mathbb{F}_p \to \mathrm{U}(1)$, $t \mapsto e^{2\pi i t/p}$, of the subgroup of parallel displacements.
(d) Prove that all the other irreducible representations of A have dimension one.

Problem 6.11 (The Heisenberg Group Over $\mathbb{F}_p$ for $p > 2$) Let L be a vector space of dimension n over the residue field $\mathbb{F}_p = \mathbb{Z}/(p)$ with $p > 2$. The *Heisenberg group* H_p^n consists of all triples $(x, u, u^*) \in \mathbb{F}_p \times L \times L^*$ with the composition law

$$(x_1, u_1, u_1^*) \circ (x_2, u_2, u_2^*)$$
$$\stackrel{\text{def}}{=} \big(x_1 + x_2 + \big(\langle u_2^*, u_1 \rangle - \langle u_1^*, u_2 \rangle\big)/2,\ u_1 + u_2,\ u_1^* + u_2^*\big)\ .$$

Write $H' \simeq \mathbb{F}_p \times L \subset H_p^n$ for the subgroup formed by all triples $(x, u, 0)$.

(a) Show that H_p^n actually is a group, and enumerate the conjugacy classes of H_p^n.
(b) Check that H_p^1 is isomorphic to the group of upper unitriangular 3×3 matrices over $\mathbb{F}_p$.
(c) For $a \in \mathbb{F}_p^*$, write W_a for the representation of H_p^n induced by the 1-dimensional H'-module with the character $\psi_a(x, u, 0) = e^{2\pi i a x/p}$. Show that all W_a are irreducible, and calculate their characters.
(d) Verify that all the representations W_a are nonisomorphic, and all the other irreducible representations of H_p^n have dimension one.

Problem 6.12 (The Heisenberg Group Over $\mathbb{F}_2$) Write H for the group generated by $4n + 4$ elements $\pm 1, \pm u_1, \dots, \pm u_{2n+1}$ constrained by the relations

$$u_i^2 = -1\,, \quad u_i u_j = -u_j u_i\,,$$

---

[19]See Sect. 6.2.3 on p. 140.

[20]Recall that $Q_8 = \{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\} \subset \mathbb{H}$ is the group of quaternionic units, and D_4 the group of the square.

and "a minus times a minus is equal to a plus." Verify that H consists of 2^{2n+2} distinct elements $\pm u_I = \pm u_{i_1} u_{i_2} \cdots u_{i_k}$, where $I = \{i_1, i_2, \dots, i_k\}$ runs through the increasing subsets in $\{1, 2, \dots, (n+1)\}$ and $u_\varnothing = 1$. Check that elements $\pm u_I$ labeled by all the I's of even cardinality form a subgroup[21] $H_2^n \subset H$, and $H_2^1 \simeq Q_8$ is the group of quaternionic units. Describe the center $Z(H_2^n)$. Enumerate the conjugacy classes and all complex irreducible representations of H_2^n.

Problem 6.13* Let $\varrho : G \to \mathrm{GL}(V)$ be an effective[22] representation of a finite group G. Prove that every irreducible representation of G appears with nonzero multiplicity in the isotypic decomposition of some tensor power $V^{\otimes m}$.

[21] Called the *Heisenberg group* over $\mathbb{F}_2$.

[22] That is, with trivial kernel $\ker \varrho = e$.

Chapter 7
Representations of Symmetric Groups

7.1 Action of S_n on Filled Young Diagrams

7.1.1 Row and Column Subgroups Associated with a Filling

A Young diagram λ of weight $|\lambda| = n$ filled by nonrepeating numbers $1, 2, \dots, n$ is called a *standard filling* of shape λ. Given a filling T, we write $\lambda(T)$ for its shape. Associated with every standard filling T of shape $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$, $\sum \lambda_i = n$, are the *row subgroup* $R_T \subset S_n$ and the *column subgroup* $C_T \subset S_n$ permuting the elements $1, 2, \dots, n$ only within the rows and within the columns of T respectively. Thus, $R_T \simeq S_{\lambda_1} \times S_{\lambda_2} \times \cdots \times S_{\lambda_k}$ and $C_T \simeq S_{\lambda_1^t} \times S_{\lambda_2^t} \times \cdots \times S_{\lambda_m^t}$, where $\lambda^t = (\lambda_1^t, \lambda_2^t, \dots, \lambda_m^t)$ is the transposed Young diagram. For example, the standard filling

$$T = \begin{array}{|c|c|c|c|} \hline 7 & 1 & 3 & 5 \\ \hline 2 & 4 & 8 \\ \cline{1-3} 6 \\ \cline{1-1} \end{array}$$

picks out the following row and column subgroups in $S_8 = \mathrm{Aut}(\{1, 2, \dots, 8\})$:

$$R_T = \mathrm{Aut}(\{1, 3, 5, 7\}) \times \mathrm{Aut}(\{2, 4, 8\}) \times \mathrm{Aut}(\{6\}) \simeq S_4 \times S_3\,,$$

$$C_T = \mathrm{Aut}(\{2, 6, 7\}) \times \mathrm{Aut}(\{1, 4\}) \times \mathrm{Aut}(\{3, 8\}) \times \mathrm{Aut}(\{5\}) \simeq S_3 \times S_2 \times S_2\,.$$

Exercise 7.1 Convince yourself that S_n acts transitively by the permutations of filling numbers on the set of all standard fillings of shape λ, and $R_{gT} = gR_Tg^{-1}$, $C_{gT} = gC_Tg^{-1}$ for every $g \in S_n$ and standard filling T.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_7

Recall that we say that a Young diagram λ *dominates*[1] a Young diagram μ, and write $\lambda \trianglerighteq \mu$, if $\lambda_1 + \lambda_2 + \cdots + \lambda_k \geqslant \mu_1 + \mu_2 + \cdots + \mu_k$ for all $k \in \mathbb{N}$. Also, we write $\lambda > \mu$ for the total lexicographic order[2] on the set of all Young diagrams. Note that μ cannot dominate λ if $\lambda > \mu$.

Lemma 7.1 *Let U, T be standard fillings of shapes μ, λ with the same weight $|\lambda| = |\mu|$. If μ does not strictly dominate λ, then either there are two numbers in the same row of T and in the same column of U, or $\lambda = \mu$ and $pT = qU$ for some $p \in R_T$, $q \in C_U$.*

Proof Suppose that the elements of every row in T are in different columns of U. Since the elements from the top row of T are distributed among different columns of U, the inequality $\lambda_1 \leqslant \mu_1$ holds, and there exists $q_1 \in C_U$ moving all the elements from the top row of T to the top row of $q_1 U$. Since the elements from the second row of T are still distributed among different columns of $q_1 U$, there exists $q_2 \in C_{q_1 U} = C_U$ that leaves all the elements from the first row of T fixed and moves all the elements from the second row of T to the top two rows of $q_2 q_1 U$. Here we have the inequality $\lambda_1 + \lambda_2 \leqslant \mu_1 + \mu_2$. Repeating this argument, we get a sequence of permutations $q_1, q_2, \dots, q_k \in C_U$, where k is the number or rows in the diagram λ, such that every q_i leaves fixed all the elements lying simultaneously within the top i rows of T and $i-1$ rows of $q_{i-1} \cdots q_1 U$, and lifts all the remaining elements from the ith row of T to the top i rows of $q_i q_{i-1} \cdots q_1 U$. In particular, $\lambda_1 + \lambda_2 + \cdots + \lambda_i \leqslant \mu_1 + \mu_2 + \cdots + \mu_i$ for all i. By the assumption of the lemma, $\lambda \trianglelefteq \mu$ forces $\lambda = \mu$, and therefore, each q_i sends the elements from the ith row of T to the ith row of $q_i q_{i-1} \cdots q_1 U$. Thus, $q_k \cdots q_1 U = pT$ with $p \in R_T$. $\square$

Corollary 7.1 *A permutation $g \in S_n$ is factorized as $g = pq$ with $p \in R_T$, $q \in C_T$ if and only if the elements of every row in T appear in different columns of gT. Such a factorization is unique if it exists.*

Proof If $U = pqT$, where $p \in R_T$, $q \in C_T$, then all elements of every row in T are in different columns of U, because q shifts these elements along the columns and p permutes the resulting set of shifted elements within itself. Conversely, if every row of T is distributed between different columns of $U = gT$, then by Lemma 7.1, there exist $p \in R_T$ and $q \in C_U$ such that $pT = qU = qgT$. Hence, $p = qg$. Since $q \in C_{gT} = gC_T g^{-1}$ can be written as $gq_1 g^{-1}$ with $q_1 \in C_T$, we conclude that $g = pq_1^{-1}$, as required. The factorization $g = pq$ is unique, because of $R_T \cap C_T = \{e\}$. $\square$

[1] See formula (4.11) on p. 89.

[2] This means that $\lambda_i > \mu_i$ for the minimal $i \in \mathbb{N}$ such that $\lambda_i \neq \mu_i$.

7.1.2 Young Symmetrizers $s_T = r_T \cdot c_T$

Given a standard filling T of shape λ with $|\lambda| = n$, the elements

$$r_T = \sum_{\sigma \in R_T} \sigma \,, \quad c_T = \sum_{\sigma \in C_T} \mathrm{sgn}(\sigma) \cdot \sigma \,, \tag{7.1}$$

$$s_T = r_T \cdot c_T = \sum_{p \in R_T} \sum_{q \in C_T} \mathrm{sgn}(q) \cdot pq \,, \tag{7.2}$$

of the group algebra $\mathbb{C}[S_n]$ are called, respectively, the *row*, *column*, and *total Young symmetrizers*. They have the following obvious properties:

$$\forall g \in S_n \,, \quad r_{gT} = g r_T g^{-1} \,, \quad c_{gT} = g c_T g^{-1} \,, \quad s_{gT} = g s_T g^{-1} \,, \tag{7.3}$$

$$\forall\, p \in R_T ,\ p r_T = r_T p = r_T \quad \text{and} \quad \forall\, q \in C_T ,\ q c_T = c_T q = \mathrm{sgn}(q) \cdot c_T \,, \tag{7.4}$$

$$\forall\, p \in R_T ,\ \forall\, q \in C_T ,\ p s_T q = \mathrm{sgn}(q) \cdot s_T \,. \tag{7.5}$$

Moreover, the total Young symmetrizer $s_T \in \mathbb{C}[S_n]$ is uniquely determined up to proportionality by the property (7.5), because of the following claim.

Lemma 7.2 *The vector space*

$$E_T \overset{\text{def}}{=} \{\sigma \in \mathbb{C}[S_n] \mid \forall p \in R_T ,\ \forall q \in C_T \,,\, p\sigma q = \mathrm{sgn}(q) \cdot \sigma\}$$

has dimension 1 *and is spanned by the Young symmetrizer* s_T.

Proof Let us show that every element $\sigma = \sum_{g \in S_n} x_g g \in E_T$ is equal to $x_e \cdot s_T$. The equality $p\sigma q = \mathrm{sgn}(q) \cdot \sigma$ means that $x_{pgq} = \mathrm{sgn}(q) \cdot x_g$ for all $g \in S_n$. In particular, for $g = e$, we get $x_{pq} = \mathrm{sgn}(q) \cdot x_e$, and therefore $\sigma = x_e \cdot s_T + \sum_{g \notin R_T C_T} x_g g$. It remains to verify that every coefficient x_g in the latter sum is zero. By Corollary 7.1, for every $g \notin R_T C_T$, there are two elements of the alphabet $\{1, 2, \dots, n\}$ situated in the same row of T and the same column of $U = gT$. The transposition $\tau \in S_n$ of these elements belongs to both subgroups R_T and $C_U = g C_T g^{-1}$, the latter of which means that $g^{-1} \tau g \in C_T$. The equality $x_{pgq} = \mathrm{sgn}(q) \cdot x_g$ written for $p = \tau$, $q = g^{-1}\tau g$ becomes $x_g = -x_g$. Hence, $x_g = 0$. □

Lemma 7.3 *For every filling T, the equalities $s_T \cdot \mathbb{C}[S_n] \cdot s_T = \mathbb{C} \cdot s_T$ and $s_T^2 = n_\lambda \cdot s_T$ hold, where*

$$n_\lambda = \frac{n!}{\dim\left(\mathbb{C}[S_n] \cdot s_T\right)}$$

is a positive rational number depending only on the shape λ of the filling T.

Proof It follows from (7.4) and (7.5) that for every $x \in \mathbb{C}[S_n]$, the element $s_T \cdot x \cdot s_T$ possesses the property (7.5) and therefore lies in the dimension-one subspace

$E_T = \mathbb{C} \cdot s_T$ from Lemma 7.2. In particular, $s_T^2 = n_T \cdot s_T$ for some $n_T \in \mathbb{C}$, which can be evaluated by computing the trace of the endomorphism

$$\varphi : \mathbb{C}[S_n] \to \mathbb{C}[S_n] , \quad x \mapsto x \cdot s_T ,$$

in two different ways, as follows. Formula (7.2) implies that the coefficient of g in the expansion of the product $g \cdot s_T$ equals 1 for all $g \in S_n$. Hence,

$$\operatorname{tr}(\varphi) = |S_n| = n! .$$

On the other hand, the left regular S_n-module $\mathbb{C}[S_n]$ is completely reducible, and there exists an S_n-submodule $W \subset \mathbb{C}[S_n]$ such that $\mathbb{C}[S_n] = W \oplus \mathbb{C}[S_n] \cdot s_T$. Right multiplication by s_T maps W to $\mathbb{C}[S_n] \cdot s_T$ and acts on $\mathbb{C}[S_n] \cdot s_T$ as scalar multiplication by n_T. Thus, $\operatorname{tr}(\varphi) = n_T \cdot \dim(\mathbb{C}[S_n] \cdot s_T)$. This forces $n_T = n!/\dim(\mathbb{C}[S_n] \cdot s_T)$ to be positive and rational. Since $s_{gT} = g s_T g^{-1}$, and therefore

$$s_{gT}^2 = g s_T^2 g^{-1} = n_T g s_T g^{-1} = n_T s_{gT} ,$$

the number $n_T = n_{\lambda(T)}$ depends only on the shape $\lambda = \lambda(T)$ of the filling T. □

Lemma 7.4 *If the shape of a filling T is lexicographically bigger than the shape of a filling U, then*

$$r_T \cdot \mathbb{C}[S_n] \cdot c_U = c_U \cdot \mathbb{C}[S_n] \cdot r_T = s_T \cdot \mathbb{C}[S_n] \cdot s_U = 0 .$$

Proof It is enough to check that $r_T \cdot g \cdot c_U = c_U \cdot g \cdot r_T = 0$ for all $g \in S_n$. To begin with, let $g = e$. Then by Lemma 7.1, there are two elements lying in the same row of T and column of U. The transposition τ of these elements belongs to $R_T \cap C_U$. Hence,

$$r_T \cdot c_U = (r_T \cdot \tau) \cdot c_U = r_T \cdot (\tau \cdot c_U) = -r_T \cdot c_U$$

and

$$c_U \cdot r_T = -(c_U \cdot \tau) \cdot r_T = -c_U \cdot (\tau \cdot r_T) = -c_U \cdot r_T .$$

This forces $r_T \cdot c_U = c_U \cdot r_T = 0$. Now, for every $g \in S_n$, we have

$$r_T \cdot g \cdot c_U = r_T \cdot g c_U g^{-1} \cdot g = \left(r_T \cdot c_{gU}\right) \cdot g = 0$$

and

$$c_U \cdot g \cdot r_T = c_U \cdot g r_T g^{-1} \cdot g = \left(c_U \cdot r_{gT}\right) \cdot g = 0 .$$

□

Theorem 7.1 *For every standard filling T, the representation of S_n by left multiplication in the left ideal*

$$V_T \stackrel{\text{def}}{=} \mathbb{C}[S_n] \cdot s_T \subset \mathbb{C}[S_n]$$

is irreducible. Two such representations V_T, V_U are isomorphic if and only if the fillings T, U have the same shape, $\lambda = \lambda(T) = \lambda(U)$. Every simple S_n-module is isomorphic to some V_T with $|\lambda(T)| = n$.

Proof Let $W \subset V_T$ be an S_n-submodule. Write $\pi : \mathbb{C}[S_n] \twoheadrightarrow W$ for an S_n-linear projection, and let $w = \pi(1) \in W$. Then $\pi(x) = \pi(x \cdot 1) = x \cdot \pi(1) = x \cdot w$ for all $x \in \mathbb{C}[S_n]$. This forces $W = \mathbb{C}[S_n] \cdot w$ and $w \cdot w = \pi(w) = w$. Since

$$s_T \cdot W \subset s_T \cdot V_T = s_T \cdot \mathbb{C}[S_n] \cdot s_T = \mathbb{C} \cdot s_T\,,$$

the image of the map $s_T : W \to W$, $x \mapsto s_T x$, is either 0 or $E_T = \mathbb{C} \cdot s_T$. In the first case, $W \cdot W \subset V_T \cdot W = \mathbb{C}[S_n] \cdot s_T \cdot W = 0$. Hence, $w = w \cdot w = 0$ and $W = 0$. In the second case, $s_T \in s_T \cdot W \subset W$. Hence, $V_T = \mathbb{C}[S_n] \cdot s_T \subset W$ and $W = V_T$. We conclude that V_T is a simple S_n-module.

Let two fillings T, U have different shapes, say $\lambda(T) > \lambda(S)$ lexicographically. By Lemma 7.4 on p. 154, left multiplication by s_T annihilates the S_n-module V_U and acts nontrivially on V_T, because $s_T \in V_T$ is an eigenvector of s_T with the nonzero eigenvalue $n_{\lambda(T)}$. Therefore, the representations V_T and V_U are not isomorphic.

Let us fix some filling T_λ for every Young diagram λ of weight n. Then all the irreducible representations V_{T_λ} are distinct and are in bijection with the conjugacy classes of S_n. Therefore, every irreducible S_n-module is isomorphic to one and only one module V_{T_λ}. In particular, for every filling S of a given shape λ, the irreducible S_n-module V_S is isomorphic to V_{T_λ}, because $V_{T_\mu} \not\simeq V_S$ for $\mu \neq \lambda(S)$, as we have just seen. □

Notation 7.1 We write V_λ for the isomorphism class of the irreducible representation $\mathbb{C}[S_n] \cdot s_{T_\lambda}$ from Theorem 7.1, where T_λ is some standard filling of the shape λ. As λ runs through the Young diagrams of weight n, the classes V_λ form the complete list $\mathrm{Irr}(S_n)$ of simple S_n-modules up to isomorphism.

7.1.3 Young Symmetrizers $s'_T = c_T \cdot r_T$

In general, the subsets $R_T C_T$ and $C_T R_T$ in S_n are distinct. For example, the standard filling

$$T = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}$$

leads to the set $R_T C_T$ containing exactly one 3-cycle $|12\rangle \circ |13\rangle = |132\rangle$, whereas the only 3-cycle in $C_T R_T$ is $|13\rangle \circ |12\rangle = |123\rangle$. Thus, swapping the factors in (7.2) leads to the symmetrizer

$$s'_T = c_T \cdot r_T = \sum_{p \in R_T} \sum_{q \in C_T} \operatorname{sgn}(q) \cdot qp, \tag{7.6}$$

which is different from the symmetrizer $s_T = r_T \cdot c_T$ in general. The symmetrizers s'_T and s_T go to each other under the *antipodal antiautomorphism* $\alpha : \mathbb{C}[S_n] \xrightarrow{\sim} \mathbb{C}[S_n]$, $g \mapsto g^{-1}$, which leaves the factors r_T, c_T unchanged but reverses their order in the product.

Exercise 7.2 For the Young symmetrizer s'_T, formulate and prove the analogues of the relations (7.5), Lemma 7.4, Lemma 7.3, and Theorem 7.1.

Lemma 7.5 *The representations of S_n by left multiplication in the ideals $V_T = \mathbb{C}[S_n] \cdot s_T$ and $V'_T = \mathbb{C}[S_n] \cdot s'_T$ are isomorphic.*

Proof Right multiplication by c_T and r_T assigns homomorphisms of the left S_n-modules

$$V'_T = \mathbb{C}[S_n] \cdot c_T r_T \underset{x \cdot r_T \,\leftarrow\, x}{\overset{x \mapsto x \cdot c_T}{\rightleftarrows}} \mathbb{C}[S_n] \cdot r_T c_T = V_T\,.$$

The composition $x \mapsto x \cdot r_T c_T = x \cdot s_T$ acts on $V_T = \mathbb{C}[S_n] \cdot s_T$ as scalar multiplication by $n_{\lambda(T)}$. Therefore, right multiplication by c_T and right multiplication by $n_\lambda^{-1} r_T$ are isomorphisms of S_n-modules that are inverse to each other. □

Theorem 7.2 *The classes of the irreducible representations V_λ and V_{λ^t} corresponding to the transposed Young diagrams λ and λ^t are obtained from each other by taking the tensor product with the sign representation.*

Proof Let us fix some standard filling T of shape λ and the transposed filling T^t of shape λ^t. Then $R_{T^t} = C_T$, $C_{T^t} = R_T$, and

$$s_{T^t} = \sum_{p \in R_T} \sum_{q \in C_T} \operatorname{sgn}(p) \cdot qp = \sum_{p \in R_T} \sum_{q \in C_T} \operatorname{sgn}(q) \cdot \operatorname{sgn}(pq) \cdot qp = \sigma\left(s'_T\right),$$

where $\sigma : \mathbb{C}[S_n] \to \mathbb{C}[S_n]$, $g \mapsto \operatorname{sgn}(g) \cdot g$, is the *sign automorphism* of the group algebra. For every representation $\varrho : \mathbb{C}[S_n] \to \operatorname{End}(W)$, the tensor product with the sign representation $W \otimes \operatorname{sgn}$ is isomorphic to the representation

$$\varrho \circ \sigma \colon \mathbb{C}[S_n] \to \operatorname{End}(W).$$

In particular, $V_T \otimes \operatorname{sgn} \simeq V'_T \otimes \operatorname{sgn}$ is isomorphic to the representation of S_n in the space $V'_T = \mathbb{C}[S_n] \cdot s'_T$ by the rule

$$g : x \cdot s'_T \mapsto \operatorname{sgn}(g) \cdot gx \cdot s'_T\,. \tag{7.7}$$

The sign automorphism maps the space V'_T isomorphically onto the space

$$V_{\lambda^t} = \mathbb{C}[S_n] \cdot s_{T^t} = \mathbb{C}[S_n] \cdot \sigma\left(s'_T\right)$$

and transforms the action (7.7) to the left regular action $g : \sigma(x) \cdot s_{T^t} \mapsto g\sigma(x) \cdot s_{T^t}$. $\square$

7.2 Modules of Tabloids

The R_T-orbit of a standard filling T is called a *tabloid* of shape $\lambda = \lambda(T)$ and is denoted by $\{T\}$. The tautological action of S_n on the standard fillings $g : T \mapsto gT$ induces the well-defined action $g : \{T\} \mapsto \{gT\}$ on the tabloids, because

$$gR_T T = gR_T g^{-1} gT = R_{gT} gT .$$

Write M_λ for the complex vector space with a basis formed by the tabloids of shape λ. The permutation representation of S_n in M_λ by the rule $g : \{T\} \mapsto \{gT\}$ is called the *tabloid representation*. Equivalently, the tabloid module $M_\lambda \simeq \operatorname{ind}_{R_T}^{S_n} \mathbb{1}$ is described as the representation of S_n induced from the trivial 1-dimensional representation of the subgroup $R_T \subset S_n$. Indeed, the tabloids of shape λ are in bijection with the left cosets $gR_T \in S_n/R_T$, and the action of S_n on the tabloids coincides with the left action on these cosets.

Exercise 7.3 Show that the tabloid representation M_λ is isomorphic to the representation of S_n by left multiplication in the ideal $\mathbb{C}[S_n] \cdot r_T$.

We write ψ_λ for the character of the tabloid representation M_λ. Recall that $C_\eta \in \mathrm{Cl}(S_n)$ means the conjugacy class formed by all permutations of cyclic type η.

Proposition 7.1 *Let $m_\lambda = m_{\lambda_1} m_{\lambda_2} \cdots m_{\lambda_n}$ be the standard monomial basis*[3] *of the $\mathbb{Z}$-module of symmetric polynomials in $x_1, x_2, \dots, x_n$, and*

$$p_\eta(x) = p_{\eta_1} p_{\eta_2} \cdots p_{\eta_n} = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_n(x)^{n_n}$$

the Newton symmetric polynomial.[4] *The value $\psi_\lambda(C_\eta)$ equals the coefficient of m_λ in the expansion of p_η through the monomial basis.*

Proof The n_ith power of the ith Newton polynomial is expanded as

$$p_i(x)^{n_i} = \left(x_1^i + x_2^i + \cdots + x_n^i\right)^{n_i} = \sum_{\sum_j \varrho_{ij} = n_i} \frac{n_i!}{\varrho_{i1}! \varrho_{i2}! \cdots \varrho_{in}!} x_1^{i \cdot \varrho_{i1}} x_2^{i \cdot \varrho_{i2}} \cdots x_n^{i \cdot \varrho_{in}} .$$

[3] Recall that it is numbered by the Young diagrams of length at most n; see formula (3.3) on p. 58.

[4] See formula (3.12) on p. 62. Note that $n_j = n_j(\eta)$ equals the number of length-j rows in the diagram η.

Therefore, the coefficient of $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ in the expansion of

$$p_\eta(x) = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_n(x)^{n_n}$$

is equal to the sum

$$\sum_{\varrho_{ij}} \frac{n_1! \cdot n_2! \cdots n_n!}{\prod_{ij} \varrho_{ij}!} \tag{7.8}$$

running over all collections of nonnegative integers ϱ_{ij} such that

$$\textstyle\sum_j \varrho_{ij} = n_i \quad \text{and} \quad \sum_i i \cdot \varrho_{ij} = \lambda_j \,. \tag{7.9}$$

On the other hand, it follows from formula (6.29) on p. 145 for the character of an induced representation that

$$\psi_\lambda(C_\eta) = [S_n : R_T] \cdot \frac{|C_\eta \cap R_T|}{|C_\eta|}\,, \tag{7.10}$$

where

$$[S_n : R_T] = \frac{n!}{\prod_j \lambda_j!}\,, \quad |C_\eta| = \frac{n!}{\prod_i i^{n_i} n_i!}\,,$$

and $C_\eta \cap R_T$ splits into a disjoint union of R_T-conjugacy classes of permutations of cyclic type η lying in R_T. The elements of every independent cycle of a permutation $\sigma \in C_\eta \cap R_T$ belong to the same row of the filling T. Two such permutations are conjugate within R_T if and only if both permutations have the same number ϱ_{ij} of length-i cycles formed by elements from the jth row of T for all $1 \leqslant i, j \leqslant n$. Since every collection ϱ of numbers ϱ_{ij} is obviously constrained by the conditions (7.9), the R_T-conjugacy classes $D_\varrho \subset C_\eta \cap R_T$ are in bijection with the summands of (7.8). The stabilizer of a permutation $\sigma \in \Delta_\varrho$ under conjugation by the elements of R_T consists of $\prod \varrho_{ij}!$ independent permutations of cycles having equal lengths, and $\prod i^{n_i}$ independent cyclic permutations of elements within the cycles. Hence,

$$|C_\eta \cap R_T| = \sum_\varrho |D_\varrho| = \sum_\varrho \frac{\prod_j \lambda_j!}{\prod_{ij} i^{n_i} \varrho_{ij}!}\,.$$

Substituting these values in (7.10) leads to (7.8) after obvious cancellations. □

7.3 Specht Modules

7.3.1 Description and Irreducibility

Associated with a filling T of shape λ is the vector

$$v_T = c_T\{T\} = \sum_{q \in C_T} \operatorname{sgn}(q) \cdot \{qT\} \in M_\lambda \,. \tag{7.11}$$

By Lemma 7.1 on p. 152, the equality $pq_1T = q_2T$ never holds for

$$q_1, q_2 \in C_T = C_{q_1T}, p \in R_{q_1T},$$

because every two elements sharing the same column in T are certainly in different rows of q_1T. Therefore, the summands on the right-hand side of (7.11) are distinct basis vectors of M_λ taken with coefficients ± 1. In particular, each vector v_T is nonzero. Since

$$gv_T = gc_T\{T\} = gc_Tg^{-1}\{gT\} = c_{gT}\{gT\} = v_{gT}$$

for all $g \in S_n$, the linear span of all vectors v_T, where T is a standard filling of shape λ, is an S_n-submodule in M_λ. It is called the *Specht module* and denoted by S_λ.

Lemma 7.6 *If the shape λ of a filling T does not strictly dominate a Young diagram μ, then*

$$c_TM_\mu = \begin{cases} 0 & \text{for } \mu \neq \lambda \,, \\ \mathbb{C} \cdot v_T & \text{for } \mu = \lambda \,. \end{cases}$$

Proof Let U be a standard filling of shape μ. If there is a transposition $\tau \in R_U \cap C_T$, then

$$c_T\{U\} = c_T\{\tau U\} = c_T \cdot \tau\{U\} = -c_T\{U\} \,. \tag{7.12}$$

Hence, $c_T\{U\} = 0$. If there are no transpositions in $R_U \cap C_T$, then $\lambda = \mu$ and $pU = qT$ for some $p \in R_U$, $q \in C_T$ by Lemma 7.1. In this case,

$$c_T\{U\} = c_T\{pU\} = c_T\{qT\} = \operatorname{sgn}(q) \cdot c_T\{T\} = \pm v_T.$$

□

Theorem 7.3 *The Specht module S_λ is simple and belongs to the class V_λ, i.e., is isomorphic to the left ideal $\mathbb{C}[S_n] \cdot s_T$, where T is a standard filling of shape λ.*

Proof Let T be a standard filling of shape λ. Assume that $S_\lambda = V \oplus W$ is a direct sum of S_n-modules. Since $c_TS_\lambda \subset c_T \cdot M_\lambda = \mathbb{C} \cdot v_T$ by Lemma 7.6, and c_T maps each of the submodules V, W to itself, v_T belongs to one of them, say $v_T \in V$. Then V contains all vectors $v_{gT} = gv_T$, $g \in S_n$, and therefore coincides with S_λ. Hence, S_λ is an irreducible representation of S_n. Moreover, $S_\lambda \not\simeq S_\mu$ for $\mu \neq \lambda$. Indeed, let $\lambda < \mu$ lexicographically. By Lemma 7.6, the action of c_T annihilates $S_\mu \subset M_\mu$ and is nontrivial on S_λ, because $c_T v_T = c_T c_T\{T\} = |C_T| \cdot c_T\{T\} = |C_T| \cdot v_T$. Thus, the Specht modules S_λ form a complete list of distinct simple S_n-modules up to isomorphism. Since c_T annihilates all irreducible representations V_μ with $\mu < \lambda$ by Lemma 7.4 on p. 154, we conclude that S_λ belongs to the class V_λ. □

Corollary 7.2 *The multiplicity of the simple submodule S_μ in the tabloid module M_λ may be nonzero only if $\mu \trianglerighteq \lambda$. For all λ, the multiplicity of S_λ in M_λ equals* 1.

Proof Since c_T sends the whole of M_λ inside $S_\lambda \subset M_\lambda$ and acts nontrivially on S_λ, there is exactly one simple submodule isomorphic to S_λ in M_λ. If there exists an S_n-linear injection $S_\mu \hookrightarrow M_\lambda$ for $\mu \neq \lambda$, then the operator c_U, constructed from every filling U of shape μ, does not annihilate M_λ. Thus, Lemma 7.6 forces $\mu \vartriangleright \lambda$. □

7.3.2 *Standard Basis Numbered by Young Tableaux*

Let us define the *column scanning* of a filling T of shape λ to be the word obtained by reading the columns of T from the bottom upward one by one from left to right. For example, the column scan of the standard tableau

$$T = \begin{ytableau} 1 & 3 & 4 \\ 2 & 5 \end{ytableau}$$

is the word 21534. We write $T \succ U$ if the maximal element in different cells of T, U appears in the column scan of T in a position to the left of that in the scan of U.

Exercise 7.4 For every Young diagram λ, verify that the relation $T \succ U$ provides the set of all standard fillings of shape λ with a total order.

For example, the 120 standard fillings of the Young diagram $\ydiagram{2,2,1}$ are ordered as

$$\begin{ytableau} 3 & 1 \\ 4 & 2 \\ 5 \end{ytableau} \succ \begin{ytableau} 3 & 2 \\ 4 & 1 \\ 5 \end{ytableau} \succ \begin{ytableau} 2 & 1 \\ 4 & 3 \\ 5 \end{ytableau} \succ \begin{ytableau} 1 & 2 \\ 4 & 3 \\ 5 \end{ytableau} \succ \begin{ytableau} 2 & 3 \\ 4 & 1 \\ 5 \end{ytableau} \succ \begin{ytableau} 1 & 3 \\ 4 & 2 \\ 5 \end{ytableau} \succ \begin{ytableau} 4 & 1 \\ 3 & 2 \\ 5 \end{ytableau} \succ \cdots$$

$$\succ \begin{ytableau} 4 & 5 \\ 2 & 3 \\ 1 \end{ytableau} \succ \begin{ytableau} 1 & 5 \\ 2 & 4 \\ 3 \end{ytableau} \succ \begin{ytableau} 2 & 5 \\ 1 & 4 \\ 3 \end{ytableau} \succ \begin{ytableau} 2 & 5 \\ 3 & 4 \\ 1 \end{ytableau} \succ \begin{ytableau} 1 & 5 \\ 3 & 4 \\ 2 \end{ytableau} \succ \begin{ytableau} 3 & 5 \\ 1 & 4 \\ 2 \end{ytableau} \succ \begin{ytableau} 3 & 5 \\ 2 & 4 \\ 1 \end{ytableau}.$$

The main feature of the order $\succ$ is that for every *standard tableau*[5] T, the inequalities $pT \succ T \succ qT$ hold for all $p \in R_T$, $q \in C_T$, because the maximal element of every independent cycle of p is shifted by p to the left, and the maximal element of every independent cycle of q is raised by q. This forces every standard tableau T to be

[5] See Sect. 7.1 on p. 151.

the minimal element of its R_T-orbit $R_T T$. In particular, for every filling $U \prec T$, the tabloids $\{U\}$ and $\{T\}$ are distinct in the module M_λ.

Exercise 7.5 Prove that $c_T\{U\} = 0$ for every pair of standard tableaux $U \succ T$.

Theorem 7.4 *The vectors v_T, where T runs through the standard tableaux of shape λ, form a basis of the Specht module S_λ. In particular,* $\dim S_\lambda = d_\lambda$ *equals the number of standard Young tableaux*[6] *of shape λ.*

Proof Let us first check that the d_λ vectors v_T are linearly independent. The linear expression of the vector $v_T = \sum_{q \in C_T} \operatorname{sgn}(q) \cdot \{qT\}$ through the basis vectors $\{U\}$ of M_λ has the form

$$v_T = \{T\} + \sum_{U \prec T} \varepsilon_U \cdot \{U\}\,, \text{ where } \varepsilon_U = -1,\ 0,\ 1\,.$$

Every nontrivial linear relation between such vectors also can be written[7] as $v_T = \sum_{U \prec T} x_U \cdot v_U$. Expanding v_T and v_U as linear combinations of tabloids leads to an equality of the form

$$\{T\} = \sum_{U \prec T} y_U \cdot \{U\}\,,$$

which never holds, because $\{T\} \neq \{U\}$ in M_λ for $U \prec T$. The linear independence of the vectors v_T implies the inequality $\dim S_\lambda \geqslant d_\lambda$. At the same time, it follows from formula (4.6) on p. 85 and the relation on the sum of squares of dimensions of irreducible representations from Corollary 5.8 on p. 118 that

$$\sum d_\lambda^2 = n! = \sum \dim^2 S_\lambda\,.$$

Therefore, $\dim S_\lambda = d_\lambda$. $\square$

7.4 Representation Ring of Symmetric Groups

Write $\mathfrak{R}_n$ for the additive abelian group of the representation ring[8] of S_n, i.e., for the $\mathbb{Z}$-linear span of the irreducible characters in the space of all functions $S_n \to \mathbb{C}$. We also put $\mathfrak{R}_0 \overset{\text{def}}{=} \mathbb{Z}$. We are going to equip the direct sum of abelian groups

$$\mathfrak{R} \overset{\text{def}}{=} \bigoplus_{n \geqslant 0} \mathfrak{R}_n$$

[6] See Example 4.2 on p. 85.

[7] By moving all terms but v_T with the maximal T to the right-hand side.

[8] See Sect. 6.2.3 on p. 140.

with the structure of a graded commutative ring with unit, that is, with a commutative multiplication such that $\mathfrak{R}_k \cdot \mathfrak{R}_m \subset \mathfrak{R}_{k+m}$ for all k, n. Do not confuse this new multiplication with that discussed in Sect. 6.2.3 on p. 140, corresponding to the tensor product of representations $[U], [W] \mapsto [U \otimes W]$ and existing separately within each $\mathfrak{R}_n$. To prevent confusion with tensor multiplication, the multiplication $\mathfrak{R}_k \times \mathfrak{R}_m \to \mathfrak{R}_{k+m}$ that we are going to define will be called the *Littlewood–Richardson product*.

7.4.1 Littlewood–Richardson Product

Associated with a pair of linear representations $\varphi : S_k \to \mathrm{GL}(U)$, $\psi : S_m \to \mathrm{GL}(W)$ is the linear representation

$$\varphi \times \psi : S_k \times S_m \to \mathrm{GL}(U \otimes W)\,, \quad (g,h) : u \otimes w \mapsto gu \otimes hw\,. \tag{7.13}$$

Let us embed $S_k \times S_m$ into S_{k+m} as the subgroup of permutations mapping both parts of the partition

$$\{1, 2, \dots, k+m\} = \{1, 2, \dots, k\} \sqcup \{k+1, k+2, \dots, k+m\} \tag{7.14}$$

to itself. Write $\mathrm{ind}(\varphi \times \psi)$ for the representation of S_{k+m} induced from the representation (7.13) of this subgroup, and put $[\varphi]\cdot[\psi] \overset{\text{def}}{=} [\mathrm{ind}(\varphi\times\psi)]$, where $[f]$, $[\psi]$, and $[\mathrm{ind}(\varphi \times \psi)]$ mean the isomorphism classes of corresponding representations[9] in $\mathfrak{R}_k$, $\mathfrak{R}_n$, and $\mathfrak{R}_{k+m}$ respectively. The *Littlewood–Richardson product* $\mathfrak{R} \times \mathfrak{R} \to \mathfrak{R}$ is the $\mathbb{Z}$-bilinear extension of this product to the finite $\mathbb{Z}$-linear combinations of irreducible characters.

A different embedding $S_k \times S_m \hookrightarrow S_{k+m}$ provided by another disjoint union decomposition

$$\{1, \dots, k+m\} = \{i_1, i_2, \dots, i_k\} \sqcup \{j_1, j_2, \dots, j_m\}$$

leads to the subgroup of S_{k+m} conjugate to that obtained from the decomposition (7.14), and therefore, to the isomorphic induced representation $\mathrm{ind}(\varphi \times \psi)$ of S_{k+m}.

Exercise 7.6 Let $\varphi, \psi : H \hookrightarrow G$ be two injective homomorphisms of groups such that $\varphi(H) = g\psi(H)g^{-1}$ for some $g \in G$, and $\varrho : H \to \mathrm{GL}(V)$ a linear representation. Construct an isomorphism of the G-modules induced by the representations $\varrho\varphi^{-1}$, $\varrho\psi^{-1}$ of the subgroups $\varphi(H), \psi(H) \subset G$ respectively.

Hence, the Littlewood–Richardson product is commutative and does not depend on the splitting $\{1, \dots, k+m\} = I \sqcup J$ used to embed $S_k \times S_m$ into S_{k+m}. Since for every

[9] Or equivalently, their characters.

three representations $\xi : S_k \to \mathrm{GL}(U)$, $\eta : S_\ell \to \mathrm{GL}(V)$, $\zeta : S_m \to \mathrm{GL}(W)$, the classes $([\xi] \cdot [\eta]) \cdot [\zeta]$ and $[\xi] \cdot ([\eta] \cdot [\zeta])$ coincide with the class of the S_{m+n+k}-module induced from the representation

$$S_k \times S_\ell \times S_m \to \mathrm{GL}(U \otimes V \otimes W)\,, \quad (g_1, g_2, g_3) \mapsto \xi(g_1) \otimes \eta(g_2) \otimes \zeta(g_3)\,,$$

the Littlewood–Richardson product is associative as well.

Exercise 7.7 Check this carefully, and use the distributivity isomorphisms from Proposition 1.3 on p. 12 to verify that the Littlewood–Richardson product is distributive with respect to addition[10] in $\mathfrak{R}$.

Lemma 7.7 *The graded commutative ring $\mathfrak{R}$ is the ring of polynomials with integer coefficients in the countable set of variables $[\mathbb{1}_k]$, $k \in \mathbb{N}$, the classes of trivial S_k-modules of dimension one. The isomorphism classes of tabloid representations*

$$[M_\lambda] = [\mathbb{1}_{\lambda_1}] \cdot [\mathbb{1}_{\lambda_2}] \cdots [\mathbb{1}_{\lambda_n}] = [\mathbb{1}_1]^{m_1} [\mathbb{1}_2]^{m_2} \cdots [\mathbb{1}_n]^{m_n}\,, \tag{7.15}$$

where λ runs through all Young diagrams, and $m_i = m_i(\lambda)$ means the number of length-i rows in λ, form a basis of $\mathfrak{R}$ as a $\mathbb{Z}$-module.

Proof It follows from Corollary 7.2 that the transition matrix from the isomorphism classes $[M_\lambda]$ to the classes of irreducible representations $[S_\lambda]$ is integer upper unitriangular. Therefore, the classes $[M_\lambda]$ also form a basis of $\mathfrak{R}$ over $\mathbb{Z}$. Since the tabloid module M_λ is induced from the trivial representation of the row subgroup $S_{\lambda_1} \times S_{\lambda_2} \times \cdots S_{\lambda_n} \subset S_{|\lambda|}$, the equality (7.15) holds in $\mathfrak{R}$ by the definition of the Littlewood–Richardson product. The set of all formal monomials in the variables $[\mathbb{1}_k]$ coincides with the set of classes $[M_\lambda]$, because $[\mathbb{1}_{\lambda_i}] = [M_{(\lambda_i)}]$ is a particular tabloid representation corresponding to the Young diagram formed by one row of length λ_i, and these representations are multiplied in $\mathfrak{R}$ exactly as the formal variables $[\mathbb{1}_k]$ are multiplied within the polynomial ring. □

7.4.2 *Scalar Product on $\mathfrak{R}$*

Write $([U], [W])$ for the Euclidean inner product in $\mathfrak{R}$ such that the irreducible classes $[V_\lambda]$ form an orthonormal basis. Then the direct sum $\mathfrak{R} = \oplus \mathfrak{R}_k$ becomes orthogonal, and the inner product of every two classes

$$[U] = \sum_{|\lambda|=n} k_\lambda \cdot [V_\lambda] \quad \text{and} \quad [W] = \sum_{|\lambda|=n} m_\lambda \cdot [V_\lambda]$$

[10] Recall that it corresponds to the direct sum of representations; see Sect. 6.2.3.

belonging to the same component $\mathfrak{R}_n$ can be interpreted as

$$([U],[W]) = \sum_{|\lambda|=n} k_\lambda m_\lambda = \dim \operatorname{Hom}_{S_n}(U,W) = (\chi_U, \chi_W)_n \;, \tag{7.16}$$

where $(\chi_U, \chi_W)_n$ means the inner product of characters in the algebra[11] $\mathbb{C}^{S_n}$, that is,

$$\frac{1}{n!}\sum_{g\in S_n} \chi_U(g)\chi_W(g) = \frac{1}{n!}\sum_{\mu} |C_\mu| \cdot \chi_U(C_\mu)\chi_W(C_\mu) = \sum_{\mu} z_\mu^{-1} \cdot \chi_U(C_\mu)\chi_W(C_\mu) \,,$$

where the summation is over all Young diagrams of weight n, $C_\mu \subset S_n$ denotes the conjugacy class formed by permutations of cyclic type μ, and the combinatorial factor[12]

$$z_\mu = \prod_i m_i! \cdot i^{m_i} \tag{7.17}$$

is related to the cardinality of C_μ by the equality $|C_\mu| = n!/z_\mu$. Therefore,

$$([U],[W]) = \sum_{\mu} z_\mu^{-1} \cdot \chi_U(C_\mu)\chi_W(C_\mu) \,. \tag{7.18}$$

7.4.3 The Isometric Isomorphism $\mathfrak{R} \xrightarrow{\sim} \mathbf{\Lambda}$

Recall[13] that the ring of symmetric functions Λ has the Euclidean inner product $\langle *, * \rangle$ such that the Schur polynomials s_λ form an orthonormal basis, that the basis consisting of complete symmetric functions h_λ is dual to the monomial basis m_λ, and that the Newton polynomials p_λ are orthogonal, with $\langle p_\lambda , p_\lambda \rangle = z_\lambda$. By Proposition 7.1 on p. 157, the value $\psi_\lambda(C_\mu)$, of the tabloid character ψ_λ on the conjugacy class C_μ coincides with the coefficient of m_λ in the linear expression of the Newton polynomial p_μ through the monomial basis:

$$p_\mu = \sum_\lambda \psi_\lambda(C_\mu) \cdot m_\lambda \,.$$

This forces $\psi_\lambda(C_\mu) = \langle p_\mu , h_\lambda \rangle$, because the complete symmetric functions h_λ form the Euclidean dual basis to m_λ. The same inner product $\langle p_\mu , h_\lambda \rangle$ equals the

[11] See Remark 6.2 on p. 138.

[12] Here $m_i = m_i(\mu)$ is the number of rows of length i in μ.

[13] See Sect. 4.6 on p. 95.

coefficient of $z_\mu^{-1} \cdot p_\mu$ in the linear expression of h_λ through the Newton basis p_λ,

$$h_\lambda = \sum_\mu z_\mu^{-1} \langle p_\mu , h_\lambda \rangle p_\mu = \sum_\mu z_\mu^{-1} \cdot \chi_{M_\lambda}(C_\mu) \cdot p_\mu \, . \tag{7.19}$$

Comparison of (7.19) with (7.18) leads to the following claim.

Theorem 7.5 *The map*

$$\mathrm{ch} : \mathfrak{R} \xrightarrow{\sim} \Lambda \, , \quad [U] \mapsto \sum_\mu z_\mu^{-1} \cdot \chi_U(C_\mu) \cdot p_\mu \, , \tag{7.20}$$

is simultaneously a (well-defined[14] *over* $\mathbb{Z}$*) isomorphism of graded commutative rings and a Euclidean isometry. It sends the classes of tabloid representations* $[M_\lambda]$ *to the complete symmetric functions* h_λ*, and the classes of irreducible representations* $[S_\lambda]$ *to the Schur polynomials* s_λ*. It transfers the tensor multiplication by sign representation to the involution*[15] ω *on* Λ*, which swaps* s_λ *with* s_{λ^t} *and* h_λ *with* e_λ*.*

Proof The map (7.20) is linear in $[U]$:

$$\begin{aligned} \mathrm{ch}([U] + [W]) = \mathrm{ch}([U \oplus W]) &= \sum_\mu z_\mu^{-1} \cdot \chi_{U \oplus W}(C_\mu) \cdot p_\mu \\ &= \sum_\mu z_\mu^{-1} \cdot \big(\chi_U(C_\mu) + \chi_W(C_\mu)\big) \cdot p_\mu = \mathrm{ch}([U]) + \mathrm{ch}([W]) \, . \end{aligned}$$

By Lemma 7.7 on p. 163 and Corollary 3.3 on p. 62, the rings $\mathfrak{R}$, Λ are polynomial rings in the countable sets of variables $[\mathbb{1}_k]$ and h_k respectively. It follows from (7.19) that the map (7.20) sends every basis monomial

$$[M_\lambda] = [\mathbb{1}_{\lambda_1}] \cdot [\mathbb{1}_{\lambda_2}] \cdots [\mathbb{1}_{\lambda_n}] = [\mathbb{1}_1]^{m_1} [\mathbb{1}_2]^{m_2} \cdots [\mathbb{1}_n]^{m_n}$$

(where m_i is the number of length-i rows in the diagram λ) to the basis monomial

$$h_\lambda = h_{\lambda_1} \cdot h_{\lambda_2} \cdots h_{\lambda_n} = h_1^{m_1} h_2^{m_2} \cdots h_n^{m_n} \, ,$$

and respects the multiplication of the variables, because $\mathrm{ch}\,([\mathbb{1}_k]) = h_k$. Therefore, the assignment $[U] \mapsto \mathrm{ch}([U])$ establishes a well-defined isomorphism of graded rings $\mathfrak{R} \xrightarrow{\sim} \Lambda$. Since the Newton polynomials form an orthogonal basis of $\mathbb{Q} \otimes \Lambda$

[14] Although the right-hand side of (7.20) contains denominators.

[15] See Proposition 4.4 on p. 94.

and have $\langle p_\lambda \,, p_\lambda \rangle = z_\lambda$, formula (7.18) implies that χ preserves the inner product:

$$\begin{aligned} \langle \operatorname{ch}([U]) \,, \operatorname{ch}([W]) \rangle &= \sum_{\lambda,\mu} z_\lambda^{-1} z_\mu^{-1} \cdot \chi_U(C_\lambda)\chi_W(C_\mu) \cdot \big\langle p_\mu \,, p_\lambda \big\rangle \\ &= \sum_\mu z_\mu^{-1} \cdot \chi_U(g)\chi_W(g) = ([U],[W]) \ . \end{aligned}$$

It follows from Corollary 7.2 on p. 160 that the transition matrix from the orthonormal basis $[S_\lambda]$ to the basis $[M_\lambda]$ is lower unitriangular:

$$[S_\lambda] = [M_\lambda] + \sum_{\mu \rhd \lambda} x_{\mu\lambda}[M_\mu] \,.$$

By formula (4.23) on p. 94, the transition matrix from the complete symmetric functions h_λ to the Schur polynomials s_λ is lower unitriangular as well[16]:

$$h_\lambda = \sum_\mu K_{\mu,\lambda} \cdot s_\mu = s_\lambda + \sum_{\mu \rhd \lambda} K_{\mu,\lambda} \cdot s_\mu \,.$$

Therefore, the transition matrix from the polynomials $\operatorname{ch}([S_\lambda])$ to the Schur polynomials is also lower unitriangular:

$$\operatorname{ch}([S_\lambda]) = \operatorname{ch}\big([M_\lambda] + \sum_{\mu \rhd \lambda} x_{\mu\lambda}[M_\mu]\big) = h_\lambda + \sum_{\mu \rhd \lambda} x_{\mu\lambda} h_\mu = s_\lambda + \sum_{\mu \rhd \lambda} y_{\mu\lambda} s_\mu \,.$$

Since

$$\begin{aligned} 1 = ([S_\lambda],[S_\lambda]) = \langle \operatorname{ch}([S_\lambda]) \,, \operatorname{ch}([S_\lambda]) \rangle = \langle s_\lambda \,, s_\lambda \rangle + \sum_{\mu \rhd \lambda} y_{\mu\lambda}^2 \big\langle s_\mu \,, s_\mu \big\rangle \\ = 1 + \sum_{\mu \rhd \lambda} y_{\mu\lambda}^2 \,, \end{aligned}$$

we conclude that all $y_{\mu\lambda}$ are equal to 0, that is, $\operatorname{ch}([S_\lambda]) = s_\lambda$. The tensor multiplication by the sign representation is transformed by the isomorphism (7.20) to the involution ω by Theorem 7.2 on p. 156 and Proposition 4.4 on p. 94. □

Corollary 7.3 (Young's Rule) *The multiplicity of the Specht module S_μ in the tabloid representation M_λ equals the Kostka number $K_{\mu,\lambda}$.*

[16]Recall that the *Kostka number* $K_{\mu,\lambda}$ is the number of Young tableaux of shape μ filled by λ_1 ones, λ_2 twos, etc. It is nonzero only for $\mu \trianglerighteq \lambda$. All $K_{\lambda,\lambda} = 1$. (See formulas (4.10) and (4.11) on p. 88.)

Corollary 7.4 (Littlewood–Richardson Rule) *The multiplicity of* $[S_\nu]$ *in the product* $[S_\lambda]\cdot[S_\mu]$ *is equal to the Littlewood–Richardson coefficient*[17] $c^\nu_{\lambda\mu}$ *from the expansion* $s_\lambda \cdot s_\mu = \sum_\nu c^\nu_{\lambda\mu}\cdot s_\nu$ *in* Λ.

Corollary 7.5 (Ramification Rules) *Let* $S_n \subset S_{n+1}$ *be embedded as the stabilizer of some element. Then the representation of* S_{n+1} *induced by an irreducible representation* S_λ *of* S_n *is a direct sum of simple modules* S_μ*, each taken with multiplicity one, for all Young diagrams* μ *obtained by adding one cell to the diagram* λ*. Conversely, the restriction of a simple* S_{n+1}*-module* S_μ *on* S_{n-1} *splits into a direct sum of simple modules* S_λ*, each taken with multiplicity one, for all Young diagrams* λ *obtained by removing one cell from the diagram* μ.

Proof Since $[\mathrm{ind}(S_\lambda)] = [S_\lambda]\cdot[\mathbb{1}_1]$, the first statement follows from the Littlewood–Richardson rule and Pieri's formula,[18] which expands $s_\lambda \cdot h_1$ as a linear combination of Schur polynomials. The second formula follows from the first by Frobenius reciprocity: the multiplicity of S_λ in $\mathrm{res}\, S_\mu$ equals the multiplicity of S_μ in $\mathrm{ind}\, S_\lambda$. □

Corollary 7.6 (Frobenius Formula for Characters of S_n**)** *The value of an irreducible character* χ_λ *of a symmetric group* S_n *on a conjugacy class* $C_\mu \subset S_n$ *equals each of the following three coinciding integers:*

- *the coefficient of* $z_\mu^{-1}\cdot p_\mu(x)$ *in the expansion of the Schur polynomial* $s_\lambda(x)$ *through the basis* $z_\mu^{-1}\cdot p_\mu(x)$ *of the vector space* $\mathbb{Q}\otimes\Lambda$*;*
- *the coefficient of* $s_\lambda(x)$ *in the expansion of the Newton polynomial* $p_\mu(x)$ *through the Schur basis* $s_\lambda(x)$ *of the* $\mathbb{Z}$*-module* Λ*;*
- *the coefficient of the monomial* $x^{\lambda+\delta} = x_1^{\lambda_1+n-1}x_2^{\lambda_2+n-2}\cdots x_n^{\lambda_n}$ *in the alternating polynomial*

$$p_\mu(x)\cdot\Delta_\delta(x) = p_1(x)^{m_1}p_2(x)^{m_2}\cdots p_n(x)^{m_n}\cdot\prod_{i<j}(x_i-x_j)\,;$$

where $p_k(x) = \sum_i x_i^k$ *is the Newton sum of powers,* m_i *means the number of length-i rows in the Young diagram* μ*, and* $\Delta_\delta(x) = \det\bigl(x_j^{n-i}\bigr)$ *is the Vandermonde determinant.*

Proof The first item follows directly from Theorem 7.5. To prove the second, recall that the Newton polynomials p_μ form an orthogonal basis of $\mathbb{Q}\otimes\Lambda$ with $\bigl(p_\mu, p_\mu\bigr) = z_\mu$. Therefore, the coefficient of $z_\mu^{-1}\cdot p_\mu(x)$ in the linear expression of s_λ through the basis $z_\mu^{-1}\cdot p_\mu(x)$ equals the inner product $\bigl(s_\lambda, p_\mu\bigr)$, which is simultaneously the coefficient of s_λ in the expansion of p_μ through the Schur orthonormal basis s_λ. The third follows from the Jacobi–Trudi formula[19]

[17]See Theorem 4.2 on p. 92.

[18]See Exercise 4.9 on p. 92.

[19]See Sect. 4.5.1 on p. 93.

$s_\lambda(x) = \Delta_{\lambda+\delta}(x)/\Delta_\delta(x)$. Namely, multiplying both sides of the expansion

$$p_\mu(x) = \sum_\lambda \chi_\lambda(C_\mu) \cdot \frac{\Delta_{\lambda+\delta}(x)}{\Delta_\delta(x)}$$

by Δ_δ leads to the equality $p_\mu(x) \cdot \Delta_\delta(x) = \sum_\lambda \chi_\lambda(C_\mu) \cdot \Delta_{\lambda+\delta}(x)$, which states that $\chi_\lambda(C_\mu)$ is the coefficient of $\Delta_{\lambda+\delta}(x)$ in the linear expression of the alternating polynomial $p_\mu(x) \cdot \Delta_\delta(x)$ through the determinantal basis.[20] □

7.4.4 Dimensions of Irreducible Representations

By the Frobenius formula, $\dim S_\lambda = \chi_\lambda(1)$ is equal to the coefficient of

$$x^{\lambda+\delta} = x_1^{\lambda_1+n-1} x_2^{\lambda_2+n-2} \cdots x_n^{\lambda_n}$$

in the polynomial

$$\begin{aligned} p_1^n \cdot \Delta_\delta &= \left(\sum x_i\right)^n \cdot \det\left(x_j^{n-i}\right) \\ &= \sum_{m_1 m_2 \dots m_n} \frac{n!}{m_1! \cdot m_2! \cdots m_n!} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} \cdot \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot x_1^{n-\sigma(1)} x_2^{n-\sigma(2)} \cdots x_n^{n-\sigma(n)} . \end{aligned}$$

Write $\eta_i = \lambda_i + n - i$ for the strictly decreasing row lengths of the diagram $\eta = \lambda + \delta$. Then the coefficient of the monomial $x^\eta = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n}$ in the previous product equals

$$\begin{aligned} &\sum_\sigma \frac{\operatorname{sgn}(\sigma) \cdot n!}{\prod_j \left(\eta_j - n + \sigma(j)\right)!} \\ &\quad = \frac{n!}{\eta_1! \cdot \eta_2! \cdots \eta_n!} \cdot \sum_\sigma \operatorname{sgn}(\sigma) \cdot \prod_j \eta_j \cdot \left(\eta_j - 1\right) \cdots \left(\eta_j - n + \sigma(j) + 1\right) , \end{aligned}$$

where the summation is over all permutations $\sigma \in S_n$ such that all n of the numbers $\eta_j - n + \sigma(j)$ are nonnegative. Every product $\eta_j \cdot \left(\eta_j - 1\right) \cdots \left(\eta_j - n + \sigma(j) + 1\right)$ in this sum consists of $n - \sigma(j)$ positive integers decreasing sequentially by one, and

[20]See formula (3.4) on p. 58.

the whole sum is equal to the standard expansion of the determinant

$$\det \begin{pmatrix} \eta_1 \cdots (\eta_1 - n + 1) & \eta_2 \cdots (\eta_2 - n + 1) & \cdots & \eta_n \cdots (\eta_n - n + 1) \\ \vdots & \vdots & \vdots & \vdots \\ \eta_1(\eta_1 - 1) & \eta_2(\eta_2 - 1) & \cdots & \eta_n(\eta_n - 1) \\ \eta_1 & \eta_2 & \cdots & \eta_n \\ 1 & 1 & \cdots & 1 \end{pmatrix} .$$

Exercise 7.8 Convince yourself that this determinant equals $\prod_{i<j}(\eta_i - \eta_j)$.

We have proved the following claim.

Corollary 7.7 (Frobenius Formula for Dimensions of Irreducible S_n-Modules) *Let $\eta = \lambda + \delta$, that is, $\eta_i = \lambda_i + n - i$. Then*

$$\dim S_\lambda = \frac{n!}{\eta_1! \cdot \eta_2! \cdots \eta_n!} \cdot \prod_{i<j} (\eta_i - \eta_j) .$$

□

Exercise 7.9 (Hook Length Formula) Given a Young diagram λ and a cell $a \in \lambda$, the *hook* of a is the Γ-shaped subdiagram $\Gamma(a) \subset \lambda$ formed by the cell a and all the cells below a in the column of a and to the right of a in the row of a. The number of cells in the hook of a is called the *hook length* of a. Prove that

$$\dim S_\lambda = \frac{n!}{\prod_{a \in \lambda} |\Gamma(a)|} .$$

For example, the hook lengths of the cells in the Young diagram $\lambda = (4, 2, 1)$ are

$$\begin{array}{|c|c|c|c|} \hline 6 & 4 & 2 & 1 \\ \hline 3 & 1 \\ \cline{1-2} 1 \\ \cline{1-1} \end{array} ,$$

and therefore, the Specht representation $S_{(4,2,1)}$ of the symmetric group S_7 has dimension

$$\frac{7!}{6 \cdot 4 \cdot 3 \cdot 2} = 7 \cdot 5 = 35 .$$

A highly nontrivial combinatorial consequence of Exercise 7.9 and Theorem 7.4 on p. 161 is that the number d_λ of standard Young tableaux of shape λ can be calculated by the hook-length formula. For example, the previous computation shows that there are 35 standard Young tableaux of shape $\begin{array}{|c|c|c|c|} \hline \, & \, & \, & \, \\ \hline \, & \, \\ \cline{1-2} \, \\ \cline{1-1} \end{array}$.

Problems for Independent Solution to Chapter 7

Problem 7.1 For every standard filling T, show that the representations of S_n by left multiplication in the ideals $\mathbb{C}[S_n]\cdot r_T$ and $\mathbb{C}[S_n]\cdot c_T$ are induced, respectively, by the trivial representation of the row subgroup $R_T \subset S_n$ and by the sign representation of the column subgroup $C_T \subset S_n$.

Problem 7.2 Show that in general, the left ideal $\mathbb{C}[S_n] \cdot s_T$ is not contained in the left ideal $\mathbb{C}[S_n] \cdot r_T$.

Problem 7.3 For all irreducible representations of groups S_3, S_4, and S_5 constructed by hand in Example 5.5 on p. 120, Example 6.2 on p. 135, Exercise 6.7 on p. 138, and Example 6.3 on p. 139, indicate explicitly the Young diagram λ such that the Specht module S_λ is isomorphic to the handmade representation in question.

Problem 7.4 For the $(n-1)$-dimensional simplicial representation V_Δ of the group S_n, establish the following isomorphisms:
(a) $\Lambda^k V_\Delta \simeq V_{((n-k),\,1^k)}$, **(b)** $V_\Delta^{\otimes 2} \simeq \mathbb{C} \oplus V_\Delta \oplus V_{((n-2),2)} \oplus V_{((n-2),1,1)}$.

Problem 7.5 Prove the following equalities: **(a)** $\chi_{((n-2),1,1)}(C_\mu) = \binom{m_1-1}{2} - m_2$, **(b)** $\chi_{((n-2),2)}(C_\mu) = \binom{m_1-1}{2} + m_2 - 1$.

Problem 7.6 Find the multiplicities of the sign and simplicial representations of S_n in the representation induced from the 1-dimensional complex representation of an n-cycle by multiplication by $e^{2\pi i/n}$.

Problem 7.7 Show that the value of an irreducible character χ_λ of the symmetric group S_n on the n-cycle equals $(-1)^k$ for $\lambda = \big((n-k),\, 1^k\big)$ and vanishes for all other λ.

Problem 7.8 Let a self-conjugate diagram $\lambda = \lambda^t$ be constructed from k disjoint symmetric hooks of lengths $\gamma_i = 2(\lambda_i - i + 1) - 1$, $1 \leqslant i \leqslant k$, with vertices on the main diagonal of λ. Show that $\chi_\lambda(C_\gamma) = (-1)^{(n-k)/2}$.

Problem 7.9 Prove that the simple S_m-module S_μ has nonzero multiplicity in the representation of S_m induced from an irreducible representation S_ν of a subgroup[21] $S_n \subset S_m$ if and only if $\mu \supset \nu$, and this multiplicity equals the number of standard skew tableaux of shape[22] $\mu \smallsetminus \nu$.

Problem 7.10 Formulate and prove the dual version of Problem 7.9 about the restricted representations.

Problem 7.11 Prove that the Specht module S_λ is the only common irreducible component of the representations M_λ and $M_\lambda \otimes \mathrm{sgn}$.

Problem 7.12 Prove that $[S_\nu] \cdot [S_{(1^n)}] = \sum [S_\mu]$, where the summation is over all Young diagrams μ obtained from ν by adding n cells in n distinct rows.

[21]Embedded as a pointwise stabilizer of some $m - n$ elements.

[22]That is, the fillings of the complement $\mu \smallsetminus \nu$ by nonrepeated numbers $1, 2, \dots, m-n$ such that the numbers strictly increase from top to bottom in the columns and from left to right in the rows.

Problem 7.13 Prove that the multiplicity of S_λ in $S_\mu \otimes S_\nu$ is equal to

$$\sum_\eta z_\eta^{-1} \chi_\lambda(C_\eta) \chi_\mu(C_\eta) \chi_\nu(C_\eta) \,.$$

Verify that it becomes $\delta_{\mu,\nu}$ for $\lambda=(n)$, one row of length n, and δ_{μ,ν^t} for $\lambda=(1^n)$, one column of height n, where the *Kronecker symbol* $\delta_{\alpha,\beta}$ equals 1 for $\alpha = \beta$ and 0 otherwise.

Problem 7.14 Verify that $\dim S_\lambda < |\lambda|$ only in the following cases: the trivial, simplicial, sign, and tensor products of simplicial and sign representations of S_n for all n; $S_{(2,2)}$ for S_4; $S_{(2,2,2)}$ and $S_{(3,3)}$ for S_6.

Chapter 8
$\mathfrak{sl}_2$-Modules

Everywhere in this section we assume by default that $\Bbbk$ is a field of characteristic zero.

8.1 Lie Algebras

A vector space $\mathfrak{g}$ over $\Bbbk$ is called a *Lie algebra* if it is equipped with a skew-symmetric bilinear operation $\mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, $X, Y \mapsto [X, Y] = -[Y, X]$, called a *Lie bracket*, such that the *Jacobi identity* $[X, [Y, Z]] = [[X, Y], Z] + [Y, [X, Z]]$ holds for all $X, Y, Z \in \mathfrak{g}$.

Example 8.1 (Commutator Algebra of an Associative Algebra) Associated with every associative $\Bbbk$-algebra A is the *commutator Lie algebra* of A with the Lie bracket provided by the commutator in A,

$$[a, b] \stackrel{\text{def}}{=} ab - ba \, .$$

Exercise 8.1 Verify the Jacobi identity for the commutator bracket.

8.1.1 Universal Enveloping Algebra

For every Lie algebra $\mathfrak{g}$ over $\Bbbk$, there exist an associative $\Bbbk$-algebra $\mathfrak{U}(\mathfrak{g})$ and a linear map $\nu : \mathfrak{g} \to \mathfrak{U}(\mathfrak{g})$ such that

$$\forall \, X, Y \in \mathfrak{g} \, , \quad \nu([X, Y]) = [\nu(X), \nu(Y)] = \nu(X)\nu(Y) - \nu(Y)\nu(X) \, ,$$

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_8

and the following universal property holds: given an associative $\Bbbk$-algebra A and a linear map $\psi : \mathfrak{g} \to A$ with $\psi([X, Y]) = [\psi(X), \psi(Y)]$ for all $X, Y \in \mathfrak{g}$, there exists a unique homomorphism of associative algebras $\widetilde{\psi} : \mathfrak{U}(\mathfrak{g}) \to A$ such that $\psi = \widetilde{\psi} \circ \nu$.

Exercise 8.2 Verify that this universal property determines both an algebra $\mathfrak{U}(\mathfrak{g})$ and a linear map ν uniquely up to a unique isomorphism of associative $\Bbbk$-algebras commuting with ν.

The algebra $\mathfrak{U}(\mathfrak{g})$ is called the *universal enveloping algebra* of the Lie algebra $\mathfrak{g}$. It can be constructed as the quotient algebra of the tensor algebra $\mathsf{T}(\mathfrak{g})$ by the (inhomogeneous) two-sided ideal generated by all the differences

$$[X, Y] - X \otimes Y - Y \otimes X \in \mathfrak{g} \oplus \mathfrak{g}^{\otimes 2}$$

with $X, Y \in \mathfrak{g}$.

Exercise 8.3 Verify that this quotient algebra possesses the above universal property.

8.1.2 Representations of Lie Algebras

A linear map $\varrho : \mathfrak{g} \to \mathrm{End}(V)$ is called a *linear representation* of the Lie algebra $\mathfrak{g}$ if it sends the Lie bracket to the commutator of linear endomorphisms, i.e.,

$$\varrho([A, B]) = [\varrho(A), \varrho(B)]$$

for all $A, B \in \mathfrak{g}$. In this case, the vector space V is called a $\mathfrak{g}$-*module*. It follows from the universal property of $\mathfrak{U}(\mathfrak{g})$ that the linear representations $\varrho : \mathfrak{g} \to \mathrm{End}(V)$ of a Lie algebra $\mathfrak{g}$ are in canonical bijection with the linear representations

$$\widetilde{\varrho} : \mathfrak{U}(\mathfrak{g}) \to \mathrm{End}(V)$$

of the universal enveloping algebra $\mathfrak{U}(\mathfrak{g})$. The representation $\widetilde{\varrho}$ sends a class of the tensor

$$A_1 \otimes A_2 \otimes \cdots \otimes A_m \in \mathsf{T}(\mathfrak{g})$$

to the composition of endomorphisms $\varrho(A_1) \circ \varrho(A_2) \circ \cdots \circ \varrho(A_m) \in \mathrm{End}(V)$. Note that $\mathrm{im}\,\widetilde{\varrho}$ coincides with the associative envelope $\mathrm{Ass}\big(\varrho(\mathfrak{g})\big) \subset \mathrm{End}(V)$.

The direct sum $U \oplus W$ of $\mathfrak{g}$-modules U, W has a natural $\mathfrak{g}$-module structure with action $F(u+w) \stackrel{\text{def}}{=} (Fu)+(Fw)$ for all $u \in U$, $w \in W$. The tensor products and tensor, symmetric, and exterior powers of $\mathfrak{g}$-modules also inherit the natural structures of $\mathfrak{g}$-modules. However, in contrast to the representations of groups, the action of an element $F \in \mathfrak{g}$ is extended to products not as a multiplicative homomorphism but as a derivation, that is, by the *Leibniz rules*:

$$\begin{aligned} F(u \otimes w) &\stackrel{\text{def}}{=} (Fu) \otimes w + u \otimes (Fw)\,, \\ F(u \wedge w) &\stackrel{\text{def}}{=} (Fu) \wedge w + u \wedge (Fw)\,, \\ F(u \cdot w) &\stackrel{\text{def}}{=} (Fu) \cdot w + u \cdot (Fw)\,. \end{aligned} \tag{8.1}$$

For every $\mathfrak{g}$-module W and $\mathfrak{g}$-submodule $U \subset W$, the quotient space $V = W/U$ possesses a well-defined $\mathfrak{g}$-module structure with the action $F[v] \stackrel{\text{def}}{=} [Fv]$.

Exercise 8.4 Verify that all the actions of $F \in \mathfrak{g}$ on the products and residue classes introduced above are well defined and map Lie brackets to commutators.

Given a linear representation $\varrho : \mathfrak{g} \to \mathrm{End}(V)$, its *dual representation*

$$\varrho^* : \mathfrak{g} \to \mathrm{End}(V^*)$$

is defined by the assignment $\varrho^*(F) \stackrel{\text{def}}{=} -\varrho(F)^*$. It interacts with the contraction between vectors and covectors by the formula

$$\langle \varrho^*(F)\,\xi, w\rangle + \langle\, \xi\,, \varrho(F)\, w\,\rangle = 0\,. \tag{8.2}$$

For every two $\mathfrak{g}$-modules U, W, the algebra $\mathfrak{g}$ acts on the space of $\Bbbk$-linear maps $\mathrm{Hom}(U, W)$ by the rule

$$F : \varphi \mapsto [F, \varphi] \stackrel{\text{def}}{=} F\varphi - \varphi F\,. \tag{8.3}$$

Exercise 8.5 Verify that the action (8.3) agrees with (8.2) and the first formula in (8.1) under the canonical isomorphism $U^* \otimes V \simeq \mathrm{Hom}(U, V)$. Check by a direct computation that the action (8.3) maps the Lie bracket to the commutator of linear endomorphisms of the vector space $\mathrm{Hom}(U, W)$.

The fixed vectors of the action (8.3) form an associative algebra denoted by

$$\mathrm{Hom}_{\mathfrak{g}}(U, V) \stackrel{\text{def}}{=} \{\varphi : U \to V \mid \forall\, F \in \mathfrak{g}\ F\varphi = \varphi F\}$$

and called the algebra of $\mathfrak{g}$-*invariant* operators.[1]

[1]Also known as $\mathfrak{g}$-*linear* operators and *homomorphisms of* $\mathfrak{g}$-*modules* (or just $\mathfrak{g}$-*homomorphisms* for short).

8.2 Finite-Dimensional Simple $\mathfrak{sl}_2$-Modules

The traceless 2×2 matrices form a Lie algebra denoted by

$$\mathfrak{sl}_2(\Bbbk) \stackrel{\text{def}}{=} \{A \in \mathrm{Mat}_2(\Bbbk) \mid \operatorname{tr} A = 0\}.$$

The notation is justified by the fact that the vector subspace $\mathfrak{sl}_2(\Bbbk) \subset \mathrm{Mat}_2(\Bbbk)$ consists of all tangent vectors to the quadric

$$\mathrm{SL}_2(\Bbbk) = \{g \in \mathrm{Mat}_2(\Bbbk) \mid \det g = 1\}$$

at the point $E \in \mathrm{SL}_2$, in the sense that a line $E + tA$, $t \in \Bbbk$, touches the affine quadric $\mathrm{SL}_2(\Bbbk) \subset \mathrm{Mat}_2(\Bbbk)$ at E if and only if $A \in \mathfrak{sl}_2(\Bbbk) \smallsetminus \{0\}$.

Exercise 8.6 Verify this claim.

We will use the matrices

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{8.4}$$

as the standard basis of the vector space $\mathfrak{sl}_2(\Bbbk)$ over $\Bbbk$. They commute by the rules

$$[X, Y] = H, \quad [H, X] = 2X, \quad [H, Y] = -2Y. \tag{8.5}$$

The linear representations of the Lie algebra $\mathfrak{sl}_2$ appear under different names in many branches of mathematics and mathematical physics. Thus, their complete description is a good working example of general concepts discussed in Chap. 5. We restrict ourselves to the finite-dimensional $\mathfrak{sl}_2$-modules. Such a module V is a finite-dimensional vector space over $\Bbbk$ equipped with a triple of linear endomorphisms $X, Y, H : V \to V$ satisfying the commutation relations (8.5).

Example 8.2 (Standard $\mathfrak{sl}_2$-Modules) The differential operators

$$X = x \frac{\partial}{\partial y}, \quad Y = y \frac{\partial}{\partial x}, \quad H = x \frac{\partial}{\partial x} - y \frac{\partial}{\partial y} \tag{8.6}$$

act on the space of polynomials $\Bbbk[x, y]$ and preserve the degree. Write $V_n \subset \Bbbk[x, y]$ for the subspace of homogeneous polynomials of degree n. Certainly, X, Y, H annihilate the 1-dimensional space of constants $V_0 \simeq \Bbbk$. For this reason, V_0 is called the *trivial* $\mathfrak{sl}_2$-module. The action of X, Y, H on the basis x, y of the space of linear forms V_1 is described exactly by the matrices (8.4), which satisfy the relations (8.5) and therefore provide V_1 with an $\mathfrak{sl}_2$-module structure isomorphic to the tautological representation of $\mathfrak{sl}_2 \subset \mathrm{Mat}_2(\Bbbk)$ on the coordinate space $\Bbbk^2$. For this reason, V_1 is called the *tautological* $\mathfrak{sl}_2$-module. The action of the operators (8.6) on the space

$V_n = S^n V_1$ is nothing but the extension of the tautological representation onto its symmetric power by the Leibniz rule (8.1).

Exercise 8.7 Verify that every linear differential operator

$$F = a(x,y)\frac{\partial}{\partial x} + b(x,y)\frac{\partial}{\partial y}$$

of first order satisfies the Leibniz rule $F(gh) = F(g)\cdot h + g\cdot F(h)$, and the commutator of such operators is again a linear differential operator of first order.

The $\mathfrak{sl}_2$-modules V_n are called *standard*. The action of X, Y, H on the basis $e_k = x^k y^{n-k}$, $0 \leqslant k \leqslant n$, of V_n is described by the formulas

$$X(e_k) = (n-k)\, e_{k+1}\,, \quad Y(e_k) = k\, e_{k-1}\,, \quad H(e_k) = (2k-n)\, e_k\,. \tag{8.7}$$

Proposition 8.1 *All the standard $\mathfrak{sl}_2$-modules V_n are simple.*

Proof Write an arbitrary vector $v \in V_n$ as a linear combination of basis vectors $e_k = x^k y^{n-k}$, and let m be the maximal index such that the coefficient of e_m in the expansion of v is not zero. It follows from formula (8.7) that $X^k Y^m v$ is a nonzero multiple of e_k for all $0 \leqslant k \leqslant n$. We conclude that the $\mathfrak{sl}_2$-orbit of every nonzero vector contains all the basis vectors e_k and therefore coincides with V_n. □

Lemma 8.1 *Let W be an $\mathfrak{sl}_2$-module, and let $W_\lambda \stackrel{\text{def}}{=} \{w \in W \mid Hw = \lambda w\}$, $\lambda \in \Bbbk$, be an eigensubspace (possibly zero) of H. Then $X(W_\lambda) \subset W_{\lambda+2}$ and $Y(W_\lambda) \subset W_{\lambda-2}$ for all $\lambda \in \Bbbk$.*

Proof If $Hw = \lambda w$, then it follows from the commutation relations $HX - XH = 2X$ and $HY - YH = -2Y$ that $HXw = XHw + 2Xw = (\lambda + 2)Xw$ and

$$HYw = YHw - 2Yw = (\lambda - 2)Yw.$$ □

Definition 8.1 Let V be a linear representation of the Lie algebra $\mathfrak{sl}_2$. The eigenvalues $\lambda \in \operatorname{Spec} H$ of the operator $H \in \operatorname{End} V$ are called *weights* of the $\mathfrak{sl}_2$-module V. An eigenvector of H with an eigenvalue $\lambda \in \operatorname{Spec} H$ is called a *weight vector* of weight λ. A nonzero λ-eigenspace is called the *weight space* of weight λ, and its dimension is called the *multiplicity* of the weight λ. The weight vectors lying in the kernel of X are called *primitive* vectors.

Lemma 8.2 *Every finite-dimensional $\mathfrak{sl}_2$-module over an algebraically closed field $\Bbbk$ possesses a primitive vector.*

Proof Since $\Bbbk$ is algebraically closed, we have $\operatorname{Spec} H \neq \varnothing$, and there exists a weight vector $v \neq 0$. The nonzero vectors in the chain $v, Xv, X^2v, \dots$ are the eigenvectors of H with strictly increasing eigenvalues. Since they are linearly independent, there is only a finite number of such vectors. Thus, the last nonzero vector of the chain is primitive. □

Lemma 8.3 *Let W be a finite-dimensional $\mathfrak{sl}_2$-module over a field of characteristic zero. Then every primitive vector in W has nonnegative integer weight, and the $\mathfrak{sl}_2$-orbit of every primitive vector of weight m is isomorphic to the standard $\mathfrak{sl}_2$-module V_m.*

Proof Let $Hv = \lambda v$ and $Xv = 0$ for a nonzero vector $v \in W$. By Lemma 8.1, nonzero vectors of the chain $v, Yv, Y^2v, \dots$ are the eigenvectors of H with eigenvalues $\lambda, (\lambda - 2), (\lambda - 4), \dots$. Hence, there exists $m \in \mathbb{N}$ such that $Y^{m+1}v = 0$ and $Y^m v \neq 0$. Let us put

$$v_0 = Y^m v\,,\; v_1 = Y^{m-1} v\,,\; v_2 = Y^{m-1} v\,,\; \dots\,,\; v_m = v$$

and rewrite the chain of vectors $v, Yv, Y^2v, \dots$ in the reverse order as

$$0 \xleftarrow{Y} v_0 \xleftarrow{Y} v_1 \xleftarrow{Y} v_2 \xleftarrow{Y} \cdots \xleftarrow{Y} v_{m-1} \xleftarrow{Y} v_m \xrightarrow{X} 0\,.$$

Then $Hv_i = \big(\lambda - 2\,(m - i)\big)\, v_i$ for all i. The action of X on v_i is recovered from the relations $Xv_m = 0$ and $XY = YX + H$ as follows:

$$\begin{aligned}
Xv_m &= 0\,,\\
Xv_{m-1} &= XYv_m = YXv_m + Hv_m = \lambda v_m\,,\\
Xv_{m-2} &= XYv_{m-1} = YXv_{m-1} + Hv_{m-1} = (2\lambda - 2)\, v_{m-1}\,,\\
Xv_{m-3} &= XYv_{m-2} = YXv_{m-2} + Hv_{m-2} = (3\lambda - (2 + 4))\, v_{m-2}\,,\\
&\dots\\
Xv_{m-k} &= XYv_{m-k+1} = YXv_{m-k+1} + Hv_{m-k+1}\\
&= (k\lambda - (2 + 4 + \dots + 2(k-1)))\; v_{m-k+1} = k\,(\lambda - k + 1)\, v_{m-k+1}\,,\\
&\dots\\
Xv_0 &= m\,(\lambda - m + 1)\, v_1\,.
\end{aligned}$$

The next step leads to the zero vector

$$0 = XYv_0 = YXv_0 + Hv_0 = (m + 1)(\lambda - m)\, v_0$$

and forces $\lambda = m$. Therefore, the operators X, Y, H act on the vectors v_i by the rules

$$X(v_k) = (m - k)(k + 1)\, v_{k+1}\,, \quad Y(v_k) = v_{k-1}\,, \quad H(v_k) = (2k - m)\, v_k\,.$$

Formula (8.7) shows that the map $v_k \mapsto e_k/k! = x^k y^{n-k}/k!$ identifies the linear span of vectors v_k with the standard module V_m from Example 8.2. □

Theorem 8.1 *The simple finite-dimensional $\mathfrak{sl}_2$-modules over a field $\Bbbk$ of characteristic zero are exhausted (up to isomorphism) by the standard modules V_n from Example 8.2.*

Proof Let $\overline{\Bbbk} \subset \Bbbk$ be the algebraic closure[2] of the field $\Bbbk$. The tensor product of vector spaces $\overline{V} = \overline{\Bbbk} \otimes V$ over $\Bbbk$ is a vector over $\overline{\Bbbk}$ with the action of $\overline{\Bbbk}$ by the rule[3] $\lambda \cdot (\mu \otimes v) \stackrel{\text{def}}{=} (\lambda\mu) \otimes v$. Every $\Bbbk$-linear map $F : V \to V$ can be extended to a $\overline{\Bbbk}$-linear map $\overline{F} \stackrel{\text{def}}{=} \mathrm{Id} \otimes F : \overline{V} \to \overline{V}$.

Exercise 8.8 For every basis $e_1, e_2, \dots, e_n$ of V over $\Bbbk$, verify that the vectors $\overline{e}_p = 1 \otimes e_p$ form a basis of $\overline{V}$ over $\overline{\Bbbk}$, and the matrix of $\overline{F}$ in this basis coincides with the matrix of F in the basis $e_1, e_2, \dots, e_n$.

If a vector space V is an $\mathfrak{sl}_2$-module, then the operators $\overline{X}$, $\overline{Y}$, $\overline{H}$ provide $\overline{V}$ with an $\mathfrak{sl}_2$-module structure extending that on V. By the previous two lemmas, the operator $\overline{H}$ has an integer eigenvalue $m \in \operatorname{Spec} \overline{H}$. By Exercise 8.8, $\operatorname{Spec} H = \operatorname{Spec} \overline{H} \cap \Bbbk$. Hence, there exists a nonzero eigenvector of H in V as well. The arguments from the proof of Lemma 8.2 show that V possesses a primitive vector. By Lemma 8.3, it spans a standard simple $\mathfrak{sl}_2$-submodule of V, which must coincide with V, because V is simple. □

Example 8.3 (Isomorphism $V_n^* \simeq V_n$) Let V_n^* be the dual $\mathfrak{sl}_2$-module to the standard irreducible $\mathfrak{sl}_2$-module V_n, and suppose that the vectors $e_k^* \in V_n^*$ form the dual basis to the standard basis $e_k = x^k y^{n-k}$ in V_n. In accordance with formula (8.2) on p. 175 and formula (8.7) on p. 177, the operators X, Y, Z act in V_n^* by the rules

$$X(e_k^*) = -(n-k+1)\, e_{k-1}^*\,, \quad Y(e_k^*) = -(k+1)\, e_{k+1}^*\,, \quad H(e_k^*) = -(2k-n)\, e_k^*\,.$$

Hence, the $\mathfrak{sl}_2$-module V_n^* has the same weights $-n$, $-n-2$, ... , $n-2$, n as V_n. Therefore, $V_n^* \simeq V_n$, and by Schur's lemma, such an isomorphism is unique up to proportionality.

8.3 Semisimplicity of Finite-Dimensional $\mathfrak{sl}_2$-Modules

Associated with every element F of a Lie algebra $\mathfrak{g}$ is the linear endomorphism

$$\mathrm{ad}_F : \mathfrak{g} \to \mathfrak{g}\,, \quad X \mapsto [F, X]\,.$$

Sending every $F \in \mathfrak{g}$ to $\mathrm{ad}_F \in \mathrm{End}_{\Bbbk}(\mathfrak{g})$ leads to the *adjoint representation*

$$\mathrm{ad} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g}).$$

[2] See Theorem 13.4 on p. 303.

[3] Compare with Sect. 6.3 on p. 141.

Exercise 8.9 Verify that $\mathrm{ad}_{[X,Y]} = [\mathrm{ad}_X, \mathrm{ad}_Y]$ for all $X, Y \in \mathfrak{g}$.

The adjoint representation of $\mathfrak{g}$ allows us to equip the vector space $\mathrm{End}_{\Bbbk}(\mathfrak{g})$ with the structure of a $\mathfrak{g}$-module in which the action of an element $F \in \mathfrak{g}$ on an endomorphism $\varphi : \mathfrak{g} \to \mathfrak{g}$ is given by the formula

$$F\varphi \stackrel{\text{def}}{=} [\mathrm{ad}_F, \varphi]\,, \tag{8.8}$$

where the bracket means the commutator of endomorphisms of $\mathfrak{g}$, i.e., the commutator in the associative algebra $\mathrm{End}_{\Bbbk}(\mathfrak{g})$.

Exercise 8.10 Verify that $[X, Y]\varphi = XY\varphi - YX\varphi$ for all $X, Y \in \mathfrak{g}$ and all $\varphi \in \mathrm{End}(\mathfrak{g})$, where the bracket on the left-hand side means the Lie bracket in $\mathfrak{g}$.

Recall that the endomorphism algebra $\mathrm{End}(\mathfrak{g})$ is equipped with the inner product $(\varphi, \psi) = \mathrm{tr}(\varphi\psi)$. The restriction of this product to the image of the adjoint representation provides every Lie algebra $\mathfrak{g}$ with a symmetric bilinear form

$$(X, Y) \stackrel{\text{def}}{=} \mathrm{tr}(\mathrm{ad}_X \circ \mathrm{ad}_Y)\,, \tag{8.9}$$

called the *Killing form* on $\mathfrak{g}$.

Exercise 8.11 Verify that the Gram matrix of the Killing form on $\mathfrak{sl}_2$ in the standard basis[4] X, Y, H is

$$\begin{pmatrix} 0 & 4 & 0 \\ 4 & 0 & 0 \\ 0 & 0 & 8 \end{pmatrix}.$$

We conclude that the Killing form of the Lie algebra $\mathfrak{sl}_2$ is nondegenerate, and the basis of $\mathfrak{sl}_2$ dual to X, Y, H with respect to the Killing form is formed by the elements

$$X^* = \frac{1}{4}Y\,, \quad Y^* = \frac{1}{4}X\,, \quad H^* = \frac{1}{8}H\,.$$

The correlation map $\mathfrak{sl}_2 \xrightarrow{\sim} \mathfrak{sl}_2^*$ provided by the Killing form takes an element $F \in \mathfrak{sl}_2$ to the linear form $Z \mapsto (F, Z)$. Write $\gamma : \mathfrak{sl}_2^* \xrightarrow{\sim} \mathfrak{sl}_2$ for the inverse isomorphism and extend it to the isomorphism

$$\gamma \otimes \mathrm{Id} : \mathfrak{sl}_2^* \otimes \mathfrak{sl}_2 \simeq \mathrm{End}(\mathfrak{sl}_2) \xrightarrow{\sim} \mathfrak{sl}_2 \otimes \mathfrak{sl}_2\,, \tag{8.10}$$

which sends the identity endomorphism $\mathrm{Id}_{\mathfrak{sl}_2} \in \mathrm{End}(\mathfrak{sl}_2)$ to the *Casimir tensor*

$$X^* \otimes X + Y^* \otimes Y + H^* \otimes H = \frac{1}{4}\,(X \otimes Y + Y \otimes X) + \frac{1}{8}H \otimes H\,.$$

[4]See formula (8.4) on p. 176.

We write $K \in \mathfrak{U}(\mathfrak{sl}_2)$ for the class of the Casimir tensor in the universal enveloping algebra of $\mathfrak{sl}_2$ and call it the *Casimir element*.

By the universal property of $\mathfrak{U}(\mathfrak{sl}_2)$, every linear representation $\varrho : \mathfrak{sl}_2 \to \mathrm{End}(V)$ can be uniquely extended to a linear representation $\widetilde{\varrho} : \mathfrak{U}(\mathfrak{sl}_2) \to \mathrm{End}(V)$, which takes a class of the tensor $A \otimes B \in \mathfrak{sl}_2 \otimes \mathfrak{sl}_2$ to the linear endomorphism $\varrho(A)\varrho(B) \in \mathrm{End}(V)$. To simplify the notation, we omit the precise reference to the representation and denote the images of X, Y, Z, K in $\mathrm{End}(V)$ by the same letters X, Y, Z, K, as we were doing before. Then the Casimir endomorphism of V can be written as

$$K = \frac{1}{4}\,(XY + YX) + \frac{1}{8}\,H^2\,.$$

Exercise 8.12 Verify by direct computation that K commutes with X, Y, H and acts on the simple $\mathfrak{sl}_2$-module V_m as multiplication by the rational scalar $\big(m^2 + 2m\big)/8$.

Exercise 8.13 Verify that for every linear representation $\varrho : \mathfrak{sl}_2 \to \mathrm{End}(V)$, a homomorphism of $\mathfrak{sl}_2$-modules is provided by the composition of maps

$$\mathrm{End}(\mathfrak{sl}_2) \xrightarrow{\gamma\otimes\mathrm{Id}} \mathfrak{sl}_2 \otimes \mathfrak{sl}_2 \to \mathfrak{U}(\mathfrak{sl}_2) \xrightarrow{\widetilde{\varrho}} \mathrm{End}(V)\,,$$

where the middle arrow is the restriction of the quotient map $\mathsf{T}(\mathfrak{sl}_2) \twoheadrightarrow \mathfrak{U}(\mathfrak{sl}_2)$, and the $\mathfrak{sl}_2$-module structures on the left and right spaces are such that an element $F \in \mathfrak{sl}_2$ acts on $\varphi \in \mathrm{End}(\mathfrak{sl}_2)$ and $\psi \in \mathrm{End}(V)$ by the rules[5] $F\varphi \stackrel{\mathrm{def}}{=} [\mathrm{ad}_F, \varphi]$ and $F\psi \stackrel{\mathrm{def}}{=} [\varrho(F), \psi]$.

Note that Exercise 8.13 implies the first statement of Exercise 8.12 without any computation: since the identity $\mathrm{Id} \in \mathrm{End}(\mathfrak{sl}_2)$ commutes with all endomorphisms of $\mathfrak{sl}_2$, in particular with all elements ad_F for $F \in \mathfrak{sl}_2$, its image $K \in \mathrm{End}(V)$ commutes with all operators $\varrho(F)$, in particular with X, Y, H.

Lemma 8.4 *Let V be an $\mathfrak{sl}_2$-module and $U \subset V$ an $\mathfrak{sl}_2$-submodule of codimension* 1. *Then there exists a trivial $\mathfrak{sl}_2$-submodule $L \simeq V_0$ in V such that $V = U \oplus L$.*

Proof Note that every 1-dimensional $\mathfrak{sl}_2$-module L is trivial, because the algebra $\mathrm{End}_{\Bbbk}(L) \simeq \Bbbk$ is commutative and therefore $H = [X, Y] = 0$, $2X = [H, X] = 0$, $2Y = [Y, H] = 0$ in $\mathrm{End}_{\Bbbk}(L)$. In particular, the quotient module V/U is trivial, i.e., the images of the operators X, Y, H lie inside U. We construct a submodule $L \subset V$ complementary to U by induction on $\dim U$.

If $\mathfrak{sl}_2$ annihilates U (e.g., if $\dim U = 1$), then the operators $H = XY - YX$, $X = (HX - XH)/2$, $Y = (YH - HY)/2$ annihilate the whole of V by the previous remark, and therefore, we can take any subspace L complementary to U.

[5] Compare with Exercise 8.10 and the preceding paragraph.

If $U \simeq V_m$ is a nontrivial simple $\mathfrak{sl}_2$-module, then the operator

$$\frac{8}{m^2 + 2\,m}\,K : V \to U$$

is $\mathfrak{sl}_2$-linear and acts on U as the identity by Exercise 8.12. Thus, it provides V with an $\mathfrak{sl}_2$-linear projector onto U, and therefore, $L = \ker K$ is the required submodule.

If U is not simple and $W \subsetneq U$ is a nontrivial $\mathfrak{sl}_2$-submodule, then by the inductive hypothesis, the quotient module V/W splits into a direct sum of $\mathfrak{sl}_2$-submodules $(V/W) = (U/W) \oplus L'$, where $\dim L' = 1$. Then

$$\widetilde{L} = \left\{v \in V \mid v \,(\mathrm{mod}\, W) \ \in L'\right\}$$

is a proper $\mathfrak{sl}_2$-submodule of V such that $\widetilde{L} \cap U = W$ and $\dim(\widetilde{L}/W) = 1$. Thus, by the inductive hypothesis applied to the pair $W \subset \widetilde{L}$, there is a direct sum decomposition $\widetilde{L} = W \oplus L$, where $L \subset \widetilde{L}$ is a trivial 1-dimensional $\mathfrak{sl}_2$-submodule transversal to U. □

Theorem 8.2 *Every finite-dimensional $\mathfrak{sl}_2$-module V is semisimple, i.e., splits into a direct sum of standard simple $\mathfrak{sl}_2$-modules V_m from Example 8.2 on p. 176.*

Proof Let $U \subset V$ be a proper nonzero $\mathfrak{sl}_2$-submodule. It is enough to show that there exists an $\mathfrak{sl}_2$-linear projector $\pi : V \twoheadrightarrow U$. The vector spaces

$$W = \{\varphi : V \to U \mid \varphi|_U = \lambda \mathrm{Id}_U \text{ for some } \lambda \in \Bbbk\}\,,$$
$$W' = \{\varphi \in W | \varphi|_U = 0\}\,,$$

form a pair of $\mathfrak{sl}_2$-submodules $W' \subset W$ in the $\mathfrak{sl}_2$-module $\mathrm{Hom}_{\Bbbk}(V, U)$, and $\mathrm{codim}_W W' = 1$.

Exercise 8.14 Check this.

It follows from Lemma 8.4 applied to the pair $W' \subset W$ that $W = W' \oplus L$ for some trivial 1-dimensional $\mathfrak{sl}_2$-submodule $L \subset W$. Since every nonzero operator $\varphi \in L$ is $\mathfrak{sl}_2$-linear and acts on U as scalar multiplication, there exists $\pi \in L$ acting identically on U. □

Example 8.4 (Exterior Squares of Standard Simple Modules) Since the standard basis vector $e_k = x^k y^{n-k}$ in V_n is an eigenvector of H with eigenvalue $2k - n$ for all $0 \leqslant k \leqslant n$, the products $e_{ij} \stackrel{\text{def}}{=} e_i \wedge e_j$, $0 \leqslant i < j \leqslant n$, are weight vectors of the $\mathfrak{sl}_2$-module $\Lambda^2 V_n$ with weights $2i - n + 2j - n = 2(i + j - n)$. Thus, the weights of $\Lambda^2 V_n$ are $-2(n-1)\,,\ -2(n-2)\,,\ \dots\ ,-2\,,0\ 2\,,\ \dots\ ,\ 2(n-2)\,,\,2(n-1)$. For every $\nu = 1,\, 2,\, \dots\,,\, n$, the multiplicity of each of the weights $\pm 2|n - \nu|$ is $[(\nu + 1)/2]$, the number of nonnegative integer solutions (i,j), $i < j$, of the equation $i + j = \nu$.

We conclude that the $\mathfrak{sl}_2$-isotypic decomposition of $\Lambda^2 V_n$ is

$$\Lambda^2 V_n \simeq V_{2n-2} \oplus V_{2n-6} \oplus V_{2n-10} \oplus \cdots = \bigoplus_{s=0}^{[(n-1)/2]} V_{2(n-2s-1)} \,. \tag{8.11}$$

For example, $\Lambda^2 V_3 \simeq V_4 \oplus V_0$. This means that there exists a skew-symmetric form ω on V_3^*, unique up to proportionality, such that $\omega(Z\varphi, \psi) + \omega(\varphi, Z\psi) = 0$ for all $Z \in \mathfrak{sl}_2$ and $\varphi, \psi \in V_3^*$.

Exercise 8.15 Verify that every nonzero element of the second summand provides $\Lambda^2 V_3$ with such a form, and conversely.

The right correlation map[6] $\omega : V_3 \xrightarrow{\sim} V_3^*$ of ω is a skew-symmetric isomorphism[7] of $\mathfrak{sl}_2$-modules. Its inverse map $\omega^{-1} : V_3^* \xrightarrow{\sim} V_3$ coincides (up to proportionality) with the isomorphism from Example 8.3 on p. 179 for $n = 3$.

Problems for Independent Solution to Chapter 8

Problem 8.1 Show that in every finite-dimensional $\mathfrak{sl}_2$-module over a field of characteristic zero, $X, Y \in \mathfrak{sl}_2$ are represented by nilpotent operators and $H \in \mathfrak{sl}_2$ by a diagonalizable operator.

Problem 8.2 Show that on every Lie algebra $\mathfrak{g}$, the Killing form[8]

$$(A, B) = \mathrm{tr}(\mathrm{ad}_A \circ \mathrm{ad}_B)$$

satisfies the relation $([A, B], C) + (B, [A, C]) = 0$ for all $A, B, C \in \mathfrak{g}$.

Problem 8.3 Convince yourself that the *Pauli matrices*

$$\sigma_1 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

[6]See formula (16.1) in Sect. 16.1.1 of Algebra I.

[7]Meaning that $\omega^* = -\omega$, where $\omega^* : V_3^{**} \simeq V_3 \xrightarrow{\sim} V_3^*$ is the dual correlation.

[8]See formula (8.9) on p. 180.

form a basis of $\mathfrak{sl}_2(\mathbb{C})$ over $\mathbb{C}$, and compute: **(a)** their commutators, **(b)** the Gram matrix of the Killing form in this basis, **(c)** the dual basis $\sigma_1^*, \sigma_2^*, \sigma_3^*$ with respect to the Killing form, **(d)** the Casimir element K in terms of $\sigma_1, \sigma_2, \sigma_3$.

Problem 8.4 (Clebsch–Gordan Decomposition) Decompose $V_m \otimes V_n$ into a direct sum of standard simple $\mathfrak{sl}_2$-modules and indicate all m, n such that this decomposition contains **(a)** V_0, **(b)** V_1.

Problem 8.5 Show that the $\mathfrak{sl}_2$-invariant isomorphism $V_1 \simeq V_1^*$ is provided by the right correlation map[9] of the skew-symmetric bilinear form det on V_1, which sends a degree-one polynomial $\beta(x,y) = b_1x + b_2y \in V_1$ to the linear functional

$$\det(*, \beta) : V_1 \to \Bbbk\,, \quad \alpha(x,y) = a_1x + a_2y \mapsto \det(\alpha, \beta) = \det\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}.$$

Problem 8.6 Find the dimension of the space of all bilinear forms $\beta : V_n \times V_n \to \Bbbk$ such that $\beta(Zu, w) + \beta(u, Zw) = 0$ for all $v, w \in V_n$, $Z \in \mathfrak{sl}_2$. Is there a nondegenerate **(a)** symmetric, **(b)** skew-symmetric, form in this space? Verify that the correlation map of every such form establishes an $\mathfrak{sl}_2$-invariant isomorphism[10] $V_n \simeq V_n^*$. How does it interact with the nth symmetric power of the isomorphism $V_1 \simeq V_1^*$ from the previous problem?

Problem 8.7 Find all nonnegative integers m, n, k such that there exists an $\mathfrak{sl}_2$-invariant linear map $\varepsilon_{mn}^k : V_m \otimes V_n \to V_k$. For all these m, n, k, find the dimension of the space of such maps.

Problem 8.8 Let the elements $F \in \mathfrak{sl}_2$ act on $W = \mathrm{End}_{\Bbbk}(V_1)$ by the rule

$$F : \varphi \mapsto [F, \varphi].$$

Find the isotypic decompositions of W, $W^{\otimes 2}$, S^2W, and Λ^2W.

Problem 8.9 Show that $S^nV_2 = \bigoplus_{i=0}^{[n/2]} V_{2n-4i}$.

Problem 8.10 Let $\mathbb{P}_1 = \mathbb{P}(V_1)$, $\mathbb{P}_2 = \mathbb{P}(V_2) = \mathbb{P}(S^2V_1)$, and let $C_2 \subset \mathbb{P}_2$ be the *Veronese conic*,[11] that is, the image of the quadratic Veronese embedding

$$\mathbb{P}_1 \hookrightarrow \mathbb{P}_2, \alpha(x,y) \mapsto \alpha^2(x,y).$$

Use the $\mathfrak{sl}_2$-invariant isomorphism $V_2 \simeq V_2^*$ provided by Problem 8.6 and the induced isomorphisms $S^nV_2 \simeq S^nV_2^*$ to establish the following geometric interpretations of $\mathfrak{sl}_2$-isotypic decomposition from Problem 8.9 for $n = 2, 3$.

[9] See Sect. 16.1.1 of Algebra I, especially formula (16.1), and also Example 7.7.

[10] Compare with Example 8.3 on p. 179.

[11] See Example 11.6 of Algebra I.

(a) Show that the action of $\mathfrak{sl}_2$ on $S^2V_2 \simeq S^2V_2^*$ annihilates the equation of the Veronese conic. Verify that the first summand in the decomposition

$$S^2V_2^* \simeq S^0V_1^* \oplus S^4V_1^*$$

is spanned by the equation of C_2 and that the second summand is linearly generated by the squares of linear forms determining the tangent lines to C_2.

(b) Show that the first summand in the decomposition $S^3V_2^* \simeq S^2V_1^* \oplus S^6V_1^*$ consists of the cubic curves on $\mathbb{P}_2 = \mathbb{P}(V_2)$ splitting into a union of C_2 and some line, and the isomorphism between the space of such cubics and $S^2V_1^*$ maps the equation of such a cubic to the quotient formed by dividing it by the equation of C_2, i.e., to the equation of the corresponding line. Also, show that the $\mathfrak{sl}_2$-invariant projection onto the second summand is provided by the *evaluation map* that sends a cubic polynomial f on S^2V_1 to the degree-six polynomial on V_1 whose value on a vector $v \in V_1$ is $f(v^2)$.

Problem 8.11 Under the notation of the previous problem, let

$$\mathbb{P}_3 = \mathbb{P}(V_3) = \mathbb{P}(S^3V_1),$$

and let $C_3 \subset \mathbb{P}_3$ be the *Veronese cubic*,[12] that is, the image of the cubic Veronese embedding $\mathbb{P}_1 \hookrightarrow \mathbb{P}_3$, $\alpha(x,y) \mapsto \alpha^3(x,y)$. Establish the $\mathfrak{sl}_2$-isotypic decomposition $S^2V_3^* \simeq S^2V_1^* \oplus S^6V_1^*$ and verify that:

(a) The first summand $S^2V_1^* \subset S^2V_3^*$ consists of all quadrics on $\mathbb{P}_3$ containing the Veronese cubic.

(b) The second summand $S^6V_1^* \subset S^2V_3^*$ is spanned by the squares of linear forms determining the *osculating planes*[13] of the Veronese cubic.

(c) The $\mathfrak{sl}_2$-invariant projection $S^2V_3^* \twoheadrightarrow S^6V_1^*$ is provided by the evaluation map sending a quadratic form q on S^3V_1 to the degree-six polynomial on V_1 whose value on a vector $v \in V_1$ is $q(v^3)$.

(d) The $\mathfrak{sl}_2$-invariant projection $S^2V_3^* \twoheadrightarrow S^2V_1^*$, considered as a quadratic map $V_3 \to V_2$, sends a cubic polynomial $f(x,y) \in V_2$ to its *Hessian*

$$\mathrm{Hes}_f(x,y) \stackrel{\text{def}}{=} \det \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} \end{pmatrix}.$$

Problem 8.12 In the notation of the previous problem, show that the map $\mathbb{P}_3 \xrightarrow{\sim} \mathbb{P}_3^\times$ provided by the projectivization of the skew-symmetric isomorphism $V_3 \xrightarrow{\sim} V_3^*$

[12] See Example 11.6 of Algebra I.

[13] By definition, the *osculating plane* to a parametrically given projective curve $t \mapsto \varphi(t)$ at a point $\varphi(a)$ is spanned by $\varphi(a)$, $\varphi'(a)$ (the velocity), and $\varphi''(a)$ (the acceleration) considered as points of the projective space in which the curve lives.

from Example 8.4 sends each point of the Veronese cubic $C_3 \subset \mathbb{P}_3$ to the osculating plane[14] of C_3 at this point.

Problem 8.13 Show that $S^3V_3^* \simeq S^3V^* \oplus S^5V^* \oplus S^9V^*$, where the first summand is spanned by the equations of cones over the Veronese cubic with vertices at arbitrary points of $\mathbb{P}_3$, the sum of the first two factors consists of all cubic surfaces containing the Veronese cubic, and the projection onto the third summand is given by the evaluation map sending a cubic form f on S^3V_1 to the degree-nine polynomial on V_1 whose value on a vector $v \in V_1$ is $f(v^3)$. Try to give an explicit description of the $\mathfrak{sl}_2$-invariant projection $S^3V_3^* \twoheadrightarrow S^5V^*$.

Problem 8.14 Describe the $\mathfrak{sl}_2$-isotypic decomposition for $S^4V_3^*$. In particular, show that the surface formed by tangent lines to the Veronese cubic has degree 4 and spans the trivial component of $S^4V_3^*$.

Problem 8.15 Show that $S^2V_4 \simeq S^0V_1 \oplus S^4V_1 \oplus S^8V_1$, where the first summand is spanned by the unique quadric containing all tangent lines to the Veronese quartic curve $C_4 \subset \mathbb{P}_4 = \mathbb{P}(V_4)$, and the first two summands form the space of all quadrics containing the Veronese quartic. Describe explicitly the $\mathfrak{sl}_2$-invariant projections of $S^2V_4^*$ onto the last two summands.

Problem 8.16 Show that[15] $S^2V_n = \bigoplus_{i=0}^{[n/2]} V_{2n-4i}$, where for every $k \geqslant 0$, the subsum $\bigoplus_{i>k} V_{2n-4i}$ is formed by the quadrics containing all osculating subspaces of dimension k to the nth-degree Veronese curve $C_n \subset \mathbb{P}_n = \mathbb{P}(V_n)$.

Problem 8.17 Describe explicitly the $\mathfrak{sl}_2$-invariant projection $\Lambda^2V_n \twoheadrightarrow V_{2n-2}$ in the isotypic decomposition from formula (8.11) on p. 183.

Problem 8.18* **(Hermite Reciprocity)** Prove that for all $m, n \in \mathbb{N}$, one has $S^mV_n \simeq S^nV_m$ as $\mathfrak{sl}_2$-modules.

Problem 8.19* Prove that $\Lambda^mV_n \simeq S^mV_{n+1-m}$ as $\mathfrak{sl}_2$-modules.

[14] Considered as a point of the dual space $\mathbb{P}_3^\times = \mathbb{P}(V_3^*)$.

[15] Compare with Problem 8.9.

Chapter 9
Categories and Functors

9.1 Categories

9.1.1 Objects and Morphisms

A *category* $\mathcal{C}$ is formed by a *class*[1] *of objects* $\mathrm{Ob}\,\mathcal{C}$ and a class of disjoint sets $\mathrm{Hom}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(X,Y)$, one set for each ordered pair of objects $X, Y \in \mathrm{Ob}\,\mathcal{C}$. Elements of the set $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ are called *morphisms* from X to Y in the category $\mathcal{C}$. We will depict them by arrows $\varphi : X \to Y$ and refer to the objects X, Y as the *source* (or *domain*) and *target* (or *codomain*) of φ respectively. Morphisms $\varphi, \psi \in \mathrm{Mor}\,\mathcal{C}$ are called *composable* if the source of φ coincides with the target of ψ. For every ordered triple of objects $X, Y, Z \in \mathrm{Ob}\,\mathcal{C}$, the *composition map*

$$\mathrm{Hom}(Y,Z) \times \mathrm{Hom}(X,Y) \to \mathrm{Hom}(X,Z)\,, \quad (\varphi,\psi) \mapsto \varphi \circ \psi\,, \tag{9.1}$$

is defined. It is associative, meaning that $(\eta \circ \varphi) \circ \psi = \eta \circ (\varphi \circ \psi)$ for all composable pairs η, φ and φ, ψ. Finally, for every $X \in \mathrm{Ob}\,\mathcal{C}$, there exists an *identity endomorphism*

$$\mathrm{Id}_X \in \mathrm{End}_{\mathcal{C}}(X) \stackrel{\text{def}}{=} \mathrm{Hom}_{\mathcal{C}}(X,X)$$

[1]For formal logical reasons, the collection of all sets (even all finite sets) is not itself a set. Similarly, the collections of all rings, groups, topological spaces, etc., are not sets, but something larger, namely *classes*. The notion of class enlarges the notion of set and makes it possible to formulate correct statements about the classes of all sets, groups, rings, vector spaces, etc. To the extent that we have omitted a discussion of rigorous set theory, we shall refer the reader to a basic course in mathematical logic for the rigorous theory of classes and their interaction with sets. For our purposes, it is enough to know that such a theory exists and that it allows us to deal with the categories of sets, algebras, topological spaces, etc.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_9

such that $\varphi \circ \mathrm{Id}_X = \varphi$ and $\mathrm{Id}_X \circ \psi = \psi$ for all morphisms $\varphi : X \to Y$, $\psi : Z \to X$ in $\mathcal{C}$. It is actually unique for every $X \in \mathrm{Ob}\,\mathcal{C}$, because $\mathrm{Id}'_X = \mathrm{Id}'_X \circ \mathrm{Id}''_X = \mathrm{Id}''_X$ for every two such endomorphisms $\mathrm{Id}'_X, \mathrm{Id}''_X \in \mathrm{Hom}(X, X)$.

A *subcategory* $\mathcal{D} \subset \mathcal{C}$ is a category with $\mathrm{Ob}\,\mathcal{D} \subset \mathrm{Ob}\,\mathcal{C}$ and

$$\mathrm{Hom}_{\mathcal{D}}(X, Y) \subset \mathrm{Hom}_{\mathcal{C}}(X, Y) \text{ for all } X, Y \in \mathrm{Ob}\,\mathcal{D}$$

such that the compositions and identity endomorphisms of $\mathcal{D}$ coincide with those in $\mathcal{C}$. A subcategory $\mathcal{D} \subset \mathcal{C}$ is called *full* if

$$\mathrm{Hom}_{\mathcal{D}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y) \text{ for all } X, Y \in \mathrm{Ob}\,\mathcal{D}\,.$$

The disjoint union $\mathrm{Mor}\,\mathcal{C} \overset{\text{def}}{=} \bigsqcup_{X,Y} \mathrm{Hom}_{\mathcal{C}}(X, Y)$ is called the *class of morphisms* of the category $\mathcal{C}$. We will often say an "arrow of $\mathcal{C}$" instead of an "element of $\mathrm{Mor}\,\mathcal{C}$," and write $\varphi\psi$ instead of $\varphi \circ \psi$ for the composition of arrows.

A category $\mathcal{C}$ is called *small* if $\mathrm{Ob}\,\mathcal{C}$ is a set, not a larger class. In this case, $\mathrm{Mor}\,\mathcal{C}$ is a set as well.

Example 9.1 (Nonsmall Categories) The following nonsmall categories are commonly used in practice: the category of all sets $\mathcal{S}et$ and all maps between them; the category of topological spaces $\mathcal{T}op$ and continuous maps between them; the category $\mathcal{V}ec_{\Bbbk}$ of all vector spaces over a field $\Bbbk$ and $\Bbbk$-linear maps between them, and its full subcategory $vec_{\Bbbk}$ formed by the finite-dimensional vector spaces; the categories R-$\mathcal{M}od$ and $\mathcal{M}od$-R of the left and right modules over a ring R and R-linear maps between them; the full subcategories R-$mod \subset R$-$\mathcal{M}od$, and mod-$R \subset \mathcal{M}od$-R of *finitely presented*[2] modules. The category of abelian groups $\mathcal{A}b = \mathbb{Z}$-$\mathcal{M}od$ and their homomorphisms. The category $\mathcal{G}rp$ of all groups and group homomorphisms. The category of commutative rings with unit $\mathcal{C}mr$ and the ring homomorphisms sending the unit to the unit. All these categories are subcategories of $\mathcal{S}et$, and all but $\mathcal{S}et$ are not full in $\mathcal{S}et$.

Example 9.2 (Posets and Topologies) Every poset[3] M can be considered a small category whose objects are the elements $m \in M$ and whose arrows are the inequalities in M, i.e.,

$$\mathrm{Hom}_M(n, m) = \begin{cases} \text{one element for } n \leqslant m\,, \\ \varnothing \text{ otherwise}\,. \end{cases}$$

The composition of arrows $k \leqslant \ell$ and $\ell \leqslant n$ is the arrow $k \leqslant n$. The associativity and existence of the identity endomorphisms can be rephrased as the transitivity and reflexivity of the partial order.

[2]An R-module is called *finitely presented* if it is isomorphic to the quotient module of a free R-module of finite rank by a finitely generated R-submodule of relations.

[3]That is, a partially ordered set; see Sect. 1.4.1 of Algebra I.

An important example of such a category is the category $\mathcal{U}(X)$ of all *open sets* of a topological space[4] X. The arrows in $\mathcal{U}(X)$ are the inclusions of open sets

$$\mathrm{Hom}_{\mathcal{U}(X)}(U, W) = \begin{cases} \text{the inclusion } U \hookrightarrow W & \text{for } U \subseteq W\,, \\ \varnothing & \text{for } U \not\subseteq W\,. \end{cases}$$

Example 9.3 (Small Categories Versus Associative Algebras) Every associative algebra A with unit $e \in A$ over a commutative ring K can be viewed as a small category with just one object e and the set of morphisms $\mathrm{Hom}(e, e) = A$, where the composition is the multiplication in A. Conversely, associated with every small category $\mathcal{C}$ and commutative ring K is the associative *K-algebra of arrows*[5] $K[\mathcal{C}]$, the free K-module with basis $\mathrm{Mor}\,\mathcal{C}$ and the K-bilinear multiplication defined on the basis vectors by the assignment

$$\varphi\psi \stackrel{\text{def}}{=} \begin{cases} \varphi \circ \psi & \text{for composable } \varphi, \psi\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

For example, if $\mathcal{C}$ consists of just one object whose endomorphisms form a group G, then $K[G]$ becomes the group algebra of G with coefficients in K. In the general case, the algebra $K[\mathcal{C}]$ can be thought of as the algebra of finitely supported matrices whose rows and columns are numbered by the objects of $\mathcal{C}$. The only elements allowed in the (Y, X)-entry of such a matrix are the finite formal linear combinations of arrows $\varphi : X \to Y$ with coefficients in K, and all but a finite number of entries in every matrix vanish. In general, this algebra is noncommutative. If $\mathrm{Ob}\,\mathcal{C}$ is infinite, there is no unit element in $K[\mathcal{C}]$; however, for every $f \in K[\mathcal{C}]$, there exists an idempotent element $e_f = e_f^2$ in $K[\mathcal{C}]$ such that $e_f \circ f = f \circ e_f = f$. For example, one can define e_f to be the sum of the identity endomorphisms Id_X taken over all $X \in \mathrm{Ob}\,\mathcal{C}$ appearing as sources or targets of the $\varphi \in \mathrm{Mor}\,\mathcal{C}$ that appear in f with nonzero coefficients.

9.1.2 Mono-, Epi-, and Isomorphisms

An arrow φ in a category $\mathcal{C}$ is called *injective* or a *monomorphism* if it is left cancellable, that is, if $\varphi\alpha = \varphi\beta \Rightarrow \alpha = \beta$ for all $\alpha, \beta \in \mathrm{Mor}\,\mathcal{C}$ composable with φ from the right. Symmetrically, φ is called *surjective* or an *epimorphism* if it

[4] A set X is called a *topological space* if a set $\mathcal{U}(X)$ of subsets in X is chosen such that $\varnothing, X \in \mathcal{U}(X)$, $U \cap W \in \mathcal{U}(X)$ for all $U, W \in \mathcal{U}(X)$, and $\bigcup_\nu U_\nu \in \mathcal{U}(X)$ for every set of $U_\nu \in \mathcal{U}(X)$. The elements $U \in \mathcal{U}(X)$ and their complements $X \smallsetminus U$ are called, respectively, the *open* and *closed* subsets of X.

[5] Also known as the *path algebra* of $\mathcal{C}$.

is right cancellable, i.e., if $\alpha\varphi = \beta\varphi \Rightarrow \alpha = \beta$. A morphism $\varphi : X \to Y$ is called *invertible* or an *isomorphism* if there exists an arrow $\psi : Y \to X$ such that $\varphi\psi = \mathrm{Id}_Y$ and $\psi\varphi = \mathrm{Id}_X$. In this case, the objects X, Y are called *isomorphic*, and morphisms φ, ψ are called *inverses* of each other.

Example 9.4 (Combinatorial Simplices) Write Δ_{big} for the category of finite totally ordered sets with the order-preserving maps[6] between them, and $\Delta \subset \Delta_{\mathrm{big}}$ for its small full subcategory, called the *simplicial category*, formed by the sets

$$[n] \stackrel{\text{def}}{=} \{0, 1, \dots, n\}, \quad n \geqslant 0, \tag{9.2}$$

equipped with the standard orderings. The set $[n]$ is called the *combinatorial n-simplex*. Though the whole category Δ_{big} is not small, every object $X \in \mathrm{Ob}\,\Delta_{\mathrm{big}}$ admits a unique isomorphism $\eta_X : X \xrightarrow{\sim} [n_X]$ with the unique combinatorial simplex $[n_X] \in \mathrm{Ob}\,\Delta$, namely, the numbering of elements in X by $0, 1, \dots, n_X$, where $n_X = |X| - 1$, in the increasing order.

Exercise 9.1 Find the cardinality of the set $\mathrm{Hom}_\Delta([n], [m])$ for all n, m. How many injective and surjective maps, expressed as a function of n and m, are there in $\mathrm{Hom}_\Delta([n], [m])$?

Exercise 9.2 Prove that the algebra $\mathbb{Z}[\Delta]$ is generated by the arrows

$$e_n = \mathrm{Id}_{[n]}, \qquad \text{the identity map}, \tag{9.3}$$

$$\partial_n^{(i)} : [n-1] \hookrightarrow [n], \qquad \text{the injection such that } i \notin \mathrm{im}\,\partial_n^{(i)}, \tag{9.4}$$

$$s_n^{(i)} : [n+1] \twoheadrightarrow [n], \qquad \text{the surjection such that } s_n^{(i)}(i) = s_n^{(i)}(i+1), \tag{9.5}$$

and indicate some generators for the ideal of relations between these arrows.

9.1.3 Reversing of Arrows

Associated with every category $\mathcal{C}$ is its *opposite category* $\mathcal{C}^{\mathrm{opp}}$ with the same class of objects and reversed arrows:

$$\mathrm{Ob}\,\mathcal{C}^{\mathrm{opp}} = \mathrm{Ob}\,\mathcal{C}, \quad \mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X), \quad \varphi^{\mathrm{opp}} \circ \psi^{\mathrm{opp}} = (\psi \circ \varphi)^{\mathrm{opp}}.$$

In the language of associative algebras, the reversing of arrows means the replacement of the algebra of arrows $C = K[\mathcal{C}]$ by its *opposite algebra* C^{opp}, which consists of the same elements multiplied in the reverse order: the product $\varphi_1\varphi_2 \cdots \varphi_s$ in C^{opp} means the product $\varphi_s\varphi_{s-1} \cdots \varphi_1$ in C.

[6]That is, $\varphi : X \to Y$ such that $x_1 \leqslant x_2 \Rightarrow \varphi(x_1) \leqslant \varphi(x_2)$.

9.2 Functors

9.2.1 Covariant Functors

A *functor*[7] $F : \mathcal{C} \to \mathcal{D}$ from a category $\mathcal{C}$ to a category $\mathcal{D}$ is a map of classes $\operatorname{Ob}\mathcal{C} \to \operatorname{Ob}\mathcal{D}$, $X \mapsto F(X)$, together with a class of maps[8] of sets

$$\operatorname{Hom}_{\mathcal{C}}(X,Y) \to \operatorname{Hom}_{\mathcal{D}}(F(X),F(Y)), \quad \varphi \mapsto F(\varphi), \tag{9.6}$$

such that $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$ for all $X \in \operatorname{Ob}\mathcal{C}$ and $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$ for all composable arrows $\varphi, \psi \in \operatorname{Mor}\mathcal{C}$. In the language of associative algebras, the functors are the homomorphisms between the algebras of arrows. A functor F is called *full* if all the maps (9.6) are surjective. The image of a full functor is a full subcategory in $\mathcal{D}$. If all the maps (9.6) are injective, the functor F is called *faithful*. In terms of algebras, the faithful functors give the injective homomorphisms between the algebras of arrows. A functor is called *fully faithful* if it is simultaneously full and faithful.

The simplest examples of functors are provided by the *identity endofunctor*[9] $\mathrm{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$, which acts as the identity map on both the objects and arrows, and by the *forgetful functors* acting from categories of sets equipped with some extra structures[10] and morphisms respecting the structure to the category $\mathcal{S}et$. A forgetful functor just forgets the extra structure: it sends every object to its underlaying set and acts identically on the arrows. Such a functor is not full as soon there are some maps between underlying sets that do not respect the structure, and it is not faithful if there exist distinct morphisms of structures with identical action on the underlaying sets.

Example 9.5 (Geometric Realization of Combinatorial Simplices) The *geometric realization* functor from the simplicial category to the category of topological spaces $\Delta \to \mathcal{T}op$, $[n] \mapsto \Delta^n$, sends every combinatorial n-simplex to the regular n-simplex

$$\Delta^n = \left\{ (x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1} \;\middle|\; \sum x_\nu = 1\,,\ x_\nu \geqslant 0 \right\}, \tag{9.7}$$

the convex hull of heads of the standard basis vectors $e_0, e_1, \dots, e_n$ in $\mathbb{R}^{n+1}$. Under the geometric realization, an order-preserving map $\varphi : [n] \to [m]$ goes to the unique affine map $\varphi_* : \Delta^n \to \Delta^m$ acting on the basis vectors by the rule $e_\nu \mapsto e_{\varphi(\nu)}$. The geometric realization is faithful but not full. Under the geometric realization, the generating elements (9.4), (9.5) of the algebra $\mathbb{Z}[\Delta]$ go respectively to the *inclusion of the ith hyperface* $\Delta^{(n-1)} \hookrightarrow \Delta^n$, which identifies $\Delta^{(n-1)}$ with the convex hull

[7] Or more precisely, a *covariant functor*.

[8] One map per each ordered pair of objects $X, Y \in \operatorname{Ob}\mathcal{C}$.

[9] In the same way as an endomorphism means a map of a set to itself, an *endofunctor* means a functor from a category to itself.

[10] Such as $\mathcal{T}op$, $\mathcal{G}rp$, $\mathcal{C}mr$.

of all but the ith vertices of Δ^n, and to the *degeneration along the ith edge*, which projects Δ^n onto $\Delta^{(n-1)}$ by contracting the edge $[i, i+1]$ to the ith vertex of $\Delta^{(n-1)}$.

9.2.2 Presheaves

A functor $F : \mathcal{C}^{\text{opp}} \to \mathcal{D}$ is called a *contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$ or a *presheaf* of objects of the category $\mathcal{D}$ on the category $\mathcal{C}$. Such a functor inverts the order of arrows in compositions, $F(\varphi \circ \psi) = F(\psi) \circ F(\varphi)$ for all composable $\varphi, \psi \in \operatorname{Mor} \mathcal{C}$. In the language of associative algebras, the presheaves are the *antihomomorphisms* between the path algebras.

Example 9.6 (Triangulated Spaces) Write $\Delta_s \subset \Delta$ for the nonfull subcategory formed by the same objects $[n]$, $n \in \mathbb{N}$, like the simplicial category Δ but with only the strictly increasing[11] maps $\varphi : [n] \to [m]$ allowed as morphisms. The category Δ_s is called the *semisimplicial category*.

Exercise 9.3 Verify that the algebra $\mathbb{Z}[\Delta_s]$ is generated by the identity endomorphisms $e_n = \mathrm{Id}_{[n]}$ and the inclusions of hyperfaces $\partial_n^{(i)}$ from (9.4).

A presheaf of sets $X : \Delta_s^{\text{opp}} \to \mathcal{S}et$ on the semisimplicial category Δ_s is called a *semisimplicial set*. Such a presheaf is nothing but the explicit combinatorial description for some *triangulated topological space* denoted by $|X|$ and called the *geometric realization* of the semisimplicial set X. Namely, for every nonnegative integer n, the functor X assigns the set $X_n = X([n])$, whose points can be viewed as disjoint n-dimensional regular simplices Δ_x^n, $x \in X_n$, from which the space $|X|$ will be glued. The arrows $\varphi : [n] \to [m]$ of the category Δ_s are in bijection with the n-dimensional faces of the m-dimensional regular simplex Δ^m. For every such face φ, the functor X assigns the map $\varphi^* = X(\varphi) : X_m \to X_n$, which provides X with the following gluing rule: for every m-simplex Δ_x^m, $x \in X_m$, the n-simplex Δ_y^m with $y = \varphi^*(x) \in X_n$ is glued to Δ_x^m as the φth n-dimensional face.

For example, shown in Fig. 9.1 is the triangulation of 2-dimensional torus by one 0-simplex, three 1-simplices, and two 2-simplices, where the arrows show inequalities between the vertices as in Example 9.2 on p. 188. The vertical edges e_2 in Fig. 9.2 are glued together into the meridian circle of the torus in Fig. 9.1; the horizontal edges e_1 are glued into the exterior equator of the torus. The corresponding semisimplicial set has $X_0 = \{v\}$, $X_1 = \{e_1, e_2, e_3\}$, $X_2 = \{f_1, f_2\}$, and $X_i = \varnothing$ for all $i \geqslant 3$. The maps $X(\varphi)$ act as follows:

$$X\left(\partial_1^0\right) = X\left(\partial_1^1\right) : X_1 \to X_0\,, \quad e_i \mapsto v \ \text{ for all } i = 1, 2, 3\,,$$

$$X\left(\partial_2^0\right) : X_2 \to X_1\,, \quad f_1 \mapsto e_1\,,\ f_2 \mapsto e_2\,,$$

$$X\left(\partial_2^1\right) : X_2 \to X_1\,, \quad f_1 \mapsto e_3\,,\ f_2 \mapsto e_3\,,$$

$$X\left(\partial_2^2\right) : X_2 \to X_1\,, \quad f_1 \mapsto e_2\,,\ f_2 \mapsto e_1\,.$$

[11] That is, injective and order-preserving.

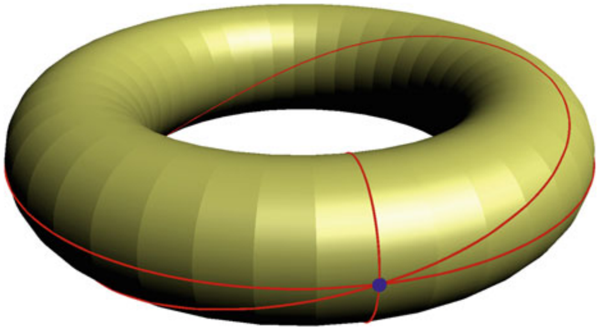


Fig. 9.1 Triangulated torus

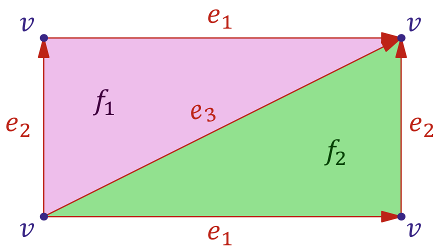


Fig. 9.2 The simplices of the triangulation

Exercise 9.4 Is there a triangulation of the circle S^1 by **(a)** three 0-simplices and three 1-simplices?[12] **(b)** one 0-simplex and one 1-simplex? Is there a triangulation of 2-sphere S^2 by **(c)** four 0-simplices, six 1-simplices, and four 2-simplices? **(d)** two 0-simplices, one 1-simplex, and one 2-simplex? If such a triangulation exists, explicitly describe all its maps $X(\varphi)$; if not, explain why.

Example 9.7 (Simplicial Sets) A presheaf of sets $X : \Delta^{\text{opp}} \to \mathcal{S}et$ on the whole simplicial category is called a *simplicial set*. Every simplicial set X also possesses the *geometric realization* $|X|$ glued from regular simplices $\Delta^n_x, x \in X_n$, in accordance with the maps $\varphi^* = X(\varphi) : X_m \to X_n$ attached by the functor X to all the order-preserving maps $\varphi \in \mathrm{Hom}_\Delta([n],[m])$. Namely, for every $x \in X_m$ and every

$$\varphi : [n] \to [m],$$

every point $s \in \Delta^n_{\varphi^*(x)}$ is glued to the point $\varphi_*(s) \in \Delta^m_x$, where $\varphi_* : \Delta^n \to \Delta^m$ is the affine map of simplices acting on the vertices by means of φ. Formally, the result of this gluing procedure is described in topology as the quotient space of the

[12]In other words, can S^1 be homeomorphic to the geometric realization of a semisimplicial set X such that both sets X_0, X_1 consist of three elements and all the other X_i equal to $\varnothing$?

topological direct product[13] $\prod_{n\geqslant 0} X_n \times \Delta^n$ by the equivalence relation generated by all the identifications

$$(x, \varphi_* s) \sim \left(\varphi^* x, s\right) , \quad \varphi : [n] \to [m] , \quad x \in X_m , \quad s \in \Delta^n .$$

Note that an arrow $\varphi = \delta\sigma : [n] \to [m]$ composed from a surjection $\sigma : [n] \twoheadrightarrow [k]$ and an injection $\delta : [k] \hookrightarrow [m]$ forces every n-simplex Δ^n_z with

$$z = \sigma^* y = \sigma^* \delta^* x \in \operatorname{im} \varphi^*$$

to appear in $|X|$ as a k-simplex Δ^k_y, the image of the linear projection $\sigma_* : \Delta^n \twoheadrightarrow \Delta^k$, and this k-simplex is situated in $|X|$ as the δth face of the m-simplex Δ^m_x. For this reason, a simplex Δ^n_z, $z \in X_n$, is called *degenerate* if $z \in \operatorname{im} \sigma^*$ for some $\sigma : [k] \to [n]$ with $k > n$. All degenerate simplices are visible within $|X|$ as simplices of strictly smaller dimension.

The use of degenerate simplices allows us to give a precise combinatorial description for cellular decompositions more general than triangulations. For example, the n-sphere S^n can be viewed as the quotient space of the regular n-simplex by its boundary[14] $S^n = \Delta^n/\partial\Delta^n$. This leads to the cellular decomposition of S^n into one 0-cell $p \in S^n$ and one n-cell, the images of $\partial\Delta^n$ and Δ^n under the quotient map, such that the interior of the n-cell covers $S^n \smallsetminus p$. This decomposition is the geometric realization $|X|$ of the simplicial set $X : \Delta^{\mathrm{opp}} \to \mathcal{S}et$ described as follows. Every set $X_k = X(k)$ is the quotient of the set $\operatorname{Hom}_\Delta([k], [n])$ obtained by collapsing all nonsurjective maps into one element. The gluing rule $\varphi^* : X_m \to X_k$ corresponding to an order-preserving map $\varphi : [k] \to [m]$ sends the class of an arrow $\zeta : [k] \to [n]$ to the class of the composition $\varphi\zeta : [k] \to [n]$.

Exercise 9.5 Verify that this is a well-defined presheaf and find the cardinalities of sets X_k for all $k \in \mathbb{Z}_{\geqslant 0}$.

Example 9.8 (Presheaves and Sheaves of Sections) Historically, the term "presheaf" first appeared in the context of the category $\mathcal{C} = \mathcal{U}(X)$ of all open sets $U \subset X$ of a given topological space X. Such a presheaf $F : \mathcal{U}(X)^{\mathrm{opp}} \to \mathcal{D}$ attaches an object $F(U) \in \operatorname{Ob} \mathcal{D}$, called *sections*, to every open $U \subset X$. Depending on the target category $\mathcal{D}$, the sections can form a set, vector space, algebra, topological space, etc. Associated with every inclusion of open sets $U \subset W$ is the morphism $F(W) \to F(U)$ called the *restriction of sections* from W to U. The restriction of a section $s \in F(W)$ to $U \subset W$ is commonly denoted by $s|_U$. Below are some typical examples of such presheaves:

---

[13]Where all the sets X_n are considered with the *discrete topology* and all the simplices $\Delta^n \subset \mathbb{R}^{n+1}$ with the standard topology induced from the ambient spaces $\mathbb{R}^{n+1}$.

[14]That is, the space obtained from Δ^n by collapsing its boundary to one point. For example, the 2-sphere S^2 is obtained in this way from the triangle.

(1) The presheaf Γ_E of *local sections* of a continuous map $p : E \to X$. Its sections $\Gamma_E(U)$ are continuous maps $s : U \to E$ such that[15] $p \circ s = \mathrm{Id}_U$. The restrictions are the usual restrictions of maps onto smaller subsets.
(2) The presheaf of local sections of the projection $p : X \times Y \to X$ is denoted by $C^0(X, Y)$ and called the presheaf of *local continuous maps* from X to Y. Its sections over open sets $U \subset X$ are continuous maps $s : U \to Y$.
(3) Further specialization of (2) leads to so-called *structure presheaves* $\mathcal{O}_X$. These are the local differentiable functions $X \to \mathbb{R}$ on a real smooth manifold X, local analytic functions $X \to \mathbb{C}$ on a complex analytic manifold X, local rational functions $X \to \Bbbk$ on an algebraic manifold[16] X over a field $\Bbbk$, etc. All of them are presheaves of algebras over the corresponding ground fields $\mathbb{R}$, $\mathbb{C}$, and $\Bbbk$.
(4) The *constant presheaf* S, where $S \in \mathrm{Ob}\,\mathcal{D}$ is a fixed object, has $S(U) = S$ for all U and all the restriction morphisms equal to Id_S. For example, the constant presheaf of sets S has the same set of sections S over all open sets $U \subset X$.

Presheaves $F : \mathcal{U}(X)^{\mathrm{opp}} \to \mathcal{S}et$ are usually called just *presheaves on* X. Such a presheaf F is called a *sheaf* if for every set of open subsets U_i and local sections $s_i \in F(U_i)$ such that $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ for all i, j, there exists a unique section $s \in F\left(\bigcup_i U_i\right)$ such that $s|_{U_i} = s_i$ for all i. A presheaf F is called *separated* if only the uniqueness of such a section s holds but the section may not exist as well. All the presheaves (1)–(4) above are separated, and only the last of them, the constant presheaf, is usually not a sheaf, because for disjoint nonempty open sets U_1, U_2 and two different constants $s_1, s_2 \in S$ considered as the sections $s_i \in S(U_i)$, there is no constant $s \in S(U_1 \sqcup U_2)$ simultaneously restricted to s_1 and s_2. However, there exists also

(5) the *constant sheaf* $S^{\sim}$, whose sets of sections $S^{\sim}(U)$ consist of the *continuous*[17] functions $U \to S$, where the set S is considered with the *discrete*[18] topology.

Exercise 9.6 Describe all antiderivatives of the real function $y = 1/x$.

9.2.3 The Functors Hom

Associated with an object $X \in \mathrm{Ob}\,\mathcal{C}$ of an arbitrary category $\mathcal{C}$ are the functor $h^X : \mathcal{C} \to \mathcal{S}et$ and presheaf $h_X : \mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$ sending an object $Y \in \mathrm{Ob}\,\mathcal{C}$ to the sets

$$h^X(Y) \overset{\text{def}}{=} \mathrm{Hom}(X, Y) \quad \text{and} \quad h_X(Y) \overset{\text{def}}{=} \mathrm{Hom}(Y, X)\,,$$

[15] This means that every point $x \in U$ is mapped to the fiber $p^{-1}(x)$ over x.

[16] Algebraic manifolds will be defined and studied in Chap. 12.

[17] Equivalently, the *locally* constant functions.

[18] In which every subset $U \subset X$ is declared to be open.

and an arrow $\varphi : Y_1 \to Y_2$ to the maps $h^X(\varphi) \overset{\text{def}}{=} \varphi_*$ and $h_X(\varphi) \overset{\text{def}}{=} \varphi^*$ provided, respectively, by left and right multiplication by φ in $\operatorname{Mor} \mathcal{C}$,

$$\varphi_* : \operatorname{Hom}(X, Y_1) \to \operatorname{Hom}(X, Y_2)\,, \quad \psi \mapsto \varphi \circ \psi\,,$$
$$\varphi^* : \operatorname{Hom}(Y_2, X) \to \operatorname{Hom}(Y_1, X)\,, \quad \psi \mapsto \psi \circ \varphi\,.$$

For example, the presheaf of sets $h_U : \mathcal{U}(X) \to \mathcal{S}et$ on a topological space X has exactly one section over every open $W \subset U$ and the empty sets of sections over all $W \not\subset U$.

Example 9.9 (Standard Triangulation of a Simplex) The presheaf $h_{[n]} : \Delta_s \to \mathcal{S}et$ on the semisimplicial category Δ_s describes the standard triangulation of the n-simplex Δ^n. Indeed, every set $h_{[n]}([k]) = \operatorname{Hom}([k],[n])$ coincides with the set of k-dimensional faces of Δ^n. The gluing rule $\varphi^* : \operatorname{Hom}([k],[n]) \to \operatorname{Hom}([m],[n])$ provided by an arrow $\varphi : [k] \hookrightarrow [m]$ identifies a k-dimensional face $\Delta^k_\xi \subset \Delta^n$ corresponding to the map $\xi : [k] \hookrightarrow [m]$ from $h_{[n]}([k])$, with the φth face of the m-dimensional face $\Delta^m_{\xi\varphi} \subset \Delta^n$, corresponding to the map $\xi \circ \varphi : [k] \hookrightarrow [n]$ from $h_{[n]}([m])$.

Example 9.10 (Duality of Vector Spaces) The presheaf $h_{\Bbbk} : \mathcal{V}ec_{\Bbbk}^{\text{opp}} \to \mathcal{V}ec_{\Bbbk}$ maps a vector space V to the dual space

$$h_{\Bbbk}(V) = \operatorname{Hom}(V, \Bbbk) = V^*\,,$$

and a linear map $\varphi : V \to W$ to the dual map $\varphi^* : W^* \to V^*$ sending a linear form $\xi : W \to \Bbbk$ to the linear form $\xi \circ \varphi : V \to \Bbbk$.

Example 9.11 (Duality of Ordered Sets) This is the combinatorial version of the previous example. Write ∇_{big} for the category of finite ordered sets consisting of at least two elements with $\operatorname{Hom}_{\nabla_{\text{big}}}(X, Y)$ formed by all order-preserving maps $X \to Y$ sending the minimal and maximal elements[19] of X to the minimal and maximal elements of Y respectively. The tautological inclusion of categories $\nabla_{\text{big}} \hookrightarrow \Delta_{\text{big}}$ is faithful but not full. The presheaves $h_{[1]}$ on the categories Δ_{big}, ∇_{big} send an ordered set X to the set X^* consisting of maps $X \to \{0, 1\}$ ordered by the relation $\varphi \leqslant \psi$, meaning that $\varphi(x) \leqslant \psi(x)$ for all x.

Exercise 9.7 Convince yourself that this ordering is total and that

$$\operatorname{Hom}_{\Delta_{\text{big}}}(X, [1]) \in \operatorname{Ob} \nabla_{\text{big}}\,,$$

whereas $\operatorname{Hom}_{\nabla_{\text{big}}}(X, [1]) \in \operatorname{Ob} \Delta_{\text{big}}$ for all X. In other words, the presheaves $h_{[1]}$ on the categories Δ_{big} and ∇_{big} can be viewed as functors $\Delta_{\text{big}}^{\text{opp}} \to \nabla_{\text{big}}$ and $\nabla_{\text{big}}^{\text{opp}} \to \Delta_{\text{big}}$ respectively.

[19]Note that they are distinct, because $|X| \geqslant 2$.

Equivalently, one could say that the presheaves $h_{[1]}$ map a finite ordered set X to the set X^* of the *Dedekind cuts* of X, i.e., decompositions $X = X_0 \sqcup X_1$ such that $x_0 < x_1$ for all $x_0 \in X_0$, $x_1 \in X_1$, where for $X \in \operatorname{Ob} \Delta_{\text{big}}$, the empty parts X_0, X_1 are allowed, whereas for $Y \in \operatorname{Ob} \nabla_{\text{big}}$, both parts X_0, X_1 must be nonempty. The Dedekind cuts behave contravariantly with respect to the morphisms. Given an order-preserving map $Z_1 \to Z_2$, a Dedekind cut of Z_2 induces a Dedekind cut of Z_1 but not conversely.

9.3 Natural Transformations

Given two functors $F, G : \mathcal{C} \to \mathcal{D}$, a *natural*[20] *transformation* $f : F \to G$ is a class of arrows $f_X : F(X) \to G(X)$ in the category $\mathcal{D}$, one arrow for each object $X \in \operatorname{Ob} \mathcal{C}$, such that for every morphism $\varphi : X \to Y$ in $\mathcal{C}$, the diagram in $\mathcal{D}$

$$\begin{tikzcd} F(X) \arrow[r, "F(\varphi)"] \arrow[d, "f_X"'] & F(Y) \arrow[d, "f_Y"] \\ G(X) \arrow[r, "G(\varphi)"'] & G(Y) \end{tikzcd} \tag{9.8}$$

is commutative. In the language of associative algebras, a homomorphism

$$F : K[\mathcal{C}] \to K[\mathcal{D}]$$

provides $K[\mathcal{D}]$ with the structure of a left $K[\mathcal{C}]$-module, where $a \cdot b \stackrel{\text{def}}{=} F(a) \cdot b$ for $a \in K[\mathcal{C}]$, $b \in K[\mathcal{D}]$. Two functors $F, G : \mathcal{C} \to \mathcal{D}$ equip $K[\mathcal{D}]$ with two $K[\mathcal{C}]$-module structures. A natural transformation $f : F \to G$ is nothing but a $K[\mathcal{C}]$-linear map between these two modules, because for every $\varphi \in K[\mathcal{C}]$, the actions of operators $F(\varphi)$, $G(\varphi)$ on $K[\mathcal{D}]$ are related as $f \circ F(\varphi) = G(\varphi) \circ f$.

A natural transformation $f : F \to G$ is called an *isomorphism of functors* or a *canonical isomorphism*[21] if the maps $f_X : F(X) \xrightarrow{\sim} G(X)$ are isomorphisms in $\mathcal{D}$ for all $X \in \operatorname{Ob} \mathcal{C}$. We write $F \simeq G$ if there is an isomorphism between the functors F, G.

For a small category $\mathcal{C}$, the functors from $\mathcal{C}$ to an arbitrary category $\mathcal{D}$ form the category $\mathcal{F}un(\mathcal{C}, \mathcal{D})$, whose objects are the functors $\mathcal{C} \to \mathcal{D}$, and the sets

$$\operatorname{Hom}_{\mathcal{F}un(\mathcal{C},\mathcal{D})}(F, G)$$

[20] Or *functorial*.

[21] Whenever the words "canonical isomorphism" have been used previously in this course, it was precisely in this explicit sense.

consist of the natural transformations $f : F \to G$. We write

$$\mathcal{PreSh}(\mathcal{C}, \mathcal{D}) \overset{\text{def}}{=} \mathcal{Fun}(\mathcal{C}^{\text{opp}}, \mathcal{D})$$

for the category of presheaves on $\mathcal{C}$ with values in $\mathcal{D}$. By default, if the letter $\mathcal{D}$ is omitted in this notation, it means that $\mathcal{D} = \mathcal{S}et$, i.e.,

$$\mathcal{PreSh}(\mathcal{C}) \overset{\text{def}}{=} \mathcal{Fun}\left(\mathcal{C}^{\text{opp}}, \mathcal{S}et\right) .$$

Exercise 9.8 Convince yourself that for every small category $\mathcal{C}$, the assignments[22]

$$X \mapsto h_X \quad \text{and} \quad X \mapsto h^X$$

can be canonically extended to the functors

$$\mathcal{C} \to \mathcal{PreSh}(\mathcal{C}) \quad \text{and} \quad \mathcal{C}^{\text{opp}} \to \mathcal{Fun}(\mathcal{C}, \mathcal{S}et) .$$

9.3.1 Equivalence of Categories

Two categories $\mathcal{C}$, $\mathcal{D}$ are called *equivalent* if there exist functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$, said to be *quasi-inverse to each other*, such that $GF \simeq \mathrm{Id}_{\mathcal{C}}$ and $FG \simeq \mathrm{Id}_{\mathcal{D}}$. This means the existence of transformations

$$GF(X) \xrightarrow{\sim} X \quad \text{and} \quad FG(Y) \xrightarrow{\sim} Y , \tag{9.9}$$

functorial in $X \in \operatorname{Ob}\mathcal{C}$ and $Y \in \operatorname{Ob}\mathcal{D}$, which are isomorphisms of objects in the categories $\mathcal{C}$ and $\mathcal{D}$ for all X, Y. Note that the existence of canonical isomorphisms (9.9) means neither the equality $FG = \mathrm{Id}_{\mathcal{D}}$ nor $GF = \mathrm{Id}_{\mathcal{C}}$. The objects $GF(X)$ and X, as well as the objects $FG(Y)$ and Y, may differ for all X, Y.

Example 9.12 (A Choice of Basis) Write $vec = vec_{\Bbbk}$ for the category of all finite-dimensional vector spaces over a field $\Bbbk$ and $\Bbbk$-linear maps between them. Write $\mathcal{C} \subset vec$ for the small full subcategory formed by coordinate vector spaces $\Bbbk^n$ for all $n \in \mathbb{Z}_{\geqslant 0}$, including $\Bbbk^0 \overset{\text{def}}{=} \{0\}$. Fixing a basis in a vector space $V \in \operatorname{Ob}(vec)$ means fixing an isomorphism[23]

$$f_V : V \xrightarrow{\sim} \Bbbk^{\dim(V)} . \tag{9.10}$$

Let us choose such an isomorphism for every finite-dimensional vector space V, and for each coordinate space $\Bbbk^n$, put $f_{\Bbbk^n} = \mathrm{Id}_{\Bbbk^n}$. Write $F : vec \to \mathcal{C}$ for the functor that

[22] See Sect. 9.2.3 on p. 195.

[23] Sending a vector to the sequence of its coordinates in the chosen basis.

sends a vector space V to the coordinate space $\Bbbk^{\dim V}$ and a linear map $\varphi : V \to W$ to the composition

$$F(\varphi) = f_W \circ \varphi \circ f_V^{-1} : \Bbbk^{\dim V} \to \Bbbk^{\dim W},$$

which can be treated as the matrix of φ in the chosen bases of V and W. Then F is an equivalence of categories quasi-inverse to the tautological inclusion $G : \mathcal{C} \hookrightarrow \mathcal{vec}$. Indeed, by the construction, $FG = \mathrm{Id}_{\mathcal{C}}$ (this the explicit coincidence of functors, not just a canonical isomorphism). The reverse composition $GF : \mathcal{vec} \to \mathcal{vec}$ takes values in the small subcategory $\mathcal{C} \subset \mathcal{vec}$, whose cardinality is incompatible with the cardinality of the class $\mathcal{vec}$. However, isomorphisms (9.10) determine the natural transformation $f : \mathrm{Id}_{\mathcal{vec}} \simeq GF$, because all the diagrams (9.8)

$$\begin{tikzcd}
\mathrm{Id}_{\mathcal{vec}}(V) = V \arrow[r, "\varphi = \mathrm{Id}_{\mathcal{vec}}(\varphi)"] \arrow[d, "f_V"'] & W = \mathrm{Id}_{\mathcal{vec}}(W) \arrow[d, "f_W"] \\
GF(V) = \Bbbk^{\dim V} \arrow[r, "GF(\varphi) = f_W \circ \varphi \circ f_V^{-1}"] & \Bbbk^{\dim W} = GF(W)
\end{tikzcd}$$

are commutative by the definition of the action of F on the morphisms. Thus, the identity endofunctor $\mathrm{Id}_{\mathcal{vec}}$ is canonically isomorphic to GF.

Exercise 9.9 Prove that the category Δ_{big} from Example 9.4 on p. 190 is canonically[24] equivalent to the simplicial subcategory $\Delta \subset \Delta_{\text{big}}$.

Proposition 9.1 *A functor $G : \mathcal{C} \to \mathcal{D}$ is an equivalence of categories if and only if G is fully faithful*[25] *and essentially surjective, meaning that for every $Y \in \mathrm{Ob}\,\mathcal{D}$, there exist $X \in \mathrm{Ob}\,\mathcal{C}$, depending on Y, and an isomorphism $Y \simeq G(X)$.*

Proof We will prove the "if" part and leave the converse statement as an exercise for the reader. For every $Y \in \mathrm{Ob}\,\mathcal{D}$, we fix an object $X = X(Y) \in \mathrm{Ob}\,\mathcal{C}$ and isomorphism $f_Y : Y \simeq G(X)$. Moreover, if $Y = G(X)$ for some $X \in \mathrm{Ob}(\mathcal{C})$, then we put $X(Y) = X$ for one of those X and $f_Y = \mathrm{Id}_Y$. Write $F : \mathcal{D} \to \mathcal{C}$ for the functor that sends an object $Y \in \mathrm{Ob}\,\mathcal{D}$ to the object $X(Y)$ and an arrow $\varphi : Y_1 \to Y_2$ to the unique arrow $\psi : X_1 = X(Y_1) \to X(Y_2) = X_2$ such that $G(\psi) = f_{Y_2} \circ \varphi \circ f_{Y_1}^{-1}$ fits in the commutative diagram

$$\begin{tikzcd}
Y_1 \arrow[r, "\varphi"] \arrow[d, "f_{Y_1}"'] & Y_2 \arrow[d, "f_{Y_2}"] \\
G(X_1) \arrow[r, "G(\psi)"] & G(X_2)
\end{tikzcd}$$

[24] Meaning that there is a unique pair of quasi-inverse equivalences between them.

[25] That is, all maps $G : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(G(X), G(Y))$ are bijective.

The arrow $\psi = F(\varphi)$ is well defined, because

$$G : \mathrm{Hom}(X_1, X_2) \xrightarrow{\sim} \mathrm{Hom}\big(G(X_1), G(X_2)\big)$$

is bijective for all X_1, X_2. By construction, the exact equality $FG = \mathrm{Id}_C$ holds, and for every morphism $\varphi : Y_1 \to Y_2$, the diagram

$$\begin{tikzcd}
\mathrm{Id}_D(Y_1) = Y_1 \arrow[r, "\varphi"] \arrow[d, "f_{Y_1}"'] & Y_2 = \mathrm{Id}_D(Y_2) \arrow[d, "f_{Y_2}"] \\
GF(Y_1) = X_1 \arrow[r, "GF(\varphi)=G(\psi)"] & X_2 = GF(Y_2)
\end{tikzcd}$$

is commutative, which means that the maps $f_Y : Y \xrightarrow{\sim} G(X) = GF(Y)$ give the canonical isomorphism of functors $\mathrm{Id}_D \xrightarrow{\sim} GF$. $\square$

Exercise 9.10 Prove the "only if" part.

Exercise 9.11 Show that the dualization functors $h_{\Bbbk} : vec^{\mathrm{opp}} \to vec$ and $h_{[1]} : \Delta_{\mathrm{big}}^{\mathrm{opp}} \to \nabla_{\mathrm{big}}$ from Example 9.10 and Example 9.11 are equivalences of categories.

9.4 Representable Functors

A presheaf $F : C^{\mathrm{opp}} \to \mathcal{S}et$ is called *representable* if it is naturally isomorphic to the presheaf h_X for some $X \in \mathrm{Ob}\, C$, called the *representing object* of the presheaf F. Dually, a functor $F : C \to \mathcal{S}et$ is called *corepresentable* if it is naturally isomorphic to the functor h^X for some $X \in \mathrm{Ob}\, C$, called the *corepresenting object* of the functor F. In Corollary 9.2 below, we will see that the (co)representing objects naturally depend on the functors they represent. This forces the (co)representing objects to be uniquely determined by the functors up to the canonical isomorphism.

Exercise 9.12 Convince yourself that for given vector spaces U, W, their tensor product $U \otimes W$ corepresents the functor $vec \to \mathcal{S}et$ mapping a vector space V to the set of all bilinear maps $U \times W \to V$.

For a semisimplicial set $X : \Delta_{\mathrm{s}}^{\mathrm{opp}} \to \mathcal{S}et$, the set $X_n = X([n])$ of all n-simplices of the triangulated topological space[26] $|X|$ can be described as the set of all *simplicial maps* $\Delta^n \to X$, where the standard n-simplex Δ^n is considered a triangulated space with[27] $\Delta^n([k]) = \mathrm{Hom}_{\Delta_{\mathrm{s}}}([k], [n])$, and the term "simplicial map" means a natural

[26]See Example 9.6 on p. 192.

[27]See Example 9.9 on p. 196.

transformation of presheaves.[28] In other words, $X([n]) = \mathrm{Hom}_{\mathcal{P}re\mathcal{S}h(\Delta_s)}\big(h_{[n]}, X\big)$ for every presheaf of sets X on the semisimplicial category Δ_s. The same equality holds for all presheaves of sets on an arbitrary category.

Lemma 9.1 (Yoneda Lemma for Presheaves) *Let $F : \mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$ be a presheaf of sets on a category $\mathcal{C}$. There is a bijection*

$$F(A) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{P}re\mathcal{S}h(\mathcal{C})}(h_A, F) \tag{9.11}$$

functorial in F and A. It maps an element $a \in F(A)$ to the natural transformation

$$f_X : \mathrm{Hom}(X, A) \to F(X) \tag{9.12}$$

sending an arrow $\varphi : X \to A$ to the value of the map $F(\varphi) : F(A) \to F(X)$ at a. The inverse to the map (9.11) sends a natural transformation (9.12) to the value of the map $f_A : h_A(A) \to F(A)$ at the identity endomorphism $\mathrm{Id}_A \in h_A(A)$.

Proof For every natural transformation (9.12), object $X \in \mathrm{Ob}\,\mathcal{C}$, and arrow

$$\varphi : X \to A,$$

one has the commutative diagram (9.8),

$$\begin{array}{ccc} h_A(A) = \mathrm{Hom}(A, A) & \xrightarrow{h_A(\varphi)} & \mathrm{Hom}(X, A) = h_A(X) \\ \downarrow{\scriptstyle f_A} & & \downarrow{\scriptstyle f_X} \\ F(A) & \xrightarrow{F(\varphi)} & F(X) \end{array} \tag{9.13}$$

whose upper map takes Id_A to φ. Therefore, $f_X(\varphi) = F(\varphi)\big(f_A(\mathrm{Id}_A)\big)$. This equality uniquely recovers the action of all maps (9.12) on all elements $\varphi \in h_A(X)$ from just one element $a = f_A(\mathrm{Id}_A) \in F(A)$. Given such an element $a \in F(A)$, the corresponding transformation (9.12) maps $\varphi \in \mathrm{Hom}(X, A)$ to $f_X(\varphi) = F(\varphi)(a) \in F(X)$. It is natural, because for every arrow $\psi : Y \to X$ and all $\varphi \in h_A(X)$, the equalities $f_Y(h_A(\psi)\varphi) = f_Y(\varphi\psi) = F(\varphi\psi)a = F(\psi)F(\varphi)a = F(\psi)(f_X(\varphi))$ hold, and therefore $f_Y \circ h_A(\psi) = F(\psi) \circ f_X$ as maps $h_A(X) \to F(Y)$. □

[28] Intuitively, a simplicial map of triangulated spaces $|X| \to |Y|$ is a continuous map respecting the triangulations. The latter property is formalized as a natural transformation of presheaves $X \to Y$. In particular, this forces a simplicial map to send every k-simplex of the triangulation on $|X|$ to a k-simplex of the triangulation on $|Y|$ via an affine map, and to respect the incidences between the simplices.

Exercise 9.13 (Yoneda Lemma for Covariant Functors) For every category $\mathcal{C}$ and functor $F : \mathcal{C} \to \mathcal{S}et$, construct a bijection

$$F(A) \xrightarrow{\sim} \operatorname{Hom}_{\mathcal{F}un(\mathcal{C},\mathcal{S}et)}\left(h^A, F\right)$$

functorial in F, A.

Corollary 9.1 *The prescriptions $X \mapsto h_X$ and $X \mapsto h^X$ assign fully faithful functors $\mathcal{C} \hookrightarrow \mathcal{P}re\mathcal{S}h(\mathcal{C})$ and $\mathcal{C}^{\mathrm{opp}} \hookrightarrow \mathcal{F}un(\mathcal{C}, \mathcal{S}et)$ respectively. In particular, one has the bijections*

$$\operatorname{Hom}_{\mathcal{P}re\mathcal{S}h(\mathcal{C})}(h_A, h_B) \simeq \operatorname{Hom}_{\mathcal{C}}(A, B) \quad \textit{and} \quad \operatorname{Hom}_{\mathcal{F}un(\mathcal{C})}(h^A, h^B) \simeq \operatorname{Hom}_{\mathcal{C}}(B, A)\,,$$

functorial in $A, B \in \operatorname{Ob}\mathcal{C}$.

Proof Apply the Yoneda lemmas to the functors $F = h_B$ and $F = h^B$. □

Corollary 9.2 *If a functor $F' : \mathcal{C} \to \mathcal{S}et$ (respectively a presheaf $F : \mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$) is corepresented (respectively represented), then its corepresenting (respectively representing) object $A \in \operatorname{Ob}\mathcal{C}$ is unique up to canonical isomorphism. More precisely, given two natural isomorphisms $\alpha : F \xrightarrow{\sim} h^A$ and $\beta : F \xrightarrow{\sim} h^B$ (respectively $\alpha : F \xrightarrow{\sim} h_A$ and $\beta : F \xrightarrow{\sim} h_B$), there exists a unique pair of inverse isomorphisms $\varphi : A \xrightarrow{\sim} B$, $\psi : B \xrightarrow{\sim} A$ such that for every $X \in \operatorname{Ob}\mathcal{C}$, the diagram*

$$\begin{tikzcd}
 & h^A(X) \arrow[d, shift left, "\psi^*"] \\
F(X) \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & \\
 & h^B(X) \arrow[u, shift left, "\varphi^*"]
\end{tikzcd}$$

where $\psi^* : \operatorname{Hom}(A, X) \to \operatorname{Hom}(B, X)$, $\varphi^* : \operatorname{Hom}(B, X) \to \operatorname{Hom}(A, X)$ are the right multiplications by ψ, φ, is commutative (respectively the diagram

$$\begin{tikzcd}
 & h_A(X) \arrow[d, shift left, "\varphi_*"] \\
F(X) \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & \\
 & h_B(X) \arrow[u, shift left, "\psi_*"]
\end{tikzcd}$$

where $\varphi_* : \mathrm{Hom}(X, A) \to \mathrm{Hom}(X, B)$*,* $\psi_* : \mathrm{Hom}(X, B) \to \mathrm{Hom}(X, A)$ *are left multiplication by* φ*,* ψ*, is commutative).*

Proof Given natural isomorphisms $\beta\alpha^{-1} : h^A \xrightarrow{\sim} h^B$ and $\beta^{-1}\alpha : h^B \xrightarrow{\sim} h^A$, then by Corollary 9.1, there exist unique isomorphisms $\psi : B \xrightarrow{\sim} A$, $\varphi : A \xrightarrow{\sim} B$ such that $\beta\alpha^{-1} = \psi^*$ and $\beta^{-1}\alpha = \varphi^*$. Since $\beta\alpha^{-1}$ and $\beta^{-1}\alpha$ are inverse to each other, ψ and φ are too. The case of presheaves is completely symmetric. □

9.4.1 Definitions via Universal Properties

Corollary 9.2 allows us to transfer many set-theoretic constructions from the category $\mathcal{S}et$ to an arbitrary category $\mathcal{C}$. Namely, let us say that an object $X \in \mathrm{Ob}\,\mathcal{C}$ is the result of some set-theoretic operation applied to a collection of objects $X_i \in \mathrm{Ob}\,\mathcal{C}$ if X represents the presheaf $\mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$ mapping $Y \in \mathrm{Ob}\,\mathcal{C}$ to the result of this operation applied to the sets $\mathrm{Hom}(Y, X_i)$ in $\mathcal{S}et$. Such an implicit definition gives no guarantee that the object X exists, because the presheaf in question may not be representable. However, if it is representable, then the representing object X possesses some universal properties provided by the construction, and it is unique up to a unique isomorphism respecting those properties. Moreover, every definition of this sort has a dual version, obtained by applying the set-theoretic operation to the sets $\mathrm{Hom}(X_i, Y)$ covariant in Y and taking the corepresenting object of the resulting functor $\mathcal{C} \to \mathcal{S}et$.

Example 9.13 (Direct Product $A \times B$) The *direct product* $A \times B$ of objects $A, B \in \mathrm{Ob}\,\mathcal{C}$ in an arbitrary category $\mathcal{C}$ is defined as the representing object for the presheaf $\mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$, $Y \mapsto \mathrm{Hom}(Y, A) \times \mathrm{Hom}(Y, B)$. If the object $A \times B$ exists, then there is an isomorphism

$$\beta_Y : \mathrm{Hom}(Y, A \times B) \xrightarrow{\sim} \mathrm{Hom}(Y, A) \times \mathrm{Hom}(Y, B)$$

functorial in $Y \in \mathrm{Ob}\,\mathcal{C}$. For $Y = A \times B$, it produces the pair of arrows

$$A \xleftarrow{\pi_A} A \times B \xrightarrow{\pi_B} B$$

representing the element

$$\beta_{A \times B}(\mathrm{Id}_{A \times B}) \in \mathrm{Hom}(A \times B, A) \times \mathrm{Hom}(A \times B, B)\,.$$

These arrows are universal in the following sense. For every pair of arrows

$$A \xleftarrow{\varphi} Y \xrightarrow{\psi} B\,,$$

there exists a unique morphism $\varphi \times \psi : Y \to A \times B$ such that $\varphi = \pi_A \circ (\varphi \times \psi)$ and $\psi = \pi_B \circ (\varphi \times \psi)$.

Exercise 9.14 Convince yourself that for every diagram $A \xleftarrow{\pi'_A} C \xrightarrow{\pi'_B} B$ possessing this universal property, there exists a unique isomorphism $\gamma : C \xrightarrow{\sim} A \times B$ such that $\pi_A \circ \gamma = \pi'_A$ and $\pi_B \circ \gamma = \pi'_B$.

In the category $\mathcal{T}op$, the direct product of topological spaces $X \times Y$ coincides with their direct product in $\mathcal{S}et$. The topology on $X \times Y$ is the *product topology*, whose base of open sets is formed by the products of open sets in X, Y. In the categories of groups, rings, and modules over a fixed ring, the direct products also coincide with those in $\mathcal{S}et$. The algebraic operations are defined componentwise.

Example 9.14 (Direct Coproduct $A \otimes B$) The dual version of the direct product is the *direct coproduct* $A \otimes B$ of objects $A, B \in \operatorname{Ob} \mathcal{C}$ in a category $\mathcal{C}$. It is defined as the corepresenting object for the covariant functor

$$\mathcal{C} \to \mathcal{S}et, Y \mapsto \operatorname{Hom}(A, Y) \times \operatorname{Hom}(B, Y).$$

Reversing arrows in Example 9.13 shows that the coproduct fits in the diagram $A \xrightarrow{i_A} A \otimes B \xleftarrow{i_B} B$, universal in the following sense. For every pair of arrows $A \xrightarrow{\varphi} Y \xleftarrow{\psi} B$, there exists a unique morphism $\varphi \otimes \psi : A \otimes B \to Y$ such that $\varphi = (\varphi \otimes \psi) \circ i_A$ and $\psi = (\varphi \otimes \psi) \circ i_B$.

Exercise 9.15 Verify that if the universal diagram $A \xrightarrow{i_A} A \otimes B \xleftarrow{i_B} B$ exists, then it is unique up to a unique isomorphism of the middle objects commuting with $i_{A,B}$.

Exercise 9.16 Verify that in the categories $\mathcal{S}et$ and $\mathcal{T}op$, the coproduct is the disjoint union.

In the category $\mathcal{M}od_K$ of modules over a commutative ring[29] K, the coproduct coincides with the product and equals the direct sum of modules.

Exercise 9.17 Verify that the diagram

$$A \xrightarrow{i_A} A \oplus B \xleftarrow{i_B} B, \quad i_A : a \mapsto (a, 0), i_B : b \mapsto (0, b)\,,$$

is the universal coproduct diagram in the category $\mathcal{M}od_K$.

In the category $\mathcal{C}mr$ of commutative rings with unit and homomorphisms respecting units, the coproduct $A \otimes B$ coincides with the tensor product of additive abelian groups. The multiplication is defined on decomposable tensors by the prescription

$$(a_1 \otimes b_1)(a_2 \otimes b_2) \overset{\text{def}}{=} (a_1 a_2) \otimes (b_1 b_2)\,.$$

[29] In particular, in the category $\mathcal{A}b = \mathcal{M}od_{\mathbb{Z}}$.

Exercise 9.18 Verify that it is correctly extended by the distributivity law to all of $A \otimes B$, and provides $A \otimes B$ with the structure of a commutative ring with the unit $1 \otimes 1$. Check that the diagram

$$A \xrightarrow{i_A} A \otimes B \xleftarrow{i_B} B, \quad i_A : a \mapsto a \otimes 1,\ i_B : b \mapsto 1 \otimes b,$$

is the universal diagram of the coproduct.

In the category $\mathcal{G}rp$, the coproduct of groups G, H is called the *free product* and denoted by $G * H$. It can be constructed as the quotient of the free group[30] on the alphabet $G \sqcup H$ by the relations that remove the identity elements e_G, e_H from the words and replace every pair of sequential letters from the same group by their product in that group. For example, $F_k * F_m \simeq F_{k+m}$ for the free groups F_k, F_m, in particular $\mathbb{Z} * \mathbb{Z} \simeq F_2$. More generally, if G, H are presented, respectively, by generators Γ_G, Γ_H and relators R_G, R_H, then $G*H$ is presented by generators $\Gamma_G \sqcup \Gamma_H$ and relators $R_G \sqcup R_H$.

Exercise 9.19 Verify that the universal property of the coproduct holds for the free product of groups.

9.5 Adjoint Functors

Let $\mathcal{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathcal{D}$ be two functors between arbitrary categories $\mathcal{C}$, $\mathcal{D}$. If there exists an isomorphism

$$\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \tag{9.14}$$

functorial in $X \in \mathrm{Ob}\,\mathcal{C}$, $Y \in \mathrm{Ob}\,\mathcal{D}$, then we say that F is *left adjoint* to G, whereas G is *right adjoint* to F, and we write $F \dashv G$. Associated with every pair of adjoint functors $F \dashv G$ are the natural transformations

$$\lambda : F \circ G \to \mathrm{Id}_{\mathcal{D}} \quad \text{and} \quad \varrho : \mathrm{Id}_{\mathcal{C}} \to G \circ F \tag{9.15}$$

such that the morphism $\lambda_Y : FG(Y) \to Y$, which describes the action of λ over $Y \in \mathrm{Ob}\,\mathcal{D}$, corresponds to the identity endomorphism $\mathrm{Id}_{G(Y)}$ under the bijection (9.14), written for $X = G(Y)$,

$$\mathrm{Hom}_{\mathcal{D}}(FG(Y), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(G(Y), G(Y)) \ni \mathrm{Id}_{G(Y)}\,,$$

[30] See Sect. 13.1.1 of Algebra I.

and symmetrically, the morphism $\varrho_X : X \to GF(X)Y$ corresponds to $\mathrm{Id}_{F(X)}$ under the bijection (9.14), written for $Y = F(X)$,

$$\mathrm{Id}_{F(X)} \in \mathrm{Hom}_{\mathcal{D}}(F(X), F(X)) \simeq \mathrm{Hom}_{\mathcal{C}}(X, GF(X)) \,.$$

Example 9.15 (Free Modules) Write $R\text{-}\mathcal{M}od$ for the category of left modules over a fixed ring R (not necessarily commutative), and $G : R\text{-}\mathcal{M}od \to \mathcal{S}et$ for the forgetful functor taking a module to the set of its elements. For every set $E \in \mathrm{Ob}\,\mathcal{S}et$, the functor

$$R\text{-}\mathcal{M}od \to \mathcal{S}et\,, \quad M \mapsto \mathrm{Hom}_{\mathcal{S}et}\big(E, G(M)\big)$$

is corepresentable by the *free* R-module with basis E. Let us write $R \otimes E$ for this free module. By definition, $R \otimes E$ consists of formal linear combinations $\sum_{e\in E} x_e e$ with the coefficients $x_e \in R$, all but a finite number of which vanish.

Exercise 9.20 Establish the isomorphism

$$\mathrm{Hom}_{R\text{-}\mathcal{M}od}(R \otimes E, M) \simeq \mathrm{Hom}_{\mathcal{S}et}\big(E, G(M)\big) \tag{9.16}$$

functorial in $M \in \mathrm{Ob}\,R\text{-}\mathcal{M}od$, $E \in \mathrm{Ob}\,\mathcal{S}et$.

The isomorphism (9.16) means that the functor $\mathcal{S}et \to R\text{-}\mathcal{M}od$, $E \mapsto R \otimes E$, is the left adjoint to the forgetful functor $G : R\text{-}\mathcal{M}od \to \mathcal{S}et$. The natural transformation

$$\varrho_E : E \hookrightarrow G(A \otimes E)$$

embeds E as a subset of the standard basis vectors in the set of all vectors in $R \otimes E$. The natural transformation

$$\lambda_M : R \otimes G(M) \twoheadrightarrow M$$

is the map of the huge free R-module $R \otimes G(M)$, whose basis is formed by the set of all nonzero vectors in M, onto the module M. It sends every basis vector $m \in R \otimes G(M)$ to the element $m \in M$. This map is surjective and sends a formal linear combination $\sum_{m\in M} x_m m$ to the result of its evaluation within M. For example, for $M = R = \mathbb{R}$, the vector space $\mathbb{R} \otimes G(\mathbb{R})$ is isomorphic to the space of all functions $\mathbb{R} \to \mathbb{R}$ with finite support, and the transformation $\lambda_{\mathbb{R}}$ sends such a function to the sum of its (nonzero) values.

9.5.1 Tensor Products Versus Hom Functors

Let R be an arbitrary ring. For every right R-module M and left R-module N, the *tensor product* $M \otimes_R N$ is defined as the quotient of the tensor product of abelian groups[31] $M \otimes N$ by the subgroup generated by all the differences

$$(mr) \otimes n - m \otimes (rn) , \text{ where } m \in M , \ r \in R , \ n \in N .$$

Note that by definition, $M \otimes_R N$ is just an abelian group without any action of R from either the left or right side. Instead of such an action, the relations

$$(mr) \otimes_R n = m \otimes_R (rn)$$

hold in $M \otimes_R N$ for all $m \in M$, $r \in R$, $n \in N$, i.e., the elements of R can be moved through the tensor product sign. Thus, associated with every left R-module N is the functor

$$\mathcal{M}od\text{-}R \to \mathcal{A}b , \quad X \mapsto X \otimes_R N , \tag{9.17}$$

provided by the right tensor multiplication of objects by N and sending a homomorphism of right R-modules $\varphi : X_1 \to X_2$ to the homomorphism of abelian groups $\varphi \otimes_R 1 : m \otimes_R n \mapsto \varphi(m) \otimes_R n$. Symmetrically, every right R-module M assigns the functor

$$R\text{-}\mathcal{M}od \to \mathcal{A}b , \quad X \mapsto M \otimes_R X , \quad \varphi \mapsto 1 \otimes_R \varphi , \tag{9.18}$$

on the category R-$\mathcal{M}od$ of left R-modules. Let S be another ring, and let M possess simultaneously right R-module and left S-module structures such that the right action of R on M commutes with the left action of S. In this case, M is called an *S-R-bimodule*. For such a bimodule M, the functor (9.18) actually takes values in the subcategory S-$\mathcal{M}od \subset \mathcal{A}b$ of left S-modules, because $M \otimes X$ has the left S-module structure functorial in X defined by the prescription $s(m \otimes x) = (sm) \otimes x$. At the same time, the covariant Hom-functor

$$h^M : S\text{-}\mathcal{M}od \to \mathcal{A}b , \quad Y \mapsto \mathrm{Hom}_S(M, Y) , \tag{9.19}$$

actually takes values in the subcategory R-$\mathcal{M}od \subset \mathcal{A}b$: the left action of an element $r \in R$ on $\mathrm{Hom}_S(M, Y)$ functorial in Y is provided by the right R-module structure on M and sends an S-linear map $\varphi : M \to Y$ to the map $r\varphi : m \mapsto \varphi(mr)$. In particular, the identity $(\varphi r)n = \varphi(rn)$ holds for all $r \in R$, $n \in N$.

Exercise 9.21 Verify that this is in fact a *left* action of R on $h^M(Y)$.

Proposition 9.2 *For every two rings R, S and S-R-bimodule M, the functor*

$$R\text{-}\mathcal{M}od \to S\text{-}\mathcal{M}od , \quad X \mapsto M \otimes_R X ,$$

is left adjoint to the functor

$$h^M : S\text{-}\mathcal{M}od \to R\text{-}\mathcal{M}od , \quad Y \mapsto \mathrm{Hom}_S(M, Y) .$$

---

[31] That is, $\mathbb{Z}$-modules.

In other words, there exists an isomorphism, functorial in the R-module X and S-module Y, of abelian groups

$$\mathrm{Hom}_S\left(M \otimes_R X, Y\right) \simeq \mathrm{Hom}_R\left(X, \mathrm{Hom}_S(M, Y)\right). \tag{9.20}$$

Proof The map from the left- to the right-hand side of (9.20) is constructed as follows. An S-linear homomorphism $\varphi : M \otimes_R X \to Y$ produces the family of maps

$$\psi_x : M \to Y, \quad m \mapsto \varphi(m \otimes x)$$

depending on $x \in X$. Every map ψ_x is S-linear:

$$\psi_x(sm) = \psi(sm \otimes_R x) = \psi\left(s(m \otimes_R x)\right) = s\psi(m \otimes_R x) = s\psi_x(m).$$

Let us send φ to the map $\psi : X \to \mathrm{Hom}_S(M, Y)$, $x \mapsto \psi_x$, which is R-linear, because $\varphi_{rx}m = \varphi(m \otimes_R rx) = \varphi(mr \otimes_R x) = \varphi_x(mr) = (r\varphi_x)m$ for all $m \in M$. The inverse map from the right- to the left-hand side of (9.20) sends a homomorphism

$$\psi : X \to \mathrm{Hom}_S(M, Y),$$

which can be thought of as a family of S-linear maps $\psi_x : M \to Y$ depending R-linearly on $x \in X$, to the S-linear homomorphism

$$\varphi : M \otimes_R X \to Y, \quad m \otimes_R x \mapsto \psi_x(m).$$

□

Exercise 9.22 Verify that both maps between the two sides of (9.20) are well defined and inverse to each other.

Example 9.16 (Induced and Coinduced Modules) Let B be an arbitrary ring with unit and $A \subset B$ a subring with the same unit. Every left B-module X can be viewed as a left A-module. This leads to the *restriction functor*[32]

$$\mathrm{res} : B\text{-}\mathcal{M}od \to A\text{-}\mathcal{M}od. \tag{9.21}$$

Consider B an A-B-bimodule and put $S = A$, $M = R = B$ in Proposition 9.2. Then for every left B-module X, the left A-module $B \otimes_B X \simeq X$ is isomorphic to the restriction $\mathrm{res}\, X$ of X to A, and the isomorphism (9.20) functorial in the B-module X and A-module Y takes the form

$$\mathrm{Hom}_A(\mathrm{res}\, X, Y) \simeq \mathrm{Hom}_B\left(X, \mathrm{Hom}_A(B, Y)\right).$$

[32] Compare with Sect. 6.3 on p. 141 and Sect. 6.3.4 on p. 146.

The left B-module $\operatorname{coind} Y \stackrel{\text{def}}{=} \operatorname{Hom}_A(B, Y)$ is called *coinduced* by the left A-module Y. Thus, the *coinduction functor* $\operatorname{coind} : A\text{-}\mathcal{M}od \to B\text{-}\mathcal{M}od$, $Y \mapsto \operatorname{coind} Y$, is right adjoint to the restriction functor (9.21).

Now consider B as a B-A-bimodule and put $S = M = B$, $R = A$ in Proposition 9.2. For every left B-module Y, the left A-module $\operatorname{Hom}_B(B, Y) \simeq Y$ is isomorphic to the restriction $\operatorname{res} Y$ of Y on A. The isomorphism (9.20) functorial in the A-module X and B-module Y takes the form

$$\operatorname{Hom}_B(B \otimes_A X, Y) \simeq \operatorname{Hom}_A(X, \operatorname{res} Y) .$$

The left B-module $\operatorname{ind} X \stackrel{\text{def}}{=} B \otimes_A X$ is called *induced* by the left A-module X. The *induction functor* $\operatorname{ind} : A\text{-}\mathcal{M}od \to B\text{-}\mathcal{M}od$, $X \mapsto \operatorname{ind} X$, is left adjoint to the restriction functor.

For the group algebras $A = \Bbbk[H]$, $B = \Bbbk[G]$ of a finite group G and subgroup $H \subset G$, the induction and coinduction functors become the induction and coinduction of linear representations considered in Sect. 6.3 on p. 141 and Sect. 6.3.4 on p. 146.

Exercise 9.23 (Right Module Version of Proposition 9.2) For every two rings R, S and R-S-bimodule N, introduce a structure of a right S-module functorial in $X \in \mathcal{M}od\text{-}R$ on the abelian group $X \otimes_R N$, and the structure of a right R-module functorial in $Y \in \mathcal{M}od\text{-}S$ on the abelian group $h^N(Y) = \operatorname{Hom}_{\mathcal{M}od\text{-}S}(N, Y)$. Prove that the functor $\mathcal{M}od\text{-}R \to \mathcal{M}od\text{-}S$, $X \mapsto X \otimes_R N$, is left adjoint to the functor $h^N : \mathcal{M}od\text{-}S \to \mathcal{M}od\text{-}R$, $Y \mapsto \operatorname{Hom}_{\mathcal{M}od\text{-}S}(N, Y)$, i.e., that there exists an isomorphism of abelian groups

$$\operatorname{Hom}_{\mathcal{M}od\text{-}S}\big(X \otimes_R N, Y\big) \simeq \operatorname{Hom}_{\mathcal{M}od\text{-}R}\big(X, \operatorname{Hom}_{\mathcal{M}od\text{-}S}(N, Y)\big) \tag{9.22}$$

functorial in $X \in \operatorname{Ob} \mathcal{M}od\text{-}R$, $Y \in \operatorname{Ob} \mathcal{M}od\text{-}S$.

Example 9.17 (Singular Simplices) Associated with every topological space Y is the simplicial set[33] $S(Y) : \Delta^{\text{opp}} \to \mathcal{S}et$, called the *set of singular simplices*. It maps $[n] \in \operatorname{Ob} \Delta$ to the set $S_n(Y) \stackrel{\text{def}}{=} \operatorname{Hom}_{\mathcal{T}op}(\Delta^n, Y) = h_Y(\Delta^n)$ of all continuous maps[34] $f : \Delta^n \to Y$, where $\Delta^n \subset \mathbb{R}^{n+1}$ is the standard regular n-simplex considered with the topology induced from $\mathbb{R}^{n+1}$. An order-preserving map $\varphi : [n] \to [m]$ is sent by $S(Y)$ to the map $\varphi^* : \operatorname{Hom}_{\mathcal{T}op}(\Delta^m, Y) \to \operatorname{Hom}_{\mathcal{T}op}(\Delta^n, Y), f \mapsto f \circ \varphi_*$, provided by right composition with the affine map $\varphi_* : \Delta^n \to \Delta^m$ acting on the vertices of Δ^n in accordance with φ.

Exercise 9.24 Verify that these prescriptions define a functor

$$S : \mathcal{T}op \to \mathcal{P}re\mathcal{S}h(\Delta), Y \mapsto S(Y) .$$

[33] See Example 9.7 on p. 193.

[34] Every such continuous map is called a *singular simplex* of Y.

Let us show that this functor is right adjoint to the geometric realization functor

$$\mathcal{PreSh}(\Delta) \to \mathcal{Top}\,, \quad X \mapsto |X|\,,$$

described in Example 9.7 on p. 193, i.e., that there is a bijection

$$\mathrm{Hom}_{\mathcal{Top}}(|X|, Y) \simeq \mathrm{Hom}_{\mathcal{PreSh}}(X, S(Y)) \tag{9.23}$$

functorial in the simplicial set X and topological space Y. In fact, this isomorphism is a version of the isomorphism (9.22) reformulated in terms of functors on categories instead of modules over rings. Namely, the geometric realization functor embeds the simplicial category Δ into the category $\mathcal{Top}$ as a set of disjoint regular simplices $D = \bigsqcup_{n\geqslant 0}\Delta^n$. The arrows $\varphi \in \mathrm{Mor}\,\Delta$ act on D from both sides via composition with the affine maps φ_*. The right action of $\mathrm{Mor}\,\Delta$ commutes with the left action of $\mathrm{Mor}\,\mathcal{Top}$, which maps D to other topological spaces Y. The category $\mathcal{PreSh}(\Delta^{\mathrm{opp}}, \mathcal{Set})$, of simplicial sets $X : \Delta^{\mathrm{opp}} \to \mathcal{Set}$, is completely analogous to the category of right modules over Δ: the arrows of Δ act from the right on every simplicial set via $x \mapsto x\varphi \overset{\text{def}}{=} X(\varphi)x$. In particular, the geometric realization of every simplicial set X can be thought of as the tensor product $|X| = X \otimes_\Delta D$, that is, the quotient of the disjoint union $\bigsqcup_{n\geqslant 0} X_n \times \Delta^n$ by the relations $(x\varphi, s) = (x, \varphi s)$. Thus, the right Δ-modules $S(Y) = \mathrm{Hom}_{\mathcal{Top}}(D, Y)$ and $|X| = X \otimes_\Delta D$ fit into the isomorphism (9.22) as

$$\mathrm{Hom}_{\mathcal{Top}}\left(X \otimes_\Delta D, Y\right) \simeq \mathrm{Hom}_{\mathcal{Mod}\text{-}\Delta}\left(X, \mathrm{Hom}_{\mathcal{Top}}(D, Y)\right). \tag{9.24}$$

This is exactly the same as (9.23).

Exercise 9.25 Use Exercise 9.23 to give explicit descriptions of the inverse isomorphisms between the left and right sides of (9.24).

Proposition 9.3 *A functor $G : \mathcal{D} \to \mathcal{C}$ admits the left adjoint functor $F : \mathcal{C} \to \mathcal{D}$ if and only if for every $X \in \mathrm{Ob}\,\mathcal{C}$, the functor*

$$h_G^X : \mathcal{D} \to \mathcal{Set}\,, \quad Y \mapsto \mathrm{Hom}_{\mathcal{C}}\left(X, G(Y)\right), \tag{9.25}$$

is corepresentable. In this case, $F(X)$ corepresents the functor (9.25) for all $X \in \mathrm{Ob}\,\mathcal{C}$.

Proof The "only if" part follows directly from the definitions of adjoint functors and corepresenting objects. Let us prove the opposite implication. Assume that for every $X \in \mathrm{Ob}\,\mathcal{C}$, there exist an object $F(X) \in \mathrm{Ob}\,\mathcal{D}$ and a natural isomorphism of functors $f^X : h^{F(X)} \simeq h_G^X$. The action of F on the arrows of $\mathcal{C}$ is defined as follows. Every arrow $\varphi : X_1 \to X_2$ produces the natural transformation $\varphi^* : h_G^{X_2} \to h_G^{X_1}$, the right multiplication by φ, which sends an arrow $\gamma : X_2 \to G(Y)$ to the arrow $\gamma\varphi : X_1 \to G(Y)$. By Corollary 9.1 on p. 202, the composition of natural transformations $\left(f^{X_1}\right)^{-1} \circ \varphi^* \circ f^{X_2} : h^{F(X_2)} \to h^{F(X_1)}$ is realized as the right multiplication by an appropriate arrow $\psi : F(X_1) \to F(X_2)$, uniquely determined by this property. We put $F(\varphi) = \psi$. It remains to show that the isomorphism $f^X : \mathrm{Hom}_{\mathcal{D}}(F(X), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, G(Y))$ functorial in $Y \in \mathrm{Ob}\,\mathcal{D}$ is functorial in $X \in \mathrm{Ob}\,\mathcal{C}$ as well, i.e., for every arrow $\varphi : X_1 \to X_2$ and $Y \in \mathrm{Ob}\,\mathcal{D}$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(F(X_2), Y) \arrow[r, "F(\varphi)^*"] \arrow[d, "f^{X_2}"'] & \mathrm{Hom}_{\mathcal{D}}(F(X_1), Y) \arrow[d, "f^{X_1}"] \\
\mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \arrow[r, "\varphi^*"'] & \mathrm{Hom}_{\mathcal{C}}(X, G(Y))
\end{tikzcd}$$

is commutative. This follows directly from the construction of $F(\varphi)$. □

Exercise 9.26 Prove the dual version of Proposition 9.3: a functor $F : \mathcal{C} \to \mathcal{D}$ admits the right adjoint functor $G : \mathcal{D} \to \mathcal{C}$ if and only if for every $Y \in \mathrm{Ob}\,\mathcal{D}$, the presheaf

$$h_Y^F : \mathcal{C} \to \mathcal{S}et\,, \quad X \mapsto \mathrm{Hom}_{\mathcal{D}}\left(F(X), Y\right),$$

is representable, and in this case, $G(Y)$ represents it for all $Y \in \mathrm{Ob}\,\mathcal{D}$.

Proposition 9.4 *A functor $F : \mathcal{C} \to \mathcal{D}$ is left adjoint to a functor $G : \mathcal{D} \to \mathcal{C}$ if and only if there exist natural transformations $t : F \circ G \to \mathrm{Id}_{\mathcal{D}}$ and $s : \mathrm{Id}_{\mathcal{C}} \to G \circ F$ such that the compositions $F \xrightarrow{F \circ s} FGF \xrightarrow{t \circ F} F$ and $G \xrightarrow{s \circ G} GFG \xrightarrow{G \circ t} G$ are the identity transformations of the functors F, G to themselves.*

Proof If there exist bijections

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}\left(F(X), Y\right) \arrow[rr, bend left, "\varrho"] & & \mathrm{Hom}_{\mathcal{C}}\left(X, G(Y)\right) \arrow[ll, bend left, "\lambda"]
\end{tikzcd} \tag{9.26}$$

functorial in $X \in \mathrm{Ob}\,\mathcal{C}$, $Y \in \mathrm{Ob}\,\mathcal{D}$ and inverse to each other, then for every arrow $\varphi : X_1 \to X_2$ in $\mathcal{C}$ and every $Y \in \mathrm{Ob}\,\mathcal{D}$, we have the commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(F(X_1), Y) & \mathrm{Hom}_{\mathcal{C}}(X_1, G(Y)) \arrow[l, "\lambda"', "\sim"] \\
\mathrm{Hom}_{\mathcal{D}}(F(X_2), Y) \arrow[u, "F(\varphi)^*"'] & \mathrm{Hom}_{\mathcal{C}}(X_2, G(Y)) \arrow[l, "\lambda"', "\sim"] \arrow[u, "\varphi^*"']
\end{tikzcd} \tag{9.27}$$

whose vertical maps are the right multiplications by $F(\varphi)$ and φ respectively. For the arrow

$$\varphi = s_X : X \to GF(X)\,,$$

which realizes the natural transformation[35] $s : \mathrm{Id}_{\mathcal{C}} \to GF$ over X, and the object $Y = F(X)$, the commutative diagram (9.27) takes the form

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(F(X), F(X)) & \mathrm{Hom}_{\mathcal{C}}(X, GF(X)) \arrow[l, "\lambda"', "\sim"] \\
\mathrm{Hom}_{\mathcal{D}}(FGF(X), F(X)) \arrow[u, "F(s_X)^*"'] & \mathrm{Hom}_{\mathcal{C}}(GF(X), GF(X)) \arrow[l, "\lambda"', "\sim"] \arrow[u, "s_X^*"']
\end{tikzcd}$$

where the top arrow λ sends s_X to $\mathrm{Id}_{F(X)}$, and the bottom arrow λ sends $\mathrm{Id}_{GF(X)}$ to the morphism $t_{F(X)} : FGF(X) \to F(X)$ realizing the second natural transformation[36] $t : FG \to \mathrm{Id}_{\mathcal{D}}$ over $F(X)$. Therefore,

$$\begin{aligned}
\mathrm{Id}_{F(X)} &= \lambda(s_X) = \lambda s_X^* \left(\mathrm{Id}_{GF(X)}\right) = F(s_X)^* \lambda \left(\mathrm{Id}_{GF(X)}\right) = F(s_X)^* \left(t_{F(X)}\right) \\
&= t_{F(X)} \circ F(s_X)\,,
\end{aligned}$$

that is, the composition $F \xrightarrow{F \circ s} FGF \xrightarrow{t \circ F} F$ gives the identity transformation from F to itself. A symmetric argument, using ϱ instead of λ, shows that the composition $G \xrightarrow{s \circ G} GFG \xrightarrow{G \circ t} G$ is the identity transformation of G to itself.

Conversely, let $s : \mathrm{Id}_{\mathcal{C}} \to GF$ and $t : FG \to \mathrm{Id}_{\mathcal{D}}$ be natural transformations satisfying the conditions of the proposition. Define the values of the maps λ, ϱ in (9.26) on arrows $\varphi : F(X) \to Y$ and $\psi : X \to G(Y)$ by the formulas

$$\varrho(\varphi) = G(\varphi) \circ s_X \quad \text{and} \quad \lambda(\psi) = t_Y \circ F(\psi)\,,$$

whose right-hand sides mean the compositions of morphisms

$$X \xrightarrow{s_X} GF(X) \xrightarrow{G(\varphi)} G(Y) \quad \text{and} \quad F(X) \xrightarrow{F(\psi)} FG(Y) \xrightarrow{t_Y} Y\,.$$

[35] See formula (9.15) on p. 205.

[36] See the same formula (9.15).

Thus, the composition $\lambda\varrho(\varphi) = t_Y \circ FG(\varphi) \circ F(s_X) : F(X) \to Y$ is taken along the path from the lower left corner to the upper right corner in the diagram

$$\begin{tikzcd}
& F(X) \arrow[rr, "\varphi"] & & Y & \\
F(X) \arrow[ur, equal, "\mathrm{Id}_{F(X)}"] \arrow[rr, "F(s_X)"] & & FGF(X) \arrow[ul, "t_{F(X)}"'] \arrow[rr, "FG(\varphi)"] & & FG(Y) \arrow[ul, "t_Y"']
\end{tikzcd}$$

where the right parallelogram is commutative because t is a natural transformation, and the left triangle is commutative because $F \xrightarrow{F \circ s} FGF \xrightarrow{t \circ F} F$ is the identity transformation of the functor F to itself. Therefore,

$$\lambda\varrho(\varphi) = \varphi \text{ for all } \varphi \in \mathrm{Hom}(F(X), Y)\,.$$

For $\varphi \in \mathrm{Hom}(X, G(Y))$, the equality $\varrho\lambda(\psi) = \psi$ is checked by a symmetric argument. □

9.6 Limits of Diagrams

Every small category $\mathcal{N}$ can be thought of as a diagram formed by the arrows $\varphi \in \mathrm{Mor}\,\mathcal{N}$ drawn between the vertices $\nu \in \mathrm{Ob}\,\mathcal{N}$. A *diagram of shape* $\mathcal{N}$ in an arbitrary category $\mathcal{C}$ is a functor $X : \mathcal{N} \to \mathcal{C}$. Such a diagram is formed by the objects $X_\nu = X(\nu) \in \mathrm{Ob}\,\mathcal{C}$ labeled by $\nu \in \mathrm{Ob}\,\mathcal{N}$, and morphisms $\varphi_X : X_\alpha \to X_\beta$ labeled by arrows $\varphi : \alpha \to \beta$ of the category $\mathcal{N}$ such that $\varphi_X\psi_X = \zeta_X$ if $\zeta = \varphi\psi$ in $\mathrm{Mor}\,\mathcal{N}$. The category $\mathcal{N}$ is also referred to as the *index category* of the diagram X. For example, associated with every object $Y \in \mathrm{Ob}\,\mathcal{C}$ is the *constant diagram* $\overline{Y}$ formed by the objects $\overline{Y}_\nu = Y$ for all $\nu \in \mathrm{Ob}\,\mathcal{N}$ and the arrows $\varphi_{\overline{Y}} = \mathrm{Id}_Y$ for all $\varphi \in \mathrm{Mor}\,\mathcal{N}$.

All the diagrams of a given shape $\mathcal{N}$ in a given category $\mathcal{C}$ form the category[37] $\mathcal{F}un(\mathcal{N}, \mathcal{C})$, whose morphisms are natural transformations of diagrams $f : X \to Y$, i.e., collections of arrows $f_\nu : X_\nu \to Y_\nu$, $\nu \in \mathrm{Ob}\,\mathcal{N}$, such that $f_\beta\varphi_X = \varphi_Y f_\alpha$ for every arrow $\varphi : \alpha \to \beta$ in $\mathcal{N}$. Every diagram $X \in \mathcal{F}un(\mathcal{N}, \mathcal{C})$ produces the presheaf

$$\mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et\,, \quad Y \mapsto \mathrm{Hom}_{\mathcal{F}un(\mathcal{N},\mathcal{C})}\left(\overline{Y}, X\right).$$

If it is representable, the representing object is denoted by $\lim X \in \mathrm{Ob}\,\mathcal{C}$ and called the *limit*[38] of the diagram X. It comes together with a bijection

$$\mathrm{Hom}_{\mathcal{C}}(Y, \lim X) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{F}un(\mathcal{N},\mathcal{C})}\left(\overline{Y}, X\right) \tag{9.28}$$

[37] See Sect. 9.3 on p. 197.

[38] Or the *projective limit*.

natural in $Y \in \operatorname{Ob} \mathcal{C}$. For $Y = \lim X$, this map sends the identity endomorphism of $\lim X$ to the natural transformation $\pi : \overline{\lim X} \to X$, that is, the collection of arrows $\pi_\nu : \lim X_\nu \to X_\nu$ commuting with the arrows of the diagram X. The arrows π_ν possess the following universal property. For every object $Y \in \operatorname{Ob} \mathcal{C}$ equipped with a collection of arrows $\psi_\nu : Y \to X_\nu$ commuting with the arrows of X, there exists a unique morphism $\alpha : Y \to \lim X$ such that $\psi_\nu = \pi_\nu \circ \alpha$ for all ν.

Symmetrically, associated with every diagram $X \in \mathcal{Fun}(\mathcal{N}, \mathcal{C})$ is a functor

$$\mathcal{C} \to \mathcal{Set}\,, \quad Y \mapsto \operatorname{Hom}_{\mathcal{Fun}(\mathcal{N},\mathcal{C})}\left(X, \overline{Y}\right).$$

Its corepresenting object (assuming that it exists) is called the *colimit*[39] of the diagram X and denoted by $\operatorname{colim} X$. It comes together with a bijection

$$\operatorname{Hom}_{\mathcal{C}}(\operatorname{colim} X, Y) \simeq \operatorname{Hom}_{\mathcal{Fun}(\mathcal{N},\mathcal{C})}\left(X, \overline{Y}\right) \tag{9.29}$$

functorial in $Y \in \operatorname{Ob} \mathcal{C}$. For $Y = \operatorname{colim} X$, the identity endomorphism of $\operatorname{colim} X$ is mapped by (9.29) to the collection of arrows $\iota_\nu : X_\nu \to \operatorname{colim} X$, commuting with the arrows of X and having the following universal property. For every object $Y \in \operatorname{Ob} \mathcal{C}$ equipped with a collection of arrows $\psi_\nu : X_\nu \to Y$ commuting with the arrows of X, there exists a unique morphism $\beta : \operatorname{colim} X_\nu \to Y$ such that $\psi_\nu = \beta \circ \iota_\nu$ for all ν.

Exercise 9.27 Check that $\lim X$ and $\operatorname{colim} X$, if they exist, are unique up to a unique isomorphism commuting with the canonical arrows π_ν and ι_ν respectively.

Example 9.18 (Initial, Terminal, and Zero Objects) The simplest index category is the empty category $\varnothing$. It produces empty diagrams without any objects and arrows at all. The limit of the empty diagram in a category $\mathcal{C}$ (assuming that it exists) is denoted by $\mathbb{T}$ and called the *terminal object* of $\mathcal{C}$, because for every $C \in \operatorname{Ob} \mathcal{C}$, there exists a unique morphism $C \to \mathbb{T}$. Certainly, $\mathbb{T}$ is uniquely determined by this property up to the unique isomorphism. Dually, the colimit of the empty diagram (assuming that it exists) is denoted by $\mathbb{I}$ and called the *initial* or *coterminal object* of $\mathcal{C}$. For every object $C \in \mathcal{C}$, there is exactly one arrow $\mathbb{I} \to C$. If a category $\mathcal{C}$ has both initial and terminal objects and they coincide, then the object $\mathbb{I} = \mathbb{T}$ is called the *zero object* and denoted by 0.

Exercise 9.28 Indicate the initial and terminal objects in the categories $\mathcal{Set}$, $\mathcal{Top}$, $\mathcal{Ab}$, $\mathcal{Mod}_K$, R-$\mathcal{Mod}$, $\mathcal{Grp}$, $\mathcal{Cmr}$, and in the categories of presheaves of sets and abelian groups on a topological space[40] X. Which of these categories have the zero object?

Example 9.19 (Direct (Co)products) A small category $\mathcal{N}$ is called *discrete* if $\operatorname{Mor} \mathcal{N}$ is exhausted by the identity endomorphisms of the objects of $\mathcal{N}$. A discrete

[39] Or the *injective limit*.

[40] See Example 9.8 on p. 194.

diagram $X : \mathcal{N} \to \mathcal{C}$ is just a family of objects X_ν in $\mathcal{C}$ without arrows between them. The (co) limit of such a diagram is called the *direct* (*co*)*product* of objects X_ν. They are denoted by

$$\prod_\nu X_\nu \stackrel{\text{def}}{=} \lim X \quad \text{and} \quad \coprod_\nu X_\nu \stackrel{\text{def}}{=} \operatorname{colim} X\,.$$

If $\mathcal{N}$ consists of two objects, these definitions agree with those given in Example 9.13 and Example 9.14 on p. 204. An obvious induction shows that the existence of the direct (co) product of two objects implies the existence of (co) products of a finite number of sets of objects.

Exercise 9.29 Describe the infinite (co) products in $\mathcal{T}op$.

Example 9.20 ((Co) equalizers) The (co) limit of a diagram of shape $\bullet \rightrightarrows \bullet$ is called the (*co*) *equalizer* of two arrows of the diagram. In the category of sets, the equalizer of maps

$$X \underset{\psi}{\overset{\varphi}{\rightrightarrows}} Y$$

is the set of solutions of the equation $\varphi(x) = \psi(x)$ on $x \in X$, or equivalently, the preimage of the diagonal[41] $\Delta_Y \subset Y \times Y$ under the canonical map $\varphi \times \psi : X \to Y \times Y$. The coequalizer is the quotient set of Y by the equivalence relation generated by the image of the map[42] $\varphi \times \psi$, i.e., by the equalities $\varphi(x) = \psi(x)$ for all $x \in X$.

Exercise 9.30 Check this, and explicitly describe the (co) equalizers in the categories $\mathcal{S}et$, $\mathcal{T}op$, $\mathcal{A}b$, $\mathcal{M}od_K$, R-$\mathcal{M}od$, $\mathcal{M}od$-R, $\mathcal{G}rp$, $\mathcal{C}mr$.

Intuitively, the existence of equalizers allows one to define "subobjects" by means of equations, whereas the coequalizers allow one to define "quotient objects" by imposing relations. For example, the (co) kernel of a homomorphism of abelian groups $f : A \to B$ can be described as the (co) equalizer of f and the zero homomorphism in the category $\mathcal{A}b$.

Exercise 9.31 Prove this last statement.

Example 9.21 (Pullback, or Fibered Product) The limit of a diagram of shape

$$\bullet \to \bullet \leftarrow \bullet$$

is called the *pullback* of the arrows of the diagram or the *fibered product* of the side objects of the diagram over the middle object. For a concrete realization of this

---

[41] Recall that $\Delta_Y = \{(y, y) \in Y \times Y \mid y \in Y\}$; compare with Sect. 1.2.2 of Algebra I.

[42] That is, the intersection of all equivalences $R \subset Y \times Y$ containing $\operatorname{im}(\varphi \times \psi)$; see Sect. 1.2.2 of Algebra I.

diagram in a category $\mathcal{C}$,

$$X \xrightarrow{\xi} B \xleftarrow{\eta} Y\,,$$

the fibered product is denoted by $X \times_B Y$. It fits in the commutative diagram

$$\begin{tikzcd} X \times_B Y \arrow[r, "\psi"] \arrow[d, "\varphi"'] & Y \arrow[d, "\eta"] \\ X \arrow[r, "\xi"] & B \end{tikzcd} \tag{9.30}$$

called the *Cartesian square* or *pullback diagram*, which has the following universal property. For every commutative square

$$\begin{tikzcd} Z \arrow[r, "\psi'"] \arrow[d, "\varphi'"'] & Y \arrow[d, "\eta"] \\ X \arrow[r, "\xi"] & B \end{tikzcd}$$

there exists a unique morphism $\varphi' \times \psi' : Z \to X \times_B Y$ such that

$$\varphi' = \varphi \circ (\varphi' \times \psi') \quad \text{and} \quad \psi' = \psi \circ (\varphi' \times \psi')\,.$$

Exercise 9.32 Check that this universal property determines the upper angle of the diagram (9.30) uniquely up to a unique isomorphism commuting with φ and ψ.

In the category of sets, the fiber of the map $X \times_B Y \to B$ over a point $b \in B$ is the direct product of fibers $\varphi^{-1}(b) \times \psi^{-1}(b)$. This justifies the term "fibered product." We have already met an example of the Cartesian square in Theorem 4.1 on p. 83. In the category $\mathcal{U}(X)$ of open subsets in a topological space X, the fibered product over X coincides with the intersection: $U \times_X V = U \cap V$.

Example 9.22 (Pushforward, or Fibered Coproduct) Reversing all the arrows in the previous example leads to the notion of the *pushforward* of two arrows with a common source. It is defined as the colimit of the diagram $\bullet \leftarrow \bullet \rightarrow \bullet$, and is also called the *fibered coproduct* of the side objects over the middle one. For a particular realization

$$X \xleftarrow{\xi} B \xrightarrow{\eta} Y\,,$$

the fibered coproduct is denoted by $X \otimes_B Y$. It fits in the commutative *cocartesian square*

$$\begin{array}{ccc} B & \xrightarrow{\eta} & Y \\ {\scriptstyle\xi}\big\downarrow & & \big\downarrow{\scriptstyle\psi} \\ X & \xrightarrow{\varphi} & X \otimes_B Y \end{array} \tag{9.31}$$

also known as the *pushforward diagram*, and has the following universal property. For every commutative square

$$\begin{array}{ccc} B & \xrightarrow{\eta} & Y \\ {\scriptstyle\xi}\big\downarrow & & \big\downarrow{\scriptstyle\psi'} \\ X & \xrightarrow{\varphi'} & Z \end{array}$$

there exists a unique morphism $\varphi' \otimes \psi' : X \otimes_B Y \to Z$ such that

$$\varphi' = (\varphi' \otimes \psi') \circ \varphi \quad \text{and} \quad \psi' = (\varphi' \otimes \psi') \circ \psi\,.$$

Exercise 9.33 Describe explicitly the pullbacks and pushforwards[43] in the categories $\mathcal{S}et$, $\mathcal{T}op$, $\mathcal{A}b$, $\mathcal{M}od_K$, $\mathcal{G}rp$, $\mathcal{C}mr$.

9.6.1 (Co) completeness

A category $\mathcal{C}$ is called *(co) complete* if all diagrams $\mathcal{N} \to \mathcal{C}$, for all small categories $\mathcal{N}$, have (co) limits in $\mathcal{C}$.

Proposition 9.5 *If a category $\mathcal{C}$ possesses a terminal object, direct products of all sets of objects, and equalizers of all pairs of arrows with common source and target, then $\mathcal{C}$ is complete. Dually, $\mathcal{C}$ is cocomplete if it has an initial object, direct coproducts of all sets of objects, and coequalizers of all pairs of arrows with common source and target.*

Proof We will prove the first statement; the second follows from it by reversing the arrows. Given a diagram $X : \mathcal{N} \to \mathcal{C}$, we have to find the universal set of arrows φ_ν with a common source and targets at X_ν satisfying the equations $\varphi_\mu = \varkappa_{\mu\nu}\varphi_\nu$, where

[43] In the categories of groups and commutative rings, the pushforwards are traditionally called the *amalgamated* and *tensor* products respectively.

$\varkappa_{\mu\nu} = X(\nu \to \mu) : X(\nu) \to X(\mu)$ runs through the arrows of the diagram X. Write $A = \prod_\mu X_\mu$ for the direct product of all objects in the diagram, and $B = \prod_{\nu\to\mu} F_{\nu\mu}$ for the direct product of the objects $F_{\nu\mu} \stackrel{\text{def}}{=} X_\mu$. Thus, for every $\mu \in \operatorname{Ob}\mathcal{N}$, the factors X_μ in B are in bijection with the arrows ending at the μth node of the diagram. For every arrow $\nu \to \mu$ in $\mathcal{N}$, consider the morphisms

$$f_{\nu\mu} = \mathrm{Id}_{X_\mu} \circ \pi_\mu : A \to F_{\nu\mu} ,$$

$$g_{\nu\mu} = \varkappa_{\mu\nu} \circ \pi_\nu : A \to F_{\nu\mu} ,$$

where $\pi_\alpha : A \to X_\alpha$ is the canonical arrow from the direct product to a factor. By the universal property of the product B, there exist two morphisms $f, g : A \to B$ lifting the arrows $f_{\nu\mu}$, $g_{\nu\mu}$ along the canonical morphisms $\pi_{\mu\nu} : B \to F_{\mu\nu}$. Let L be the equalizer of f, g. It joins the arrow $\varphi : L \to A$ such that the arrows $\varphi_\mu = \pi_\mu \circ \varphi : L \to X_\nu$ solve the equations $\varphi_\mu = \varkappa_{\mu\nu}\varphi_\nu$ and satisfy the universal property of the limit. Thus, $L = \lim X$. □

Remark 9.1 In order to have the (co) limits of all *finite* diagrams in a category $\mathcal{C}$, it is enough to require the existence of products $X \times Y$ for all $X, Y \in \operatorname{Ob}\mathcal{C}$ in Proposition 9.5. This forces all finite direct products to exist in $\mathcal{C}$, and the above proof will work for every finite diagram.

Corollary 9.3 *The categories $\mathcal{S}et$, $\mathcal{T}op$, $\mathcal{A}b$, $\mathcal{M}od_K$, R-$\mathcal{M}od$, $\mathcal{M}od$-R, $\mathcal{G}rp$, $\mathcal{C}mr$ are bicomplete, meaning that they are both complete and cocomplete.*

Proof This follows from Exercises 9.28–9.30. □

9.6.2 Filtered Diagrams

A nonempty category $\mathcal{F}$ is called *filtered* if for every two objects in $\mathcal{F}$, there are two arrows with common target sourced at these objects, and for every two arrows φ, ψ with common source and common target, there exists an arrow ζ such that $\zeta\varphi = \zeta\psi$. For example, a poset every two elements of which have a common upper bound is a filtered category.[44] Given a small filtered category $\mathcal{F}$, diagrams $\mathcal{F} \to \mathcal{C}$ and $\mathcal{F}^{\text{opp}} \to \mathcal{C}$ are respectively called *filtered* and *cofiltered*.[45] The colimit of a filtered diagram $X : \mathcal{F} \to \mathcal{S}et$ is the quotient of the disjoint union $\coprod_\nu X_\nu$ by the equivalence relation identifying elements $x_\alpha \in X_\alpha$ and $x_\beta \in X_\beta$ if and only if $\varphi_X(x_\alpha) = \psi_X(x_\beta)$ for some arrows

$$\alpha \xrightarrow{\varphi} \gamma \xleftarrow{\psi} \beta$$

in $\mathcal{F}$, where φ_X, ψ_X denote the images $X(\varphi)$, $X(\psi)$ of those arrows in $\operatorname{Mor}(\mathcal{S}et)$.

[44]Compare with Example 9.2 on p. 188.

[45]Filtered diagrams are also called *direct* or *inductive* systems of morphisms. Cofiltered diagrams are also called *inverse* or *projective* systems of morphisms.

Exercise 9.34 Verify that this is an equivalence relation and check that the quotient by this equivalence is $\operatorname{colim} X$.

Example 9.23 (Open Neighborhoods and Stalks of Presheaves) In the category $\mathcal{U}(X)$ of open subsets of a topological space X, every family of open sets closed with respect to intersections forms a cofiltered diagram. For example, all open sets containing a given subset $Z \subset X$ form such a cofiltered diagram. In general, it has no limit in $\mathcal{U}(X)$, whereas in $\mathcal{S}et$, the limit coincides with the intersection $\bigcap_{U \supset Z} U$. For every presheaf $F : \mathcal{U}(X)^{\mathrm{opp}} \to \mathcal{S}et$, the sets of sections $F(U)$ over all $U \supset Z$ form a filtered diagram in $\mathcal{S}et$. Its colimit $F_Z \overset{\text{def}}{=} \operatorname{colim}_{U \supset Z} F(U)$ is called the *stalk* of F over Z. By the above construction, it is formed by the equivalence classes of pairs s_U, where $U \supset Z$ is an open neighborhood of Z and $s_U \in F(U)$ is a section of F over U modulo the relation $s_U \sim s_W$, meaning that $s_U|_V = s_W|_V$ for some open V such that $Z \subset V \subset U \cap W$. These equivalence classes are called *germs of sections* of F near Z.

Example 9.24 (Localization) Let K be a commutative ring with unit and $S \subset K$ a multiplicative system.[46] Then S can be viewed as a small category whose objects are the elements of S, and

$$\operatorname{Hom}_S(s,t) \overset{\text{def}}{=} \{a \in K \mid as = t\}\,.$$

Exercise 9.35 Verify that this category is filtered.

Consider the diagram $F : S \to \mathcal{M}od_K$ whose objects $F_s = K \cdot \left[\frac{1}{s}\right]$ are the free K-modules of rank 1 with the basis vectors denoted by $\left[\frac{1}{s}\right]$, and the linear map $F_s \to F_{as}$, corresponding to the arrow $a : s \to as$ in S, acts on the basis by the rule $\left[\frac{1}{s}\right] \mapsto a \cdot \left[\frac{1}{as}\right]$. By the above construction, the colimit $\operatorname{colim} F$ consists of the equivalence classes of elements $a/s \overset{\text{def}}{=} a \cdot \left[\frac{1}{s}\right]$ modulo the relation $a/s \sim b/t$, meaning that $af = bg$ for some $f, g \in K$ such that sf equals tg and lies in S.

Exercise 9.36 Check that this happens if and only if $(at - bs) \cdot r = 0$ for some $r \in S$.

This means that $\operatorname{colim} F = KS^{-1}$ is the *localization*[47] of K in S.

9.6.3 Functorial Properties of (Co) limits

Recall that a natural transformation of a diagram $X : \mathcal{N} \to \mathcal{C}$ to a diagram $Y : \mathcal{N} \to \mathcal{C}$ is a collection of arrows $f_\nu : X_\nu \to Y_\nu$, one arrow for each $\nu \in \operatorname{Ob} \mathcal{N}$, commuting with the arrows of the diagrams. Let the diagrams $X : \mathcal{N} \to \mathcal{C}$ and $Y : \mathcal{M} \to \mathcal{C}$ have limits $L_X = \lim X_\nu$ and $L_Y = \lim Y_\mu$ in the category $\mathcal{C}$. Then for

[46] This means that $1 \in S$ and $st \in S$ for all $s, t \in S$; see Sect. 4.1.1 of Algebra I.

[47] Or *ring of fractions* with numerators in K and denominators in S; see Sect. 4.1.1 of Algebra I.

every functor $\tau : \mathcal{M} \to \mathcal{N}$ and every natural transformation $f : X \circ \tau \to Y$, there exists a unique morphism $\lim f : L_X \to L_Y$ such that the diagram[48]

$$\begin{tikzcd} L_X \arrow[r, "\pi_{\tau(\mu)}"] \arrow[d, "\lim f"'] & X_{\tau(\mu)} \arrow[d, "f_\mu"] \\ L_Y \arrow[r, "\pi_\mu"] & Y_\mu \end{tikzcd} \tag{9.32}$$

is commutative for every $\mu \in \operatorname{Ob} \mathcal{M}$. Indeed, the compositions

$$f_\mu \circ \pi_{\tau(\mu)} : L_X \to Y_\mu$$

commute with all arrows within Y, and therefore, by the universal property of $L_Y = \lim Y$, there exists a unique morphism $L_X \to L_Y$ such that all diagrams (9.32) are commutative.

Dually, if there exist the colimits $C_X = \operatorname{colim} X_\nu$, $C_Y = \operatorname{colim} Y_\mu$, then for every functor $\tau : \mathcal{N} \to \mathcal{M}$ and every natural transformation $f : X \to Y \circ \tau$, there exists a unique morphism $\operatorname{colim} f : C_X \to C_Y$ such that the diagrams[49]

$$\begin{tikzcd} X_\nu \arrow[r, "\iota_\nu"] \arrow[d, "f_\nu"'] & C_X \arrow[d, "\operatorname{colim} f"] \\ Y_{\tau(\nu)} \arrow[r, "\iota_{\tau(\nu)}"] & C_Y \end{tikzcd}$$

are commutative for all $\nu \in \operatorname{Ob} \mathcal{N}$. In particular, for $\mathcal{M} = \mathcal{N}$ and $\tau = \mathrm{Id}$, we conclude that the limit and colimit are the functors from the category of the diagrams $\mathcal{F}un(\mathcal{N}, \mathcal{C})$ to the category $\mathcal{C}$. In fact, even more follows immediately from Proposition 9.3 on p. 210 and the equalities (9.28), (9.29) on p. 214.

Proposition 9.6 *For every small category $\mathcal{N}$ and (co) complete category $\mathcal{C}$, the functors* colim $: \mathcal{F}un(\mathcal{N}, \mathcal{C}) \to \mathcal{C}$ *and* lim $: \mathcal{F}un(\mathcal{N}, \mathcal{C}) \to \mathcal{C}$ *are respectively left and right adjoints to the functor $\mathcal{C} \to \mathcal{F}un(\mathcal{N}, \mathcal{C})$, $C \mapsto \overline{C}$, which maps an object to the associated constant diagram.* □

Remark 9.2 If the category $\mathcal{C}$ is not (co) complete, then the (co)limit remains functorial on those diagrams that have a (co)limit.

[48]The horizontal arrows in (9.32) are the canonical morphisms from the limit to the nodes of the diagram.

[49]Whose horizontal arrows are the canonical morphisms from the nodes of the diagram to the colimit.

Definition 9.1 (Commutativity with (Co) limits) A functor $F : \mathcal{C} \to \mathcal{D}$ is said to *commute* with *(co) limits* if for every object $L \in \operatorname{Ob}\mathcal{C}$ and every diagram

$$X : \mathcal{N} \to \mathcal{C},$$

the equality $L = (\mathrm{co})\lim X$ in $\mathcal{C}$ implies the equality $F(L) = (\mathrm{co})\lim F \circ X$ in $\mathcal{D}$.

Proposition 9.7 *If a functor $F : \mathcal{C} \to \mathcal{D}$ is left adjoint to a functor $G : \mathcal{D} \to \mathcal{C}$, then F commutes with limits and G commutes with colimits.*

Proof Since $F \wr G$, we have the following chain of isomorphisms functorial in $D \in \operatorname{Ob}\mathcal{D}$:

$$\operatorname{Hom}_{\mathcal{D}}\left(F(\operatorname{colim} X), D\right) \simeq \operatorname{Hom}_{\mathcal{C}}\left(\operatorname{colim} X, G(D)\right) \simeq \operatorname{Hom}_{\mathcal{F}un(\mathcal{N},\mathcal{C})}\left(X, \overline{G(D)}\right)$$
$$\simeq \operatorname{Hom}_{\mathcal{F}un(\mathcal{N},\mathcal{D})}\left(F \circ X, \overline{D}\right) .$$

Therefore, $F(\operatorname{colim} X) \simeq \operatorname{colim}(F \circ X)$. The case of limits is similar (and even easier). □

Corollary 9.4 *Limits commute with limits and colimits commute with colimits if they exist. More precisely, let $F : \mathcal{M} \to \mathcal{F}un(\mathcal{N}, \mathcal{C})$ be a diagram of the natural transformations of the diagrams $F_\mu : \mathcal{N} \to \mathcal{C}$ formed by objects $F_{\mu\nu} = F_\mu(\nu)$. Write $F(\nu) : \mathcal{M} \to \mathcal{C}$ for the diagram formed by the arrows realizing the natural transformations $F(\operatorname{Mor}(\mathcal{M}))$ over the object $\nu \in \operatorname{Ob}\mathcal{N}$. If for all $\mu \in \operatorname{Ob}\mathcal{M}$, $\nu \in \operatorname{Ob}\mathcal{N}$ there exist $\lim_\mu F_{\mu\nu} \stackrel{\text{def}}{=} \lim F_\mu$ and $\lim_\nu F_{\mu\nu} \stackrel{\text{def}}{=} \lim F(\nu)$ (respectively $\operatorname{colim}_\mu F_{\mu\nu} \stackrel{\text{def}}{=} \operatorname{colim} F_\mu$ and $\operatorname{colim}_\nu F_{\mu\nu} \stackrel{\text{def}}{=} \operatorname{colim} F(\nu)$), then there exist $\lim_\mu \lim_\nu F_{\mu\nu} \simeq \lim_\nu \lim_\mu F_{\mu\nu}$ (respectively $\operatorname{colim}_\mu \operatorname{colim}_\nu F_{\mu\nu} \simeq \operatorname{colim}_\nu \operatorname{colim}_\mu F_{\mu\nu}$).* □

Corollary 9.5 *Let $X, Y : \mathcal{N} \to \mathcal{A}b$ be two diagrams of abelian groups, and*

$$f : X \to Y$$

a natural transformation provided by the homomorphisms

$$f_\nu : X_\nu \to Y_\nu , \quad \nu \in \operatorname{Ob}\mathcal{N} .$$

Write $K = \ker f$ and $C = \operatorname{coker} f$ for the diagrams $\mathcal{N} \to \mathcal{A}b$ formed by the kernels and cokernels of the homomorphisms f_ν. Then $\lim K = \ker(\lim f : \lim X \to \lim Y)$ and $\operatorname{colim} K = \operatorname{coker}(\operatorname{colim} f : \operatorname{colim} X \to \operatorname{colim} Y)$.

Proof Since a (co) kernel is the (co) limit of a diagram,[50] it commutes with (co) limits. □

[50]Namely, the (co) kernel of a homomorphism is the (co)equalizer of this homomorphism and the zero homomorphism.

Corollary 9.6 *Let N be a right module over an arbitrary ring S. Then the functor S-$\mathcal{M}od \to \mathcal{A}b$, $X \mapsto N \otimes_S X$ commutes with the colimits of the diagrams of left S-modules. In particular,*

$$\operatorname{coker}\left(\mathrm{Id}_N \otimes_S \varphi : N \otimes_S K \to N \otimes_S L\right) \simeq N \otimes_S \operatorname{coker}(\varphi)$$

for every S-linear map $\varphi : K \to L$.

Proof Proposition 9.2 on p. 207 applied to the rings S and $R = \mathbb{Z}$ shows that the functor

$$S\text{-}\mathcal{M}od \to \mathcal{A}b\,, \quad X \mapsto N \otimes_S X\,,$$

is left adjoint to the functor $\mathcal{A}b \to S$-$\mathcal{M}od$, $Y \mapsto \mathrm{Hom}_{\mathcal{A}b}(N, Y)$. Therefore, it commutes with colimits. □

Problems for Independent Solution to Chapter 9

Problem 9.1 (Cyclic category) For every nonnegative integer m, consider the set of complex $(m+1)$th roots of unity $[m]_{\text{cyc}} \overset{\text{def}}{=} \{e^{2\pi i k/(m+1)} \in S^1 \subset \mathbb{C} \mid 0 \leqslant k \leqslant m\}$ as the category in which $\mathrm{Hom}_{[m]_{\text{cyc}}}(x, y)$ consists of the path from $x \in [m]_{\text{cyc}}$ to $y \in [m]_{\text{cyc}}$ provided by the counterclockwise oriented arc of the unit circle $S^1 \subset \mathbb{C}$, and all paths obtained from it by adding every positive number of full counterclockwise turns. Thus, the arrows $x \to y$ are in bijection with nonnegative integers measuring the number of full turns contained in the arrow. For every $x \in \mathrm{Ob}[m]_{\text{cyc}}$, write $T_x \in \mathrm{End}(x)$ for one full turn. The *cyclic category $\mathcal{C}yc$* is formed by the objects $[m]_{\text{cyc}}$, $m \in \mathbb{Z}_{\geqslant 0}$, and sets $\mathrm{Hom}_{\mathcal{C}yc}([n]_{\text{cyc}}, [m]_{\text{cyc}})$ consisting of all functors $\varphi : [n]_{\text{cyc}} \to [m]_{\text{cyc}}$ such that $\varphi(T_x) = T_{\varphi(x)}$ for all $x \in \mathrm{Ob}[n]_{\text{cyc}}$. Show that the representable presheaf $h_{[0]_{\text{cyc}}} : [m]_{\text{cyc}} \mapsto \mathrm{Hom}_{\mathcal{C}yc}([m]_{\text{cyc}}, [0]_{\text{cyc}})$ can be viewed as a functor $\mathcal{C}yc^{\text{opp}} \to \mathcal{C}yc$, and prove that it establishes an equivalence between $\mathcal{C}yc$ and $\mathcal{C}yc^{\text{opp}}$.

Problem 9.2 Construct the left adjoint functor to the forgetful functor $\mathcal{C} \to \mathcal{S}et$ for the following categories $\mathcal{C}$: **(a)** $\mathcal{V}ec_{\Bbbk}$, **(b)** $\mathrm{Ass}_{\Bbbk}$, **(c)** $\mathcal{C}mr$, **(d)** $\mathcal{G}rp$. In each case, describe explicitly both natural transformations between the composition of adjoint functors and the identity endofunctor.

Problem 9.3 Prove that the pullback of the diagram $X \xrightarrow{\xi} B \xleftarrow{\eta} Y$ is canonically isomorphic to the equalizer of maps $\xi \circ \pi_X, \eta \circ \pi_Y : X \times Y \to B$, where

$$\pi_X : X \times Y \to X\,, \quad \pi_Y : X \times Y \to Y$$

are the canonical projections. For a category with terminal object $\mathbb{T}$, check that

$$X \times_{\mathbb{T}} Y \simeq X \times Y$$

for all X, Y.

Problem 9.4 Formulate and prove the dual statements to the previous problem.

Problem 9.5 Show that in Proposition 9.5 on p. 217, the existence of all equalizers and coequalizers can be replaced by the existence of all pullbacks and pushforwards respectively.

Problem 9.6 Fix some prime $p \in \mathbb{N}$. For all $m > n$, let $\psi_{nm} : \mathbb{Z}/(p^m) \twoheadrightarrow \mathbb{Z}/(p^n)$ be the quotient homomorphism of additive groups, and $\varphi_{mn} : \mathbb{Z}/(p^n) \hookrightarrow \mathbb{Z}/(p^m)$ the embedding of additive groups mapping $[1] \mapsto [p^{m-n}]$. In the category of abelian groups, show that:

(a) The limit of the diagram formed by the arrows ψ_{nm} is the additive group $\mathbb{Z}_p$ of p-adic integers.[51]

(b) The colimit of the diagram formed by the arrows φ_{mn} is isomorphic to the multiplicative group of all p^nth roots of unity for all $n \in \mathbb{N}$, or equivalently, the additive group of classes of fractions z/p^{ℓ}, $z \in \mathbb{Z}$, $\ell \in \mathbb{N}$, in the quotient group $\mathbb{Q}/\mathbb{Z}$.

Problem 9.7 For all $n \mid m$, let $\psi_{nm} : \mathbb{Z}/(m) \twoheadrightarrow \mathbb{Z}/(n)$ be the quotient homomorphism of additive groups, and $\varphi_{mn} : \mathbb{Z}/(n) \hookrightarrow \mathbb{Z}/(m)$ the embedding of additive groups such that $[1] \mapsto [m/n]$. In the category of abelian groups, show that:

(a) The limit of the diagram formed by the arrows ψ_{nm} is isomorphic to the product of additive groups $\prod_p \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the group of p-adic integers.

(b) The colimit of the diagram formed by the arrows φ_{mn} is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

Problem 9.8 For an arbitrary poset $\mathcal{N}$, give an explicit construction of the limit and colimit of a diagram $X : \mathcal{N} \to \mathcal{S}et$.

Problem 9.9 (Adjoint Presheaves) Presheaves

$$F : \mathcal{C}^{\text{opp}} \to \mathcal{D} \quad \text{and} \quad G : \mathcal{D}^{\text{opp}} \to \mathcal{C}$$

are called respectively *left adjoint* and *right adjoint* if there exist respective bijections $\text{Hom}_{\mathcal{C}}\big(G(D), C\big) \simeq \text{Hom}_{\mathcal{D}}\big(F(C), D\big)$ and $\text{Hom}_{\mathcal{C}}\big(C, G(D)\big) \simeq \text{Hom}_{\mathcal{D}}\big(D, F(C)\big)$ functorial in $C \in \text{Ob}\,\mathcal{C}$, $D \in \text{Ob}\,\mathcal{D}$. Prove that left adjoint

[51] That is, the completion of $\mathbb{Z}$ with respect to the *p-adic distance* $|x, y|_p = \|x - y\|_p$, where the *p-adic norm* $\|z\|_p$ of an integer $z = p^s m$, $\text{GCD}(m, p) = 1$, equals p^{-s}.

presheaves send colimits to limits, whereas right adjoint presheaves send limits to colimits.

Problem 9.10 (Noncommutative Fractions) Let R be an arbitrary ring with unit and $S \subset R$ a multiplicative system[52] satisfying the following two *Ore conditions*: (1) for all $\lambda \in R$, $s \in S$, there exist $\varrho \in R$, $t \in S$ such that $\lambda s = t\varrho$; (2) for all $\lambda_1, \lambda_2 \in R$, the existence of $s \in S$ with $\lambda_1 s = \lambda_2 s$ implies the existence of $t \in S$ with $t\lambda_1 = t\lambda_2$. Consider S the category whose objects are the elements of S, and $\mathrm{Hom}_S(s,t) \stackrel{\text{def}}{=} \{\lambda \in R \mid \lambda s = t\}$. Define the functor $F : S \to R\text{-}\mathcal{M}od$ by sending an object $s \in S$ to the free left R-module of rank 1 whose basis vector we denote by $\left[\frac{1}{s}\right]$, and sending an arrow $\lambda : s \to \lambda s$ to the R-linear (from the right) homomorphism acting on the basis vector by the rule $\left[\frac{1}{s}\right] \mapsto \lambda \cdot \left[\frac{1}{\lambda s}\right]$. Prove that F is a filtered diagram and $\operatorname{colim} F = S^{-1}R$ is formed by the classes of formal records $s^{-1}r$, where $s \in S$, $r \in R$, modulo the equivalence $s_1^{-1}r_1 \sim s_2^{-1}r_2$, meaning the existence of $x_1, x_2 \in R$ such that $x_1 s_1 = x_2 s_2 \in S$ and $x_1 r_1 = x_2 r_2$. Further, provide $S^{-1}R$ with a ring structure with unit.

Problem 9.11 (Exact Functors) Recall[53] that two composable arrows

$$* \xrightarrow{\varphi} * \xrightarrow{\psi} *$$

in the category of abelian groups are called *exact* if $\ker\psi = \operatorname{im}\varphi$. A longer sequence of arrows is *exact* if every pair of sequential arrows is exact. Exact sequences of the form

$$0 \to A \to B \to C \to 0$$

are called *short exact sequences* or *exact triples*. A functor $F : \mathcal{A}b \to \mathcal{A}b$ (respectively a presheaf $F : \mathcal{A}b^{\mathrm{opp}} \to \mathcal{A}b$) is called *left exact* if it maps kernels (respectively cokernels) to kernels, or equivalently, exact sequences of the form $0 \to A \to B \to C$ (respectively $A \to B \to C \to 0$) to exact sequences $0 \to F(A) \to F(B) \to F(C)$ (respectively $0 \to F(C) \to F(B) \to F(A)$). Dually, F is called *right exact* if it maps cokernels (respectively kernels) to cokernels, that is, sends exact sequences of the form $A \to B \to C \to 0$ (respectively $0 \to A \to B \to C$) to exact sequences $F(A) \to F(B) \to F(C) \to 0$ (respectively $F(C) \to F(B) \to F(A) \to 0$). A functor is called *exact* if it is both left exact and right exact. Prove that:

(a) A functor is exact if and only if it sends short exact sequences to short exact sequences, and in that case, it preserves the exactness of arbitrary exact sequences of arrows.

(b) Functors $h^A : X \mapsto \mathrm{Hom}(A,X)$ and $h_A : X \mapsto \mathrm{Hom}(X,A)$ are left exact for all $A \in \operatorname{Ob}\mathcal{A}b$.

---

[52] That is, $1 \in S$ and $st \in S$ for all $s, t \in S$.

[53] See Problem 7.8 of Algebra I.

(c) All right adjoint functors are left exact, and left adjoint functors are right exact.
(d) Colimits of filtered diagrams are exact functors.[54]

Problem 9.12 Give explicit examples of $A, B, N \in \operatorname{Ob} \mathcal{A}$ such that the endofunctors $\mathcal{A}b \to \mathcal{A}b$ sending $X \in \operatorname{Ob} \mathcal{A}b$ respectively to $\operatorname{Hom}(A, X)$, $\operatorname{Hom}(X, B)$, and $N \otimes X$ are not exact.[55]

Problem 9.13 Prove that a sequence of maps $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ in $\mathcal{A}b$ is exact if for every $X \in \operatorname{Ob} \mathcal{A}b$, the sequence of natural transformations

$$0 \to h_A(X) \xrightarrow{\alpha_*} h_B(X) \xrightarrow{\beta_*} h_C(X) \to 0 \tag{9.33}$$

is exact. Give an example of ashort exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ for which the sequence (9.33) is not exact.

Problem 9.14 (Projective Modules) Prove that the following three conditions on a left module P over a ring R are equivalent[56] in the category R-$\mathcal{M}od$:

1. The functor $h^P : R\text{-}\mathcal{M}od \to \mathcal{A}b$, $X \mapsto \operatorname{Hom}(P, X)$, is exact.
2. For every morphism $\varphi : P \to X$ and every epimorphism $\psi : Y \twoheadrightarrow X$, there exists a morphism $\eta : P \to Y$ such that $\varphi = \psi\eta$.
3. For every epimorphism $\psi : Z \twoheadrightarrow P$, there exists an isomorphism

$$\gamma : Z \xrightarrow{\sim} \ker \pi \oplus P$$

such that $\psi = \pi_P \gamma$, where $\pi_P : \ker \pi \oplus P \twoheadrightarrow P$ is the canonical projection.

Problem 9.15 (Injective Modules) Prove that the following three conditions on a left module I over a ring R are equivalent[57] in the category R-$\mathcal{M}od$:

1. The presheaf $h_I : R\text{-}\mathcal{M}od \to \mathcal{A}b$, $X \mapsto \operatorname{Hom}(X, I)$, is exact.
2. For every monomorphism $\psi : X \hookrightarrow Y$ and every morphism $\varphi : X \to I$, there exists a morphism $\eta : Y \to I$ such that $\eta\psi = \varphi$.
3. For every monomorphism $\psi : I \hookrightarrow Z$, there exists an isomorphism

$$\gamma : I \oplus \operatorname{coker} \iota \xrightarrow{\sim} Z$$

such that $\psi = \gamma\iota_I$, where $\iota_I : I \hookrightarrow I \oplus \operatorname{coker} \iota$ is the canonical inclusion.

[54] By Corollary 9.5 on p. 221, it is enough to show that filtered colimits commute with kernels.

[55] This means that the first two functors are not right exact, and the third is not left exact.

[56] A module P with these properties is called *projective*.

[57] A module I possessing these properties is called *injective*.

Problem 9.16 Prove that the abelian groups $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective $\mathbb{Z}$-modules. For every $A \in \operatorname{Ob} \mathcal{A}b$ and $a \in A$, prove that there exists a homomorphism of abelian groups $\psi : A \to \mathbb{Q}/\mathbb{Z}$ such that $\psi(a) \neq 0$.

Problem 9.17 For every ring R, equip the abelian group $I_R = \operatorname{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ with the left R-module structure provided by the right action of R on itself.[58] Prove that **(a)** I_R is an injective R-module, **(b)** the functor h_{I_R} is faithful.[59]

Problem 9.18 For every ring R with unit and all $m, n \in \mathbb{N}$, prove that the categories of left modules over the matrix rings $\operatorname{Mat}_n(R)$ and $\operatorname{Mat}_m(R)$ are exactly equivalent.[60]

[58] That is, $r\varphi(x) \stackrel{\text{def}}{=} \varphi(xr)$ for all $r, x \in R$, $\varphi : R \to \mathbb{Q}/\mathbb{Z}$.

[59] See Sect. 9.2 on p. 191.

[60] That is, an equivalence can be established by means of *exact* quasi-inverse functors.

Chapter 10
Extensions of Commutative Rings

Everywhere in this section, the term "ring" means by default a commutative ring with unit. All ring homomorphisms are assumed to map the unit to the unit.

10.1 Integral Elements

10.1.1 Definition and Properties of Integral Elements

An *extension of rings* is a pair $A \subset B$, where A is a subring of a ring B and both rings have a common unit. Given such a ring extension, an element $b \in B$ is called *integral* over A if it satisfies the conditions of the following lemma.

Lemma 10.1 (Characterization of Integral Elements) *The following properties of an element $b \in B$ in a ring extension $A \subset B$ are equivalent:*

(1) $b^m = a_1 b^{m-1} + \cdots + a_{m-1} b + a_m$ *for some* $m \in \mathbb{N}$ *and* $a_1, a_2, \dots, a_m \in A$.
(2) *The A-linear span of all nonnegative integer powers b^m is a finitely generated A-module.*
(3) *There exists a finitely generated A-module $M \subset B$ such that $bM \subset M$ and $b'M \neq 0$ for all nonzero $b' \in B$.*

Proof The implications (1) ⇒ (2) ⇒ (3) are obvious. We will show that (3) implies (1). Fix some $e_1, e_2, \dots, e_m$ spanning M over A and write $Y \in \mathrm{Mat}_m(A)$ for the matrix of the A-linear map $b : M \to M$, $m \mapsto bm$, in this system of generators. Then

$$(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y . \tag{10.1}$$

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_10

The matrix identity[1] $\det X \cdot E = X \cdot X^{\vee}$, where X is a square matrix, E the identity matrix of the same size, and $X^{\vee}$ the adjunct matrix of X, shows that the image of multiplication by $\det X$ lies in the linear span of the columns of the matrix X. For $X = (bE - Y) \in \mathrm{Mat}_m(B)$, this means that $\det(bE - Y) \cdot M$ is contained in the B-linear span of vectors $(e_1, e_2, \dots, e_m) \cdot (bE - Y)$, which is zero because of (10.1). The last property in (3) forces $\det(bE - Y) = 0$. Since all elements of Y lie in A, the latter equality can be rewritten in the form appearing in (1). □

Definition 10.1 Let $A \subset B$ be an extension of rings. The set of all elements $b \in B$ integral over A is called the *integral closure* of A in B. If it coincides with A, then A is said to be *integrally closed* in B. If all elements of B are integral over A, then the extension $A \subset B$ is called an *integral ring extension*, and we say that B is *integral* over A.

Example 10.1 ($\mathbb{Z}$ is Integrally Closed in $\mathbb{Q}$) Let $A = \mathbb{Z}$, $B = \mathbb{Q}$. If a fraction $p/q \in \mathbb{Q}$ with coprime $p, q \in \mathbb{Z}$ satisfies a monic polynomial equation

$$\frac{p^m}{q^m} = a_1 \frac{p^{m-1}}{q^{m-1}} + \cdots + a_{m-1} \frac{p}{q} + a_m$$

with $a_i \in \mathbb{Z}$, then $p^m = a_1 q p^{m-1} + \cdots + a_{m-1} q^{m-1} p + a_m q^m$ is divisible by q. Since p, q are coprime, we conclude that $q = \pm 1$. Hence, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Example 10.2 (Invariants of a Finite Group) Let a finite group G act on a ring B by ring automorphisms, and let $B^G \stackrel{\text{def}}{=} \{a \in B \mid \forall\, g \in G \;\; ga = a\}$ be the *subring of G-invariants*. Then B is integral over B^G. Indeed, write $b_1, b_2, \dots, b_n$ for the G-orbit of an arbitrary element $b = b_1 \in B$. Then b is a root of the monic polynomial

$$f(t) = \prod (t - b_i) \in B^G[t]\,,$$

as required in the first property of Lemma 10.1.

Proposition 10.1 *Let $A \subset B$ be an extension of rings, and $\overline{A}_B \subset B$ the integral closure of A in B. Then $\overline{A}_B$ is a subring of B, and for every ring extension $B \subset C$, every element $c \in C$ integral over $\overline{A}_B$ is integral over A as well.*

Proof If elements $p, q \in B$ satisfy the monic polynomial equations

$$p^m = x_1\, p^{m-1} + \cdots + x_{m-1}\, p + x_m\,,$$
$$q^n = y_1\, q^{n-1} + \cdots + y_{n-1}\, q + y_n\,,$$

for some $x_\nu, y_\mu \in A$, then the products $p^i q^j$, where

$$0 \leqslant i < m - 1, 0 \leqslant j < n - 1,$$

[1] See Sect. 9.6.1 of Algebra I, especially formula (9.29).

span a finitely generated A-module containing the unit and mapped to itself by multiplication by p and by q. Therefore, it satisfies condition (3) from Lemma 10.1 for both $b = p + q$ and $b = pq$. Similarly, if the monic polynomial equations

$$c^r = z_1\, c^{r-1} + \cdots + z_{r-1}\, c + z_r\,,$$
$$z_k^{m_k} = a_{k,1}\, z^{m_k-1} + \cdots + a_{k,m_k-1}\, z_k + a_{k,m_k} \quad 1 \leqslant k \leqslant r\,,$$

hold for some $c \in C$, $z_1, z_2, \dots, z_r \in \overline{A}_B$, and $a_{k,\ell} \in A$, then the A-linear span of products

$$c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}\,, \quad 0 \leqslant i < r-1\,,\ 0 \leqslant j_k < m_k - 1\,,$$

contains the unit and goes to itself under multiplication by c. Therefore, c is integral over A. □

Proposition 10.2 (Gauss–Kronecker–Dedekind lemma) *Let $A \subset B$ be an extension of rings, and $f, g \in B[x]$ monic polynomials of positive degree. Then all coefficients of the product fg are integral over A if and only if all coefficients of the polynomials f, g are integral A.*

Proof Let $C \supset B$ be an extension of rings such that the polynomials f, g are completely factorizable in $C[x]$ as $f(x) = \prod(x-\alpha_\nu)$ and $g(x) = \prod(x-\beta_\mu)$ for some $\alpha_\nu, \beta_\mu \in C$. Then $h(x) = \prod(x-\alpha_\nu)\prod(x-\beta_\mu)$ is also completely factorizable.

Exercise 10.1 Given a finite set of monic polynomials of positive degree in $B[x]$, prove that there is an extension of rings $B \subset C$ such that all polynomials become completely factorizable in $C[x]$.

If all coefficients of h are integral over A, then all the roots $\alpha_\nu, \beta_\mu \in C$ are integral over $\overline{A}_B$ and therefore integral over A by Proposition 10.1. Since integral elements form a ring, all coefficients of f, g, that are the symmetric functions of α_ν, β_μ are also integral over A. The same arguments work in the opposite direction as well. □

Proposition 10.3 *Let $A \subset B$ be an integral extension of rings. If B is a field, then A is a field too. Conversely, if A is a field and B has no zero divisors, then B is a field.*

Proof Let B be an integral field over A. Then for every nonzero $a \in A$, the inverse element $a^{-1} \in B$ satisfies a monic polynomial equation

$$a^{-m} = \alpha_1\, a^{1-m} + \cdots + \alpha_{m-1}\, a^{-1} + \alpha_0$$

for some $\alpha_\nu \in A$. Multiplication of both sides by a^{m-1} shows that

$$a^{-1} = \alpha_1 + \cdots + \alpha_{m-1}\, a^{m-2} + \alpha_0\, a^{m-1} \in A\,.$$

Conversely, if B is an integral algebra over a field A, then for every $b \in B$, the nonnegative integer powers b^m span a finite-dimensional vector space V over A. For $b \neq 0$, the linear endomorphism $b : V \to V$, $x \mapsto bx$, is injective if B has no zero divisors. This forces it to be bijective. The preimage of the unit $1 \in V$ is b^{-1}. □

10.1.2 Algebraic Integers

Let $K \supset \mathbb{Q}$ be a field of finite dimension $d = \dim_{\mathbb{Q}} K$ as a vector space over $\mathbb{Q}$. In this case, the elements of K are called *algebraic numbers*, because they all are integral over $\mathbb{Q}$, and therefore algebraic.[2] The dimension $d = \dim_{\mathbb{Q}} K$ is usually referred to as the *degree* of K over $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is called the *ring of algebraic integers* in K and traditionally denoted by $O_K \subset K$.

Exercise 10.2 Show that for every $\xi \in K$, there exists $n \in \mathbb{N}$ such that $n\xi \in O_K$.

It follows from the exercise that the quotient field of the ring of integers O_K coincides with K. Moreover, for every basis $e_1, e_2, \dots, e_d$ of K over $\mathbb{Q}$, there exists $n \in \mathbb{N}$ such that $ne_i \in O_K$ for all i. In particular, every field of finite degree over $\mathbb{Q}$ admits an integer basis over $\mathbb{Q}$. As a $\mathbb{Z}$-module, O_K has no torsion, and every set of $d + 1$ elements of O_K are linearly related over $\mathbb{Z}$, because they are linearly related over $\mathbb{Q}$ within K. We conclude that O_K is a free $\mathbb{Z}$-module of rank $d = \dim_{\mathbb{Q}} K$.

Exercise 10.3 Show that $z \in K$ is an integer if and only if there exists a basis of K over $\mathbb{Q}$ such that the multiplication operator $z : K \to K$, $x \mapsto zx$, has an integer matrix.[3]

Definition 10.2 For every algebraic number $z \in K$, the trace and determinant of the $\mathbb{Q}$-linear endomorphism $z : K \to K$, $x \mapsto zx$, are called the *trace* and the *norm* of z and denoted by $\operatorname{tr}(z)$ and $N(z)$ respectively. Note that both $\operatorname{tr}(z)$ and $N(z)$ lie in $\mathbb{Q}$. The $\mathbb{Q}$-bilinear form $\operatorname{Sp} : K \times K \to \mathbb{Q}$, $\operatorname{Sp}(a, b) \overset{\text{def}}{=} \operatorname{tr}(ab)$, is called the *trace form*. Its Gram determinant in an arbitrary basis of O_K over $\mathbb{Z}$ is called the *discriminant* of the field K.

Exercise 10.4 Verify that the trace map $\operatorname{tr} : K \to \mathbb{Q}$ is $\mathbb{Q}$-linear, the norm map $N : K \to \mathbb{Q}$ is a multiplicative (but not additive) homomorphism, the trace form Sp is symmetric and nondegenerate, and the discriminant does not depend on the choice of basis of O_K over $\mathbb{Z}$.

Example 10.3 (Quadratic Algebraic Integers) Every field $K \supset \mathbb{Q}$ of degree 2 has a form $K = \mathbb{Q}\left[\sqrt{d}\right] = \mathbb{Q}[x]/\left(x^2 - d\right)$, where $d \in \mathbb{Z}$ is square-free and differs from 0, 1. Indeed, let $\zeta \in K \setminus \mathbb{Q}$. Then $1, \zeta$ form a basis of K over $\mathbb{Q}$, and $\zeta^2 = b\zeta + c$ for some $b, c \in \mathbb{Q}$. Hence, $\zeta = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$ and $d \in \mathbb{Z}$ such that $b \neq 0$ and d is square-free. Therefore $1, \sqrt{d}$ also form a basis of K over $\mathbb{Q}$, i.e., $K = \mathbb{Q}\left[\sqrt{d}\right]$.

Exercise 10.5 Prove that $\mathbb{Q}\left[\sqrt{d_1}\right] \not\simeq \mathbb{Q}\left[\sqrt{d_2}\right]$ for $d_1 \neq d_2$ (both square-free).

Now assume that $\xi = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, is an integer of K. Let $t = \operatorname{tr}(\xi)$, $n = N(\xi)$. Since multiplication by ξ has an integer matrix in some basis of K over

[2] See Sect. 3.4.2 of Algebra I.

[3] That is, lying in $\operatorname{Mat}_d(\mathbb{Z}) \subset \operatorname{Mat}_d(\mathbb{Q})$. Indeed, this is the original definition of algebraic integers, introduced in the nineteenth century by Dedekind.

$\mathbb{Q}$, we have $t, n \in \mathbb{Z}$. In the basis $1, \sqrt{d}$, multiplication by ξ has the matrix

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Thus, $t = 2a$ and $n = a^2 - db^2 = t^2/4 - db^2$. This forces $b = s/2$ for some $s \in \mathbb{Z}$ such that $t^2 - ds^2 \equiv 0 \pmod 4$.

If $d \equiv 1 \pmod 4$, then $t^2 \equiv s^2 \pmod 4$, that is, $t \equiv s \pmod 2$, or equivalently, $s = t + 2r$ for some $r \in \mathbb{Z}$. Hence,

$$\xi = \frac{t}{2} + \frac{s}{2}\sqrt{d} = t + r\frac{1+\sqrt{d}}{2}.$$

Exercise 10.6 Verify that $\left(1+\sqrt{d}\right)/2 \in O_K$ for $d \equiv 1 \pmod 4$.

Hence, 1 and $\left(1+\sqrt{d}\right)/2$ form a basis of O_K for $d \equiv 1 \pmod 4$.

For $d \equiv 2 \pmod 4$ and $d \equiv -1 \pmod 4$, the corresponding congruences $t^2 \equiv 2s^2 \pmod 4$ and $t^2 + s^2 \equiv 0 \pmod 4$ force t, s to be even. Hence, $\xi = a + b\sqrt{d}$ has $a, b \in \mathbb{Z}$. Since $\sqrt{d} \in O_K$, we conclude that 1 and $\sqrt{d}$ form a basis of O_K for $d \equiv 2, 3 \pmod 4$. In particular, the *Gaussian* and *Kronecker integers*, that is, elements of the quadratic fields $\mathbb{Q}[i]$ integral over $\mathbb{Z}$ with $i^2 = -1$ and $\mathbb{Q}[\omega]$ with $\omega^2 + \omega + 1 = 0$, are exhausted by the integer linear combinations $a + bi$ and $a + b\omega$, $a, b \in \mathbb{Z}$, respectively.

Exercise 10.7 Evaluate the discriminant of $\mathbb{Q}\left[\sqrt{d}\right]$ depending on d.

10.1.3 Normal Rings

A commutative ring A without zero divisors is called *normal* if A is integrally closed in its field of fractions[4] Q_A. In particular, every field is normal. The same arguments as in Example 10.1 show that every unique factorization domain[5] A is normal. Indeed, a polynomial $a_0t^m + a_1t^{m-1} + \cdots + a_{m-1}t + a_m \in A[t]$ annihilates a fraction $p/q \in Q_A$ with $\operatorname{GCD}(p, q) = 1$ only if $q \mid a_0$ and $p \mid a_m$. Therefore, $a_0 = 1$ forces $q = 1$. As a consequence, all polynomial rings over a unique factorization domain are normal. For normal rings, Proposition 10.2 leads to the following classical claim going back to Gauss.

Corollary 10.1 (Gauss's Lemma II) *Let A be a normal ring, Q_A its field of fractions, and $f \in A[x]$ a monic polynomial. If $f = gh$ in $Q_A[x]$ for some monic polynomials g, h, then $f, g \in A[x]$.* □

[4]See Sect. 4.1.2 of Algebra I.

[5]See Sect. 5.4 of Algebra I.

Corollary 10.2 *Under the conditions of Corollary 10.1, let $B \supset Q_A$ be a ring extending Q_A. If an element $b \in B$ is integral over A, then the minimal polynomial*[6] *of b over Q_A lies in $A[x]$.*

Proof Since b is integral over A, there exists a monic polynomial $f \in A[x]$ such that $f(b) = 0$. Then the minimal polynomial of b over Q_A divides f in $Q_A[x]$, and the quotient is also monic. It remains to apply Corollary 10.1. □

10.2 Applications to Representation Theory

Let $\varrho : \mathbb{C}[G] \to \operatorname{End} V$ be a complex linear representation of a finite group G. For every element $g \in G$, all the eigenvalues of $\varrho(g)$ are among the roots of the monic polynomial[7] $t^{|G|} - 1$, and therefore are integral over $\mathbb{Z}$. Since $\chi_\varrho(g) = \operatorname{tr} \varrho(g)$ is a linear combination of eigenvalues with positive integer coefficients, we conclude that all values of the character of every complex representation of G are integral over $\mathbb{Z}$.

Theorem 10.1 *The dimension of every complex irreducible representation*

$$\varrho : \mathbb{C}[G] \to \operatorname{End} V$$

of a finite group G divides the index $[G : Z(G)]$ of the center of G.

Proof As our first step, we will show that $\dim V$ divides $|G|$. More precisely, we will prove that the rational number $|G|/\dim V$ is integral over $\mathbb{Z}$; then Example 10.1 forces it to be an integer. Since V is irreducible, the inner product of its character with itself equals 1. Thus,

$$(\chi_V, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \varrho\left(g^{-1}\right) \cdot \operatorname{tr} \varrho(g) = 1\,. \tag{10.2}$$

The function $g \mapsto \operatorname{tr} \varrho\left(g^{-1}\right)$ is constant on every conjugacy class. Write $\tau(K) \in \mathbb{C}$ for its value on the class $K \in \operatorname{Cl}(G)$. As we said before the theorem, $\tau(K)$ is integral over $\mathbb{Z}$ for all K. The latter equality in (10.2) can be written as

$$\frac{|G|}{\dim V} = \frac{1}{\dim V} \sum_{g \in G} \operatorname{tr} \varrho(g^{-1}) \cdot \operatorname{tr} \varrho(g) = \sum_{K \in \operatorname{Cl} G} \tau(K) \cdot \frac{1}{\dim V} \cdot \operatorname{tr} \sum_{g \in K} \varrho(g)\,. \tag{10.3}$$

---

[6]That is, the monic polynomial $\mu_b \in Q_A[x]$ of minimal positive degree such that $\mu_b(b) = 0$; see Sect. 8.1.3 of Algebra I.

[7]Recall that the eigenvalues of an operator are among the roots of every polynomial annihilating the operator; see Exercise 15.13 of Algebra I.

It remains to check that for every $K \in \mathrm{Cl}(G)$, the complex number

$$\frac{1}{\dim V} \cdot \operatorname{tr} \sum_{g \in K} \varrho(g) = \frac{1}{\dim V} \cdot \operatorname{tr} \varrho\Big(\sum_{g \in K} g\Big)$$

is integral over $\mathbb{Z}$. The element $g_K = \sum_{g \in K} g$ belongs to both the center of $\mathbb{C}[G]$ and the $\mathbb{Z}$-linear span of the group elements. The intersection $R = Z(\mathbb{C}[G]) \cap \mathbb{Z}[G]$ is a central commutative subring of $\mathbb{C}[G]$, finitely generated as a $\mathbb{Z}$-module. Since V is irreducible, it follows from Schur's lemma[8] that every central element of $\mathbb{C}[G]$ acts on V via multiplication by a scalar. The scalars corresponding to the elements of R form a subring of $\mathbb{C}$, also finitely generated as a $\mathbb{Z}$-module, and therefore integral over $\mathbb{Z}$. The scalar that represents g_K equals $\operatorname{tr} \varrho(g_K)/\dim V$. Thus, this number is integral over $\mathbb{Z}$, and therefore $|G|/\dim V \in \mathbb{Z}$.

Now let us check that the rational number $q = [G : Z(G)]/\dim V$ is integral over $\mathbb{Z}$ as well. It is enough to show that all nonnegative integer powers q^n belong to some finitely generated $\mathbb{Z}$-submodule of $\mathbb{Q}$.

Exercise 10.8 Explain why it is enough.

Consider the representation of the group $G^n = G \times G \times \cdots \times G$ in the space $W = V^{\otimes n}$ by the rule

$$(g_1, g_2, \dots, g_n) : v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto \varrho(g_1)v_1 \otimes \varrho(g_2)v_2 \otimes \cdots \otimes \varrho(g_n)v_n\,. \tag{10.4}$$

Exercise 10.9 Verify that this representation is irreducible.

Since every central element $c \in Z(G)$ acts on V via multiplication by a constant, the subgroup $C \subset G^n$ formed by the collections of central elements $(c_1, c_2, \dots, c_n)$ with the product $c_1 c_2 \cdots c_n = e$ lies in the kernel of the representation (10.4), that is, it acts identically. The group C has order $|Z(G)|^{n-1}$, because every collection $(c_1, c_2, \dots, c_{n-1}) \in Z(G)^{n-1}$ has the unique completion $(c_1, c_2, \dots, c_n) \in C$. Since C is a central subgroup, it is normal in G^n, and the formula (10.4) assigns the well-defined irreducible representation of the quotient group G^n/C, of order $|G|^n/|Z(G)|^{n-1}$, in the space of dimension $\dim^n V$. By the first step,

$$\frac{|G|^n}{(\dim V)^n |Z(G)|^{n-1}} = |Z(G)| \cdot q^n \in \mathbb{Z}\,.$$

Therefore, all powers q^n belong to the finitely generated $\mathbb{Z}$-submodule $|Z(G)|^{-1} \cdot \mathbb{Z} \subset \mathbb{Q}$, as desired. □

Theorem 10.2 *Let G be a finite group, $A \lhd G$ an abelian normal subgroup, and $\varrho : \mathbb{C}[G] \to \operatorname{End} W$ a complex irreducible representation. Then $\dim W$ divides the index $[G : A]$.*

---

[8] See Lemma 5.3 on p. 103.

Proof Consider the isotypic decomposition of the restriction of ϱ on A,

$$\operatorname{res} W = \bigoplus_{\chi \in A^\wedge} W_\chi ,$$

where W_χ is a direct sum of 1-dimensional representations in which the abelian group A acts by means of the same multiplicative character[9] $\chi : A \to \mathbb{C}^*$, that is, $aw = \chi(a)w$ for all $a \in A$, $w \in W_\chi$. Since $A \lhd G$ is normal, the group G acts on the characters of A by the rule

$$g : A^\wedge \to A^\wedge , \quad \chi \mapsto \chi^g \stackrel{\text{def}}{=} \chi \circ \operatorname{Ad}_{g^{-1}} ,$$

where $\chi^g(a) = \chi(g^{-1}ag)$ for all $a \in A$. Moreover, every element $g \in G$ maps an isotypic component W_χ isomorphically onto the isotypic component W_{χ^g}, because

$$agw = gg^{-1}agw = g\chi^g(a)w = \chi^g(a)gw$$

for all $w \in W_\chi$, $a \in A$, $g \in G$. Since W is irreducible, the action of G on the components W_χ is transitive. Therefore, all the components have the same dimension, which divides $\dim W$. If there is just one component, i.e., $\operatorname{res} W = W_\chi$ for some $\chi \in A^\wedge$, then $\varrho(A)$ lies in the center $Z\big(\varrho(G)\big)$, because all elements of A act by scalar homotheties. By Theorem 10.1, $\dim W$ divides the index

$$\big[\varrho(G) : Z(\varrho(G))\big],$$

which divides the index $[\varrho(G) : \varrho(A)]$. The latter, in turn, divides $[G : A]$, because there is the epimorphism of quotient groups $G/A \twoheadrightarrow \varrho(G)/\varrho(A)$ provided by the homomorphism ϱ. If there are several different isotypic components in $\operatorname{res} W$, write W_η for one of them, and $H = \{g \in G \mid g(W_\eta) = W_\eta\}$ for its stabilizer in G. Then the total number of components equals $[G : H]$, and $H \subset G$ is a proper subgroup containing A and equipped with a linear representation in W_η. By induction on the order of G, we can assume that $\dim W_\eta$ divides the index $[H : A]$. Therefore, $\dim W = [G : H] \cdot \dim W_\eta$ divides $[G : A] = [G : H] \cdot [H : A]$. □

10.3 Algebraic Elements in Algebras

Let B be a commutative algebra with unit over an arbitrary field $\Bbbk$. Given an element $b \in B$, we write $\Bbbk[b] \subset B$ for the smallest $\Bbbk$-subalgebra containing 1 and b. In other words, $\Bbbk[b] = \operatorname{im}(\operatorname{ev}_b)$ is the image of the evaluation homomorphism

$$\operatorname{ev}_b : \Bbbk[x] \to B , \quad f \mapsto f(b) . \tag{10.5}$$

[9] See Sect. 5.4.2 on p. 111.

Recall[10] that b is said to be *transcendental* over $\Bbbk$ if $\ker \mathrm{ev}_b = 0$. In this case, $\Bbbk[b] \simeq \Bbbk[x]$ is infinite-dimensional as a vector space over $\Bbbk$ and is not a field. If $\ker \mathrm{ev}_b \neq 0$, i.e., $f(b) = 0$ for some nonzero polynomial $f \in \Bbbk[x]$, the element b is *algebraic*. In this case, $\ker(\mathrm{ev}_b) = (\mu_b)$ is the principal ideal in $\Bbbk[x]$ generated by the minimal polynomial of b over $\Bbbk$, and $\Bbbk[b] = \Bbbk[x]/(\mu_b)$ has dimension $\deg \mu_b$ as a vector space over $\Bbbk$. This dimension is called the *degree* of b over $\Bbbk$ and denoted by $\deg_{\Bbbk}(b)$. Note that algebraicity of b over $\Bbbk$ means the same as integrality. In particular, for algebraic b, the algebra $\Bbbk[b]$ is a field if and only if it has no zero divisors,[11] that is, if and only if the minimal polynomial μ_b is irreducible. This certainly holds if there are no zero divisors in B.

Recall[12] that a commutative $\Bbbk$-algebra B with unit is said to be *finitely generated* if there exist elements $b_1, b_2, \dots, b_m \in B$ such that the evaluation homomorphism

$$\mathrm{ev}_{b_1,b_2,\dots,b_m} : \Bbbk[x_1, x_2, \dots, x_m] \to B\,, \quad x_i \mapsto b_i \quad \text{for all } i = 1,\ 2,\ \dots\ ,\ m\,,$$

is surjective. In this case,

$$B = \Bbbk[x_1, x_2, \dots, x_m]/I,$$

where the ideal $I = \ker \mathrm{ev}_{b_1,b_2,\dots,b_m}$ consists of all *polynomial relations* between the *generators*[13] $b_1, b_2, \dots, b_m$ of the algebra B.

Theorem 10.3 *If a finitely generated commutative $\Bbbk$-algebra B is a field, then every element of B is algebraic over $\Bbbk$.*

Proof Let elements $b_1, b_2, \dots, b_m$ generate B as an algebra over $\Bbbk$. We proceed by induction on m. The case $m = 1$, $B = \Bbbk[b]$, was discussed above.[14] Consider $m > 1$. If b_m is algebraic over $\Bbbk$, then $\Bbbk[b_m]$ is a field. By induction, B is algebraic over $\Bbbk[b_m]$, and Proposition 10.1 forces B to be algebraic over $\Bbbk$ as well. Thus, it is enough to check that b_m actually is algebraic over $\Bbbk$.

Assume the contrary. Then the evaluation map (10.5) is injective for $b = b_m$, and is uniquely extended to an embedding of fields $\Bbbk(x) \hookrightarrow B$ by the universal property of the quotient field.[15] Write $\Bbbk(b_m) \subset B$ for the image of this embedding. This is the smallest subfield in B containing b_m. By induction, B is algebraic over $\Bbbk(b_m)$. Therefore, every generator b_i, $1 \leqslant i \leqslant m-1$, is a root of some polynomial with

[10] See Sect. 8.1.3 of Algebra I.

[11] See Proposition 10.3 on p. 229.

[12] See Sect. 5.2.4 of Algebra I.

[13] Generators of an algebra should be not confused with generators of a module. If elements $e_1, e_2, \dots, e_m$ span a ring B over a subring $A \subset B$ as a module, this means that B consists of finite A-linear combinations of these elements e_i, whereas if $b_1, b_2, \dots, b_m$ span B as an A-algebra, then B is formed by finite linear combinations of various monomials $b_1^{s_1} b_2^{s_2} \cdots b_m^{s_m}$.

[14] If b is not algebraic, then $\Bbbk[b] \simeq \Bbbk[x]$ is not a field.

[15] See Sect. 4.1.2 of Algebra I.

coefficients in $\Bbbk(b_m)$. Multiplying this polynomial by an appropriate polynomial in b_m allows us to assume that all $m-1$ polynomials annihilating the generators $b_1, b_2, \dots, b_{m-1}$ have coefficients in $\Bbbk[b_m]$ and share the same leading coefficient, which we denote by $p(b_m) \in \Bbbk[b_m]$. Thus, the field B is integral over the subalgebra $F = \Bbbk[b_m\,,\, 1/p(b_m)] \subset B$ spanned over $\Bbbk$ by the elements b_m and $1/p(b_m)$. By Proposition 10.3, F is a field. However, the element $1 + p(b_m)$ has no inverse in F. Indeed, if there exists a polynomial $g \in \Bbbk[x_1, x_2]$ such that

$$g\,(\,b_m\,,\ 1/p(b_m)\,) \cdot \big(1 + p(b_m)\big) = 1\,, \tag{10.6}$$

then we write the rational function $g\,(\,x\,,\ 1/p(x)\,)$ as $h(x)/p^k(x)$, where $h \in \Bbbk[x]$ is not divisible by p in $\Bbbk[x]$, and multiply both sides of (10.6) by $p^k(b_m)$, obtaining the polynomial relation

$$h(b_m) \cdot (\,p(b_m) + 1) = p^{k+1}(b_m)$$

in b_m. It is nontrivial, because $p(x)$ does not divide $h(x)(1 + p(x))$ in $\Bbbk[x]$. Contradiction. □

Corollary 10.3 *Let a field $\mathbb{F}$ be finitely generated as an algebra over a subfield $\Bbbk \subset \mathbb{F}$. Then $\mathbb{F}$ has finite dimension as a vector space over $\Bbbk$.*

Proof If $\mathbb{F}$ is generated as a $\Bbbk$-algebra by algebraic elements $b_1, b_2, \dots, b_m$, then the monomials $b_1^{s_1} b_2^{s_2} \cdots b_m^{s_m}$ with $0 \leqslant s_i < \deg_{\Bbbk} b_i$ span $\mathbb{F}$ linearly over $\Bbbk$. □

10.4 Transcendence Generators

Everywhere in this section, A means a finitely generated $\Bbbk$-algebra without zero divisors. We write Q_A for the field of fractions of A, and $\Bbbk(a_1, a_2, \dots, a_m) \subset Q_A$ for the smallest subfield containing given elements $a_1, a_2, \dots, a_m \in A$. Elements $a_1, a_2, \dots, a_m \in A$ are called *algebraically independent* if the evaluation homomorphism

$$\mathrm{ev}_{(a_1,a_2,\dots,a_m)} : \Bbbk[x_1, x_2, \dots, x_m] \to A\,,\ \ x_i \mapsto a_i,\ \ 1 \leqslant i \leqslant m\,, \tag{10.7}$$

is injective, i.e., if there are no polynomial relations among $a_1, a_2, \dots, a_m$. In this case, the evaluation map (10.7) can be uniquely extended to a field isomorphism

$$\Bbbk(x_1, x_2, \dots, x_m) \xrightarrow{\sim} \Bbbk(a_1, a_2, \dots, a_m) \subset Q_A\,,$$

which maps a rational function of $(x_1, x_2, \dots, x_m)$ to its value at $(a_1, a_2, \dots, a_m)$.

Elements $a_1, a_2, \dots, a_m \in A$ are called *transcendence generators* of A over $\Bbbk$ if every element of A is algebraic over $\Bbbk(a_1, a_2, \dots, a_m)$. In this case, the whole field Q_A is also algebraic over $\Bbbk(a_1, a_2, \dots, a_m)$, because the integral closure of

$\Bbbk(a_1, a_2, \dots, a_m)$ in Q_A is a field by Proposition 10.3, and Q_A is contained in every field containing A by the universal property of the field of fractions.

An algebraically independent collection $a_1, a_2, \dots, a_m$ of transcendence generators of A over $\Bbbk$ is called a *transcendence basis* of A over $\Bbbk$. Since every proper subset of a transcendence basis is algebraically independent, a transcendence basis can be equivalently characterized as a collection of transcendence generators minimal with respect to inclusions, or as a maximal algebraically independent collection.

Similarly to the bases of vector spaces, all transcendence bases of A have the same cardinality. The proof uses the same key lemma as the similar theorem for bases of vector spaces.[16]

Lemma 10.2 (Exchange Lemma) *Let elements $a_1, a_2, \dots, a_m$ be transcendence generators of A over $\Bbbk$, and let $b_1, b_2, \dots, b_n \in A$ be algebraically independent over $\Bbbk$. Then $n \leqslant m$, and after appropriate renumbering of the a_i and replacing the first n of them by $b_1, b_2, \dots, b_n$, the resulting elements $b_1, b_2, \dots, b_n$, $a_{n+1}, \dots, a_m$ are transcendence generators of A as well.*

Proof Since b_1 is algebraic over $\Bbbk(a_1, a_2, \dots, a_m)$, there is a polynomial relation

$$f(b_1,\, a_1, a_2, \dots, a_m) = 0\,, \quad f \in \Bbbk[x_1, x_2, \dots, x_{m+1}]\,.$$

Since b_1 is transcendental over $\Bbbk$, this relation contains some a_i. After appropriate renumbering, we can assume that $i = 1$. Then a_1, and therefore all of Q_A, is algebraic over $\Bbbk(b_1, a_2, \dots, a_m)$. Assume by induction that

$$b_1, \dots, b_k, a_{k+1}, \dots, a_m$$

are transcendence generators of A over $\Bbbk$ for $k < n$. Since b_{k+1} is algebraic over $\Bbbk\,(b_1, \dots, b_k, a_{k+1}, \dots, a_m)$, there is a polynomial relation

$$f\,(b_1, \dots, b_k, b_{k+1}, a_{k+1}, \dots, a_m) = 0\,, \quad f \in \Bbbk[x_1, x_2, \dots, x_{m+1}]\,.$$

It must contain some a_{k+i}, because of the algebraic independence of $b_1, b_2, \dots, b_n$ over $\Bbbk$. Hence $m > k$, and after renumbering of the remaining elements a_i, we can assume that a_{k+1} is algebraic over $\Bbbk\,(b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_m)$. Therefore, all of Q_A is algebraic over this field too. This completes the induction step. □

Corollary 10.4 *Let A be a finitely generated commutative $\Bbbk$-algebra without zero divisors. Then all transcendence bases of A over $\Bbbk$ have the same cardinality, every system of transcendence generators of A over $\Bbbk$ contains some transcendence basis, and every algebraically independent collection of elements in A can be included in a transcendence basis.* □

[16] Compare with the exchange lemma, Lemma 6.2, from Algebra I.

Definition 10.3 The cardinality of a transcendence basis of a finitely generated commutative $\Bbbk$-algebra A without zero divisors is called the *transcendence degree* of A and denoted by $\operatorname{tr}\deg_{\Bbbk} A$.

Example 10.4 Let $A \subset \Bbbk(t)$ be a $\Bbbk$-subalgebra different from $\Bbbk$. Then $\operatorname{tr}\deg_{\Bbbk} A = 1$. Indeed, for every

$$\psi = f(t)/g(t) \in A \smallsetminus \Bbbk\,,$$

the element t satisfies the algebraic equation $\psi \cdot g(x) - f(x) = 0$ with coefficients in $\Bbbk(\psi)$. This forces the whole of $\Bbbk(t)$ to be algebraic over $\Bbbk(\psi) \subset \mathbb{Q}_A$ and ψ to be transcendental over $\Bbbk$, because otherwise, t would be algebraic over $\Bbbk$. Thus every $\psi \in A \smallsetminus \Bbbk$ is a transcendence basis for both A and $\Bbbk(t)$.

Theorem 10.4 (Lüroth's Theorem) *Every subfield $\mathbb{F} \subset \Bbbk(t)$ containing $\Bbbk$ but different from $\Bbbk$ is a simple transcendental extension of $\Bbbk$, that is, $\mathbb{F} = \Bbbk(\psi)$ for some $\psi \in \Bbbk(t) \smallsetminus \Bbbk$.*

Proof By the previous example, t is algebraic over $\mathbb{F}$. Let

$$f(x) = x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m \in \mathbb{F}[x]$$

be the minimal polynomial of t over $\mathbb{F}$. The coefficients of f are rational functions in t, and at least one of them, say a_i, must be nonconstant, because t is transcendental over $\Bbbk$. We put $\psi = a_i$ and write it as g/h with $g, h \in \Bbbk[t]$, $\operatorname{GCD}(g, h) = 1$. Since t is annihilated by the nonzero polynomial $\psi h(x) - g(x) \in \mathbb{F}[x]$, this polynomial is divisible by f in $\mathbb{F}[x]$, that is, $\psi h(x) - g(x) = f(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$. Consider both sides to be polynomials in x with the coefficients in the field of fractions of the unique factorization domain $\Bbbk[x]$, and write them in the simplified form[17] $\frac{a}{b}C(x)$, where $a, b \in \Bbbk[t]$ are coprime and $C \in \Bbbk[t][x]$ has content[18] one. Then, by the uniqueness of the simplified form, the following equality in the polynomial ring $\Bbbk[t, x]$ holds, up to a constant factor:

$$g(t)h(x) - h(t)g(x) = F(x, t)Q(x, t)\,, \tag{10.8}$$

where the left-hand side comes from the simplified form of

$$\psi h(x) - g(x) = \frac{1}{h(t)}\big(g(t)h(x) - h(t)g(x)\big)\,,$$

---

[17] See Lemma 5.3 of Algebra I.

[18] Recall that the *content* of a polynomial with coefficients in a unique factorization domain is the greatest common divisor of all the coefficients; see Sect. 5.4.4 of Algebra I.

and the polynomials $F, Q \in \Bbbk[t][x]$ come from the simplified forms of f, q. Note that the degrees of $g(t)$ and $h(t)$ in t are not greater than that of F, because $a_i(t) = g(t)/h(t)$ is the coefficient of f. Hence, the polynomial $Q(x, t)$ in (10.8) does not depend on t. Since $\mathrm{GCD}(g(t), h(t)) = 1$, the left-hand side of (10.8) cannot be divisible by a nonconstant element of $\Bbbk[t]$. This forces $Q(x, t)$ to be a constant. Thus, $F(x, t) = g(t)h(x) - h(t)g(x)$. The symmetry in t, x forces F to be of degree m in t. Therefore, at least one of f, g has degree m, that is, t has degree m over $\Bbbk(\psi)$. Since $\Bbbk(\psi) \subset \mathbb{F}$ and $\dim_{\Bbbk(\psi)} \Bbbk(t) = m = \dim_{\mathbb{F}} \Bbbk(t)$, we conclude that $\Bbbk(\psi) = \mathbb{F}$. ☐

Problems for Independent Solution to Chapter 10

Problem 10.1 (Noetherian Modules) Recall[19] that a module M over a commutative ring K is called *Noetherian* if every submodule of M is finitely generated. Prove that:

(a) Every surjective endomorphism of M is an isomorphism.
(b) If M is Noetherian, then the quotient ring $K/\operatorname{Ann}(M)$ by the ideal

$$\operatorname{Ann}(M) \stackrel{\text{def}}{=} \{x \in K \mid xM = 0\}$$

is Noetherian.[20]

Problem 10.2 Let an A-module M be linearly generated by the elements

$$m_1, m_2, \dots, m_r \in M ,$$

and suppose the A-linear endomorphism $\varphi : M \to M$ maps these generators as

$$(m_1, m_2, \dots, m_r) \mapsto (m_1, m_2, \dots, m_r) \cdot F ,$$

where $F \in \mathrm{Mat}_{r\times r}(A)$. Verify that $\det(F) \cdot M \subset \varphi(M)$. Use this to prove that if M is *faithful*, meaning that $aM \neq 0$ for all nonzero $a \in A$, then $I \cdot M \neq M$ for every proper ideal $I \subsetneq A$.

Problem 10.3 Let $\mathbb{F} \supset \Bbbk$ be a field extension of finite degree. Prove that every finitely generated $\Bbbk$-subalgebra $A \subset \mathbb{F}$ is a field, and $\deg_{\Bbbk} A \mid \deg_{\Bbbk} \mathbb{F}$.

[19] Compare with Problem 14.1 from Algebra I.

[20] See Sect. 5.1.2 of Algebra I.

Problem 10.4 Describe the ring of integers of the field

$$\mathbb{Q}\left[\sqrt[7]{1}\right] = \mathbb{Q}[x]/\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right)$$

and compute the discriminant.

Problem 10.5 Determine whether the ring $\Bbbk[x, y]$ is integral over the subring of polynomials f with $\frac{\partial f}{\partial x} f(0, 0) = 0$.

Problem 10.6 Is the ring of all continuous functions $\mathbb{R}^2 \to \mathbb{R}$ integral over the subring of all f with $f(1, 0) = f(0, 1)$?

Problem 10.7 Let $\Bbbk$ be a field, $a_1, a_2, \dots, a_n \in \Bbbk$, and $f \in \Bbbk[x_0, x_1, \dots, x_n]$. Consider the homomorphism

$$\psi : \Bbbk[t_1, t_2, \dots, t_n] \hookrightarrow \Bbbk[x_0, x_1, \dots, x_n], \quad t_i \mapsto x_i + a_i x_0 .$$

For which f and $a_1, a_2, \dots, a_n$ is the quotient ring $\Bbbk[x_0, x_1, \dots, x_n]/(f)$ integral over $\operatorname{im}(\psi) \pmod f$?

Problem 10.8 Let $\Bbbk$ be an infinite field and $f \in \Bbbk[x_1, x_2, \dots, x_n]$ a nonconstant polynomial. Find $\operatorname{tr}\deg_{\Bbbk} \Bbbk[x_1, x_2, \dots, x_n]/(f)$.

Problem 10.9 Let $B \supset A$ be an integral extension of rings and $\Bbbk$ an algebraically closed field. Show that every homomorphism $A \to \Bbbk$ can be extended to a homomorphism $B \to \Bbbk$.

Problem 10.10 Prove that every irreducible character of a finite group of dimension greater than 1 takes the zero value at some conjugacy class.

Problem 10.11 Let the quotient ring $\mathbb{Z}[x_1, x_2, \dots, x_n]/I$ be a field. Prove that it is finite.

Problem 10.12 Let $\Bbbk$ be an arbitrary field and

$$\psi = f/g \in \Bbbk(t), f, g \in \Bbbk[t], \operatorname{GCD}(f, g) = 1,$$

a nonconstant rational function. Prove that:

(a) $\Bbbk(t)$ has dimension $\max(\deg f, \deg g)$ as a vector space over $\Bbbk(\psi)$.
(b) $\Bbbk(\psi) = \Bbbk(t)$ if and only if $\psi = (at + b)/(ct + d)$ is a linear fractional function.
(c) The group $\operatorname{Aut}_{\Bbbk} \Bbbk(t) = \{\varphi : \Bbbk(t) \xrightarrow{\sim} \Bbbk(t) \mid \varphi|_{\Bbbk} = \mathrm{Id}_{\Bbbk}\}$, of automorphisms of the field $\Bbbk(t)$ acting identically on the field $\Bbbk$, is isomorphic to $\mathrm{PGL}_2(\Bbbk)$.

Problem 10.13 Let $\mathbb{F} \supset \mathbb{C}$ be a field linearly generated over $\mathbb{C}$ by at most a countable set of elements. Prove that $\mathbb{F} = \mathbb{C}$.

Problem 10.14* Let A be a normal ring. Prove that the polynomial ring $A[x]$ is normal too.

Chapter 11
Affine Algebraic Geometry

In this chapter we assume by default that $\Bbbk$ is an algebraically closed field.

11.1 Systems of Polynomial Equations

Every system of polynomial equations

$$f_\nu(x_1, x_2, \dots, x_n) = 0\,, \quad f_\nu \in \Bbbk[x_1, x_2, \dots, x_n]\,, \tag{11.1}$$

can be extended to a system whose left-hand sides form the ideal

$$J \subset \Bbbk[x_1, x_2, \dots, x_n]$$

spanned by the polynomials f_ν appearing in (11.1). The extended infinite system has the same set of solutions in the affine space $\mathbb{A}^n = \mathbb{A}(\Bbbk^n)$ as the original system, because the equalities $f_\nu = 0$ imply the equalities $\sum_\nu g_\nu f_\nu = 0$ for all $g_\nu \in \Bbbk[x_1, x_2, \dots, x_n]$. Since the polynomial ring is Noetherian,[1] the system $f = 0, f \in J$, is equivalent to a finite subsystem consisting of equations whose left-hand sides generate J. Moreover, this finite set of generators can be chosen among the original polynomials[2] f_ν from (11.1). Thus, every (even infinite) system of polynomial equations is always equivalent, on the one hand, to some finite subsystem, and on the other hand, to a system of equations $f = 0$, where f runs through some ideal in $\Bbbk[x_1, x_2, \dots, x_n]$.

Given an ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$, its zero set

$$V(J) \stackrel{\text{def}}{=} \{a \in \mathbb{A}^n \mid \forall\,, f \in J\, f(a) = 0\}$$

[1] See Sect. 5.1.2 of Algebra I.

[2] See Lemma 5.1 of Algebra I.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_11

is called the *affine algebraic variety*[3] determined by J. Note that $V(J)$ may be empty. This happens, for example, if $J = (1) = \Bbbk[x_1, x_2, \dots, x_n]$ contains the equation $1 = 0$.

Associated with an arbitrary subset $\Phi \subset \mathbb{A}^n$ is the ideal

$$I(\Phi) \stackrel{\text{def}}{=} \{f \in \Bbbk[x_1, x_2, \dots, x_n] \mid f(p) = 0 \text{ for all } p \in \Phi\},$$

called the *ideal of* Φ. Its zero set $V(I(\Phi))$ is the smallest affine algebraic variety containing Φ. For every ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$, there is the tautological inclusion

$$J \subset I(V(J)).$$

In general, it is proper. Say for $n = 1$, the ideal $J = (x^2) \subset \Bbbk[x]$ determines the variety $V(x^2) = \{0\} \subset \mathbb{A}^1$, whose ideal $I(V(x^2))$ is equal to $(x) \supsetneq (x^2)$.

Theorem 11.1 (Hilbert's Nullstellensatz) *Let $\Bbbk$ be an algebraically closed field, $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ an ideal, $\sqrt{J} \stackrel{\text{def}}{=} \{f \mid \exists\, m \in \mathbb{N} : f^m \in J\}$ the radical*[4] *of J. Then $I(V(J)) = \sqrt{J}$ (the strong Nullstellensatz). In particular, $V(J) = \varnothing$ if and only if $1 \in J$ (the weak Nullstellensatz).*

Proof Let us prove the weak Nullstellensatz first. It is enough to show that for every proper ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$, there exists a point $p \in \mathbb{A}^n$ such that $f(p) = 0$ for all $f \in J$. Without loss of generality, the ideal J can replaced by a *maximal*[5] proper ideal $\mathfrak{m} \supset J$. Then the quotient ring $\Bbbk[x_1, x_2, \dots, x_n]/\mathfrak{m}$ is a field, finitely generated as a $\Bbbk$-algebra. By Theorem 10.3, every element $\vartheta \in \Bbbk[x_1, x_2, \dots, x_n]/\mathfrak{m}$ is algebraic over $\Bbbk$, i.e., satisfies an equation $\mu(\vartheta) = 0$ for a monic irreducible polynomial $\mu \in \Bbbk[t]$. Since $\Bbbk$ is algebraically closed, the polynomial μ has to be linear, that is, $\vartheta \in \Bbbk$. Therefore, every polynomial is congruent modulo $\mathfrak{m}$ to a constant. Write $p_i \in \Bbbk$ for the constant congruent to x_i. Then the factorization homomorphism $\Bbbk[x_1, x_2, \dots, x_n] \to \Bbbk[x_1, x_2, \dots, x_n]/\mathfrak{m} \simeq \Bbbk$ maps every polynomial $f(x_1, x_2, \dots, x_n)$ to the class of constant $f(p_1, p_2, \dots, p_n) \in \Bbbk$. Since all $f \in \mathfrak{m}$ are mapped to zero, they all vanish at $p = (p_1, p_2, \dots, p_n) \in \mathbb{A}^n$, as desired.

The strong Nullstellensatz is trivial for $V(J) = \varnothing$. Assume that $V(J) \neq \varnothing$, that is, $J \neq (1)$. Consider $\mathbb{A}^n$ to be the hyperplane $t = 0$ in the affine space $\mathbb{A}^{n+1}$ with coordinates

$$(t,\ x_1, x_2, \dots, x_n).$$

[3] Compare with Sect. 11.2.4 of Algebra I.

[4] See Problem 5.6 of Algebra I.

[5] See Sect. 5.2.2 of Algebra I.

If a polynomial $f \in \Bbbk[x_1, x_2, \dots, x_n] \subset \Bbbk[t,\ x_1, x_2, \dots, x_n]$ vanishes everywhere on the cylinder $V(J) \subset \mathbb{A}^{n+1}$, then the polynomial $g(t,x) = 1 - tf(x)$ equals 1 at every point of $V(J)$. Therefore, the ideal spanned in $\Bbbk[t,\ x_1, x_2, \dots, x_n]$ by J and $g(t,x)$ has empty zero set in $\mathbb{A}^{n+1}$. By the weak Nullstellensatz, this ideal contains 1, i.e., there exist $q_0, q_1, \dots, q_s \in \Bbbk[t,\ x_1, x_2, \dots, x_n]$ and $f_1, f_2, \dots, f_s \in J$ such that

$$q_0(x,t) \cdot \big(1 - tf(x)\big) + q_1(t,x) \cdot f_1(x) + \cdots + q_s(x,t) \cdot f_s(x) = 1\,. \tag{11.2}$$

The homomorphism $\Bbbk[t,\ x_1, x_2, \dots, x_n] \to \Bbbk(x_1, x_2, \dots, x_n)$ acting on the variables by the rules

$$t \mapsto 1/f(x)\,, \quad x_\nu \mapsto x_\nu\,, \quad \text{for } 1 \leqslant \nu \leqslant n\,,$$

maps the equality (11.2) to the following equality in the field $\Bbbk(x_1, x_2, \dots, x_n)$:

$$q_1\big(1/f(x)\,,\,x\big) \cdot f_1(x) + \cdots + q_s\big(1/f(x)\,,\,x\big) \cdot f_s(x) = 1\,. \tag{11.3}$$

Since $1 \notin J$, some $q_\nu\big(1/f(x), x\big)$ have nontrivial denominators. All these denominators are canceled via multiplication by f^m for some $m \in \mathbb{N}$. Multiplying both sides by this f^m leads to the required equality

$$f^m(x) = \widetilde{q}_1(x) \cdot f_1(x) + \cdots + \widetilde{q}_s(x) \cdot f_s(x)$$

with $\widetilde{q}_\nu \in \Bbbk[x_1, x_2, \dots, x_n]$. □

11.2 Affine Algebraic–Geometric Dictionary

A map $\varphi : X \to Y$ between affine algebraic varieties $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ is called *regular* or *polynomial* if its action is described in coordinates by the rule $(x_1, x_2, \dots, x_n) \mapsto \big(\varphi_1(x), \varphi_2(x), \dots, \varphi_m(x)\big)$, where $\varphi_i(x) \in \Bbbk[x_1, x_2, \dots, x_n]$. We write $\mathcal{A}\!f\!f_{\Bbbk}$ for the category of affine algebraic varieties and regular maps between them.

11.2.1 Coordinate Algebra

A function $f : X \to \Bbbk$ on an affine algebraic variety $X \subset \mathbb{A}^n$ is called *regular* if it provides X with a regular map $f : X \to \mathbb{A}^1$, that is, if there exists some polynomial in the coordinates $x_1, x_2, \dots, x_n$ on $\mathbb{A}^n$ whose restriction to X coincides with f. Two polynomials determine the same regular function if and only if they are congruent modulo the ideal $I(X) = \{f \in \Bbbk[x_1, x_2, \dots, x_n] \mid f|_X \equiv 0\}$. The regular functions

$X \to \Bbbk$ form a $\Bbbk$-algebra with respect to the usual addition and multiplication of functions taking values in a field. This algebra is denoted by

$$\Bbbk[X] \stackrel{\text{def}}{=} \operatorname{Hom}_{\mathcal{A}ff_{\Bbbk}}\left(X, \mathbb{A}^1\right) \simeq \Bbbk[x_1, x_2, \dots, x_n]/I(X) \tag{11.4}$$

and called the *coordinate algebra* of X. Note that $\Bbbk[X]$ is *reduced*,[6] because $f^n = 0$ only for the zero function $f : X \to \Bbbk$. This forces the ideal $I(X)$ to be *radical*, i.e., to have $\sqrt{I(X)} = I(X)$, which agrees with the strong Nullstellensatz.

Lemma 11.1 *Every reduced finitely generated algebra A over an algebraically closed field $\Bbbk$ is isomorphic to the coordinate algebra $\Bbbk[X]$ of some affine algebraic variety X over $\Bbbk$.*

Proof Write A as a quotient $A = \Bbbk[x_1, x_2, \dots, x_n]/J$. Since A is reduced, $\sqrt{J} = J$. By the strong Nullstellensatz, this forces J to coincide with the ideal $I(V(J))$ of the affine algebraic variety $V(J) \subset \mathbb{A}^n$. Therefore, $A = \Bbbk[X]$ for $X = V(J)$. $\square$

11.2.2 Maximal Spectrum

Associated with every point $p \in X$ of an affine algebraic variety X is the *evaluation homomorphism* $\mathrm{ev}_p : \Bbbk[X] \to \Bbbk, f \mapsto f(p)$. It is obviously surjective, and therefore, its kernel

$$\mathfrak{m}_p \stackrel{\text{def}}{=} \ker \mathrm{ev}_p = \{f \in \Bbbk[X] \mid f(p) = 0\}$$

is a maximal ideal in $\Bbbk[X]$. It is called the *maximal ideal of the point* $p \in X$. Note that for every $g \in \Bbbk[X]$, the residue class $g \pmod{\mathfrak{m}_p}$ coincides in $\Bbbk[X]/\mathfrak{m}_p \simeq \Bbbk$ with the class of constant $g(p)$, i.e., the evaluation at p can be thought of as the factorization modulo the ideal $\mathfrak{m}_p \subset \Bbbk[X]$.

Given an arbitrary commutative $\Bbbk$-algebra A, the set of all maximal ideals $\mathfrak{m} \subset A$ is called the *maximal spectrum* of A and denoted by $\operatorname{Spec}_{\mathrm{m}}(A)$. If A is finitely generated, then for every $\mathfrak{m} \in \operatorname{Spec}_{\mathrm{m}} A$, the quotient $A/\mathfrak{m} \supset \Bbbk$ is a field, finitely generated as a $\Bbbk$-algebra. By Theorem 10.3, it must be an algebraic extension of $\Bbbk$. For algebraically closed $\Bbbk$, this forces $A/\mathfrak{m} = \Bbbk$ and allows one to interpret every element $a \in A$ as a function $a : \operatorname{Spec}_{\mathrm{m}} A \to \Bbbk$, $\mathfrak{m} \mapsto a \pmod{\mathfrak{m}} \in A/\mathfrak{m} = \Bbbk$.

Lemma 11.2 *For every affine algebraic variety X over an algebraically closed field $\Bbbk$, the maps*

$$p \mapsto \mathrm{ev}_p \mapsto \mathfrak{m}_p = \ker(\mathrm{ev}_p)$$

[6] That is, has no nilpotent elements; see Sect. 2.4.2 of Algebra I.

establish canonical bijections between the points of X, $\mathbb{k}$-algebra homomorphisms $\mathbb{k}[X] \to \mathbb{k}$, and maximal ideals $\mathfrak{m} \subset \mathbb{k}[X]$.

Proof For every finitely generated algebra A over an algebraically closed field $\mathbb{k}$, the maximal ideals $\mathfrak{m} \in \operatorname{Spec}_{\mathrm{m}} A$ are in bijection with the $\mathbb{k}$-algebra homomorphisms $\varphi : A \to \mathbb{k}$. Namely, since[7] $\varphi(1) = 1$, every homomorphism $\varphi : A \to \mathbb{k}$ is surjective, and therefore, its kernel $\ker \varphi$ is a maximal ideal in A. Conversely, for every maximal ideal $\mathfrak{m} \subset A$, the quotient map $\varphi : A \twoheadrightarrow A/\mathfrak{m}$ takes values in the field $A/\mathfrak{m} \supset \mathbb{k}$, which is algebraic over $\mathbb{k}$ and therefore coincides with $\mathbb{k}$ if $\mathbb{k}$ is algebraically closed.[8] This proves the bijectivity of the second map from the lemma.

The first map $X \to \operatorname{Spec}_{\mathrm{m}} \mathbb{k}[X]$, $p \mapsto \mathfrak{m}_p = \ker \mathrm{ev}_p$, is injective regardless of whether $\mathbb{k}$ is algebraically closed, because for $p \neq q$, there exists, for example, an affine linear function $f : \mathbb{A}^n \to \mathbb{k}$ vanishing at p and equal to 1 at q. It remains to show that over an algebraically closed field $\mathbb{k}$, every maximal ideal $\mathfrak{m} \subset \mathbb{k}[X]$ coincides with $\mathfrak{m}_p = \ker \mathrm{ev}_p$ for some $p \in X$. Write $\widetilde{\mathfrak{m}} \subset \mathbb{k}[x_1, x_2, \dots, x_n]$ for the full preimage of $\mathfrak{m}$ under the factorization homomorphism

$$\mathbb{k}[x_1, x_2, \dots, x_n] \twoheadrightarrow \mathbb{k}[X] = \mathbb{k}[x_1, x_2, \dots, x_n]/I(X).$$

Since $\mathbb{k}[x_1, x_2, \dots, x_n]/\widetilde{\mathfrak{m}} = \mathbb{k}[X]/\mathfrak{m} = \mathbb{k}$, the ideal $\widetilde{\mathfrak{m}}$ is proper (in fact, maximal), and by construction, it contains $I(X)$. By the weak Nullstellensatz, $V(\widetilde{\mathfrak{m}}) \neq \varnothing$. Let $p \in V(\widetilde{\mathfrak{m}})$. Then $p \in X$, because $I(X) \subset \widetilde{\mathfrak{m}}$. Since $\mathfrak{m}$ is maximal, the inclusion $\mathfrak{m} \subset \mathfrak{m}_p$ implies the equality $\mathfrak{m} = \mathfrak{m}_p$. □

Agreement 11.1 In what follows, we will identify the morphisms $A \to \mathbb{k}$ with their kernels and write $\operatorname{Spec}_{\mathrm{m}} A$ for both the sets of maximal ideals $\mathfrak{m} \subset A$ and $\mathbb{k}$-algebra homomorphisms $A \to \mathbb{k}$.

Exercise 11.1 Establish a natural bijection between $\operatorname{Spec}_{\mathrm{m}} \mathbb{k}[x_1, x_2, \dots, x_n]$ and $\mathbb{A}^n = \mathbb{A}(\mathbb{k}^n)$.

Definition 11.1 (Nilradical and Jacobson Radical) Let A be a commutative ring. The radical of the zero ideal in A, that is, the set of all nilpotent elements[9] of A together with the zero element, is called the *nilradical* of A and denoted by

$$\mathfrak{n}(A) \stackrel{\text{def}}{=} \sqrt{0} = \{a \in A \mid a^n = 0 \text{ for some } n \in \mathbb{N}\} .$$

[7] See Lemma 2.5 of Algebra I.

[8] If $\mathbb{k}$ is not algebraically closed, then the map $\varphi \mapsto \ker \varphi$ still embeds the set of homomorphisms $\mathbb{k}[X] \to \mathbb{k}$ into $\operatorname{Spec}_{\mathrm{m}} A$. However, some maximal ideals $\mathfrak{m} \subset A$ may not be represented as the kernels of homomorphisms $A \to \mathbb{k}$. For example, the kernel of the evaluation $\mathrm{ev}_i : \mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(i)$, where $i \in \mathbb{C}$, $i^2 = -1$, certainly is a maximal ideal in $\mathbb{R}[x]$, but it cannot be realized as the kernel of a homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{R}$, because for the latter, $\mathbb{R}[x]/\ker \varphi = \mathbb{R}$, whereas $\mathbb{R}[x]/\ker \mathrm{ev}_i = \mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

[9] See Sect. 2.4.2 of Algebra I.

The intersection of all maximal ideals in A is called the *Jacobson radical* of A and denoted by $\mathfrak{r}(A)$.

Exercise 11.2 Check that $\mathfrak{n}(A)$ is an ideal in A.

Corollary 11.1 *Let A be a finitely generated algebra over an algebraically closed field $\Bbbk$. Then $\mathfrak{n}(A) = \mathfrak{r}(A)$. In other words, the nilradical of A coincides with the kernel of the homomorphism $A \to \Bbbk^{\operatorname{Spec}_{\mathrm{m}} A}$ sending every element $a \in A$ to the function $a : \operatorname{Spec}_{\mathrm{m}} A \to \Bbbk$, $\mathfrak{m} \mapsto a \pmod{\mathfrak{m}} \in A/\mathfrak{m} = \Bbbk$.*

Proof Since $A/\mathfrak{m}$ is a field for all $\mathfrak{m} \in \operatorname{Spec}_{\mathrm{m}} A$, all nilpotent elements of A are annihilated by every quotient map $A \twoheadrightarrow A/\mathfrak{m}$ with $\mathfrak{m} \in \operatorname{Spec}_{\mathrm{m}} A$. Therefore, $\mathfrak{n}(A) \subset \mathfrak{r}(A)$. To prove the converse inclusion, let $A_{\mathrm{red}} \stackrel{\mathrm{def}}{=} A/\mathfrak{n}(A)$. Since A_{red} is finitely generated and reduced, there exists an affine algebraic variety $X \subset \mathbb{A}^n$ with the coordinate algebra $\Bbbk[X] = \Bbbk[x_1, x_2, \dots, x_n]/I(X) \simeq A_{\mathrm{red}}$. If $a \in \mathfrak{r}(A)$, then the class of a in A_{red} belongs to $\mathfrak{r}(A_{\mathrm{red}})$. This means that $a(p) = 0$ for all $p \in X$, and forces $a = 0$ in A_{red}. Hence, $a \in \mathfrak{n}(A)$. $\square$

Exercise 11.3 For every commutative ring A with unit, show that $\mathfrak{n}(A)$ coincides with the intersection of all prime[10] ideals in A.

11.2.3 Pullback Homomorphisms

Associated with every map of sets $\varphi : X \to Y$ is the *pullback homomorphism* $\varphi^* : \Bbbk^Y \to \Bbbk^X$, which maps a function $f : Y \to \Bbbk$ to the composition

$$f \circ \varphi : X \to \Bbbk \,.$$

Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be affine algebraic varieties with the coordinate algebras

$$\Bbbk[X] = \Bbbk[x_1, x_2, \dots, x_n]/I(X)\,, \quad \Bbbk[Y] = \Bbbk[y_1, y_2, \dots, y_m]/I(Y)\,,$$

and let the map $\varphi : X \to Y$ be given in coordinates by the assignment

$$(x_1, x_2, \dots, x_n) \mapsto (\varphi_1(x),\ \varphi_2(x),\ \dots\ ,\ \varphi_m(x))\ .$$

Then the pullbacks of the coordinate functions $y_i : Y \to \Bbbk$ are $\varphi^*(y_i) = \varphi_i$. Since the y_i generate the coordinate algebra $\Bbbk[Y]$, the regularity of φ, meaning that

[10] Recall that an ideal $\mathfrak{p} \subset A$ is called *prime* if the quotient ring $A/\mathfrak{p}$ has no zero divisors; see Sect. 5.2.3 of Algebra I.

$\varphi_i(x) \in \Bbbk[x_1, x_2, \dots, x_n]$, is equivalent to the inclusion $\varphi^*(\Bbbk[Y]) \subset \Bbbk[X]$, meaning that the pullback of every regular function is regular.

Exercise 11.4 Verify that a set-theoretic map of topological spaces (respectively smooth or analytic manifolds) $X \to Y$ is continuous (respectively smooth or analytic) if and only if the pullback of every continuous (respectively smooth or analytic) function on Y is a continuous (respectively smooth or analytic) function on X.

Note that the inclusion of sets $\varphi(X) \subset Y$ implies the inclusion of ideals

$$\varphi^*\big(I(Y)\big) \subset I(X)\,,$$

which forces the map $\Bbbk[y_1, y_2, \dots, y_m] \to \Bbbk[x_1, x_2, \dots, x_n]$, $y_i \mapsto \varphi_i(x_1, x_2, \dots, x_n)$, to be correctly factorized through the map

$$\Bbbk[Y] = \Bbbk[y_1, y_2, \dots, y_m]/I(Y) \to \Bbbk[x_1, x_2, \dots, x_n]/I(X) = \Bbbk[X]\,.$$

Theorem 11.2 *Let $\Bbbk$ be an algebraically closed field. Write $\mathcal{A}lg_{\Bbbk}$ for the category of finitely generated reduced $\Bbbk$-algebras with unit and $\Bbbk$-algebra homomorphisms respecting the units. Then the representable presheaf*

$$h_{\mathbb{A}^1} : \mathcal{A}\!f\!f_{\Bbbk}^{\mathrm{opp}} \to \mathcal{A}lg_{\Bbbk}\,, \quad X \mapsto \mathrm{Hom}_{\mathcal{A}\!f\!f_{\Bbbk}}(X, \mathbb{A}^1) = \Bbbk[X]\,, \tag{11.5}$$

which sends a regular map of affine algebraic varieties $\varphi : X \to Y$ to the pullback homomorphism of their coordinate algebras $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$, is an equivalence of categories.

Proof By Proposition 9.1 on p. 199, we have to show that the functor (11.5) is essentially surjective and fully faithful. The first statement was established in Lemma 11.1 on p. 244. To prove the second, consider the representable presheaf

$$h_{\Bbbk} : \mathcal{A}lg_{\Bbbk} \to \mathcal{S}et\,, \quad A \mapsto \mathrm{Hom}_{\mathcal{A}lg_{\Bbbk}}(A\,, \Bbbk) \simeq \mathrm{Spec}_{\mathrm{m}} A\,. \tag{11.6}$$

It sends a homomorphism of $\Bbbk$-algebras $\psi : A \to B$ to the pullback map

$$\psi^* : \mathrm{Spec}_{\mathrm{m}} B \to \mathrm{Spec}_{\mathrm{m}} A\,,$$

which takes the $\Bbbk$-algebra epimorphism $\mathrm{ev} : B \to \Bbbk$ with kernel $\mathfrak{m} \in \mathrm{Spec}_{\mathrm{m}} B$ to the $\Bbbk$-algebra epimorphism $\psi^*(\mathrm{ev}) = \mathrm{ev} \circ \psi$ with kernel $\psi^{-1}(\mathfrak{m}) \in \mathrm{Spec}_{\mathrm{m}} \Bbbk[X]$. We claim that the maps

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{A}\!f\!f_{\Bbbk}}(X, Y) \arrow[r, shift left, "\varphi \mapsto \varphi^*"] & \mathrm{Hom}_{\mathcal{A}lg_{\Bbbk}}\big(\Bbbk[Y], \Bbbk[X]\big) \arrow[l, shift left, "\psi^* \leftarrow\!\shortmid\, \psi"] \end{tikzcd}$$

are bijections that are inverse to each other. Indeed, let a regular morphism from $X \subset \mathbb{A}^n$ to $Y \subset \mathbb{A}^m$ act by the rule $(x_1, x_2, \dots, x_n) \mapsto (\varphi_1(x), \varphi_2(x), \dots, \varphi_m(x))$ for some $\varphi_i(x) \in \Bbbk[x_1, x_2, \dots, x_n]$. Then its pullback $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ maps $y_i \mapsto \varphi_i \pmod{I(X)}$. The pullback of φ^*, that is, the map

$$\varphi^{**} : \operatorname{Spec_m} \Bbbk[X] \to \operatorname{Spec_m} \Bbbk[Y],$$

sends the evaluation at a point $p = (p_1, p_2, \dots, p_n) \in X$,

$$\mathrm{ev}_p : \Bbbk[X] \to \Bbbk, \quad f(x) \mapsto f(p),$$

to its composition with φ^*. This composition takes every generator $y_i \in \Bbbk[Y]$ to $\varphi_i(p)$, and therefore coincides with the evaluation map at the point $\varphi(p)$. Thus, we have $\varphi^{**} = \varphi$. The equality $\psi^{**} = \psi$ for every homomorphism $\psi : \Bbbk[Y] \to \Bbbk[X]$ is checked similarly, and we leave its verification to the reader as an exercise. □

Remark 11.1 It follows from Lemma 11.2 that the functor (11.6) is almost quasi-inverse to the functor (11.5). Namely, it maps every coordinate algebra $A = \Bbbk[X]$ to the *set* $\operatorname{Spec_m} A$, in bijection with the set of points of the variety X. In fact, the set $\operatorname{Spec_m} A$ admits many different but isomorphic structures of an affine algebraic variety, where such a structure is understood as an injective map of sets $\varphi : \operatorname{Spec_m} A \hookrightarrow \mathbb{A}^n$ whose pullback homomorphism establishes a well-defined surjection $\varphi^* : \Bbbk[\mathbb{A}^n] \twoheadrightarrow A$ such that $V(\ker \varphi^*) = \varphi(\operatorname{Spec_m} A)$. The choice of such a structure is equivalent to the choice of a presentation of A by means of generators and relations, that is, to the choice of an isomorphism $A \simeq \Bbbk[x_1, x_2, \dots, x_n]/I$.

Example 11.1 (Line and Hyperbola) The points of $\operatorname{Spec_m} \Bbbk[t]$ are in bijection with the points of the affine line $\mathbb{A}^1 = \Bbbk$. Indeed, every homomorphism $\mathrm{ev} : \Bbbk[t] \to \Bbbk$ is uniquely determined by its value at the generator t, that is, uniquely determined by the point $\mathrm{ev}(t) = p \in \Bbbk$. In other words, every maximal ideal $\mathfrak{m} \subset \Bbbk[t]$ is a principal ideal of the form $(t - p)$ for a point $p \in \Bbbk$, uniquely determined by $\mathfrak{m}$. Similarly, for the algebra of Laurent polynomials, the points of $\operatorname{Spec_m} \Bbbk\left[t, t^{-1}\right]$ are in bijection with the points of the punctured line $\mathbb{A}^1 \smallsetminus \{0\} = \Bbbk^*$, because the value $p = \mathrm{ev}(t) = 1/\mathrm{ev}(t^{-1})$ can be equal to any invertible element of $\Bbbk$. If we present the algebra of Laurent polynomials by generators and relations, that is, write it as $\Bbbk[x, y]/(xy - 1)$ using the isomorphism

$$\varphi^* : \Bbbk[t, t^{-1}] \xrightarrow{\sim} \Bbbk[x, y]/(xy - 1), \quad t \mapsto x, \quad t^{-1} \mapsto y, \tag{11.7}$$

then we get the coordinate algebra of the hyperbola $xy = 1$ in the affine plane $\mathbb{A}^2$ with coordinates (x, y), i.e., we realize the same spectrum as the variety $V(xy - 1) \subset \mathbb{A}^2$. The pullback of the algebra homomorphism (11.7) maps $V(xy - 1) \xrightarrow{\sim} \mathbb{A}^1 \smallsetminus \{0\}$ via the projection of $\mathbb{A}^2$ onto the x-axis along the y-axis.

Example 11.2 (Coproduct of Affine Algebraic Varieties) Since the direct product of $\Bbbk$-algebras $\Bbbk[X] \times \Bbbk[Y]$ certainly is reduced and finitely generated, it yields the categorical direct product[11] in $\mathcal{A}lg_{\Bbbk}$. Therefore, the equivalence of Theorem 11.2 forces $\mathrm{Spec_m}\big(\Bbbk[X] \times \Bbbk[Y]\big)$ to be the categorical direct coproduct[12] in $\mathcal{A}\!f\!f_{\Bbbk}$. We conclude that for all affine algebraic varieties $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$, their disjoint union $X \sqcup Y$ admits a structure of an affine algebraic variety whose coordinate algebra is isomorphic to $\Bbbk[X] \times \Bbbk[Y]$.

Exercise 11.5 Prove directly that $\mathrm{Spec_m}\big(\Bbbk[X] \times \Bbbk[Y]\big) \simeq \mathrm{Spec_m}\,\Bbbk[X] \sqcup \mathrm{Spec_m}\,\Bbbk[Y]$ and try to describe $X \sqcup Y$ by explicit polynomial equations in some affine space $\mathbb{A}^k$ under the assumption that the equations for $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are known.

Example 11.3 (Product of Affine Algebraic Varieties) Given two $\Bbbk$-algebras A, B, let us equip the tensor product of vector spaces $A \otimes B$ with the multiplication defined by $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) \stackrel{\text{def}}{=} (a_1 a_2) \otimes (b_1 b_2)$.

Exercise 11.6 Verify that $A \otimes B$ becomes a commutative $\Bbbk$-algebra with unit $1 \otimes 1$, and the $\Bbbk$-algebra homomorphisms $A \hookrightarrow A \otimes B \hookleftarrow B$, $a \mapsto a \otimes 1$, $b \mapsto 1 \otimes b$, give the direct coproduct in the category of commutative $\Bbbk$-algebras with unit.

It follows from the universal property of the coproduct that there exists a bijection

$$\mathrm{Spec_m}(A) \times \mathrm{Spec_m}(B) \simeq \mathrm{Spec_m}(A \otimes B)$$

sending a pair of homomorphisms $\mathrm{ev}_p : A \to \Bbbk$, $a \mapsto a(p)$ and $\mathrm{ev}_q : B \to \Bbbk$, $b \mapsto b(q)$, to the homomorphism $A \otimes B \to \Bbbk$, $a \otimes b \mapsto a(p)b(q)$. If the algebras A, B are finitely generated, say by some elements $a_1, a_2, \dots, a_n \in A$, $b_1, b_2, \dots, b_m \in B$, then $A \otimes B$ is certainly generated by the elements $a_i \otimes b_j$. Let us show that the tensor product of reduced algebras A, B is reduced. Assume that an element $h \in A \otimes B$ evaluates to zero at every point of $\mathrm{Spec_m}(A \otimes B)$. It is enough to check that $h = 0$. To this end, write h as $\sum f_\nu \otimes g_\nu$, where $g_\nu \in B$ are linearly independent over $\Bbbk$. Since $(\mathrm{ev}_p \otimes \mathrm{ev}_q)h = 0$ for all $(p, q) \in \mathrm{Spec_m}(A \otimes B)$, a linear combination $\sum f_\nu(p) \cdot g_\nu \in B$ is the zero function on $\mathrm{Spec_m}\,B$ for every fixed $p \in \mathrm{Spec_m}\,A$. Since B is reduced, this linear combination is the zero element of B. Therefore, all its coefficients $f_\nu(p)$ are zero, because of the linear independence of g_ν. Since this holds for all $p \in \mathrm{Spec}\,A$, every element $f_\nu \in A$ is the zero function on $\mathrm{Spec_m}\,A$. This forces $f_\nu = 0$, because A is reduced. Hence, $h = 0$.

We conclude that the tensor product $\Bbbk[X] \otimes \Bbbk[Y]$ gives the direct coproduct in $\mathcal{A}lg_{\Bbbk}$. Therefore, $\mathrm{Spec_m}\big(\Bbbk[X] \otimes \Bbbk[Y]\big)$ equipped with the structure of an affine algebraic variety via Remark 11.1 plays the role of the direct product $X \times Y$ in the category $\mathcal{A}\!f\!f_{\Bbbk}$. Note that the previous arguments show that the set

$$\mathrm{Spec_m}\big(\Bbbk[X] \otimes \Bbbk[Y]\big)$$

gives the direct product of sets $X \times Y$ in $\mathcal{S}et$ as well. For example,

$$\Bbbk[x_1, x_2, \dots, x_n] \otimes \Bbbk[y_1, y_2, \dots, y_m] \simeq \Bbbk[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$$

---

[11]In the sense of Example 9.13 on p. 203.

[12]In the sense of Example 9.14 on p. 204.

via the mapping $x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n}\otimes y_1^{r_1}y_2^{r_2}\cdots y_m^{r_m}\mapsto x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n}y_1^{r_1}y_2^{r_2}\cdots y_m^{r_m}$. This agrees with the intuitively expected isomorphism $\mathbb{A}^n\times\mathbb{A}^m\simeq\mathbb{A}^{n+m}$ in $\mathcal{Aff}_{\Bbbk}$.

Exercise 11.7 Given polynomial equations $f_\nu(x)=0$, $g_\mu(y)=0$ describing affine algebraic varieties $X\subset\mathbb{A}^n$, $Y\subset\mathbb{A}^m$, write down an explicit system of polynomial equations whose solution set is $X\times Y\subset\mathbb{A}^n\times\mathbb{A}^m$.

11.3 Zariski Topology

The set $X=\operatorname{Spec}_{\mathrm{m}}A$ possesses the natural topology, called the *Zariski topology*, whose closed sets are the subsets of X that can be described by polynomial equations, i.e., the sets

$$\begin{aligned}V(I)&=\{x\in X\mid f(x)=0\text{ for all }f\in I\}=\{\mathfrak{m}\in\operatorname{Spec}_{\mathrm{m}}A\mid I\subset\mathfrak{m}\}\\&=\{\varphi:A\to\Bbbk\mid\varphi(I)=0\}\,,\end{aligned}$$

taken for all ideals $I\subset A$.

Exercise 11.8 Verify that **(a)** $\varnothing=V((1))$, **(b)** $X=V((0))$, **(c)** $\bigcap_\nu V(I_\nu)=V\left(\sum_\nu I_\nu\right)$, where the ideal $\sum_\nu I_\nu$ consists of finite sums of elements $f_\nu\in I_\nu$, **(d)** $V(I)\cup V(J)=V(I\cap J)=V(IJ)$, where the ideal $IJ\subset I\cap J$ consists of finite sums of products ab with $a\in I$, $b\in J$.

The Zariski topology has a purely algebraic nature. It reflects divisibility relations rather than closeness or remoteness. For this reason, some properties of the Zariski topology are discordant with intuition based on the metric topology. For example, the Zariski topology on the product $X\times Y$ is strictly finer that the product of Zariski topologies on the factors X, Y, i.e., the closed subsets $Z\subset X\times Y$ are not exhausted by the products of closed subsets in X, Y. For example, for $X=Y=\mathbb{A}^1$, every plane algebraic curve, e.g., the hyperbola $V(xy-1)$, is Zariski closed in $\mathbb{A}^1\times\mathbb{A}^1=\mathbb{A}^2$, whereas the products of closed subsets in $\mathbb{A}^1$ are exhausted by $\varnothing$, $\mathbb{A}^2$, and finite unions of points and lines parallel to the coordinate axes.

Proposition 11.1 (Base for Open Sets and Compactness) *Every Zariski open subset U of an affine algebraic variety X is a finite union of principal open sets*

$$\mathcal{D}(f)\stackrel{\text{def}}{=}X\smallsetminus V(f)=\{x\in X\mid f(x)\neq 0\}$$

for some $f\in\Bbbk[X]$, and is compact in the induced topology, meaning that every open cover of U contains a finite subcover.

Proof Let $U=X\smallsetminus V(I)$. Since $\Bbbk[X]$ is Noetherian, $I=(f_1,f_2,\dots,f_m)$ for some $f_i\in\Bbbk[X]$. Therefore $V(I)=\bigcap V(f_i)$ and $U=\bigcup(X\smallsetminus V(f_i))=\bigcup\mathcal{D}(f_i)$. Further, let U be covered by a family of principal open sets $\mathcal{D}(f_\nu)$, and I the ideal spanned by the functions f_ν. Then $V(I)\subset X\smallsetminus U$ and $I=(f_1,f_2,\dots,f_m)$ for some finite collection $f_1, f_2, \dots, f_m$ of the functions f_ν. Therefore, the open sets $\mathcal{D}(f_i)$, $1 \leqslant i \leqslant m$, cover U as well. $\square$

Proposition 11.2 (Continuity of Regular Maps) *Every regular map of affine algebraic varieties $\varphi : X \to Y$ is continuous in the Zariski topology.*

Proof For every closed set $V(I) \subset Y$, the preimage $\varphi^{-1}\big(V(I)\big)$ consists of the points $x \in X$ such that $0 = f(\varphi(x)) = \varphi^* f(x)$ for all $f \in I$. Therefore, it coincides with $V(J)$ for the ideal $J \subset \Bbbk[X]$ generated by the image of I under the pullback homomorphism $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$. $\square$

11.3.1 Irreducible Components

A topological space X is called *reducible* if $X = X_1 \cup X_2$ for some proper closed subsets $X_1, X_2 \subsetneq X$. Otherwise, X is called *irreducible*. In the usual metric topology, almost all spaces are reducible. In the Zariski topology, the irreducible affine algebraic varieties play the same role as the powers of prime numbers in arithmetic.

Proposition 11.3 *An affine algebraic variety X is irreducible if and only if its coordinate algebra $\Bbbk[X]$ has no zero divisors.*

Proof If $X = X_1 \cup X_2$ with proper closed X_1, X_2, then there exist nonzero regular functions $f_1, f_2 \in \Bbbk[X]$ such that $f_1 \in I(X_1)$, $f_2 \in I(X_2)$. Since $f_1 f_2$ vanishes at every point of X, it equals zero in $\Bbbk[X]$. Conversely, if $f_1 f_2 = 0$ for some nonzero $f_1, f_2 \in \Bbbk[X]$, then $X = V(f_1) \cup V(f_2)$, where the closed sets $V(f_1)$, $V(f_2)$ are proper. $\square$

Exercise 11.9 Verify that $V(f) \subset X$ is nonempty and proper for every nonzero noninvertible element $f \in \Bbbk[X]$.

Corollary 11.2 *Given a polynomial $g \in \Bbbk[x_1, x_2, \dots, x_n]$, the affine hypersurface $V(g) \subset \mathbb{A}^n$ is irreducible if and only if $g = q^n$ for some irreducible $q \in \Bbbk[x_1, x_2, \dots, x_n]$ and $n \in \mathbb{N}$.*

Proof Since the polynomial ring $\Bbbk[x_1, x_2, \dots, x_n]$ is a unique factorization domain,[13] a polynomial $f \in \Bbbk[x_1, x_2, \dots, x_n]$ is irreducible if and only if the quotient ring $\Bbbk[x_1, x_2, \dots, x_n]/(f)$ has no zero divisors,[14] and for every f, the radical $\sqrt{(f)}$ is the principal ideal generated by the product of all pairwise nonassociated irreducible divisors of f. Therefore, $\Bbbk[V(f)] = \Bbbk[x_1, x_2, \dots, x_n]/\sqrt{(f)}$ has no zero divisors if and only if f has a unique (up to a constant factor) irreducible divisor. $\square$

Example 11.4 (Big Open Sets) If X is irreducible, then every two nonempty open sets $U_1, U_2 \subset X$ have nonempty intersection, because otherwise, X could be

[13] See Sect. 5.4 of Algebra I.

[14] See Proposition 5.4 of Algebra I.

decomposed as $X = (X \smallsetminus U_1) \cup (X \smallsetminus U_2)$. In other words, every nonempty open subset of an irreducible variety X is dense in X. Thus, the Zariski topology is quite far from being Hausdorff.

Exercise 11.10 Let X be an irreducible algebraic variety and $f, g \in \Bbbk[X]$. Prove that if $f(p) = g(p)$ for all points p from a nonempty open subset $U \subset X$, then $f = g$ in $\Bbbk[X]$.

Theorem 11.3 *Every affine algebraic variety X admits a decomposition*

$$X = X_1 \cup X_2 \cup \cdots \cup X_k$$

that is unique up to renumbering of components, where all $X_i \subset X$ are closed and irreducible, and $X_i \not\subset X_j$ for all $i \neq j$.

Proof The existence of the decomposition is proved similarly to the existence of irreducible factorization in a Noetherian ring.[15] If X is reducible, write X as a union $X = Z_1 \cup Z_2$ of proper closed subsets $Z_1, Z_2 \subset X$ and repeat the procedure recursively for every component until it stops on some finite decomposition $X = \bigcup Z_\nu$, where all Z_ν are irreducible. If the procedure never stopped, we could choose an infinite strictly decreasing chain of closed sets

$$X \supsetneq Y_1 \supsetneq Y_2 \supsetneq \cdots ,$$

whose ideals form a strictly increasing chain $(0) \subsetneq I(Y_1) \subsetneq I(Y_2) \subsetneq \cdots$ in $\Bbbk[X]$, which is impossible, because $\Bbbk[X]$ is Noetherian. Now let

$$X_1 \cup X_2 \cup \cdots \cup X_k = Y_1 \cup Y_2 \cup \cdots \cup Y_m$$

be two decompositions satisfying the conditions of the theorem. Since $Y_1 = \bigcup_i (Y_1 \cap X_i)$ is irreducible, $Y_1 \cap X_i = Y_1$ for some i, that is, $Y_1 \subset X_i$. For the same reason, $X_i \subset Y_j$ for some j. Since $Y_1 \not\subset Y_j$ for $j \neq 1$, we conclude that $Y_1 = X_i$. Renumber the X_i in order to have $Y_1 = X_1$.

Exercise 11.11 Let $Z \subsetneq Y \subset X$ be closed, and Y irreducible. Prove that $Y = \overline{Y \smallsetminus Z}$ (the closure within X). Convince yourself that this may fail for reducible Y.

Now we can remove X_1 and Y_1, and proceed by induction on the number of components. □

Definition 11.2 The decomposition $X = X_1 \cup X_2 \cup \cdots \cup X_k$ from Theorem 11.3 is called the *irreducible decomposition* of the algebraic variety X, and its components $X_i \subset X$ are called the *irreducible components* of X.

Remark 11.2 (Noetherian Spaces) Theorem 11.3 and its proof hold for every topological space X that does not allow strictly decreasing infinite chains of closed subsets $X \supsetneq Z_1 \supsetneq Z_2 \supsetneq \cdots$. Every such topological space is called *Noetherian*.

[15]Compare with Proposition 5.3 of Algebra I.

Proposition 11.4 *A nonzero element $f \in \Bbbk[X]$ is a zero divisor if and only if f has the zero restriction on some irreducible component of X.*

Proof Let $fg = 0$ for some $g \neq 0$. Write $f_i, g_i \in \Bbbk[X_i]$ for the restrictions of f, g to the irreducible component $X_i \subset X$. Since $\Bbbk[X_i]$ has no zero divisors, at least one of f_i, g_i vanishes for every i. Since $g_i \neq 0$ for some i (otherwise, $g = 0$ in $\Bbbk[X]$), we conclude that $f_i = 0$. Conversely, if $f_i = 0$, then $fg = 0$ for every nonzero function $g \in I\left(\bigcup_{\nu \neq i} X_\nu\right)$. $\square$

11.4 Rational Functions

Given a commutative ring A, we write

$$A^\circ \stackrel{\text{def}}{=} \{a \in A \mid ab \neq 0 \text{ for all } b \in A \smallsetminus 0\}$$

for the multiplicative system of all nonzero elements that are not zero divisors.[16] Let X be an affine algebraic variety. The algebra of fractions[17] of the coordinate algebra $\Bbbk[X]$ is called the *algebra of rational functions* on X and is denoted by

$$\Bbbk(X) \stackrel{\text{def}}{=} Q_{\Bbbk[X]} = \Bbbk[X]\left(\Bbbk[X]^\circ\right)^{-1} .$$

For irreducible X, the algebra $\Bbbk(X)$ becomes the field of fractions of the integral domain $\Bbbk[X]$. The elements of $\Bbbk(X)$ are called *rational functions* on X. A rational function $f \in \Bbbk(X)$ is said to be *regular* at a point $x \in X$ if there exists a fraction $g/h = f$ such that $g \in \Bbbk[X]$, $h \in \Bbbk[X]^\circ$, and $h(x) \neq 0$. In this case, the number $f(x) \stackrel{\text{def}}{=} g(x)/h(x) \in \Bbbk$ is referred to as the *value* of f at the point $x \in X$.

Exercise 11.12 Verify that the value $f(x)$ does not depend on the choice of admissible representation $f = g/h$.

If a rational function $f = g/h$ has $h(x) \neq 0$ at some point $x \in X$, then f is regular at every point in the principal open neighborhood $\mathcal{D}(h)$ of the point x. Moreover, by Proposition 11.4, this neighborhood has nonempty intersection with every irreducible component of X, because h is not a zero divisor in $\Bbbk[X]$. Therefore, all points $x \in X$ at which f is regular form an open dense subset in X. It is called the *domain* of f and denoted by $\mathrm{Dom}(f)$.

Exercise 11.13 Verify that $f_1 = f_2$ in $\Bbbk(X)$ if and only if $f_1(x) = f_2(x)$ for all x in some open dense subset of X.

---

[16] This is the same notation as in Sect. 4.1 of Algebra I.

[17] Recall that it consists of all fractions f/g with $f \in \Bbbk[X]$, $g \in \Bbbk[X]^\circ$, and $f_1/g_1 = f_2/g_2$ if and only if $f_1g_2 = f_2g_1$. (See Sect. 4.1 of Algebra I and compare it with Problem 9.10 on p. 224.)

Proposition 11.5 *Let X be an affine algebraic variety over an infinite field, and $f \in \Bbbk(X)$ a rational function. Then* $(1/f) \overset{\text{def}}{=} \{g \in \Bbbk[X] \mid gf \in \Bbbk[X]\}$ *is an ideal in* $\Bbbk[X]$ *with the zero set* $V((1/f)) = X \smallsetminus \mathrm{Dom}(f)$.

Proof The intersection $(1/f) \cap \Bbbk[X]^\circ$ is exactly the set of all denominators q appearing in various fractional representations $f = p/q$. Thus, the closed set $X \smallsetminus \mathrm{Dom}(f)$ is determined by the system of equations $q(x) = 0$ for all $q \in (1/f) \cap \Bbbk[X]^\circ$. It remains to show that the intersection $(1/f) \cap \Bbbk[X]^\circ$ generates the ideal $(1/f)$. We will prove that it spans $(1/f)$ even as a vector space over $\Bbbk$. By Proposition 11.4, the complement $(1/f) \smallsetminus \Bbbk[X]^\circ$, that is, the set of all zero divisors in $(1/f)$, splits into a finite union of vector subspaces $(1/f) \cap I(X_i)$. Since $(1/f) \cap \Bbbk[X]^\circ \neq \varnothing$, every subspace $(1/f) \cap I(X_i)$ is proper. If the $\Bbbk$-linear span of $(1/f) \cap \Bbbk[X]^\circ$ is proper too, the vector space $(1/f)$ becomes a finite union of proper subspaces. The next exercise makes this impossible. □

Exercise 11.14 Prove that a vector space over an infinite field cannot be decomposed into a finite union of proper vector subspaces.

11.4.1 The Structure Sheaf

Given an affine algebraic variety X, for every open $U \subset X$, we put

$$\mathcal{O}_X(U) \overset{\text{def}}{=} \{f \in \Bbbk(X) \mid \mathrm{Dom}(f) \supset U\}.$$

The assignment $\mathcal{O}_X : U \mapsto \mathcal{O}_X(U)$ provides the topological space X with a presheaf of $\Bbbk$-algebras whose restriction maps are the usual restrictions of functions, or more scientifically, the tautological inclusions $\mathcal{O}_X(W) \hookrightarrow \mathcal{O}_X(U)$ for every pair of embedded open sets $U \subset W$.

Exercise 11.15 Verify that $\mathcal{O}_X$ is a sheaf.

The sheaf $\mathcal{O}_X$ is called the *structure sheaf* of the affine algebraic variety X or the *sheaf of regular rational functions* on X. For an open $U \subset X$, the algebra $\mathcal{O}_X(U)$ is often denoted by $\Bbbk[U]$ and referred to as the *algebra of rational functions regular in* U.

Proposition 11.6 *Let X be an affine algebraic variety over an algebraically closed field and $h \in \Bbbk[X]^\circ$. Then $\mathcal{O}_X(\mathcal{D}(h)) = \Bbbk[X][h^{-1}]$ is the ring of fractions with numerators in $\Bbbk[X]$ and denominators in the multiplicative system*[18] *formed by nonnegative integer powers of h.*

Proof By Proposition 11.5, a rational function $f \in \Bbbk(X)$ is regular in $\mathcal{D}(h)$ if and only if h vanishes identically on the closed subset $V((1/f)) = X \smallsetminus \mathrm{Dom}(f)$. By the strong Nullstellensatz, $h^d \in (1/f)$ for some $d \in \mathbb{N}$. Thus, $f = p/h^d$ for $p = h^d \cdot f \in \Bbbk[X]$, as required. □

[18] See Sect. 4.1.1 of Algebra I.

11.4.2 Principal Open Sets as Affine Algebraic Varieties

For every affine algebraic variety X and $h \in \Bbbk[X]^\circ$, the principal open set

$$\mathcal{D}(h) = \operatorname{Spec}_m \Bbbk[X]\left[h^{-1}\right] = \operatorname{Spec}_m \Bbbk[X][t]/(1-ht)$$

is dense in X and is itself an affine algebraic variety, which can be realized as the hypersurface $V(1-ht) \subset X \times \mathbb{A}^1$. The tautological inclusion $i : \mathcal{D} \hookrightarrow X$ is a regular morphism of affine algebraic varieties. Its pullback homomorphism $i^* : \Bbbk[X] \hookrightarrow \Bbbk[X][h^{-1}] \simeq \Bbbk[\mathcal{D}(h)]$ is the universal map $f \mapsto f/1$ from the ring to the localization. By the universal properties of rings of fractions, this inclusion can be uniquely extended to an isomorphism of the algebras of fractions

$$i^* : \Bbbk(X) \xrightarrow{\sim} \Bbbk\big(\mathcal{D}(h)\big)\,. \tag{11.8}$$

Exercise 11.16 Verify that the canonical homomorphism (11.8) is actually an isomorphism.

Remark 11.3 The notation $\Bbbk\big[\mathcal{D}(h)\big]$ can be treated either as the coordinate algebra of the affine algebraic variety $\mathcal{D}(h) = \operatorname{Spec}_m\big(\Bbbk[X][h^{-1}]\big)$ or as the subring of $\Bbbk(X)$ formed by the rational functions regular in $\mathcal{D}(h) \subset X$. These two interpretations agree by Proposition 11.6. In particular, for $h = 1$, the coordinate algebra of X coincides with the algebra of rational functions regular everywhere on X, i.e., $\Bbbk[X] = \{f \in \Bbbk(X) \mid \operatorname{Dom}(f) = X\}$.

Caution 11.1 A nonprincipal open set $U \subset X$ might not be an affine algebraic variety, and the canonical inclusion $U \hookrightarrow \operatorname{Spec}_m \mathcal{O}_X(U)$, sending a point $u \in U$ to its maximal ideal $\mathfrak{m}_u = \ker \operatorname{ev}_u \subset \mathcal{O}_X(U)$, may be nonsurjective.

Exercise 11.17 Let $n \geqslant 2$, and $U = \mathbb{A}^n \smallsetminus O$ the complement of the origin. Verify that $\mathcal{O}_{\mathbb{A}^n}[U] = \Bbbk[\mathbb{A}^n]$ and therefore $\operatorname{Spec}_m \mathcal{O}_{\mathbb{A}^n}[U] = \mathbb{A}^n \neq U$.

Proposition 11.7 *Let $X = X_1 \cup X_2 \cup \cdots \cup X_k$ be the irreducible decomposition of an affine algebraic variety X. Then $\Bbbk(X) = \Bbbk(X_1) \times \Bbbk(X_2) \times \cdots \times \Bbbk(X_k)$.*

Proof Write $I = I\big(\bigcup_{i \neq j}(X_i \cap X_j)\big) \subset \Bbbk[X]$ for the ideal of all regular functions on X vanishing on every intersection $X_i \cap X_j$, $i \neq j$.

Exercise 11.18 Prove that I is linearly spanned over $\Bbbk$ by $I \cap \Bbbk[X]^\circ$.

Let us choose some regular function $f \in I \cap \Bbbk[X]^\circ$ and write

$$f_i = f \;(\operatorname{mod} I(X_i)) \in \Bbbk[X_i]$$

for its restriction to the irreducible component $X_i \subset X$. Then the affine algebraic variety

$$W = \mathcal{D}(f) = \operatorname{Spec}_m \Bbbk[X]\left[f^{-1}\right]$$

splits into a disjoint union of affine algebraic varieties

$$W_i = W \cap X_i = \mathcal{D}(f_i) = \operatorname{Spec}_{\mathrm{m}} \Bbbk[X_i]\left[f_i^{-1}\right] .$$

By Example 11.2, $\Bbbk[W] \simeq \Bbbk[W_1] \times \Bbbk[W_2] \times \cdots \times \Bbbk[W_k]$.

Exercise 11.19 For every family of commutative rings A_ν, prove that $(\prod A_\nu)^\circ = \prod A_\nu^\circ$ as sets, and deduce from this the isomorphism $Q_{\prod A_\nu} \simeq \prod Q_{A_\nu}$ for the rings of fractions.

Therefore, $\Bbbk(X) \simeq \Bbbk(W) \simeq \prod \Bbbk(W_i) \simeq \prod \Bbbk(X_i)$ by formula (11.8). □

11.5 Geometric Properties of Algebra Homomorphisms

Every homomorphism of finitely generated reduced $\Bbbk$-algebras

$$\varphi^* : \Bbbk[Y] \to \Bbbk[X]$$

can be canonically factorized into a composition of a quotient epimorphism followed by a monomorphism:

$$\Bbbk[Y] \xrightarrow{\varphi_1^*} \Bbbk[Y]/\ker(\varphi^*) = \operatorname{im}(\varphi^*) \xhookrightarrow{\varphi_2^*} \Bbbk[X] . \tag{11.9}$$

Since $\Bbbk[Y]$ is finitely generated and $\Bbbk[X]$ is reduced, the $\Bbbk$-algebra $\Bbbk[Y]/\ker(\varphi^*) = \operatorname{im}(\varphi^*) \subset \Bbbk[X]$ is both finitely generated and reduced. Thus, it is the coordinate algebra of the affine algebraic variety

$$Z = \operatorname{Spec}_{\mathrm{m}}\left(\operatorname{im}(\varphi^*)\right) \simeq V\left(\ker(\varphi^*)\right) \subset Y .$$

The injectivity of the homomorphism $\varphi_1^* : \Bbbk[Z] \to \Bbbk[X]$ means that there are no nonzero functions $f \in \Bbbk[Z]$ vanishing on $\varphi_1(X) \subset Z$. Therefore, $\varphi_1(X)$ is *Zariski dense* in Z. In other words, $Z = \overline{\varphi(X)} \subset Y$ is the closure of $\varphi(X)$ in Y, situated within Y as the zero set $V(\ker \varphi^*)$ of the ideal $\ker \varphi^* \subset \Bbbk[Y]$. Thus, the algebraic factorization (11.9) geometrically corresponds to the factorization of a regular map of algebraic varieties $\varphi : X \to Y$ into the composition

$$X \xrightarrow{\varphi_2} Z = \overline{\varphi(X)} \xhookrightarrow{\varphi_1} Y$$

of the closed immersion $Z \hookrightarrow Y$ preceded by the regular morphism $X \to Z$ with dense image.

11.5.1 Closed Immersions

A regular morphism of affine algebraic varieties $\varphi : X \to Y$ is called a *closed immersion* if its pullback homomorphism $\varphi^* : \Bbbk[Y] \to k[X]$ is surjective. In this case, φ establishes a regular isomorphism between X and the closed subset $V(\ker \varphi^*) \subset Y$. The pullback of this isomorphism of algebraic varieties is the canonical isomorphism of $\Bbbk$-algebras $\Bbbk[Y]/\ker \varphi^* \simeq \Bbbk[X]$.

For an irreducible closed subset $Z \subset X$, the pullback homomorphism

$$i^* : \Bbbk[X] \twoheadrightarrow \Bbbk[Z]$$

of the closed immersion $i : Z \hookrightarrow X$ takes values in the integral domain $\Bbbk[Z]$, canonically embedded into its field of fractions $\Bbbk(Z)$. By the universal property of $\Bbbk(X)$, the epimorphism i^* can be uniquely extended to an epimorphism

$$\mathrm{ev}_Z : \Bbbk(X) \twoheadrightarrow \Bbbk(Z)\,, \tag{11.10}$$

which restricts the rational functions from X onto Z. Intuitively, the homomorphism (11.10) can be thought of as the evaluation of rational functions at a “generic point” of Z. The result of such an evaluation is an element of $\Bbbk(Z)$, which may be further evaluated at particular points of Z. It follows from the surjectivity of the homomorphism (11.10) that every rational function on Z is a restriction of some rational function on X, i.e., can be written as a fraction p/q whose denominator $q \in \Bbbk[X]^\circ$ is not a zero divisor in $\Bbbk[X]$. Note that such a presentation may not be obvious when $Z \subset X$ is an irreducible component of X.

Exercise 11.20 Let $X = V(xy) = \operatorname{Spec_m} \Bbbk[x,y]/(xy)$ be the union of the coordinate axes in the affine plane $\mathbb{A}^2 = \operatorname{Spec_m} \Bbbk[x,y]$, and let $Z = \operatorname{Spec_m} \Bbbk[x] = V(y)$ be its horizontal component. Write the rational function $1/x \in \Bbbk(Z)$ as a fraction $p/q \in \Bbbk(X)$, where $q \in \Bbbk[X]^\circ$.

11.5.2 Dominant Morphisms

For an irreducible variety X, a regular morphism of algebraic varieties $\varphi : X \to Y$ is said to be *dominant* if its pullback homomorphism $\varphi^* : \Bbbk[Y] \to k[X]$ is injective. As we have seen above, this means that $\overline{\varphi(X)} = Y$. For reducible X, a regular map $\varphi : X \to Y$ is *dominant* if its restriction $\varphi_i = \varphi|_{X_i}$ to every irreducible component $X_i \subset X$ assigns the dominant map $\varphi_i : X_i \to Y$. In this case, the pullback

$$\varphi_i^* : \Bbbk[Y] \hookrightarrow \Bbbk[X_i] \subset \Bbbk(X_i)$$

embeds $\Bbbk[Y]$ in the *field* $\Bbbk(X_i)$. In particular, this forces Y to be irreducible. By the universal property of $\Bbbk(Y)$, the previous inclusion can be uniquely extended to the inclusion of fields $\Bbbk(Y) \hookrightarrow \Bbbk(X_i)$. Thus, every dominant morphism $X = \bigcup X_i \to Y$ leads to the inclusion

$$\Bbbk(Y) \hookrightarrow \prod \Bbbk(X_i) = \Bbbk(X)\,.$$

Exercise 11.21 Prove that every dominant morphism of irreducible affine algebraic varieties $\varphi : X \to Y$ can be factorized as

$$X \overset{\psi}{\hookrightarrow} Y \times \mathbb{A}^m \overset{\pi}{\twoheadrightarrow} Y \,, \tag{11.11}$$

where ψ is a closed immersion, and π is the projection along $\mathbb{A}^m$.

11.5.3 Finite Morphisms

Every regular map of affine algebraic varieties $\varphi : X \to Y$ equips $\Bbbk[X]$ with the structure of a finitely generated algebra over the subring

$$\varphi^*(\Bbbk[Y]) = \Bbbk[\overline{\varphi(X)}] \subset \Bbbk[X] \,.$$

The map φ is called *finite* if $\Bbbk[X]$ is finitely generated as a *module*[19] over $\varphi^*(k[Y])$, or equivalently, if the extension of rings $\varphi^*(\Bbbk[Y]) \subset \Bbbk[X]$ is an integral extension.

Proposition 11.8 (Closeness of Finite Morphisms) *Let $\varphi : X \to Y$ be a finite morphism of affine algebraic varieties, and $Z \subset X$ a closed subset. Then $\varphi(Z) \subset Y$ is also closed, and the restriction $\varphi|_Z : Z \to \varphi(Z)$ is a finite morphism. For irreducible X and proper $Z \subsetneq X$, the image $\varphi(Z) \subsetneq Y$ is also proper.*

Proof Write $I = I(Z) \subset \Bbbk[X]$ for the ideal of Z. The pullback homomorphism of the restricted map $\varphi|_Z : Z \to Y$ can be factorized as

$$\varphi|_Z^* : k[Y] \xrightarrow{\varphi^*} \Bbbk[X] \twoheadrightarrow \Bbbk[X]/I \,,$$

where the second arrow is the quotient homomorphism. Since $\Bbbk[X]$ is finitely generated as a $\varphi^*(\Bbbk[Y])$-module, the quotient $\Bbbk[Z] = \Bbbk[X]/I$ is finitely generated as a module over

$$\Bbbk\left[\overline{\varphi(Z)}\right] = \varphi|_Z^*(\Bbbk[Y]) = \varphi^*(\Bbbk[Y])/\big(I \cap \varphi^*(\Bbbk[Y])\big) \,.$$

Therefore, the restricted map $\varphi|_Z : Z \to \overline{\varphi(Z)}$ is a finite morphism. The equality $\varphi(Z) = \overline{\varphi(Z)}$ can be proved separately for each irreducible component of Z, and in this proof, we can assume that $X = Z$, $Y = \overline{Z}$. Thus, the first statement of the proposition is equivalent to the following claim: for an irreducible affine algebraic variety Z, every finite dominant morphism $\varphi : Z \to Y$ is surjective. This claim can be translated into algebraic language as follows: given an extension of commutative

[19] That is, there exist $f_1, f_2, \dots, f_m \in \Bbbk[X]$ such that every $h \in \Bbbk[X]$ can be written as $h = \sum \varphi^*(g_i) f_i$ for appropriate $g_i \in \Bbbk[Y]$.

rings $A \subset B$ such that B has no zero divisors and is finitely generated as an A-module, every maximal ideal $\mathfrak{m} \subset A$ equals $\widetilde{\mathfrak{m}} \cap A$ for some maximal ideal $\widetilde{\mathfrak{m}} \subset B$.

Exercise 11.22 Convince yourself that the latter algebraic statement implies the previous geometric statement.

If the ideal $\mathfrak{m} \cdot B$, spanned by $\mathfrak{m}$ in B, is proper, then every maximal ideal $\widetilde{\mathfrak{m}} \supset \mathfrak{m} \cdot B$ solves the problem. It remains to check that $\mathfrak{m} \cdot B \neq B$ for every maximal ideal $\mathfrak{m} \subset A$. Assume the contrary. Let $\mathfrak{m} \cdot B = B$ for some maximal ideal $\mathfrak{m} \subset A$, and suppose that $b_1, b_2, \dots, b_m \in B$ span B as an A-module. Then each b_j can be written as $b_j = \sum_i f_i \mu_{ij}$ for some $\mu_{ij} \in \mathfrak{m}$. This leads to the matrix equality

$$(f_1, f_2, \dots, f_m) \cdot (E - M) = 0,$$

where $M = \left(\mu_{ij}\right) \in \mathrm{Mat}_m(\mathfrak{m})$, and E is the $m \times m$ identity matrix. Thus, the zero endomorphism of the A-module B acts on the generators via multiplication by the matrix $E - M$. The matrix identity[20]

$$\det(E - M) \cdot E = (E - M) \cdot (E - M)^{\vee}$$

forces multiplication by $\det(E - M)$ to annihilate B. Therefore, $\det(E - M) = 0$. Expanding the determinant shows that $1 \in \mathfrak{m}$, i.e., $\mathfrak{m}$ is not proper. This completes the proof of the first statement of the proposition.

To prove the second statement, consider a nonzero function $f \in \Bbbk[X]$ that has zero restriction onto $Z \subsetneq X$. It satisfies some polynomial equation with coefficients in $\varphi^*(k[Y])$. Let

$$\varphi^*(g_0) f^m + \varphi^*(g_1) f^{m-1} + \cdots + \varphi^*(g_{m-1}) f + \varphi^*(g_m) = 0$$

be such an equation of minimal degree. Then $g_m \neq 0$, because otherwise, the degree could be decremented by canceling[21] one f. Evaluation of the left-hand side at all points $z \in Z$ shows that $\varphi^*(g_m)|_Z = g_m|_{\varphi(Z)} = 0$. Hence, $\varphi(Z) \subset V(g_m) \subsetneq Y$ is proper. $\square$

11.5.4 *Normal Varieties*

An irreducible affine algebraic variety Y is called *normal* if its coordinate algebra $\Bbbk[Y]$ is integrally closed in the field of rational functions $\Bbbk(Y) = Q_{\Bbbk[Y]}$, i.e., $\Bbbk[Y]$ is a normal ring in the sense of Sect. 10.1.3. In particular, Y is normal if $\Bbbk[Y]$ is a unique factorization domain. For example, the affine spaces $\mathbb{A}^n$ are normal for all n.

---

[20] Here $(E - M)^{\vee}$ means the adjunct matrix of $(E - M)$; see Sect. 9.6.1 of Algebra I and the proof of Lemma 10.1 on p. 227.

[21] Recall that in the second statement, we assume $\Bbbk[X]$ to be an integral domain.

Proposition 11.9 (Openness of Finite Surjections onto Normal Varieties) *Let Y be a normal affine algebraic variety. Then every finite regular surjection $\varphi : X \twoheadrightarrow Y$ is open*[22] *and maps every irreducible component of X surjectively onto Y.*

Proof Since $\varphi^* : \Bbbk[Y] \hookrightarrow \Bbbk[X]$ is injective, we can consider $\Bbbk[Y]$ a subalgebra of $\Bbbk[X]$. It is enough to show that φ maps every principal open set $\mathcal{D}(f) \subset X$ to an open subset of Y. This means that for every point $p \in \mathcal{D}(f)$, there exists a regular function $a \in \Bbbk[Y]$ such that $\varphi(p) \in \mathcal{D}(a) \subset \varphi(\mathcal{D}(f))$ in Y. To construct such a function, consider the map

$$\psi = \varphi \times f : X \to Y \times \mathbb{A}^1 , \quad p \mapsto \big(\varphi(p), f(p)\big) .$$

Its pullback homomorphism $\psi^* : \Bbbk[Y \times \mathbb{A}^1] = \Bbbk[Y][t] \to k[X]$ evaluates polynomials in t with coefficients in $\Bbbk[Y]$ at the element $f \in \Bbbk[X]$. Write μ_f for the minimal polynomial of f over $\Bbbk(Y)$. By Corollary 10.2, the coefficients of μ_f lie in $\Bbbk[Y]$. This forces ψ^* to be the factorization homomorphism modulo the principal ideal $(\mu_f) = \ker \psi^* \subset \Bbbk[Y \times \mathbb{A}^1]$. Thus, ψ is the finite surjection of X onto the hypersurface in $Y \times \mathbb{A}^1$ defined by the equation $\mu_f = 0$. Let us write the minimal polynomial $\mu_f = \mu_f(y; t)$ as a polynomial in the coordinate t on $\mathbb{A}^1$ with coefficients in $a_i(y) \in \Bbbk[Y]$:

$$\mu_f = t^m + a_1(y)\, t^{m-1} + \cdots + a_m(y) \in \Bbbk[Y][t] = \Bbbk\left[Y \times \mathbb{A}^1\right] .$$

The restriction of μ_f to the line $y \times \mathbb{A}^1$ over a point $y \in Y$ is the polynomial in t whose roots are equal to the values of f at all points of X mapped to y by φ. In particular, $\varphi(\mathcal{D}(f))$ consists of those $y \in Y$ over which the polynomial $\mu(y; t)$ has a nonzero root. Since the polynomial $\mu_f(\varphi(p); t)$ that appears for $y = \varphi(p)$ has the root $f(p) \neq 0$, at least one of the coefficients of μ_f, say $a_k(y)$, does not vanish at $y = \varphi(p)$. This forces the polynomial $\mu_f(q; t)$ to have a nonzero root for all $q \in \mathcal{D}(a_k)$. Hence, $\mathcal{D}(a_k) \subset \varphi(\mathcal{D}(f))$, as required. To prove the second statement of the proposition, note that for every irreducible component $X_i \subset X$, the set

$$U_i = X \smallsetminus \bigcup_{\nu \neq i} X_\nu = X_i \smallsetminus \bigcup_{\nu \neq i} (X_i \cap X_\nu)$$

is open in X and dense in X_i. Since $\varphi(U_i)$ is open and Y is irreducible, $\varphi(U_i)$ is dense in Y. Therefore, $\varphi(X_i) = \overline{\varphi(U_i)} = Y$. □

[22] That is, $\varphi(U)$ is open in Y for every open $U \subset X$.

Problems for Independent Solution to Chapter 11

Problem 11.1 Let $\Bbbk$ be an algebraically closed field, $q \in \Bbbk[x_1, x_2, \dots, x_n]$ an irreducible polynomial, and suppose that the polynomial $f \in \Bbbk[x_1, x_2, \dots, x_n]$ vanishes at every point of the hypersurface $V(q) \subset \mathbb{A}^n$. Prove that q divides f.

Problem 11.2 Under the conditions of the previous problem, show that the image of the central projection of $V(f)$ from every point $p \notin V(f)$ onto every hyperplane $H \not\ni p$ contains an open dense subset of H.

Problem 11.3 Describe $\sqrt{J} \subset \Bbbk[x, y]$ for **(a)** $J = (x^2 + y^2 - 1, y - 1)$, **(b)** $J = (x^2y, xy^3)$, and indicate some $f \in I(V(J)) \smallsetminus J$.

Problem 11.4 Describe the variety $V(J) \subset \mathbb{A}^3$ and its ideal $I(V(J)) \subset \Bbbk[x, y, z]$ for **(a)** $J = \big(xy, (x - y)z\big)$, **(b)** $J = \big(xy + yz + zx, x^2 + y^2 + z^2\big)$.

Problem 11.5 Prove that the curve $V\left(x^2 - y^3\right) \subset \mathbb{A}^2 = \operatorname{Spec_m} \Bbbk[x, y]$ is irreducible but not normal.

Problem 11.6 Is the cone $V\left(x^2 - y^2 - z^2\right) \subset \mathbb{A}^3 = \operatorname{Spec_m} \Bbbk[x, y, z]$ a normal variety?

Problem 11.7 Prove that the direct product of irreducible affine algebraic varieties is irreducible.

Problem 11.8 For every $\Bbbk$-algebra A of finite dimension as a vector space over $\Bbbk$, prove that $\operatorname{Spec_m} A$ is finite. Deduce from this that every nonempty fiber of a finite morphism is finite.

Problem 11.9 Give an example of a regular nonfinite morphism all of whose nonempty fibers are finite.

Problem 11.10 Give an example of a map that is continuous in the Zariski topology but not regular.

Problem 11.11 Let $\Bbbk$ be an algebraically closed field, and $f \in \Bbbk[x_1, x_2, \dots, x_n]$ a nonconstant polynomial. Describe (in terms of f) all vectors

$$v = (\alpha_1, \alpha_2, \dots, \alpha_{n-1}, 1)$$

such that the parallel projection of the hypersurface $V(f) \subset \mathbb{A}^n$ onto the hyperplane $x_n = 0$ along the vector v is **(a)** surjective, **(b)** dominant, **(c)** finite. To begin with, consider the following toy examples in $\mathbb{A}^2$ over $\mathbb{C}$: $V(xy - 1)$, $V\left(x^2 - y\right)$, $V\left(x^2 + 2xy + y^2\right)$.

Problem 11.12 Under the conditions of the previous problem, show that the image of the central projection of $V(f)$ from every point $p \notin V(f)$ onto every hyperplane $H \not\ni p$ contains an open dense subset of H.

Problem 11.13 Prove that the image of a dominant morphism contains an open dense set.

Problem 11.14 Let U be an open subset of an affine algebraic variety X. Let us say that U is *affine* if there exist an affine algebraic variety Y and injective regular morphism $\varphi : Y \hookrightarrow X$ such that $\varphi(Y) = U$ and the pullback map

$$\mathcal{O}_X(U) \xrightarrow{\sim} \Bbbk[Y], \quad f \mapsto f\varphi,$$

is a well-defined isomorphism of $\Bbbk$-algebras. Assume that some elements

$$f_1, f_2, \dots, f_m \in \mathcal{O}_X(U)$$

span a nonproper ideal in $\mathcal{O}_X(U)$, and every principal open subset

$$U_i = \mathcal{D}(f_i) \cap U$$

is affine. Prove that U is also affine.

Problem 11.15 For every rational function $f \in \Bbbk(X)$ on an affine algebraic variety X, prove that the map $f : \mathrm{Dom}(f) \to \Bbbk$, $x \mapsto f(x)$, is continuous in the Zariski topology.

Problem 11.16 Describe $\mathrm{Dom}(f)$ for the rational functions $f = (1-y)/x$, $f = y/x$, and $f = x_1/x_3$ on the affine hypersurfaces $V\left(x^2+y^2-1\right)$, $V\left(x^3+x^2-y^2\right) \subset \mathbb{A}^2$, and $X = V(x_1x_2 - x_3x_4) \subset \mathbb{A}^4$ respectively.

Problem 11.17 (Quotient by a Finite Group Action) Let $\Bbbk$ be an algebraically closed field of characteristic zero, X an affine algebraic variety over $\Bbbk$, and G a finite group acting on X by regular automorphisms. Then G acts on $\Bbbk[X]$ by pullback automorphisms. Write $R = \Bbbk[X]^G \subset \Bbbk[X]$ for the subalgebra of G-invariants. Verify that the *Reynolds operator*

$$\Bbbk[X] \twoheadrightarrow R, \quad f \mapsto f^\natural \stackrel{\text{def}}{=} \frac{1}{|G|}\sum_{\sigma \in G} \sigma^* f,$$

is $\Bbbk$-linear and possesses the following properties, holding for all $f \in \Bbbk[X]$ and $h \in R$:

$$(1)\, f^\natural \in R \quad (2)\ h^\natural = h, \quad (3)\ (fh)^\natural = f^\natural h.$$

Use them to prove that R is a finitely generated reduced $\Bbbk$-algebra, and $\mathrm{Spec}_{\mathrm{m}} R$ can be identified with the set of G-orbits X/G in such a way that the quotient map $\pi : X \twoheadrightarrow X/G$ becomes a finite regular surjection of affine algebraic varieties and possesses the following universal property: for every regular morphism of affine algebraic varieties $\varphi : X \to Y$ satisfying the condition

$$\forall\, \sigma \in G\ \forall\, x \in X, \quad \varphi(\sigma x) = \varphi(x),$$

there exists a unique regular morphism of affine algebraic varieties

$$\psi : X/G \to Y$$

such that $\psi \circ \pi = \varphi$. (Hint: prove that this universal property determines the arrow $X \to X/G$ in the category $\mathcal{A}\!f\!f_{\Bbbk}$ uniquely up to a unique isomorphism, and then show that the arrow $X \to \operatorname{Spec_m} R$ provided by the inclusion $R \hookrightarrow \Bbbk[X]$ is universal.)

Problem 11.18 For $X = \mathbb{C}^2$ and $G = \mathbb{Z}/(n)$ acting on $\mathbb{C}^2$ by the rule

$$[k]_n : (x, y) \mapsto (e^{2\pi ik/n}x, e^{2\pi ik/n}y),$$

describe the quotient variety X/G (defined in Problem 11.17) by explicit polynomial equations in an appropriate affine space.

Problem 11.19 Describe the closure of the unit sphere

$$S^3 = \left\{(z_1, z_2) \in \mathbb{C}^2 : |z_1|^2 + |z_2|^2 = 1\right\}$$

in the Zariski topology on the affine plane $\mathbb{A}(\mathbb{C}^2)$.

Problem 11.20 For the ring $C^0(X)$ of continuous (real- or complex-valued) functions on a compact Hausdorff topological space X, prove that the canonical map $X \to \operatorname{Spec_m} C^0(X)$, $x \mapsto \ker \mathrm{ev}_x$, is bijective and identifies the Zariski topology[23] on $\operatorname{Spec_m} C^0(X)$ with the original topology on X. If the general case seems too abstract, consider $X = [0, 1] \subset \mathbb{R}$ and the algebra of real-valued continuous functions $[0, 1] \to \mathbb{R}$.

Problem 11.21 Is there a nonmaximal prime ideal in the ring of continuous real valued functions on a segment?

[23]Whose closed sets are $V(I) = \{\mathfrak{m} \in \operatorname{Spec_m} C^0(X) \mid I \subset \mathfrak{m}\}$ for all ideals $I \subset C^0(X)$.

Chapter 12
Algebraic Manifolds

Everywhere in this chapter we assume by default that the ground field $\Bbbk$ is algebraically closed.

12.1 Definitions and Examples

The definition of an algebraic manifold follows the same template as the definitions of manifold in topology and differential geometry. It can be outlined as follows: a *manifold* is a topological space X such that every point $x \in X$ possesses an open neighborhood $U \ni x$, called a *local chart*, which is equipped with a homeomorphism $\varphi_U : X_U \xrightarrow{\sim} U$ identifying some standard local model X_U with U, and every pair of local charts $\varphi_U : X_U \xrightarrow{\sim} U$, $\varphi_W : X_W \xrightarrow{\sim} W$ are *compatible*, meaning that the homeomorphism between open subsets $\varphi_U^{-1}(U \cap W) \subset X_U$ and $\varphi_W^{-1}(U \cap W) \subset X_W$ provided by the composition $\varphi_W^{-1} \circ \varphi_U$ is a regular isomorphism. In topology and differential geometry, the local model $X_U = \mathbb{R}^n$ does not depend on U, and the regularity of the *transition homeomorphism*

$$\varphi_{WU} \stackrel{\text{def}}{=} \varphi_W^{-1} \circ \varphi_U\big|_{\varphi_U^{-1}(U\cap W)} : \varphi_U^{-1}(U \cap W) \xrightarrow{\sim} \varphi_W^{-1}(U \cap W)\,, \tag{12.1}$$

means that it will be a diffeomorphism of open subsets in $\mathbb{R}^n$ in differential geometry, and means simply a homeomorphism in topology. In algebraic geometry, the local model X_U is an arbitrary algebraic variety that may depend on $U \subset X$. Thus, an algebraic manifold may look locally, for example, like a union of a line and a plane in $\mathbb{A}^3$, intersecting or parallel, and this picture may vary from chart to chart. The regularity of the homeomorphism (12.1), in algebraic geometry, means that the maps φ_{WU}, $\varphi_{UW} = \varphi_{WU}^{-1}$ are described in affine coordinates by some rational functions, which are regular within both open sets $f_U^{-1}(U \cap W)$, $\varphi_W^{-1}(U \cap W)$. This provides every algebraic manifold X with a well-defined sheaf $\mathcal{O}_X$ of *regular*

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_12

rational functions with values in the ground field $\Bbbk$, in the same manner as the *smooth* functions on a manifold are introduced in differential geometry.

Let us now give precise definitions. Given a topological space X, an *affine chart* on X is a homeomorphism $\varphi_U : X_U \xrightarrow{\sim} U$ between an affine algebraic variety X_U over $\Bbbk$, considered with the Zariski topology, and an open subset $U \subset X$, considered with the topology induced from X. Two affine charts $\varphi_U : X_U \xrightarrow{\sim} U$, $\varphi_W : X_W \xrightarrow{\sim} W$ on X are called *compatible* if the pullback map $\varphi^*_{WU} : f \mapsto f \circ \varphi_{WU}$, provided by the transition homeomorphism (12.1), establishes a well-defined isomorphism of $\Bbbk$-algebras[1] $\mathcal{O}_{X_W}\left(\varphi_W^{-1}(U \cap W)\right) \xrightarrow{\sim} \mathcal{O}_{X_U}\left(\varphi_U^{-1}(U \cap W)\right)$. An open covering $X = \bigcup U_\nu$ by mutually compatible affine charts $U_\nu \subset X$ is called an *algebraic atlas* on X. Two algebraic atlases are declared to be *equivalent* if their union is an algebraic atlas as well. A topological space X equipped with an equivalence class of algebraic atlases is called an *algebraic manifold* or *algebraic variety*.[2] An algebraic manifold is said to be of *finite type* if it allows a finite algebraic atlas.

Exercise 12.1 Verify that every algebraic manifold of finite type is a Noetherian topological space in the sense of Remark 11.2 on p. 252.

Example 12.1 (Projective Spaces) The projective space[3] $\mathbb{P}_n = \mathbb{P}\left(\Bbbk^{n+1}\right)$ with homogeneous coordinates $x = (x_0 : x_1 : \cdots : x_n)$ is covered by the $(n+1)$ standard affine charts[4] $U_i = \{(x_0 : x_1 : \cdots : x_n) \mid x_i \neq 0\}$, $0 \leqslant i \leqslant n$. Write $X_i = \mathbb{A}(\Bbbk^n)$ for the affine space with coordinates[5] $t_i = (t_{i,0}, \ldots, t_{i,i-1}, t_{i,i+1}, \ldots, t_{i,n})$. For each i, there exists a bijection

$$\varphi_i : X_i \xrightarrow{\sim} U_i\,, \quad t_i \mapsto (t_{i,0} : \cdots : t_{i,i-1} : 1 : t_{i,i+1} : \cdots : t_{i,n})\,. \tag{12.2}$$

The preimage of the intersection $U_i \cap U_j$ under this bijection is the principal open set $\mathcal{D}\left(t_{i,j}\right) \subset X_i$.

Exercise 12.2 Verify that the transition map

$$\varphi_{ji} = \varphi_j^{-1}\varphi_i : \mathcal{D}\left(t_{i,j}\right) \xrightarrow{\sim} \mathcal{D}\left(t_{j,i}\right), t_i \mapsto t_{i,j}^{-1} \cdot t_j,$$

establishes a regular isomorphism between affine algebraic varieties

$$\mathcal{D}\left(t_{i,j}\right) = \operatorname{Spec_m} \Bbbk\left[t_{i,j}^{-1}, t_{i,0}, \ldots, t_{i,i-1}, t_{i,i+1}, \ldots, t_{i,n}\right],$$
$$\mathcal{D}\left(t_{j,i}\right) = \operatorname{Spec_m} \Bbbk\left[t_{j,i}^{-1}, t_{j,0}, \ldots, t_{j,j-1}, t_{j,j+1}, \ldots, t_{j,n}\right].$$

---

[1] Recall that $\mathcal{O}_Z(V) = \{f \in \Bbbk(Z) \mid V \subset \operatorname{Dom}(f)\}$ denotes the algebra of rational functions, regular in $V \subset Z$, on an affine algebraic variety Z (see Sect. 11.4.1 on p. 254 for details).

[2] Without the epithet "affine."

[3] See Chap. 11 of Algebra I.

[4] See Example 11.2 of Algebra I.

[5] The first index i is the order number of the chart, while the second index numbers the coordinates within the ith chart and takes n values $0 \leqslant \nu \leqslant n$, $\nu \neq i$.

Therefore, transferring the Zariski topology from $X_i \simeq \mathbb{A}^n$ to U_i by means of the bijection (12.2) provides $\mathbb{P}_n$ with a well-defined topology whose restriction to $U_i \cap U_j$ does not depend on what source, X_i or X_j, it comes from. In this topology, all bijections (12.2) certainly are homeomorphisms. Thus, $\mathbb{P}_n$ is an algebraic manifold of finite type locally isomorphic to the affine space $\mathbb{A}^n$.

Example 12.2 (Grassmannians) Recall[6] that the set of all k-dimensional vector subspaces in a given vector space V over $\Bbbk$ is called the *Grassmannian* $\mathrm{Gr}(k, V)$, and for the coordinate space $V = \Bbbk^m$ we write $\mathrm{Gr}(k, m)$ instead of $\mathrm{Gr}(k, \Bbbk^m)$. We have seen in Sect. 2.6.5 that the points of $\mathrm{Gr}(k, m)$ can be viewed as the orbits of $k \times m$ matrices of rank k under the natural action of $\mathrm{GL}_k(\Bbbk)$ by left multiplication. The orbit of the matrix x corresponds to the subspace $U_x \subset \Bbbk^m$ spanned by the rows of x, and x is recovered from U_x up to the action $\mathrm{GL}_k(\Bbbk)$ as the matrix whose rows are the coordinates of some linearly independent vectors $u_1, u_2, \dots, u_k \in U_x$ in the standard basis of $\Bbbk^m$. This leads to the following covering of $\mathrm{Gr}(k, m)$ by $\binom{m}{k}$ affine charts $U_I \simeq \mathbb{A}^{k(m-k)}$, called *standard* and numbered by increasing collections of indices $I = (i_1, i_2, \dots, i_k)$, $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m$. Write $s_I(x)$ for the $k \times k$ submatrix of the $k \times m$ matrix x formed by the columns with numbers $i_1, i_2, \dots, i_k$, and U_I for the set of $\mathrm{GL}_k(\Bbbk)$-orbits of all matrices x with $\det s_I(x) \neq 0$. Every such orbit contains a unique matrix z with $s_I(z) = E$, namely, $z = s_I(x)^{-1} \cdot x$.

Exercise 12.3 Convince yourself that U_I consists of the k-dimensional subspaces $W \subset \Bbbk^m$ that are isomorphically projected onto the coordinate k-plane spanned by the standard basis vectors $e_{i_1}, e_{i_2}, \dots, e_{i_k}$ along the transversal coordinate $(m-k)$-plane spanned by the remaining standard basis vectors.

Write $X_I = \mathrm{Mat}_{k\times(m-k)}(\Bbbk) \simeq \mathbb{A}^{k(m-k)}$ for the affine space of $k \times (m-k)$ matrices whose columns are numbered in order by the collection of indices $\overline{I} = \{1, 2, \dots, m\} \smallsetminus I$, complementary to I. There is a bijection $\varphi_I : X_I \xrightarrow{\sim} U_I$, $t \mapsto \mathrm{GL}_k(\Bbbk)\cdot\varphi_I(t)$, where the $k\times m$ matrix $\varphi_I(t)$ has $s_I(\varphi_I(t)) = E$, and $s_{\overline{I}}(\varphi_I(t)) = t$, i.e., it is obtained from t by the order-preserving insertion of the columns of E between the columns of t in such the way that the columns of E are assigned the numbers $i_1, i_2, \dots, i_k$ in the resulting $k \times m$ matrix.

Exercise 12.4 Verify that the inverse bijection maps $x \mapsto s_{\overline{I}}\left(s_I(x)^{-1} \cdot x\right)$, and the result does not depend on the choice of x in the orbit $\mathrm{GL}_k(\Bbbk) \cdot x$.

Therefore, $\varphi_I^{-1}(U_I \cap U_J)$ is the principal open set $\mathcal{D}\big(\det s_J(\varphi_I(t))\big)$ in X_I. The transition map

$$\varphi_{JI} = \varphi_J^{-1}\varphi_I$$

sends $\mathcal{D}\big(\det s_J(\varphi_I(t))\big) \subset X_I$ to $\mathcal{D}\big(\det s_I(\varphi_J(t))\big) \subset X_J$ by the rule

$$t \mapsto s_{\overline{J}}\Big(s_J^{-1}\big(\varphi_I(t)\big) \cdot \varphi_I(t)\Big)$$

[6] See Sect. 2.6.4 on p. 49.

and gives a regular isomorphism of affine algebraic varieties. The inverse isomorphism maps $t \mapsto s_{\overline{I}}\left(s_I^{-1}(\varphi_J(t)) \cdot \varphi_J(t)\right)$.

Exercise 12.5 Check this.

The same arguments as in the previous example show that $\mathrm{Gr}(k, n)$ is an algebraic variety of finite type locally isomorphic to the affine space

$$\mathbb{A}^{k(m-k)} = \mathbb{A}\left(\mathrm{Mat}_{k\times(m-k)}(\Bbbk)\right) .$$

Note that for $k = 1$, $m = n + 1$, the standard algebraic atlas $\{U_I\}$ on $\mathrm{Gr}(k, m)$ is precisely the standard atlas $\{U_i\}$ on $\mathbb{P}_n$ described in Example 12.1.

Example 12.3 (Direct Product of Algebraic Manifolds) The set-theoretic direct product of algebraic manifolds X, Y is canonically equipped with the algebraic atlas formed by the mutual direct products $U \times W$ of affine charts $U \subset X$, $W \subset X$. Thus, $X \times Y$ is an algebraic manifold.

12.1.1 Structure Sheaf and Regular Morphisms

Given an algebraic manifold X, a function $f : X \to \Bbbk$ is called *regular* at a point $x \in X$ if there exist an affine chart $\varphi_W : X_W \xrightarrow{\sim} W$ with $x \in W$ and a rational function $\widetilde{f} \in \Bbbk(X_W)$ such that $\varphi_W^{-1}(x) \in \mathrm{Dom}(\widetilde{f})$ and $\varphi_W^* f(z) = \widetilde{f}(z)$ for all $z \in \mathrm{Dom}\widetilde{f}$. For an open subset $U \subset X$, the functions $U \to \Bbbk$ regular everywhere in U form a $\Bbbk$-algebra denoted by $\mathcal{O}_X(U)$ and called the *algebra of regular functions* on U. The assignment $U \mapsto \mathcal{O}_X(U)$ provides the topological space X with a sheaf of $\Bbbk$-algebras,[7] called the *structure sheaf* or the *sheaf of regular functions* on X.

Exercise 12.6 For every affine chart $\varphi_U : X_U \xrightarrow{\sim} U$ on X, verify that the pullback of the regular functions along φ_U assigns the isomorphism $\varphi_U^* : \mathcal{O}_X(U) \xrightarrow{\sim} \Bbbk[X_U]$.

A map of algebraic manifolds $f : X \to Y$ is called a *regular morphism* if f is continuous and for every open $U \subset Y$, the pullback of regular functions along $f|_U$ gives a well-defined homomorphism of $\Bbbk$-algebras $f|_U^* : \mathcal{O}_Y(U) \to \mathcal{O}_X\left(\varphi^{-1}(U)\right)$, $h \mapsto h \circ f$.

Exercise 12.7 Identify $\mathcal{O}_X(X)$ with the set of regular morphisms $X \to \mathbb{A}^1$.

12.1.2 Closed Submanifolds

Let X be an algebraic manifold. Every closed subset $Z \subset X$ possesses a natural structure of an algebraic manifold. Namely, for every affine chart $\varphi_U : X_U \xrightarrow{\sim} U$,

[7] See Example 9.8 on p. 194.

the set $\varphi_U^{-1}(Z \cap U)$ is closed in the affine algebraic variety X_U and therefore has a natural structure of an affine algebraic variety with the coordinate algebra

$$\Bbbk[X_U]/\varphi_U^* I(Z \cap U) \simeq \mathcal{O}_X(U)/I(Z \cap U)\,,$$

where $I(Z \cap U) = \{f \in \mathcal{O}_X(U) \mid f(z) = 0 \text{ for all } z \in Z \cap U\}$. The affine charts

$$\varphi_U^{-1}(Z \cap U) \simeq Z \cap U \subset Z$$

certainly form an algebraic atlas on Z. The assignment $U \mapsto I(Z \cap U)$ defines the sheaf of ideals on X, denoted by $\mathcal{I}_Z \subset \mathcal{O}_X$ and called the *ideal sheaf* of the *closed submanifold* $Z \subset X$.

Every sheaf of ideals $\mathcal{J} \subset \mathcal{O}_X$ determines a closed submanifold $V(\mathcal{J}) \subset X$ whose intersection with every affine chart $U \subset X$ is the zero set of the ideal $\mathcal{J}(U) \subset \mathcal{O}_X(U) \simeq \Bbbk[X_U]$ in the affine algebraic variety X_U. Note that the ideal sheaf $\mathcal{I}(V(\mathcal{J})) = \sqrt{\mathcal{J}}$ does not necessarily coincide with the sheaf $\mathcal{J}$ of equations describing the submanifold $V(\mathcal{J})$.

A regular morphism $f : X \to Y$ is called a *closed immersion* if $f(X) \subset Y$ is a closed submanifold of Y and f establishes an isomorphism between X and $f(X)$.

Exercise 12.8 Convince yourself that an algebraic manifold X admits a closed immersion in an affine space if and only if X is an affine algebraic variety in the sense of Sect. 11.1 on p. 241.

12.1.3 Families of Manifolds

Every regular morphism $\pi : X \to Y$ can be viewed as a family of closed submanifolds $X_y = \pi^{-1}(y) \subset X$ parametrized by the points $y \in Y$. In this case, Y is referred to as the *base* of the family π. Given two families $\pi : X \to Y$, $\pi' : X' \to Y$ over the same base Y, a regular morphism $\varphi : X \to X'$ is called a *morphism of families* or *morphism over* Y if $\pi = \pi' \circ \varphi$, i.e., if φ maps X_y to X'_y for all $y \in Y$. A family $\pi : X \to Y$ is called *constant* or *trivial* if it is isomorphic over Y to the canonical projection $\pi_Y : X_0 \times Y \to Y$ from the direct product of the base and some fixed manifold X_0.

12.1.4 Separated Manifolds

The standard atlas on $\mathbb{P}_1$ consists of two charts:

$$\varphi_i : \mathbb{A}^1 \simeq U_i \subset \mathbb{P}_1\,, \quad i = 0, 1\,.$$

Their intersection is visible within each chart as the complement to the origin,

$$\varphi_0^{-1}(U_0 \cap U_1) = \varphi_1^{-1}(U_0 \cap U_1) = \mathbb{A}^1 \smallsetminus \{O\} = \left\{t \in \mathbb{A}^1 \mid t \neq 0\right\} .$$

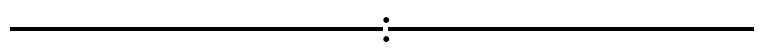
The charts are glued together along this intersection by means of the transition map

$$\varphi_{01} : t \mapsto 1/t\,. \tag{12.3}$$

If instead of the rational map (12.3), we use the much simpler gluing rule

$$\tilde{\varphi}_{01} : t \mapsto t\,, \tag{12.4}$$

we get another manifold that looks like an affine line with a double origin:

 .

Such pathology is called *nonseparateness*. It has appeared because the gluing rule (12.4) considered as a binary relation on $\mathbb{A}^1$, i.e., as a subset of $\mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2$, is not closed. Namely, it is provided by the line $x = y$ without the point $x = y = 0$. This gluing rule can be completed by continuity up to the whole line $x = y$, whereupon the double point disappears.

In the general situation, the separateness phenomenon is formalized as follows. By the universal property of the direct product, for every two affine charts U_0, U_1 on an algebraic manifold X, the inclusions $U_0 \hookleftarrow U_0 \cap U_1 \hookrightarrow U_1$ produce the inclusion

$$U_0 \cap U_1 \hookrightarrow U_0 \times U_1\,,$$

whose image is the intersection of the affine chart $U_0 \cap U_1$ on the manifold $X \times X$ with the diagonal $\Delta_X = \{(x, x) \in X \times X \mid x \in X\}$. In other words, the gluing rule for charts U_0, U_1, considered as a subset of $U_0 \times U_1$, is $\Delta \cap U_0 \times U_1$. For example, the gluing rule (12.3) corresponds to the immersion $(\mathbb{A}^1 \smallsetminus O) \hookrightarrow \mathbb{A}^2$, $t \mapsto (t\,,\, t^{-1})$, whose image $\Delta_{\mathbb{P}_1} \cap U_0 \times U_1$ is a closed subset of $U_0 \times U_1 \simeq \mathbb{A}^2$, namely, the hyperbola $xy = 1$. In contrast, the trivial transition map (12.4) produces the immersion $(\mathbb{A}^1 \smallsetminus O) \hookrightarrow \mathbb{A}^2$, $t \mapsto (t\,,\, t)$, whose image is not closed in $\mathbb{A}^2$. An algebraic manifold X is called *separated* if the diagonal $\Delta_X \subset X \times X$ is closed in $X \times X$. In more expanded form, this means that for every pair of affine charts $U, W \subset X$, the canonical map $U \cap W \hookrightarrow U \times W$ is a closed immersion.

For example, both $\mathbb{A}^n$ and $\mathbb{P}_n$ are separated, because the diagonals in $\mathbb{A}^n \times \mathbb{A}^n$ and $\mathbb{P}_n \times \mathbb{P}_n$ are described by the polynomial equations $x_i = y_i$ and $x_i y_j = x_j y_i$ respectively.[8] Every closed submanifold $X \subset Y$ in a separated manifold Y is

[8]The first formula relates $2n$ affine coordinates $(x_1, \dots, x_n, y_1, \dots, y_n)$ in $\mathbb{A}^n \times \mathbb{A}^n = \mathbb{A}^{2n}$, whereas the second deals with two collections of homogeneous coordinates $(x_0 : x_1 : \cdots : x_n)$, $(y_0 : y_1 : \cdots : y_n)$ on $\mathbb{P}_n \times \mathbb{P}_n$ (note that they cannot be combined into one collection). We will

separated as well, because the diagonal of $X \times X$ is the preimage of the diagonal $\Delta_Y \subset Y \times Y$ under the regular map $X \times X \hookrightarrow Y \times Y$ provided by the inclusion $X \hookrightarrow Y$. In particular, all affine and projective varieties are separated and have finite type.

Example 12.4 (Graph of a Regular Map) Let $\varphi : X \to Y$ be a regular morphism of algebraic manifolds. The preimage of the diagonal $\Delta_Y \subset Y \times Y$ under the map $\varphi \times \mathrm{Id}_Y : X \times Y \to Y \times Y$ is called the *graph* of φ and denoted by Γ_φ. Set-theoretically, $\Gamma_\varphi = \{(x, f(x)) \in X \times Y \mid x \in X\}$. If Y is separated, the graph of every regular morphism $\varphi : X \to Y$ is closed. For example, the graph of a regular morphism of affine algebraic varieties $\varphi : \mathrm{Spec_m}(A) \to \mathrm{Spec_m}(B)$ is described by a system of equations $1 \otimes f = \varphi^*(f) \otimes 1$ in $A \otimes B$, where f runs through B.

12.1.5 Rational Maps

Let X be an algebraic manifold and $U \subset X$ an open subset. A regular morphism $\varphi : U \to Y$ is called a *rational map* from X to Y. Given such a map, we write $\varphi : X \dashrightarrow Y$, although this discards the information about U. A regular morphism $\psi : W \to Y$ is called an *extension* of φ if $W \supset U$ and $\psi|_U = \varphi$. The union of all open sets $W \supset U$ on which φ can be extended is called the *domain* of the rational map $\varphi : X \dashrightarrow Y$ and denoted by $\mathrm{Dom}(\varphi)$.

Exercise 12.9 (Cremona's Quadratic Involution) Verify that the prescription

$$(x_0 : x_1 : x_2) \mapsto \left(x_0^{-1} : x_1^{-1} : x_2^{-1}\right)$$

determines a rational map $\varkappa : \mathbb{P}_2 \dashrightarrow \mathbb{P}_2$ whose domain is the whole of $\mathbb{P}_2$ except three points. Find these points and describe the image of $\varkappa$.

Despite its name, a rational map $\varphi : X \dashrightarrow Y$ is not a map "from X" in the set-theoretic sense, because φ may be undefined at some points. In particular, the composition of rational maps may be undefined, e.g., if the image of the first map falls outside the domain of the second. However, rational maps often appear in various applications and play an important role within algebraic geometry itself. For example, the tautological projection $\mathbb{A}(V) \dashrightarrow \mathbb{P}(V)$, which sends a point of $\mathbb{A}(V)$ provided by a vector $v \in V$ to the point of $\mathbb{P}(V)$ provided by the same vector, is a surjective rational map that is regular everywhere outside the origin.

---

see in Exercise 12.12 that the latter equations actually determine a closed submanifold of $\mathbb{P}_n \times \mathbb{P}_n$ in the sense of Sect. 12.1.2.

12.2 Projective Varieties

An algebraic manifold X is called *projective* if it admits a closed immersion into projective space, i.e., is isomorphic to a closed submanifold of $\mathbb{P}_n$ for some $n \in \mathbb{N}$.

Exercise 12.10 Verify that the solution set of every system of homogeneous polynomial equations in the homogeneous coordinates in $\mathbb{P}_n$ is a closed submanifold of $\mathbb{P}_n$.

Example 12.5 (Plücker Coordinates) The *Plücker embedding*

$$p_{k,V} : \mathrm{Gr}(k, V) \hookrightarrow \mathbb{P}(\Lambda^k V)\,, \quad U \mapsto \Lambda^k U\,, \tag{12.5}$$

from Sect. 2.6.4 on p. 49, maps the Grassmannian $\mathrm{Gr}(k, V)$ isomorphically onto the projective algebraic variety determined in $\mathbb{P}(\Lambda^k V)$ by the quadratic Plücker relations from formula (2.49) on p. 48. In the matrix notation from Example 12.2 on p. 267, the Plücker embedding maps the $k \times m$ matrix x_U formed by the coordinate rows of some basis vectors in $U \subset \Bbbk^n$ expanded through the standard basis vectors $e_i \in \Bbbk^n$ to the point of $\mathbb{P}(\Lambda^k \Bbbk^m)$ whose Ith homogeneous coordinate in the basis

$$e_I = e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$$

equals $\det s_I(x_U)$, the degree-k minor of x_U situated in the columns with numbers from I.

Exercise 12.11 Check this and convince yourself that the Plücker embedding is regular.

The collection of $\binom{k}{n}$ minors $\det s_I(x_U)$ is called the set of *Plücker coordinates* of the subspace $U \subset \Bbbk^n$. Since the pullbacks of the coordinate functions on $\mathbb{P}(\Lambda^k \Bbbk^n)$ are polynomials in affine coordinates on the Grassmannian, the map (12.5) is a regular closed immersion of the Grassmannian into projective space. Therefore, the Grassmannians, as well as all their closed submanifolds, are projective algebraic varieties.

Exercise 12.12 Show that the direct product of projective manifolds is projective, and use this to prove that every subset of $\mathbb{P}_{n_1} \times \mathbb{P}_{n_2} \times \cdots \times \mathbb{P}_{n_m}$ defined by a system of polynomial equations in homogeneous coordinates such that every equation is homogeneous in every set of coordinates is a projective algebraic variety.

Example 12.6 (Blowup of a Point on $\mathbb{P}_n$) All the lines passing through a given point $p \in \mathbb{P}_n$ form the projective space $E \simeq \mathbb{P}_{n-1}$. The incidence graph

$$\mathcal{B}_p = \{(q, \ell) \in \mathbb{P}_n \times E \mid q \in \ell\}$$

is called the *blowup* of the point $p \in \mathbb{P}_n$. The projection $\sigma_p : \mathcal{B}_p \twoheadrightarrow \mathbb{P}_n$ is one-to-one over $\mathbb{P}_n \smallsetminus \{p\}$, whereas the preimage of p coincides with the whole space E,

$$\sigma_p^{-1}(p) = \{p\} \times E \subset \mathbb{P}_n \times E\,.$$

This fiber is called the *exceptional divisor*[9] of the blowup. The second projection $\varrho_E : \mathcal{B}_p \twoheadrightarrow E$ represents $\mathcal{B}_p$ as a *line bundle* over E, i.e., the family of projective lines $(pq) \subset \mathbb{P}_n$ parametrized by the points $q \in E$. This line bundle is called the *tautological line bundle* over the projective space E. It follows from Exercise 12.12 that $\mathcal{B}_p$ is a projective algebraic manifold. Indeed, choose homogeneous coordinates in $\mathbb{P}_n$ such that $p = (1 : 0 : \cdots : 0)$, and identify E with the projective hyperplane $Z(x_0) = \{(0 : \lambda_1 : \cdots : \lambda_n)\} \subset \mathbb{P}_n$ by mapping a line $\ell \ni p$ to the point $\lambda = \ell \cap Z(x_0)$. Then the collinearity of points p, q, λ is equivalent to the following system of homogeneous quadratic equations in the pair $(q, \lambda) \in \mathbb{P}_n \times E$:

$$\operatorname{rk}\begin{pmatrix} 1 & 0 & \cdots & 0 \\ q_0 & q_1 & \cdots & q_n \\ 0 & \lambda_1 & \cdots & \lambda_n \end{pmatrix} = 2 \quad \text{or} \quad q_i t_j = q_j t_i\,,\ 1 \leqslant i < j \leqslant n\,.$$

Geometrically, the blowup of $p \in \mathbb{P}_n$ can be imagined as the replacement of the point p by the projective space E glued to the space $\mathbb{P}_n$, punctured at p, in such a way that every line $\ell \subset \mathbb{P}_n$ approaching p passes through the point $\ell \in E$.

Lemma 12.1 *Every closed submanifold $X \subset \mathbb{P}_n$ can be described as a set of solutions to some system of homogeneous polynomial equations in homogeneous coordinates in $\mathbb{P}_n$.*

Proof We write $(x_0 : x_1 : \cdots : x_n)$ for the homogeneous coordinates in $\mathbb{P}_n$ and use the notation from Example 12.1 on p. 266 for the standard affine charts $U_i \subset \mathbb{P}_n$ and the standard affine coordinates $t_{i,j}$ therein. For each i, the intersection $X \cap U_i$ is the zero set $V(I_i)$ of some ideal I_i in the polynomial ring in n variables $t_{i,\nu} = x_\nu / x_i$, $0 \leqslant \nu \leqslant n$, $\nu \neq i$. Every polynomial f in this ring can be rewritten as[10] $\overline{f}(x_0, x_1, \ldots, x_n)/x_i^d$, where $d = \deg f$ and $\overline{f} \in \Bbbk[x_0, x_1, \ldots, x_n]$ is the unique homogeneous polynomial of degree d such that

$$\overline{f}\,(t_{i,0}, \ldots, t_{i,i-1}, 1, t_{i,i+1}, \ldots, t_{i,n}) = f\,(t_{i,0}, \ldots, t_{i,i-1}, t_{i,i+1}, \ldots, t_{i,n})\ .$$

Let us fix generators $f_{i,\alpha}$ of the ideal I_i and write $\overline{f}_{i,\alpha} \in \Bbbk[x_0, x_1, \ldots, x_n]$ for their homogenizations just described. Then X coincides with the solution set Z of the system of polynomial equations $x_i \cdot \overline{f}_{i,\alpha}(x_0, x_1, \ldots, x_n) = 0$, where $0 \leqslant i \leqslant n$ and for each i, α numbers the chosen generators $f_{i,\alpha}$ of the ideal I_i. To check

[9] Given an irreducible algebraic manifold X, a (*Weil*) *divisor* on X is an element of the free abelian group generated by all closed irreducible submanifolds of codimension 1 in X (the dimensions of algebraic varieties will be discussed in Sect. 12.5 on p. 281).

[10] Compare with Sect. 11.3.2 of Algebra I.

this, it is enough to establish the coincidence $Z \cap U_i = X \cap U_i$ for every i. In terms of the affine coordinates $t_{i,j}$ on U_i, the intersection of U_i with the zero set $Z\big(x_i \cdot \overline{f}(x_0, x_1, \dots, x_n)\big) \subset \mathbb{P}_n$ of a homogeneous polynomial $x_i\overline{f}$ is described by the equation

$$\overline{f}\,(t_{i,0}, \dots, t_{i,i-1}, 1, t_{i,i+1}, \dots, t_{i,n}) = f\,(t_{i,0}, \dots, t_{i,i-1}, t_{i,i+1}, \dots, t_{i,n}) = 0\,.$$

Hence, U_i intersects the set of common zeros of the polynomials $x_i \cdot \overline{f}_{i,\alpha}$, whose i coincides with i of the chart, exactly along the set $X \cap U_i$. Therefore, $Z \cap U_i \subset X \cap U_i$. It remains to check that every homogeneous polynomial $x_j \cdot \overline{f}_{j,\beta}$ with $j \neq i$ vanishes on $X \cap U_i$ as well. The first factor x_j vanishes along the hyperplane $V(t_{i,j}) \subset U_i$. The principal open set in $X \cap U_i$ complementary to this hyperplane lies within

$$X \cap U_i \cap U_j \subset X \cap U_j.$$

As we have already seen, the second factor $\overline{f}_{j,\beta}$ vanishes on $\overline{f}_{j,\beta}$. □

Example 12.7 (Illustration to the Proof of Lemma 12.1) The zero set of the homogeneous polynomial $x_0x_1x_2$ on $\mathbb{P}_2$ is the union of three lines complementary to the standard affine charts. The affine equations of this set in the charts U_0, U_1, U_2 are, respectively, $t_{0,1}t_{0,2} = 0$, $t_{1,0}t_{1,2} = 0$, $t_{2,0}t_{2,1} = 0$. Let $X \subset \mathbb{P}_2$ be the closed submanifold locally described by these equations. Applied to this X, the previous proof transforms the left-hand sides of the local affine equations to the homogeneous polynomials $\overline{f}_{0,1} = x_1x_2$, $\overline{f}_{1,1} = x_0x_2$, $\overline{f}_{2,1} = x_0x_1$, and then gives $x_0 \cdot \overline{f}_{0,1} = 0$, $x_1 \cdot \overline{f}_{1,1} = 0$, $x_2 \cdot \overline{f}_{2,1} = 0$ as the global homogeneous equations for X. They all coincide with the initial equation $x_0x_1x_2 = 0$ in our case.

12.3 Resultant Systems

Given a system of homogeneous polynomial equations

$$\begin{cases} f_1(x_0, x_1, \dots, x_n) = 0\,, \\ f_2(x_0, x_1, \dots, x_n) = 0\,, \\ \quad \cdots \\ f_m(x_0, x_1, \dots, x_n) = 0\,, \end{cases} \tag{12.6}$$

where every $f_i \in \Bbbk[x_0, x_1, \dots, x_n]$ is homogeneous of degree d_i, the set of its solutions, considered up to proportionality, is the intersection of m projective hypersurfaces $S_i = Z(f_i) \subset \mathbb{P}(V)$, where $V = \Bbbk^{n+1}$. The projective hypersurfaces of degree d in $\mathbb{P}(V)$ can be viewed as points of the projective space $\mathbb{P}(S^dV^*)$. All collections of hypersurfaces $(S_1, S_2, \dots, S_m)$ of given degrees $d_1, d_2, \dots, d_m$ with nonempty intersection $\bigcap_i S_i \neq \varnothing$ form the figure

$$\mathcal{R}(n+1;\, d_1, d_2, \dots, d_m) \subset \mathbb{P}(S^{d_1}V^*) \times \mathbb{P}(S^{d_2}V^*) \times \cdots \times \mathbb{P}(S^{d_m}V^*)\,, \tag{12.7}$$

called the *resultant variety* of the homogeneous system (12.6). When $m = n + 1$ and all $d_i = 1$, the system (12.6) becomes a system of linear equations $Ax = 0$ with square matrix $A = \left(a_{ij}\right)$. It has a nonzero solution if and only if $\det\left(a_{ij}\right) = 0$. Thus, in this simplest case, the resultant variety is a projective variety determined by one multilinear equation of total degree $n + 1$ in the coefficients $a_{i,j}$. We are going to check that the resultant variety (12.7) can always be described by a system of polynomial equations in the coefficients of the polynomials f_i. This system is called a *resultant system*. It depends only on the number of variables and degrees d_i, and every equation of the system is homogeneous in the coefficients of each polynomial.

Write $J = (f_1, f_2, \dots, f_m) \subset \Bbbk[x_0, x_1, \dots, x_n]$ for the ideal spanned by the polynomials. If $V(J)$ is exhausted by the origin, then every coordinate linear form x_i vanishes on $V(J)$, and therefore, all x_i^m belong to J for some $m \in \mathbb{N}$ by the strong Nullstellensatz. This forces J to contain all homogeneous polynomials of degree $d > (m-1)(n+1)$. Conversely, if $J \supset S^d V^*$ for all $d \gg 0$, then the system (12.6) implies the equations $x_0^d = x_1^d = \cdots = x_n^d = 0$ and therefore has only the zero solution. For every $d \in \mathbb{N}$, the intersection $J \cap S^d V^*$ coincides with the image of the $\Bbbk$-linear map

$$\mu_d : S^{d-d_1} V^* \oplus S^{d-d_2} V^* \oplus \cdots \oplus S^{d-d_m} V^* \xrightarrow{(g_0, g_1, \dots, g_n) \mapsto \sum g_\nu f_\nu} S^d . \tag{12.8}$$

The matrix of this map in the standard monomial basis consists of zeros and the coefficients of the polynomials f_ν. For $d \gg 0$, the dimension of the left-hand side in (12.8) grows as

$$\sum_{\nu=1}^{m} \binom{n + d - d_\nu}{n} \sim \frac{m}{n!} d^n$$

and becomes greater than the dimension of the right-hand side, which grows as

$$\binom{n+d}{n} \sim \frac{1}{n!} d^n .$$

Thus, for every $d \gg 0$, the condition $S^d V^* \not\subset J$, that is, the nonsurjectivity of the map (12.8), means that the rank of the matrix of μ_d is not maximal. This is equivalent to the vanishing of all minors of the matrix of maximal degree. Thus, the resultant variety is the zero set of all these equations written for all d such that the dimension of the left-hand side of (12.8) is not less than that of the right-hand side. Since the polynomial ring is Noetherian, this huge system of equations is equivalent to some finite subsystem. If the ideal of the resultant variety (12.7) is not principal, such a system of resultants is not unique in general.

12.3.1 Resultant of Two Binary Forms

If a ground field $\Bbbk$ is algebraically closed, every homogeneous binary form $A(t_0, t_1) = a_0\, t_1^d + a_1\, t_0\, t_1^{d-1} + a_2\, t_0^2\, t_1^{d-2} + \cdots + a_{d-1}\, t_0^{d-1}\, t_1 + a_d\, t_0^d$ splits into a product of linear forms[11]

$$A(t_0, t_1) = \prod_{i=0}^{d} \left(\alpha_i'' t_0 - \alpha_i' t_1\right) = \prod_{i=0}^{d} \det \begin{pmatrix} t_0 & t_1 \\ \alpha_i' & \alpha_i'' \end{pmatrix}$$

corresponding to the roots[12] $\alpha_1, \alpha_2, \dots, \alpha_d \in \mathbb{P}_1$, $\alpha_i = (\alpha_i' : \alpha_i'')$, of the polynomial A. The coefficients of A are expressed as homogeneous polynomials in the roots by means of the *homogeneous Viète formulas*

$$a_k = (-1)^{d-k} \sigma_k \left(\alpha', \alpha''\right)\,, \text{ where } \sigma_k \left(\alpha', \alpha''\right) = \sum_{\#I=k} \Big(\prod_{i \in I} \alpha_i' \cdot \prod_{j \notin I} \alpha_j'' \Big)\,,$$

where I runs through the strictly increasing sequences of k indices. In particular, a_k is bihomogeneous of bidegree $(k, d-k)$ in (α', α''). Let us fix two degrees $r, s \in \mathbb{N}$ and consider the polynomial ring $\Bbbk[\alpha', \alpha'', \beta', \beta'']$ in four collections of variables

$$\alpha' = (\alpha_1', \alpha_2', \dots, \alpha_s')\,, \quad \alpha'' = (\alpha_1'', \alpha_2'', \dots, \alpha_s'')\,,$$
$$\beta' = (\beta_1', \beta_2', \dots, \beta_r')\,, \quad \beta'' = (\beta_1'', \beta_2'', \dots, \beta_r'')\,.$$

Within this ring, consider the product

$$R_{AB} \stackrel{\text{def}}{=} \prod_{i,j} \left(\alpha_i' \beta_j'' - \alpha_i'' \beta_j'\right) = \prod_{j=1}^{s} A(\beta_j) = (-1)^{rs} \prod_{i=1}^{r} B(\alpha_i)\,.$$

It evaluates to zero if and only if two binary forms

$$A(t_0, t_1) = \sum_{i=0}^{s} a_i\, t_0^i\, t_1^{n-i} \quad \text{and} \quad B(t_0, t_1) = \sum_{j=0}^{r} b_j\, t_0^j\, t_1^{m-j}$$

with coefficients $a_i = (-1)^{n-i} \sigma_i(\alpha', \alpha'')$ and $b_j = (-1)^{m-j} \sigma_j(\beta', \beta'')$ have a common root in $\mathbb{P}_1$. The polynomial $R_{A,B}$ is bihomogeneous of bidegree (rs, rs) in (α, β). Let us show that it can be expressed as a polynomial in the coefficients of

[11] See Example 11.6 of Algebra I, especially formula (11.14) there.

[12] That is, to the points of the "hypersurface" $Z(A) \subset \mathbb{P}_1$, some of which may be multiple.

the forms A, B by *Sylvester's formula*

$$R_{AB} = \det \underbrace{\begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_s & & & \\ & a_0 & a_1 & \cdots & \cdots & a_s & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_s \\ b_0 & b_1 & \cdots & \cdots & b_r & & & \\ & b_0 & b_1 & \cdots & \cdots & b_r & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & b_0 & b_1 & \cdots & \cdots & b_r \end{pmatrix}}_{r+s} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} s \end{matrix} \,. \tag{12.9}$$

For $n = 1$, $m = 2$, the linear map (12.8) becomes $\mu_d : S^{d-s}V^* \oplus S^{d-r}V^* \to S^dV^*$, where

$$\dim V^* = 2 \quad \text{and} \quad h_1(t), h_2(t) \mapsto A(t)h_1(t) + B(t)h_2(t)\,.$$

For $d = s + r - 1$, the dimensions of the source and target spaces become equal to $r + s$, and the map $\mu_{r+s-1} : S^{r-1}V^* \oplus S^{s-1}V^* \to S^{r+s-1}V^*$ is represented in the standard monomial basis $t_0^{\mu}t_1^{\nu}$ with $\mu + \nu = r - 1,\ s - 1,\ r + s - 1$ by the square matrix that is the transpose of that from (12.9).

Exercise 12.13 Check this.

Write $S = S(\alpha', \alpha'', \beta', \beta'')$ for the Sylvester determinant (12.8) considered as a polynomial in α', α'', β', β'', and let $D_{ij} = \alpha'_i\beta''_j - \alpha''_i\beta'_j$. For every point $(\alpha, \beta) \in Z(D_{ij})$, we have $(\alpha''_i t_0 - \alpha'_i t_1) = (\beta''_i t_0 - \beta'_i t_1)$ up to a constant factor, and this linear form divides $A(t)$, $B(t)$, and all polynomials $A(t)h_1(t) + B(t)h_2(t)$. Thus we have $\operatorname{im}\mu_{m+n-1} \neq S^{m+n-1}V^*$, and S vanishes. This forces some power of S to be divisible by D_{ij}. Since this quadratic form is irreducible and the polynomial ring is factorial, D_{ij} divides S. Since all quadratic forms D_{ij} are nonproportional, S is divisible by their product R_{AB}. Comparison of the degrees and coefficients of the lexicographically maximal monomials in S and $R_{AB} = \prod_{i,j}(\alpha'_i\beta''_j - \alpha''_i\beta'_j)$ shows that these two polynomials are equal.

Thus, the resultant variety (12.7) for a pair of binary forms A, B of degrees s, r is the hypersurface[13] in $\mathbb{P}_s \times \mathbb{P}_r$ determined by one equation $R_{AB} = 0$ in A, B. The polynomial $R_{A,B}$ is called the *resultant* of A, B. For $t_0 = 1$, $t_1 = x$, it is specialized to the resultant $R_{f,g}$ of two inhomogeneous polynomials $f(x) = A(1,x)$, $g(x) = B(1,x)$. Under the assumption that[14] $a_0b_0 \neq 0$, the resultant $R_{f,g}$ vanishes if and only if the polynomials f, g have a common root in $\Bbbk = \mathbb{A}^1 = \mathbb{P}^1 \smallsetminus \{(0:1)\}$.

[13] In Example 12.9 on p. 288, we will see that the same holds for every system of homogeneous polynomial equations such that the number of equations equals the number of unknowns.

[14] This means that both binary forms A, B do not vanish at the point $(0:1)$.

12.4 Closeness of Projective Morphisms

The algebraicity of the resultant variety forces every regular morphism from a projective manifold to an arbitrary separated algebraic manifold to be *closed*, i.e., to map every closed subset of the source manifold to a closed subset of the target manifold. Informally, this means that projective varieties are similar, in some sense, to compact manifolds in differential geometry.

Lemma 12.2 *The projection* $\pi : \mathbb{P}_m \times \mathbb{A}^n \twoheadrightarrow \mathbb{A}^n$ *is closed, i.e.,* $\pi(Z) \subset \mathbb{A}^n$ *is closed for every closed* $Z \subset \mathbb{P}_m \times \mathbb{A}^n$.

Proof Write $x = (x_0 : x_1 : \cdots : x_m)$ and $t = (t_1, t_2, \ldots, t_n)$ for the homogeneous and affine coordinates on $\mathbb{P}_m$ and $\mathbb{A}^n$ respectively. Let a closed subset $Z \subset \mathbb{P}_m \times \mathbb{A}^n$ be described by a system of polynomial equations $f_\nu(x,t) = 0$, homogeneous in x. Then $\pi(Z) \subset \mathbb{A}^n$ consists of all $p \in \mathbb{A}^n$ such that the system of homogeneous equations $f_\nu(x,p) = 0$ in x has a nonzero solution. The latter holds if and only if the coefficients of the homogeneous forms $f_\nu(x,p)$ satisfy the system of resultant polynomial equations. Since the coefficients of the forms $f_\nu(x,p)$ are polynomials in p, we conclude that $\pi(Z)$ is described by polynomial equations. □

Corollary 12.1 *Let X be a projective algebraic variety. Then the projection*

$$X \times Y \twoheadrightarrow Y$$

is closed for every algebraic manifold Y.

Proof It is enough to prove this statement separately for every affine chart of Y instead of the whole of Y. Thus, we may assume that Y is affine. In this case, $X \times Y$ is a closed subset in $\mathbb{P}_m \times \mathbb{A}^n$, and the projection in question is the restriction of the projection $\mathbb{P}_m \times \mathbb{A}^n \twoheadrightarrow \mathbb{A}^n$, which is closed, to this closed subset. Therefore, it is closed as well. □

Theorem 12.1 *For every projective variety X and separated manifold Y, every regular morphism* $\varphi : X \to Y$ *is closed.*

Proof Let $\Gamma_\varphi \subset X \times Y$ be the graph[15] of the morphism $\varphi : X \to Y$. The image $\varphi(Z) \subset Y$ of every subset $Z \subset X$ can be described as the image of the intersection $\Gamma_\varphi \cap (Z \times Y) \subset X \times Y$ under the projection $X \times Y \twoheadrightarrow Y$. If Z is closed in X, then the product $Z \times Y$ is closed in $X \times Y$. We have seen in Example 12.4 on p. 271 that for separated Y, the graph Γ_φ is closed too. Therefore, if X is projective, the closed projection $X \times Y \twoheadrightarrow Y$ maps the closed subset $\Gamma_\varphi \cap (Z \times Y) \subset X \times Y$ to the closed subset $\varphi(Z) \subset Y$. □

[15]See Example 12.4 on p. 271.

Corollary 12.2 *Let X be a connected*[16] *projective variety. Then every regular map from X to an arbitrary affine algebraic variety Y contracts X to one point of Y. In particular, $\mathcal{O}_X(X) = \Bbbk$ is exhausted by constants.*

Proof Let $\varphi : X \to Y$ be a regular map to an affine variety $Y \subset \mathbb{A}^n$. Composing it with the projections of Y onto the n coordinate axes of $\mathbb{A}^n$ reduces the statement to the case $Y = \mathbb{A}^1$. Composing a regular map $X \to \mathbb{A}^1$ with the inclusion $\mathbb{A}^1 \hookrightarrow \mathbb{P}_1$, which puts $\mathbb{A}^1$ into $\mathbb{P}_1$ as the standard affine chart U_0, gives the nonsurjective regular map $X \to \mathbb{P}_1$, whose image must be a proper connected Zariski closed subset, that is, one point. □

12.4.1 Finite Projections

A regular morphism of algebraic manifolds $\varphi : X \to Y$ is called *finite* if for every affine chart $U \subset Y$, the preimage $W = \varphi^{-1}(U)$ is an affine chart on X and the restricted map $\varphi_W : W \to U$ is a finite morphism of affine algebraic varieties in the sense of Sect. 11.5.3. It follows from Proposition 11.8 on p. 258 that every finite morphism is closed, and the restriction of a finite morphism to a closed submanifold remains a finite morphism. Moreover, if X is irreducible and $Z \subsetneq X$ is a proper closed subset, then $\varphi(Z) \subsetneq Y$ is proper (and closed) in Y for every finite morphism $\varphi : X \to Y$.

Exercise 12.14 Prove that the composition of finite morphisms is finite.

Proposition 12.1 *Let $X \subsetneq \mathbb{P}_n$ be an algebraic projective variety, and $p \notin X$ an arbitrary point outside X. Then the projection $\pi_p : X \to H$ from the point p to every hyperplane $H \not\ni p$ is a finite morphism.*

Proof Let $U \subset H$ be an affine chart. Fix some homogeneous coordinates

$$(x_0 : x_1 : \cdots : x_n)$$

on $\mathbb{P}_n$ such that $p = (1 : 0 : \cdots : 0)$, $H = Z(x_0)$ consists of points q defined by $q = (0 : q_1 : \cdots : q_n)$, and the chart $U \subset H$ consists of points u defined by $u = (0 : u_1 : \cdots : u_{n-1} : 1)$. Let X be described by homogeneous equations $f_\nu(x) = 0$ in these coordinates. Since $p \notin X$, the preimage $\pi_p^{-1}(U)$ is cut out of X by the punctured cone C ruled by the lines (pu), $u \in U$, with the punctured point p. Every such line is described by a parametric equation $u + pt$, $t \in \Bbbk$, and the cone C is an affine algebraic variety isomorphic to $\mathbb{A}^n = U \times \mathbb{A}^1$. The isomorphism maps the point $(u, t) \in U \times \mathbb{A}^1$ to the point $x = u + tp \in \mathbb{P}_n$ lying on the cone. The intersection $C \cap X = \pi_p^{-1}(U)$ is described in the coordinates (u, t) on C by the equations

$$f_\nu(tp + u) = \alpha_0^{(\nu)}(u)\, t^m + \alpha_1^{(\nu)}(u)\, t^{m-1} + \cdots + \alpha_m^{(\nu)}(u) = 0 \tag{12.10}$$

[16] That is, indecomposable into a disjoint union of two nonempty closed subsets.

and therefore is an affine algebraic variety, i.e., an affine chart on X. It remains to show that its coordinate algebra $\Bbbk[C \cap X]$ is integral over $\Bbbk[U] = \Bbbk[u_1, u_2, \dots, u_{n-1}]$. By construction, $\Bbbk[C \cap X] = \Bbbk[t, u_1, u_2, \dots, u_{n-1}]/I$, where I is generated by the polynomials (12.10). This algebra is generated over $\Bbbk[U]$ by one element t. It is enough to check that t is integral over $\Bbbk[U]$, i.e., that there exists a monic polynomial in t in the ideal I. Such a polynomial exists if and only if the ideal generated in $\Bbbk[U]$ by the leading coefficients $\alpha_0^{(\nu)}(u)$ of Eq. (12.10) is nonproper. By the weak Nullstellensatz, this means that the coefficients $\alpha_0^{(\nu)}(u)$ have no common zeros in U. But this is guaranteed by the condition $p \notin X$. Indeed, if all the coefficients $\alpha_0^{(\nu)}(u)$ simultaneously vanish at some point u_0, then the homogenizations of Eq. (12.10),

$$f_\nu(\vartheta_0 p + \vartheta_1 u_0) = \alpha_0^{(\nu)}(u_0)\, \vartheta_0^m + \alpha_1^{(\nu)}(u_0)\, \vartheta_0^{m-1}\vartheta_1 + \cdots + \alpha_m^{(\nu)}(u_0)\vartheta_1^m = 0\,,$$

which describe the intersection of X with the whole unpunctured projective line (p, u_0), have the common root $(\vartheta_0 : \vartheta_1) = (1 : 0)$ on this line. This means that $p \in X$. Contradiction. □

Corollary 12.3 *Every projective variety admits a regular finite surjection onto projective space.*

Proof Let $X \subset \mathbb{P}_n$ be a projective variety. Make a finite projection $\pi_1 : X \to H_1$ from some point $p_1 \in \mathbb{P}_n \smallsetminus X$ to some hyperplane $H_1 \subset \mathbb{P}_n$. If $\pi_1(X) \neq H_1$, make a second finite projection $\pi_2 : \pi_1(X) \to H_2$ from some point $p_2 \in H_1 \smallsetminus \pi_1(X)$ to some hyperplane $H_2 \subset H_1$, etc. □

Corollary 12.4 *Every affine algebraic variety X admits a regular finite surjection onto affine space.*

Proof Let $X \subsetneq \mathbb{A}^n$, where $\mathbb{A}^n$ is placed in $\mathbb{P}_n$ as the standard affine chart U_0. Put $H_\infty \stackrel{\text{def}}{=} \mathbb{P}_n \smallsetminus U_0$ and write $\overline{X} \subset \mathbb{P}_n$ for the projective closure of X. The projection of $\overline{X}$ from every point $p \in H_\infty \smallsetminus \overline{X}$ to every projective hyperplane $L \not\ni p$ looks within the chart U_0 like the parallel projection of $X = \overline{X} \smallsetminus H_\infty$ to the affine hyperplane $U_0 \cap L = L \smallsetminus H_\infty$ in the direction of the vector p. By Proposition 12.1, this parallel projection is a finite morphism of affine algebraic varieties. If it is not surjective, we repeat the procedure within the target hyperplane, as in the proof of Corollary 12.3. □

Exercise 12.15 Check that $\overline{X} \cap H_\infty \neq H_\infty$ for $X \neq \mathbb{A}^n$.

Example 12.8 (Noether's Normalization) Given an arbitrary polynomial

$$f \in \Bbbk[x_1, x_2, \dots, x_n]\,,$$

write it as $f = f_0 + f_1 + \cdots + f_d$, where each f_k is homogeneous of degree k. Let $\mathbb{A}^n \subset \mathbb{P}_n$ be the standard chart U_0 in projective space $\mathbb{P}_n$ with homogeneous coordinates $(x_0 : x_1 : \cdots : x_n)$, and $\overline{X} \subset \mathbb{P}_n$ the closure of the affine hypersurface $X = V(f) \subset \mathbb{A}^n$. Then $\overline{X} = V(\overline{f})$ is the zero set of the homogeneous polynomial

$$\overline{f} = f_0 x_0^d + f_1 x_0^{d-1} + \cdots + f_{d-1} x_0 + f_d\,.$$

A point $p = (0 : p_1 : p_2 : \ldots : p_n)$ at infinity with respect to the chart U_0 does not belong to $\overline{X}$ if and only if $f_d(p_1, p_2, \ldots, p_n) \neq 0$. Since $f_d \neq 0$, such a point $p \notin \overline{X}$ exists and can be chosen[17] in the form $p = (0, p_1, \ldots, p_{n-1}, -1)$. The projection from this point to the affine hyperplane $x_n = 0$ looks within $\mathbb{A}^n$ like the parallel projection $\pi_p : X \to \mathbb{A}^{n-1}$ along the vector $p = (p_1, \ldots, p_{n-1}, -1)$. It maps

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1 + p_1x_n,\ x_2 + p_2x_n,\ \ldots\ ,\ x_{n-1} + p_{n-1}x_n,\ 0)\ .$$

Therefore, its pullback homomorphism

$$\pi_p^* : \Bbbk[t_1, t_2, \ldots, t_{n-1}] \to \Bbbk[x_1, x_2, \ldots, x_n]/(f)$$

takes t_i to $x_i + p_ix_n$. By Proposition 12.1, the algebra $\Bbbk[X] = \Bbbk[x_1, x_2, \ldots, x_n]/(f)$ is integral[18] over $\Bbbk[t_1, t_2, \ldots, t_{n-1}]$. Indeed, the substitution $x_i = t_i - p_ix_n$ transforms the equation $f(x_1, x_2, \ldots, x_n) = 0$ into a polynomial equation in x_n with coefficients in $\Bbbk[t_1, t_2, \ldots, t_{n-1}]$ and leading term $(-1)^d f_d(p_1, \ldots, p_{n-1}, -1) \cdot x_n^d$, whose coefficient is a nonzero constant. Thus, x_n is integral over $\Bbbk[t_1, t_2, \ldots, t_{n-1}]$, and therefore, all $x_i = t_i - p_ix_n$ are integral as well. In particular, we see that if $\Bbbk$ is algebraically closed, then for every t, there exists a point $x \in V(f)$ projected to t. Thus, every algebraic affine hypersurface $V(f)$, $f \neq$ const, over an algebraically closed field admits a finite surjective parallel projection onto a hyperplane. This claim is known as *Noether's*[19] *normalization lemma*.

12.5 Dimension of an Algebraic Manifold

Given an algebraic manifold X and a point $x \in X$, the maximal $n \in \mathbb{N}$ such that there exists a strictly increasing chain

$$\{x\} = X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_{n-1} \subsetneq X_n \subset X\,, \tag{12.11}$$

where all X_i, $0 \leqslant i \leqslant n$, are closed irreducible submanifolds, is called the *dimension* of X at the point x, and denoted by $\dim_x X$. Note that for an irreducible X, the maximality of a chain (12.11) forces $X_n = X$. Therefore, if the point x belongs to several irreducible components of X, then $\dim_x X$ equals the maximal dimension among the dimensions of those components.

Exercise 12.16 Check that $\dim_x X = \dim_x U$ for every affine chart $U \ni x$.

[17] Possibly after appropriate renumbering of the coordinates $x_1, x_2, \ldots, x_n$. Note that this holds over *every* infinite field $\Bbbk$, not necessarily algebraically closed.

[18] In particular, this implies that $\operatorname{tr}\deg \Bbbk[x_1, x_2, \ldots, x_n]/(f) = n - 1$.

[19] In honor of Emmy Noether, who proved a version of this claim in 1926.

Proposition 12.2 *For every regular surjection of irreducible manifolds* $\varphi : Y \twoheadrightarrow X$*, the inequality* $\dim_y Y \geqslant \dim_{\varphi(y)} X$ *holds at every point* $y \in Y$*.*

Proof Given a chain (12.11) with $x = \varphi(y)$, for every i the closed submanifold $\varphi^{-1}(X_i) \subset Y$ has an irreducible component Y_i such that the restricted map

$$\varphi|_{Y_i} : Y_i \to X_i$$

is dominant. These components form the strictly increasing chain

$$y \in Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_{n-1} \subsetneq Y_n$$

in Y. □

Proposition 12.3 *Given a finite morphism of irreducible algebraic varieties*

$$\varphi : X \to Y ,$$

then $\dim_x X \leqslant \dim_{\varphi(x)} Y$ *for all* $x \in X$*, and equality holds for some* $x \in X$ *if and only if* $\varphi(X) = Y$*.*

Proof Replacing Y by an affine neighborhood of $\varphi(x)$ and X by the preimage of this neighborhood allows us to assume, by Exercise 12.16, that both X and Y are affine. It follows from Proposition 11.8 on p. 258 that every chain (12.11) in X is mapped to a strictly increasing chain of closed irreducible subvarieties $\varphi(X_i)$ in Y. This leads to the required inequality. Moreover, if $\varphi(X) \neq Y$, then the last subvariety of the chain is proper in Y, and therefore the chain can be enlarged at least by Y. Thus, the inequality is strict in this case. For $\varphi(X) = Y$, the opposite inequality is provided by Proposition 12.2. □

Proposition 12.4 $\dim_x \mathbb{A}^n = n$ *for all* $x \in \mathbb{A}^n$*.*

Proof Since for every $x \in \mathbb{A}^n$ there is a chain (12.11) of strictly increasing affine subspaces $X_i = \mathbb{A}^i$ passing through x, the inequality $\dim_x \mathbb{A}^n \geqslant n$ holds. The opposite inequality is established by induction on n. It is obvious for $\mathbb{A}^0 = x$. Let $\dim \mathbb{A}^k = k$ for all $k < n$. Consider a maximal chain (12.11) for $X = \mathbb{A}^n$ and take a finite surjection of the last element X_m, $m = \dim \mathbb{A}^n - 1$, of this chain different from $\mathbb{A}^n$ onto some affine space $\mathbb{A}^k \subsetneq \mathbb{A}^n$. Then $k = m$ by Proposition 12.3, and hence $\dim \mathbb{A}^n = m + 1 = k + 1 \leqslant n$. □

Corollary 12.5 *Let X be an irreducible affine algebraic variety, and* $\varphi : X \twoheadrightarrow \mathbb{A}^m$ *a finite surjection. Then* $\dim_x X = m$ *for all* $x \in X$*. As a byproduct, the number m does not depend on the choice of* φ*, and* $\dim_x X$ *does not depend on* $x \in X$*.* □

Corollary 12.6 *For every irreducible affine algebraic variety X, the equality*

$$\dim_x X = \operatorname{tr}\deg_{\Bbbk} \Bbbk[X]$$

holds for all $x \in X$*, where* $\operatorname{tr}\deg_{\Bbbk} \Bbbk[X]$ *means the transcendence degree*[20] *of the coordinate algebra of* X *over the ground field* $\Bbbk$*.*

Proof A finite surjection $\pi : X \twoheadrightarrow \mathbb{A}^m$ forces $\Bbbk[X]$ to be an integral extension of the subalgebra $\pi^*(\Bbbk[\mathbb{A}^m]) \simeq \Bbbk[x_1, x_2, \dots, x_m]$. In particular, the pullbacks $\pi^*(x_i)$ of the coordinates on $\mathbb{A}^m$ form a transcendence basis of $\Bbbk[X]$ over $\Bbbk$. □

Exercise 12.17 Verify that $\dim(X \times Y) = \dim X + \dim Y$ for all irreducible varieties X and Y.

12.5.1 Dimensions of Subvarieties

Let X be a reducible algebraic manifold, suppose a point $x \in X$ belongs to several irreducible components of X, and let a regular nonconstant function $f \in \Bbbk[X]$ vanish identically along one of those components containing x and having maximal dimension equal to $\dim_x X$. Then the hypersurface $V(f) \subsetneq X$ has at x the same dimension as X. Fortunately, such a counterintuitive phenomenon can appear only if f is a zero divisor in $\Bbbk[X]$.

Proposition 12.5 *Let* X *be an irreducible algebraic manifold and* $f \in \mathcal{O}_X(X)$ *a nonconstant global regular function on* X*. Then* $V(f) \neq \varnothing$ *and*

$$\dim_p V(f) = \dim_p(X) - 1 \textit{ for all } p \in V(f).$$

Proof Exercise 12.16 allows us to assume that X is affine. For $X = \mathbb{A}^n$, the statement follows from Example 12.8. The general case is reduced to affine spaces by the same geometric construction as in the proof of Proposition 11.9 on p. 260. Namely, fix a finite surjection $\pi : X \twoheadrightarrow \mathbb{A}^m$ and consider the map

$$\varphi = \pi \times f : X \to \mathbb{A}^m \times \mathbb{A}^1, \quad x \mapsto \big(\pi(x), f(x)\big).$$

As we have seen in the proof of Proposition 11.9, the map φ provides X with a finite surjection onto the hypersurface $V(\mu_f) \subset \mathbb{A}^m \times \mathbb{A}^1$, the zero set of the minimal polynomial

$$\mu_f(u,t) = t^n + \alpha_1(u)\, t^{n-1} + \cdots + \alpha_n(u) \in \Bbbk[u_1, u_2, \dots, u_m][t]$$

of f over $\Bbbk(\mathbb{A}^m)$. This finite surjection maps the hypersurface $V(f) \subset X$ onto the intersection of $V(\mu_f)$ with the affine space $t = 0$. Within the latter affine space, the intersection in question is nothing but the affine hypersurface $V(a_n) \subset \mathbb{A}^m$, having dimension $m - 1$ at every point by Example 12.8. Thus,

$$\dim V(f) = \dim V(a_n) = m - 1 = \dim X - 1.$$

□

[20] See Sect. 10.4 on p. 236.

Corollary 12.7 *Let X be an affine algebraic variety and $f_1, f_2, \dots, f_m \in \Bbbk[X]$. Then*

$$\dim_p V(f_1, f_2, \dots, f_m) \geqslant \dim_p(X) - m \tag{12.12}$$

for all $p \in V(f_1, f_2, \dots, f_m)$. If the class of f_i in the quotient $\Bbbk[X]/(f_1, f_2, \dots, f_{i-1})$ does not divide zero for every[21] *$i = 1, 2, \dots, m$, then the inequality (12.12) becomes an equality.* □

Caution 12.1 Note that Corollary 12.7 does not assert that $V(f_1, f_2, \dots, f_m) \neq \varnothing$. Since the empty set contains no points p, it follows that for $V(f_1, f_2, \dots, f_m) = \varnothing$, Corollary 12.7 remains formally true but becomes empty. The weak Nullstellensatz implies that $V(f_1, f_2, \dots, f_m) = \varnothing$ if and only if the class of f_i in

$$\Bbbk[X]/(f_1, f_2, \dots, f_{i-1})$$

is invertible for some i, and this may routinely happen. For example, for $X = \mathbb{A}^3 = \operatorname{Spec_m} \Bbbk[x, y, z]$, $f_1 = x$, $f_2 = x + 1$, we get $V(x, x + 1) = \varnothing$. The same warning applies to the next corollary as well.

Corollary 12.8 *For affine algebraic varieties $X_1, X_2 \subset \mathbb{A}^n$ and every point $x \in X_1 \cap X_2$, the inequality $\dim_x(X_1 \cap X_2) \geqslant \dim_x(X_1) + \dim_x(X_2) - n$ holds.*

Proof Let $\varphi_i : X_i \hookrightarrow \mathbb{A}^n$, $i = 1, 2$, be the closed immersions corresponding to the quotient maps $\Bbbk[X_1] \twoheadleftarrow \Bbbk[x_1, x_2, \dots, x_n] \twoheadrightarrow \Bbbk[X_2]$. Then $X_1 \cap X_2$ is isomorphic to the preimage of the diagonal $\Delta_{\mathbb{A}^n} \subset \mathbb{A}^n \times \mathbb{A}^n$ under the map

$$\varphi_1 \times \varphi_2 : X_1 \times X_2 \hookrightarrow \mathbb{A}^n \times \mathbb{A}^n .$$

Within $X_1 \times X_2$, it is determined by the n equations $(\varphi_1 \times \varphi_2)^*(x_i) = (\varphi_1 \times \varphi_2)^*(y_i)$, the pullbacks of equations $x_i = y_i$ for $\Delta_{\mathbb{A}^n}$ in $\mathbb{A}^n \times \mathbb{A}^n$. It remains to apply Corollary 12.7. □

Proposition 12.6 *For irreducible projective varieties $X_1, X_2 \subset \mathbb{P}_n$, the inequality $\dim(X_1) + \dim(X_2) \geqslant n$ forces $X_1 \cap X_2 \neq \varnothing$.*

Proof Let $\mathbb{P}_n = \mathbb{P}(V)$ and $\mathbb{A}^{n+1} = \mathbb{A}(V)$. Given a nonempty irreducible projective variety $Z \subset \mathbb{P}_n$, write $Z' \subset \mathbb{A}^{n+1}$ for the affine cone over Z provided by the same homogeneous equations in the coordinates. Then the origin $O \in \mathbb{A}^{n+1}$ belongs to Z' and $\dim_O Z' \geqslant \dim Z + 1$, because every chain $\{z\} \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_m = Z$ produces the chain of cones $\{O\} \subsetneq (O, z) \subsetneq Z_1' \subsetneq \cdots \subsetneq Z_m' = Z'$ starting with the point O and the line (O, z). Therefore, by Corollary 12.8,

$$\dim_O(X_1' \cap X_2'') \geqslant \dim_O(X_1) + 1 + \dim_O(X_2) + 1 - n - 1 \geqslant 1 .$$

Thus, $X_1' \cap X_2''$ is not exhausted by O. □

[21] For $i = 1$, this means that f_1 is not a zero divisor in $\Bbbk[X]$. A sequence of functions possessing this property is called a *regular sequence*, and the corresponding subvariety $V(f_1, f_2, \dots, f_m) \subset X$ is called a *complete intersection*.

12.5.2 Dimensions of Fibers of Regular Maps

In a contrast to differential geometry and topology, the dimensions of nonempty fibers of regular maps are controlled in algebraic geometry almost as strictly as in linear algebra.

Theorem 12.2 *Let $\varphi : X \to Y$ be a dominant regular map of irreducible algebraic varieties. Then*

$$\dim_x \varphi^{-1}(\varphi(x)) \geqslant \dim X - \dim Y \tag{12.13}$$

for all $x \in X$, and there exists a dense Zariski open set $U \subset Y$ such that

$$\dim_x \varphi^{-1}(y) = \dim_x X - \dim_y Y \tag{12.14}$$

for all $y \in U$ and all $x \in \varphi^{-1}(y)$.

Proof We can replace Y by an affine chart $U \ni \varphi(x)$ and X by $\varphi^{-1}(U)$. Taking the composition of φ with a finite surjection $U \twoheadrightarrow \mathbb{A}^m$ allows us to assume that $Y = \mathbb{A}^m = \operatorname{Spec_m} \Bbbk[u_1, u_2, \dots, u_m]$ and $\varphi(x) = 0$. Replacing X by an affine neighborhood of x, we may assume that X is affine too. Then $\varphi^{-1}(0)$ is given by the m equations $\varphi^*(x_i) = 0$, the pullbacks of the equations $x_i = 0$, which describe the origin within $\mathbb{A}^m$. Thus, Corollary 12.7 implies inequality (12.13). In the second statement of the theorem, we also can assume that X, Y are affine. Let us factorize φ into the composition of a closed immersion $X \subset Y \times \mathbb{A}^m$ followed by the projection $\pi : Y \times \mathbb{A}^m \twoheadrightarrow Y$, as in formula (11.11) on p. 258.

We are going to apply Corollary 12.4 to the fibers of π. Consider the projective closure $\overline{X} \subset Y \times \mathbb{P}_m$, and fix a projective hyperplane $H \subset \mathbb{P}_m$ and a point $p \in \mathbb{P}_m \smallsetminus H$ such that the section $Y \times \{p\} \subset Y \times \mathbb{P}_m$ is not contained in $\overline{X}$. Then the fiberwise projection from p to H satisfies the conditions of Proposition 12.1 in the fibers over all $y \in Y \smallsetminus \overline{\pi}\big((Y \times \{p\}) \cap \overline{X}\big)$, where $\overline{\pi} : Y \times \mathbb{P}_m \twoheadrightarrow Y$ is the projection along $\mathbb{P}_m$. Since the latter is a closed map, the inadmissible y form a proper Zariski closed subset in Y. Therefore, there exists a nonempty principal open set $U \subset Y$ such that Proposition 12.1 can be applied fiberwise over all points $y \in U$. Since U is an affine algebraic variety as well, we can replace Y by U and X by $X \cap \pi^{-1}(U)$. After that, Corollary 12.4 gives a finite parallel fiberwise projection of X in the direction p to the affine hyperplane $Y \times \mathbb{A}^{m-1} = (Y \times H) \cap (Y \times \mathbb{A}^n)$. If it is not surjective, we repeat the procedure until we get a finite surjection $\psi : X \twoheadrightarrow Y \times \mathbb{A}^n$ whose composition with the projection to Y equals φ. This forces $\dim X = n + \dim Y$. Since the fiber $\varphi^{-1}(y)$ is surjectively and finitely mapped onto $\{y\} \times \mathbb{A}^n$ for all $y \in Y$, we conclude from Proposition 12.3 that $\dim_x \varphi^{-1}(y) = n = \dim X - \dim Y$ for all $x \in \varphi^{-1}(y)$.

□

Corollary 12.9 (Semicontinuity Theorem) *For every regular map of algebraic manifolds $\varphi : X \to Y$, the sets*

$$X_k \stackrel{\text{def}}{=} \left\{x \in X \mid \dim_x \varphi^{-1}(\varphi(x)) \geqslant k\right\}$$

are closed in X for all $k \in \mathbb{Z}$.

Proof If $\dim Y = 0$, then this is trivially true for all X and k. For $\dim Y = m > 0$, we may assume by induction that the statement holds for all X, k, and all Y with $\dim Y < m$. Replacing Y and X by irreducible components of maximal dimension passing through $\varphi(x)$ and x respectively allows us to assume that both X and Y are irreducible. Since $X_k = X$ for $k \leqslant \dim(X) - \dim(Y)$ by Theorem 12.2, the statement holds for all such k. For $k > \dim(X) - \dim(Y)$, we can replace Y and X by $Y' = Y \smallsetminus U$ and $X' = \varphi^{-1}(Y')$, where $U \subset Y$ is from Theorem 12.2, and apply the inductive hypothesis, because $X_k \subset X'$ and $\dim Y' < \dim Y$. □

Corollary 12.10 *Let $\varphi : X \to Y$ be a closed regular morphism of algebraic manifolds. Then the sets*

$$Y_k \stackrel{\text{def}}{=} \left\{y \in Y \mid \dim \varphi^{-1}(y) \geqslant k\right\}$$

are closed in Y for all $k \in \mathbb{Z}$. □

Theorem 12.3 (Dimension Criterion of Irreducibility) *Assume that a closed regular surjection of algebraic manifolds $\varphi : X \twoheadrightarrow Y$ has irreducible fibers of the same constant dimension. Then X is irreducible if Y is.*

Proof Let $X = X_1 \cup X_2$ be reducible. Since every fiber of φ is irreducible, it is entirely contained in X_1 or in X_2. Put $Y_i \stackrel{\text{def}}{=} \{y \in Y \mid \varphi^{-1}(y) \subset X_i\}$ for $i = 1, 2$. Then $Y = Y_1 \cup Y_2$, and the subsets $Y_1, Y_2 \subsetneq Y$ are proper if $X_1, X_2 \subsetneq X$ are proper. Since Y_i coincides with the locus of points in Y over which the fibers of the restricted map $\varphi|_{X_i} : X_i \to Y$ achieve their maximal value, we conclude from Corollary 12.10 that Y_i is closed in Y for $i = 1, 2$. Thus reducibility of X forces Y to be reducible. □

12.6 Dimensions of Projective Varieties

It follows from Proposition 12.6 on p. 284 that every irreducible projective manifold $X \subset \mathbb{P}_n = \mathbb{P}(V)$ of dimension $\dim X = d$ intersects all projective subspaces $H \subset \mathbb{P}_n$ of dimension $\dim H \geqslant n-d$. We are going to show that a generic projective subspace H of dimension $\dim H < n - d$ does not intersect X, and therefore, the dimension $\dim X$ is characterized as the maximal d such that X intersects all projective subspaces of codimension d. We know from Sect. 2.6.4 on p. 49 that all projective subspaces of codimension $d + 1$ in $\mathbb{P}_n = \mathbb{P}(V)$ form the Grassmannian $\mathrm{Gr}(n - d, n + 1) = \mathrm{Gr}(n - d, V)$, which is an irreducible projective manifold.

Consider the *incidence variety*

$$\Gamma \stackrel{\text{def}}{=} \{(x, H) \in X \times \mathrm{Gr}(n-d, V) \mid x \in H\} \tag{12.15}$$

and write $\pi_1 : \Gamma \twoheadrightarrow X$ and $\pi_2 : \Gamma \to \mathrm{Gr}(n-d, V)$ for the canonical projections.

Exercise 12.18 Convince yourself that Γ is a projective algebraic variety.

The fiber of the first projection $\pi_1 : \Gamma \twoheadrightarrow X$ over an arbitrary point $x \in X$ consists of all projective subspaces passing through x. It is naturally identified with the Grassmannian $\mathrm{Gr}(n-d-1, n) = \mathrm{Gr}(n-d-1, V/\Bbbk \cdot x)$ of all $(n-d-1)$-dimensional vector subspaces in the quotient space $V/\Bbbk \cdot x$. Thus, π_1 is a closed surjective morphism with irreducible fibers of the same constant dimension $(n-d-1)(d+1)$. By Theorem 12.3, the incidence variety Γ is irreducible, and

$$\dim \Gamma = d + (n-d-1)(d+1) = (n-d)(d+1) - 1\,.$$

This forces the image of the second projection $\pi_2(\Gamma) \subset \mathrm{Gr}(n-d, V)$, which consists of all $(n-d-1)$-dimensional projective subspaces intersecting X, to be a closed irreducible subvariety of dimension at most $\dim \Gamma$ in the Grassmannian $\mathrm{Gr}(n-d, V)$ of dimension $(n-d)(d+1) > \dim \Gamma$. Therefore, the codimension-$(d+1)$ projective subspaces H not intersecting X form a dense Zariski open subset in the Grassmannian $\mathrm{Gr}(n-d, V)$.

In fact, dimensional arguments allow us to say much more about the interaction of X with the projective subspaces in $\mathbb{P}_n$. If we repeat the previous construction for the Grassmannian $\mathrm{Gr}(n-d+1, V)$ of codimension-d subspaces $H' \subset \mathbb{P}(V)$ and the incidence variety

$$\Gamma' \stackrel{\text{def}}{=} \{(x, H') \in X \times \mathrm{Gr}(n-d+1, V) \mid x \in H\}\,,$$

which is an irreducible projective manifold of dimension

$$\dim X + \dim \mathrm{Gr}(n-d, n) = d + d(n-d) = d(n-d+1)$$

for the same reasons as above, we get a surjective projection

$$\pi_2 : \Gamma' \twoheadrightarrow \mathrm{Gr}(n-d+1, V)\,,$$

because $X \cap H' \neq \varnothing$ for all $H' \subset \mathbb{P}(V)$. Theorem 12.2 forces the fibers of π_2 to achieve their minimal possible dimension

$$\dim \Gamma - \dim \mathrm{Gr}(n-d+1, n+1) = d(n-d+1) - (n-d+1)d = 0$$

over all points of some open dense subset in the Grassmannian. This means that a generic projective space of codimension d intersects X in a *finite number* of points. Let us fix such a subspace H' and draw an $(n-d-1)$-dimensional subspace $H \subset H'$

through some intersection point $p \in X \cap H'$. Then $H \cap X$ is a nonempty finite set. Therefore, the second projection of the incidence variety (12.15),

$$\pi_2 : \Gamma \to \mathrm{Gr}(n-d, V)\,,$$

has a zero-dimensional fiber. This forces the minimal dimension of nonempty fibers to be zero. It follows from Theorem 12.2 that

$$\dim \pi_2(\Gamma) = \dim \Gamma = \dim \mathrm{Gr}(n-d, V) - 1\,.$$

In other words, the codimension-$(d+1)$ projective subspaces $H \subset \mathbb{P}(V)$ intersecting an irreducible variety $X \subset \mathbb{P}(V)$ of dimension d form an irreducible hypersurface in the Grassmannian $\mathrm{Gr}(n-d, V)$ of all codimension-$(d+1)$ projective subspaces in $\mathbb{P}_n = \mathbb{P}(V)$.

Exercise 12.19 Deduce from this that for every irreducible projective variety $X \subset \mathbb{P}_n$ of dimension d, there exists a unique, up to a scalar factor, irreducible homogeneous polynomial in the Plücker coordinates of a codimension-d subspace $H \subset \mathbb{P}_n$ that vanishes at a given H if and only if $H \cap X \neq \varnothing$.

The above analysis illustrates a method commonly used in geometry for calculating the dimensions of projective manifolds by means of auxiliary incidence varieties. Below are two more examples.

Example 12.9 (Resultant) Given a collection of positive integers $d_0, d_1, \dots, d_n$, write $\mathbb{P}_{N_i} = \mathbb{P}\left(S^{d_i} V^*\right)$ for the space of degree-d_i hypersurfaces in $\mathbb{P}_n = \mathbb{P}(V)$. We are going to show that the resultant variety[22]

$$\mathcal{R} = \left\{(S_0, S_1, \dots, S_n) \in \mathbb{P}_{N_0} \times \mathbb{P}_{N_1} \times \cdots \times \mathbb{P}_{N_n} \mid \bigcap_i S_i \neq \varnothing\right\}$$

of a system of $(n+1)$ homogeneous polynomial equations of given degrees in $n+1$ unknowns is an irreducible hypersurface, i.e., there exists a unique, up to proportionality, irreducible polynomial R in the coefficients of the equations, homogeneous in the coefficients of each equation, such that R vanishes at a given collection of polynomials $f_0, f_1, \dots, f_n$ if and only if the equations $f_i(x_0, x_1, \dots, x_n) = 0$, $0 \leqslant i \leqslant n$, have a nonzero solution. The polynomial R is called the *resultant* of the $n+1$ homogeneous polynomials of degrees $d_1, d_2, \dots, d_n$. Consider the incidence variety

$$\Gamma \overset{\text{def}}{=} \{(S_1, S_2, \dots, S_n, p) \in \mathbb{P}_{N_0} \times \cdots \times \mathbb{P}_{N_n} \times \mathbb{P}_n \mid p \in \cap S_i\}\,.$$

Exercise 12.20 Convince yourself that Γ is an algebraic projective variety.

[22] See Sect. 12.3 on p. 274.

Since the equation $f(p) = 0$ is linear in f, all degree-d_i hypersurfaces in $\mathbb{P}_n$ passing through a given point $p \in \mathbb{P}_n$ form a hyperplane in $\mathbb{P}_{N_i}$. Therefore, the projection $\pi_2 : \Gamma \twoheadrightarrow \mathbb{P}_n$ is surjective, and all its fibers, which are the products of projective hyperplanes in the spaces $\mathbb{P}_{N_i}$, are irreducible and have the same constant dimension

$$\sum(N_i - 1) = \left(\sum N_i\right) - n - 1\,.$$

Thus, Γ is an irreducible projective variety of dimension $(\sum N_i) - 1$.

Exercise 12.21 Choose a collection of $n+1$ hypersurfaces of the prescribed degrees d_i in $\mathbb{P}_n$ intersecting in exactly one point.

The exercise shows that the projection $\pi_1 : \Gamma \to \mathbb{P}_{N_0} \times \mathbb{P}_{N_1} \times \cdots \times \mathbb{P}_{N_n}$ has a zero-dimensional nonempty fiber. This forces a generic nonempty fiber to be zero-dimensional and implies the equality $\dim \pi_1(\Gamma) = \dim \Gamma$. Therefore, $\pi_1(\Gamma)$ is an irreducible submanifold of codimension 1 in $\mathbb{P}_{N_0} \times \cdots \times \mathbb{P}_{N_n}$.

Exercise 12.22 Show that every irreducible submanifold of codimension 1 in a product of projective spaces is the zero set of an irreducible polynomial in homogeneous coordinates on the spaces, homogeneous in the coordinates of each space.

Example 12.10 (Lines on Surfaces) Algebraic surfaces of degree d in $\mathbb{P}_3 = \mathbb{P}(V)$ form the projective space $\mathbb{P}_N = \mathbb{P}(S^d V^*)$ of dimension

$$N = \frac{1}{6}\,(d+1)(d+2)(d+3) - 1\,.$$

The lines in $\mathbb{P}_3$ form the Grassmannian $\mathrm{Gr}(2,4) = \mathrm{Gr}(2,V)$, which is isomorphic to the smooth 4-dimensional projective Plücker quadric[23]

$$P = \left\{\omega \in \Lambda^2 V \mid \omega \wedge \omega = 0\right\}$$

in $\mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$ by means of the Plücker embedding, which maps a line $(a,b) \subset \mathbb{P}_3$ to the decomposable Grassmannian quadratic form $a \wedge b \in \mathbb{P}_5$. Consider the incidence variety

$$\Gamma \overset{\text{def}}{=} \{\ (S,\ell) \in \mathbb{P}_N \times \mathrm{Gr}(2,4) \mid\ \ell \subset S\ \}\,.$$

Exercise 12.23 Convince yourself that $\Gamma \subset \mathbb{P}_N \times \mathrm{Gr}(2,4)$ is a projective algebraic variety.

The projection $\pi_2 : \Gamma \twoheadrightarrow Q_P$ is surjective, and all its fibers are projective spaces of the same constant dimension. Indeed, the line ℓ given by the equations $x_0 = x_1 = 0$

[23] Compare with Problem 17.20 of Algebra I.

lies on a surface $Z(f)$ if and only if $f = x_2 \cdot g + x_3 \cdot h$ belongs to the image of the $\Bbbk$-linear map

$$\psi : S^{d-1}V^* \oplus S^{d-1}V^* \to S^d V^*\,,\ (g,h) \mapsto x_2 g + x_3 h\,.$$

This image is isomorphic to the quotient of the space $S^{d-1}V^* \oplus S^{d-1}V^*$ by the subspace

$$\ker\psi = \left\{(g,h) = (x_3 q, -x_2 q) \mid q \in S^{d-2}V^*\right\}\,.$$

Since $\dim S^{d-1}V^* = \frac{1}{6}\,d(d+1)(d+2)$ and $\dim\ker\psi = \frac{1}{6}\,(d-1)d(d+1)$, the degree-$d$ surfaces containing ℓ form a projective space of dimension

$$\frac{1}{6}\big(2\,d(d+1)(d+2) - (d-1)d(d+1)\big) - 1 = \frac{1}{6}\,d(d+1)(d+5) - 1\,.$$

We conclude that Γ is an irreducible projective variety of dimension

$$\dim\Gamma = \frac{1}{6}\,d(d+1)(d+5) + 3\,.$$

The image of the projection $\pi_1 : \Gamma \to \mathbb{P}_N$ consists of all surfaces containing at least one line. It follows from the above analysis that $\pi_1(\Gamma)$ is an irreducible closed submanifold of $\mathbb{P}_N$.

Exercise 12.24 For every integer $d \geqslant 3$, choose a degree-d surface $S \subset \mathbb{P}_3$ containing just a finite number of lines.

The exercise shows that for $d \geqslant 3$, the projection π_1 has a nonempty fiber of dimension zero. Therefore, a generic nonempty fiber of π_1 is finite, and $\dim\pi_1(\Gamma) = \dim\Gamma$ for $d \geqslant 3$. Since we have

$$N - \dim\Gamma = \frac{1}{6}\big((d+1)(d+2)(d+3) - d(d+1)(d+5)\big) - 4 = d - 3\,,$$

we conclude that every cubic surface in $\mathbb{P}_3$ contains a line, and the set of cubic surfaces with a finite number of lines lying on them contains a dense Zariski open subset of $\mathbb{P}_N$. At the same time, there are no lines on a generic surface of degree $d \geqslant 4$.

Problems for Independent Solution to Chapter 12

Problem 12.1 Compute the resultants of the following pairs of polynomials:

(a) $x^3 - 3x^2 + 2x + 1$ and $2x^2 - x - 1$;

(b) $2x^4 - x^3 + 3$ and $3x^3 - x^2 + 4$;
(c) $2x^3 - 3x^2 - x + 2$ and $x^4 - 2x^2 - 3x + 4$;
(d*) the cyclotomic polynomials[24] Φ_n and Φ_m .

Problem 12.2 Eliminate x from each of the following the equations:

(a) $x^2 - xy + y^2 - 3 = x^2y - xy^2 - 6 = 0$;
(b) $4x^2 - 7xy + y^2 + 13x - 2y - 3 = 9x^2 - 14xy + y^2 + 28x - 4y - 5 = 0$;
(c) $5x^2 - 6xy + 5y^2 - 16 = 2x^2 - xy + y^2 - x - y - 4 = 0$.

Problem 12.3 (Discriminant) Given a polynomial $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$, the product

$$D(f) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

expanded as a polynomial in the coefficients of f is called the *discriminant* of f. Express the discriminant $D(f)$ in terms of the resultant of f and its derivative f', and prove that $D(fg) = D(f)D(g)R_{f,g}^2$.

Problem 12.4 Compute the discriminants of the following polynomials:

(a) $\sum_{k=0}^{n} x^k$, **(b)** $\sum_{k=0}^{n} x^k/k!$, **(c)** $x^n + a$, **(d)** the cyclotomic polynomial $\Phi_k(x)$.

Problem 12.5 Describe the action of quadratic Cremona involution[25]

$$(t_0 : t_1 : t_2) \mapsto \left(t_0^{-1} : t_1^{-1} : t_2^{-1}\right) \tag{12.16}$$

on the triple of lines joining the points at which the involution is indefinite.

Problem 12.6 (Graph of a Rational Map) Given a rational map $\psi : X \dashrightarrow Y$ of algebraic manifolds defined on an open dense subset $U \subset X$, the closure of the set of corresponding points

$$\{(x, \psi(x)) \in X \times Y \mid x \in U\}$$

is called the *graph* of the rational map φ and denoted by $\Gamma_\psi \subset X \times Y$. Describe the graph of the quadratic Cremona involution (12.16) and all the fibers of the projections of this graph to both the source and destination projective planes $\mathbb{P}_2$.

Problem 12.7 For every regular map of algebraic manifolds $\varphi : X \to Y$, show that the isolated points of the fibers of φ form a (possibly empty) Zariski open subset in X.

Problem 12.8 (Chevalley's Constructibility Theorem) Prove that the image of every regular morphism of algebraic varieties is *constructible*, i.e., is obtained

---

[24] See Sect. 3.5.4 of Algebra I.
[25] See Exercise 12.9 on p. 271.

from a finite number of open and closed subsets by means of a finite number of intersections, unions, and taking the difference of sets.

Problem 12.9 For every irreducible projective variety $X \subset \mathbb{P}_n = \mathbb{P}(V)$ of dimension d, show that the codimension-d projective subspaces $H \subset \mathbb{P}(V)$ intersecting X in a finite number of points form an open dense subset $W \subset \mathrm{Gr}(n+1-d, V)$, and the subspaces $H' \in W$ intersecting X in the maximal number of points form an open dense subset $W' \subset W$.

Problem 12.10 Write $\mathcal{D}_k(m,n) \subset \mathbb{P}\big(\mathrm{Mat}_{m\times n}(\Bbbk)\big)$ for the set of all $m\times n$ matrices of rank $\leqslant k$ considered up to proportionality. Use the appropriate incidence variety

$$\Gamma = \{(L, M) \mid L \subset \ker M\},$$

where L is a vector subspace and M a matrix, to show that $\mathcal{D}_k(m,n)$ is an irreducible algebraic variety and to find its dimension.

Problem 12.11 Show that the quartic surfaces in $\mathbb{P}_3$ containing at least one line form an irreducible hypersurface in the projective space of all quartics in $\mathbb{P}_3$.

Problem 12.12 Assume that some six points $p_1, p_2, \dots, p_6 \in \mathbb{P}_2 = \mathbb{P}(V)$ do not lie on a conic and no three of them are collinear. Write

$$W = \big\{f \in S^3V^* \mid \forall i\, f(p_i) = 0\big\}$$

for the vector space of cubic forms vanishing at $p_1, p_2, \dots, p_6$, and

$$\psi : \mathbb{P}_2 \setminus \{p_1, p_2, \dots, p_6\} \to \mathbb{P}(W^*)$$

for the map sending a point $p \neq p_1, p_2, \dots, p_6$ to the subspace

$$\mathrm{Ann}\, p = \{f \in W \mid f(p) = 0\}.$$

Show that $\dim W = 4$, the subspace $\mathrm{Ann}\, p \subset W$ really has codimension 1, and the closure $\overline{\mathrm{im}\,\psi}$ is a smooth[26] cubic surface $S \subset \mathbb{P}_3 = \mathbb{P}(W^*)$.

Problem 12.13 Show that the n-dimensional projective subspaces lying on a smooth $(2n+1)$-dimensional quadric in $\mathbb{P}_{2n+2}$ (respectively on a smooth $2n$-dimensional quadric in $\mathbb{P}_{2n+1}$) form an irreducible projective variety (respectively the disjoint union of two irreducible projective varieties) and find the dimensions of these varieties.

Problem 12.14 (Fano Variety) Show that the lines lying on a smooth quadric in $\mathbb{P}_4$ form a projective variety. Determine whether it is reducible, and find its dimension.

[26] That is, without singular points; see Sect. 2.5.5 on p. 40.

Problem 12.15 (Secant Variety) Let $X \subset \mathbb{P}(V)$ be an irreducible projective variety, $\mathcal{S}(X) \subset \mathrm{Gr}(2, V)$ the closure of the set of lines $(p, q) \subset \mathbb{P}(V)$ with $p, q \in X$, $p \neq q$, and $S(X) \subset \mathbb{P}(V)$ the union of all lines $\ell \subset \mathbb{P}(V)$ belonging to $\mathcal{S}(X)$. Prove that:

(a) $\mathcal{S}(X)$is irreducible and $\dim \mathcal{S}(X) = 2 \dim X$.
(b) $S(X)$ is irreducible and $\dim S(X) \leqslant 2 \dim X + 1$.
(c) $\dim S(C) = 3$ for a twisted curve[27] $C \subset \mathbb{P}_n$, $n \geqslant 3$.

[27] That is, an irreducible variety of dimension one not contained in a hyperplane.

Chapter 13
Algebraic Field Extensions

13.1 Finite Extensions

Recall that a field extension $\Bbbk \subset \mathbb{F}$ is said to be *finite* of *degree* d if $\mathbb{F}$ has dimension $d < \infty$ as a vector space over $\Bbbk$. We write $\deg \mathbb{F}/\Bbbk = d$ in this case.

Exercise 13.1 Let $\Bbbk \subset \mathbb{K} \subset \mathbb{F}$ be a tower of nested finite extensions, and let

$$f_1, f_2, \dots, f_m \in \mathbb{F} \quad \text{and} \quad t_1, t_2, \dots, t_n \in \mathbb{K}$$

be bases of $\mathbb{F}$ and $\mathbb{K}$ as vector spaces over $\mathbb{K}$ and $\Bbbk$ respectively. Verify that the mn products $f_i t_j$ form a basis of $\mathbb{F}$ over $\Bbbk$; in particular,

$$\deg \mathbb{F}/\Bbbk = \deg \mathbb{F}/\mathbb{K} \cdot \deg \mathbb{K}/\Bbbk\,. \tag{13.1}$$

Since algebraicity over a field means the same as integrality, it follows from the properties of integral elements proved in Sect. 10.1 that every commutative $\Bbbk$-algebra A of finite dimension as a vector space over $\Bbbk$ is algebraic over $\Bbbk$. Such an algebra A is a field if and only if A has no zero divisors. Conversely, every field $\mathbb{K} \supset \Bbbk$ finitely generated as a $\Bbbk$-algebra is a finite algebraic extension of $\Bbbk$. In particular, every finitely generated $\Bbbk$-subalgebra $\Bbbk[a_1, a_2, \dots, a_m]$ in a field $\mathbb{F} \supset \Bbbk$ of finite degree over $\Bbbk$ has to be a field of finite degree over $\Bbbk$, and $\deg \Bbbk[a_1, a_2, \dots, a_m]/\Bbbk$ divides $\deg \mathbb{F}/\Bbbk$ by Exercise 13.1.

In particular, every finite field $\mathbb{F}$ of characteristic p is a finite algebraic extension of the prime subfield $\mathbb{F}_p \subset \mathbb{F}$ and has cardinality $|\mathbb{F}| = p^{\deg \mathbb{F}/\mathbb{F}_p}$.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_13

13.1.1 Primitive Extensions

Let $f \in \Bbbk[x]$ be an irreducible polynomial of degree $n > 1$. Then the quotient algebra $\Bbbk[x]/(f)$ is of dimension n over $\Bbbk$ and has no zero divisors. Therefore, $\Bbbk[x]/(f)$ is a field of degree n over $\Bbbk$. Every element of this field admits a unique representation of the form $b_0 + b_1\vartheta + \cdots + b_{n-1}\vartheta^{n-1}$, where $b_i \in \Bbbk$ and $\vartheta = x \pmod f$ is a root of f. The field $\Bbbk[x]/(f)$ is called a *simple extension* of $\Bbbk$ by the *adjunction of a root* ϑ of the irreducible polynomial f. The element ϑ is referred to as a *primitive element* of the extension $\Bbbk \subset \Bbbk[x]/(f)$. If the polynomial f is clear from the context or unimportant, we abbreviate the notation $\Bbbk[x]/(f)$ to $\Bbbk[\vartheta]$ or $\Bbbk(\vartheta)$. For example, the notation $\Bbbk[\sqrt[m]{a}]$, where $a \in \Bbbk$ is such that the polynomial $x^m - a$ is irreducible in $\Bbbk[x]$, will always mean the simple extension $\Bbbk[x]/(x^m - a)$.

Example 13.1 (Cubic Extensions) Let $\Bbbk$ be an arbitrary field, and let

$$f = x^3 + a_1x^2 + a_2x + a_3 \in \Bbbk[x]$$

be an irreducible polynomial over $\Bbbk$. The simple extension $\mathbb{K} = \Bbbk[x]/(f)$ has degree 3 over $\Bbbk$ and consists of elements $b_0 + b_1\vartheta + b_2\vartheta^2$, where $b_i \in \Bbbk$ and $\vartheta = x \pmod f \in \mathbb{K}$. These elements are added and multiplied by the usual distributivity rules under the relation[1] $f(\vartheta) = 0$.

Exercise 13.2 For $\Bbbk = \mathbb{Q}$ and $f(x) = x^3+x+1$, write $(1+2\vartheta)^{-1}$ and $(1+\vartheta+\vartheta^2)^{-1}$ in the form $b_0 + b_1\vartheta + b_2\vartheta^2$.

Since $f(\vartheta) = 0$, the polynomial $f(x)$ can be factorized in $\mathbb{K}[x]$ as

$$f(x) = (x - \vartheta) \cdot q(x)$$

where the quadratic trinomial $q(x) = x^2 + c_1x + c_2 \in \mathbb{K}[x]$ either is irreducible over $\mathbb{K}$ or admits the further factorization

$$q(x) = (x - \vartheta_1)(x - \vartheta_2) \tag{13.2}$$

for some $\vartheta_1, \vartheta_2 \in \mathbb{K}$. For irreducible q, the factorization (13.2) can be written only over the simple quadratic extension $\mathbb{L} = \mathbb{K}[x]/(q) \supset \mathbb{K}$, which has degree 6 over $\Bbbk$. These two cases are distinguished by means of the *discriminant*[2]

$$D(f) = (\vartheta - \vartheta_1)^2(\vartheta - \vartheta_2)^2(\vartheta_1 - \vartheta_2)^2 = q^2(\vartheta) \cdot D(q)\,, \tag{13.3}$$

which is a symmetric polynomial in the roots, and therefore can be expressed as a polynomial in the coefficients of f. In particular, $D(f) \in \Bbbk$.

[1] Compare with Sect. 3.4 of Algebra I.

[2] Recall that the *discriminant* of a monic polynomial $f(x) = \prod(x - \vartheta_i)$ is the product $D(f) \stackrel{\text{def}}{=} \prod_{i<j}(\vartheta_i - \vartheta_j)^2$ expressed as a polynomial in the coefficients of f.

Exercise 13.3 Check that

$$D(x^2 + px + q) = p^2 - 4q, D\left(x^3 + px + q\right) = -4\,p^3 - 27\,q^2.$$

The polynomial q is reducible in $\mathbb{K}[x]$ if and only if $D(q) = (\vartheta_1 - \vartheta_2)^2$ is a perfect square in $\mathbb{K}$. By (13.3), this happens if and only if $D(f)$ is a perfect square in $\mathbb{K}$. However, if $D(f)$ is a perfect square in $\mathbb{K}$, then it has to be a perfect square in $\Bbbk$ as well, because otherwise, the polynomial $x^2 - D(f)$ would be irreducible over $\Bbbk$, the field $\mathbb{L} = \Bbbk[x]/\left(x^2 - D(f)\right)$ would be a simple quadratic extension of $\Bbbk$, and the map

$$\mathbb{L} \hookrightarrow \mathbb{K}\,, \quad x \bmod \left(x^2 - D(f)\right) \mapsto \sqrt{D(f)} \in \mathbb{K}\,,$$

would embed $\mathbb{L}$ into $\mathbb{K}$ over $\Bbbk$, which is impossible by Exercises 13.1 on p. 295, since $2 \nmid 3$. We conclude that an irreducible cubic polynomial $f \in \Bbbk[x]$ is completely factorizable as a product of three linear factors over the simple cubic extension $\Bbbk[x]/(f)$ if and only if the discriminant $D(f)$ is a perfect square in $\Bbbk$.

Exercise 13.4 Prove that the following three conditions on a real cubic trinomial $f(x) = x^3 + px + q \in \mathbb{R}[x]$ are equivalent: **(a)** $D(f) > 0$, **(b)** all the roots of f in $\mathbb{C}$ lie in $\mathbb{R} \subset \mathbb{C}$, **(c)** for appropriate $\lambda \in \mathbb{R}$, the substitution $x = \lambda t$ transforms the equation $f(x) = 0$ to the equation $4\,t^3 - 3\,t = c$ with $|c| \leqslant 1$, which has the roots $t_k = \cos\left(\frac{1}{3}\arccos(c) + \frac{2\pi k}{3}\right)$, $k = 0, 1, 2$.

13.1.2 Separability

If $\operatorname{char}\Bbbk = 3$ in Example 13.1, then the polynomial f may have a multiple root in $\mathbb{K}$, even though f is irreducible over $\Bbbk$. For example, let $\Bbbk = \mathbb{F}_3(t)$ be the field of rational functions in t over the field $\mathbb{F}_3 = \mathbb{Z}/(3)$, and $f(x) = x^3 - t \in \Bbbk[x]$. Since f has no roots in $\Bbbk$, it is irreducible. However, f is a perfect cube over the simple cubic extension $\mathbb{K} = \Bbbk\left[\sqrt[3]{t}\right] = \Bbbk[x]/(f)$, because of the identity $(a+b)^3 = a^3 + b^3$, which holds in every field of characteristic 3 and forces $x^3 - t = \left(x - \sqrt[3]{t}\right)^3$.

Recall[3] that a polynomial $f \in \Bbbk[x]$ is called *separable* if it has no multiple roots in every extension $\mathbb{K} \supset \Bbbk$. As we have seen in Example 3.4 of Algebra I, every irreducible polynomial over a field of characteristic zero is separable. The same holds for irreducible polynomials over finite prime fields $\mathbb{F}_p = \mathbb{Z}/(p)$.

Exercise 13.5 Let $\Bbbk = \mathbb{F}_p(t)$. Show that $f(x) = x^p - t \in \Bbbk[x]$ is irreducible and inseparable over $\Bbbk$.

[3] See Sect. 3.3.3 of Algebra I.

An algebraic field extension $\mathbb{F} \supset \Bbbk$, not necessarily finite, is called *separable* if the minimal polynomial μ_ϑ of every element $\vartheta \in \mathbb{F}$ is separable over $\Bbbk$. It follows from Example 3.4 of Algebra I that every finite field is separable over its prime subfield, and all field extension of characteristic zero are separable.

Example 13.2 (Roots of Unity) The roots of equation $x^n = 1$ in an arbitrary field $\Bbbk$ form a finite multiplicative group, denoted by $\boldsymbol{\mu}_n(\Bbbk)$ and called the *group of nth roots of unity* in $\Bbbk$. This group is cyclic, because every finite multiplicative subgroup in a field is cyclic by Theorem 3.2 of Algebra I. We say that the field $\Bbbk$ *contains all the nth roots of unity* if $|\boldsymbol{\mu}_n(\Bbbk)| = n$. In this case, the generators of the group $\boldsymbol{\mu}_n(\Bbbk) \simeq \mathbb{Z}/(n)$ are called the *primitive* nth roots of unity. In all, there are $\varphi(n)$ primitive roots in $\boldsymbol{\mu}_n(\Bbbk)$, where $\varphi(n)$ denotes Euler's function.[4] Note that an nth root of unity $\zeta \in \Bbbk$ is primitive if and only if all the powers ζ^m with $0 \leqslant m \leqslant n-1$ are distinct. Thus, the following three conditions are equivalent:

- A field $\Bbbk$ admits an extension containing all nth roots of unity.
- The polynomial $x^n - 1$ is separable over $\Bbbk$.
- $\operatorname{char}(\Bbbk)$ does not divide n.

If these conditions hold, then every polynomial $f(x) = x^n - a$ with a nonzero $a \in \Bbbk$ is separable, because $f'(x) = nx^{n-1} \neq 0$ has no common roots with f.

Theorem 13.1 *For every finite field extension $\mathbb{F} \supset \Bbbk$, there exists a tower of simple field extensions*

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F} \tag{13.4}$$

such that $\mathbb{L}_i = \mathbb{L}_{i-1}[\vartheta_i] \simeq \mathbb{L}_{i-1}[x]/(f_i)$ for some polynomial $f_i \in \mathbb{L}_{i-1}[x]$ irreducible over $\mathbb{L}_{i-1}$.

Proof Assume by induction that the field $\mathbb{L}_i \subset \mathbb{F}$ of level i has been constructed. If $\mathbb{L}_i \neq \mathbb{F}$, let $\vartheta \in \mathbb{F} \smallsetminus \mathbb{L}_i$, and let $f_{i+1} \in \mathbb{L}_i[x]$ be the minimal polynomial of ϑ over $\mathbb{L}_i$. Then the simple extension $\mathbb{L}_i[x]/(f)$ admits an injective homomorphism into $\mathbb{F}$ by the rule $x \pmod f \mapsto \vartheta$. Let $\mathbb{L}_{i+1} \supsetneq \mathbb{L}_i$ denote the image of this inclusion. Since the degree of $\mathbb{F}$ over $\mathbb{L}_{i+1}$ is strictly less than that over $\mathbb{L}_i$, after a finite number of steps, the whole of $\mathbb{F}$ will be exhausted. □

Theorem 13.2 (Primitive Element Theorem) *Every finite separable extension $\mathbb{K} \supset \Bbbk$ is simple, i.e., $\mathbb{K} \simeq \Bbbk[x]/(f)$ for an appropriate irreducible polynomial $f \in \Bbbk[x]$ of degree* $\deg \mathbb{K}/\Bbbk$.

Proof If $\Bbbk$ is a finite field, then $\mathbb{K}$ is also finite, and nonzero elements of $\mathbb{K}$ form a cyclic multiplicative group $\mathbb{K}^*$. Therefore, $\mathbb{K} = \Bbbk[\vartheta]$ for every generator[5] ϑ of the group $\mathbb{K}^*$. Now assume that $\Bbbk$ is infinite. Induction on the length of the tower

[4] See Sect. 2.4.3 of Algebra I.

[5] The same argument shows that every finite field, considered as an algebra over a subfield, is generated by one element. Although the separability assumption is not used explicitly in this

(13.4) allows us to assume that $\mathbb{K} = \Bbbk[\alpha, \beta] \supset \Bbbk[\alpha] \supset \Bbbk$ is obtained from $\Bbbk$ by two successive simple extensions, i.e., that it is generated as a $\Bbbk$-algebra by two separable algebraic elements α, β. We are going to find $t \in \Bbbk^*$ such that the $\Bbbk$-subalgebra generated by the element $\vartheta = \alpha + t\beta$ exhausts the whole of $\mathbb{K}$. Since every $\vartheta \in \Bbbk$ is algebraic over $\Bbbk$, the algebra $\Bbbk[\vartheta]$ is a field. It coincides with $\mathbb{K}$ if and only if it contains β, because in that case, $\alpha = \vartheta - t\beta$ also lies in $\Bbbk[\vartheta]$. Let $f_\alpha(x), f_\beta(x)$ be the minimal polynomials of α, β over $\Bbbk$. Then β is a common root of the polynomials $f_\beta(x) \in \Bbbk[x]$ and $g(x) = f_\alpha(\vartheta - tx)$, the latter of which has coefficients in the field $\Bbbk[\vartheta]$, which depends on t. By Theorem 3.1 from Algebra I, there exists a field $\mathbb{F} \supset \mathbb{K}$ such that the minimal polynomials f_α, f_β become the products of linear factors over $\mathbb{F}$. Then g is completely factorizable over $\mathbb{F}$ as well. If we choose $t \in \Bbbk^*$ such that β is the *only* common root of f_β, g in $\mathbb{F}$, then the Euclidean algorithm allows us to express $(x - \beta) = \text{GCD}\left(f_\beta(x), g(x)\right)$ in terms of the polynomials f_β, g within $\Bbbk[\vartheta][x]$, and this forces $\beta \in \Bbbk[\vartheta]$. To find such t, write $\alpha_1, \alpha_2, \dots, \alpha_m$ and $\beta_1, \beta_2, \dots, \beta_k$ for the roots of the polynomials f_α and f_β in $\mathbb{F}$, where $m = \deg f_\alpha$, $k = \deg f_\beta = \deg g$. Let $\alpha = \alpha_1$ and $\beta = \beta_1$. Then the roots of g are $(\vartheta - \alpha_i)/t = \beta_1 + (\alpha_1 - \alpha_i)/t$ for $1 \leqslant i \leqslant m$. We need

$$\beta_1 + (\alpha_1 - \alpha_i)/t \neq \beta_j \tag{13.5}$$

for all i, j, but $i = j = 1$. Since α is separable, $\alpha_1 - \alpha_i \neq 0$ for all $i \neq 1$. Therefore, every inequality (13.5) with $i \neq 1$ forbids exactly one value of t. For $i = 1$, the inequalities (13.5) say that $\beta_1 \neq \beta_j$ for all $j \neq 1$, and they hold automatically, because β is separable. Thus, only a finite set of values for t is inadmissible, and we can find a required t in the infinite field $\Bbbk$. $\square$

Corollary 13.1 *If $\mathbb{K} \supset \Bbbk$ is a separable algebraic extension and the degrees of elements[6] of $\mathbb{K}$ over $\Bbbk$ are bounded above, then $\mathbb{K}$ is finite over $\Bbbk$ and*

$$\deg \mathbb{K}/\Bbbk = \max_{\vartheta \in \mathbb{K}} \deg_{\Bbbk} \vartheta \,.$$

Proof Let $\alpha \in \mathbb{K}$ be an element of maximal degree over $\Bbbk$. If there exists some $\beta \in \mathbb{K} \smallsetminus \Bbbk[\alpha]$, then $\deg \Bbbk[a, \beta]/\Bbbk > \deg \Bbbk[a]/\Bbbk = \deg_{\Bbbk} \alpha$. This forces the primitive element of the field $\Bbbk[\alpha, \beta]$ over $\Bbbk$ to be of strictly greater degree than α. Hence, $\mathbb{K} = \Bbbk[\alpha]$ and $\deg \mathbb{K}/\Bbbk = \deg_{\Bbbk} \alpha$. $\square$

case, we know from Example 3.4 of Algebra I that all finite fields are separable over their prime subfields.

[6] Recall that the *degree* $\deg_{\Bbbk} a$ of an algebraic element a over a field $\Bbbk$ is the degree of the minimal polynomial μ_a of a over $\Bbbk$.

13.2 Extensions of Homomorphisms

Recall that every nonzero homomorphism of a field to a ring is injective, because the only ideals in the field are (0) and (1). Associated with every inclusion of fields $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ is an injective homomorphism of polynomial rings $\Bbbk[x] \hookrightarrow \mathbb{F}[x]$ that maps a polynomial $f \in \Bbbk[x]$ to the polynomial $f^{\varphi} \in \mathbb{F}[x]$ whose coefficients are the images of the coefficients of f under the homomorphism $\varphi : \Bbbk \hookrightarrow \mathbb{F}$.

Lemma 13.1 *Let $\mathbb{K} = \Bbbk[x]/(f)$ be a simple extension of a field $\Bbbk$, and $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ an embedding of $\Bbbk$ into an arbitrary field $\mathbb{F}$. The embeddings $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$ coinciding with φ on $\Bbbk \subset \mathbb{K}$ are in canonical bijection with the roots of the polynomial f^{φ} in $\mathbb{F}$. In particular, there are at most* $\deg \mathbb{K}/\Bbbk$ *such embeddings, and the number of embeddings equals* $\deg \mathbb{K}/\Bbbk$ *if and only if the polynomial f^{φ} splits over $\mathbb{F}$ into a product of* $\deg f$ *distinct linear factors.*

Proof Associated with every element $\alpha \in \mathbb{F}$ is the map

$$\varphi_{\alpha} : \Bbbk[x] \to \mathbb{F}\,, \quad g(x) \mapsto g^{\varphi}(\alpha)\,.$$

If α is a root of the polynomial $f^{\varphi} \in \mathbb{F}[x]$, then $f \in \ker \varphi_{\alpha}$ and φ_{α} can be factorized through the embedding $\widetilde{\varphi}_{\alpha} : \Bbbk[x]/(f) \hookrightarrow \mathbb{F}$, which maps the primitive element $\vartheta = x \pmod{f}$ of $\mathbb{K}$ to $\alpha \in \mathbb{F}$. Two distinct roots $\alpha \neq \beta$ of f^{φ} certainly produce distinct maps $\widetilde{\varphi}_{\alpha} \neq \widetilde{\varphi}_{\beta}$. Conversely, every embedding $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$ coinciding with φ on the subfield $\Bbbk \subset \mathbb{K}$ maps ϑ to some root of the polynomial f^{φ}, because $f^{\varphi}\left(\widetilde{\varphi}(\vartheta)\right) = \widetilde{\varphi}\big(f(\vartheta)\big) = \varphi(0) = 0$. Therefore, $\widetilde{\varphi}$ coincides with the map $\widetilde{\varphi}_{\alpha}$ provided by some root α of f^{φ}. □

Lemma 13.2 *Let $\mathbb{K} \supset \Bbbk$ be an algebraic field extension, not necessarily finite, and $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ an embedding of fields such that for every $\vartheta \in \mathbb{K}$ with minimal polynomial μ_{ϑ} over $\Bbbk$, the polynomial $\mu_{\vartheta}^{\varphi} \in \mathbb{F}[x]$ splits completely into a product of linear factors in $\mathbb{F}[x]$. Then for every $\vartheta \in \mathbb{K}$ and every root $\xi \in \mathbb{F}$ of the polynomial $\mu_{\vartheta}^{\varphi}$, there exists an embedding of fields $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$ that coincides with φ on the subfield $\Bbbk$ and takes $\widetilde{\varphi}(\vartheta)$ to ξ.*

Proof By Lemma 13.1, the embedding $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ can be extended to an embedding $\varphi_{\xi} : \Bbbk[\vartheta] \hookrightarrow \mathbb{F}\,, \quad \vartheta \mapsto \xi\,$. Consider the set $\mathcal{S}$ of all embeddings $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$ extending φ_{ξ} to subfields $\mathbb{L} \subseteq \mathbb{K}$ containing $\Bbbk[\vartheta]$. The set $\mathcal{S}$ is nonempty, because it contains φ_{ξ}, and it is partially ordered by the relation $(\mathbb{L}'', \psi'') \geqslant (\mathbb{L}', \psi')$, meaning that $\mathbb{L}'' \supseteq \mathbb{L}'$ and $\psi''|_{\mathbb{L}'} = \psi'$.

Exercise 13.6 Verify that $\mathcal{S}$ is a complete poset in the sense of Definition 1.2 of Algebra I.

By Zorn's lemma,[7] there exists a maximal element $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$ in $\mathcal{S}$. Let us show that its domain $\mathbb{L}$ is equal to $\mathbb{K}$. Assume the contrary and let $\vartheta \in \mathbb{K} \smallsetminus \mathbb{L}$. Then

[7] See Lemma 1.3 of Algebra I.

the minimal polynomial $\mu_\vartheta \in \Bbbk[x]$ of ϑ over $\Bbbk$ is divisible in $\mathbb{L}[x]$ by the minimal polynomial $\mu_{\vartheta,\mathbb{L}}$ of ϑ over $\mathbb{L}$. Since μ_ϑ^φ is a product of linear factors in $\mathbb{F}[x]$, its divisor $\mu_{\vartheta,\mathbb{L}}^\varphi$ is also the product of some of those factors. Therefore, the simple field extension $\mathbb{L} \subset \mathbb{L}[\vartheta]$ satisfies the condition of Lemma 13.1, which allows us to extend ψ to the field $\mathbb{L}[\vartheta] = \mathbb{L}[x]/(\mu_{\vartheta,\mathbb{L}})$, which is strictly larger than $\mathbb{L}$. □

Proposition 13.1 *Let $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ be an arbitrary embedding of fields, and $\mathbb{K} \supset \Bbbk$ a finite extension. Then there exist at most* $\deg \mathbb{K}/\Bbbk$ *distinct embeddings $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ extending φ. The number of such embeddings equals* $\deg \mathbb{K}/\Bbbk$ *if and only if the extension $\mathbb{K} \supset \Bbbk$ is separable and for every $\vartheta \in \mathbb{K}$, the image $\mu_\vartheta^\varphi \in \mathbb{F}[x]$ of the minimal polynomial $\mu_\vartheta \in \Bbbk[x]$ of ϑ over $\Bbbk$ splits completely over $\mathbb{F}$ into a product of linear factors.*

Proof Consider a finite tower of simple field extensions (13.4),

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{K}\,, \tag{13.6}$$

where $\mathbb{L}_i = \mathbb{L}_{i-1}[\vartheta_i] \simeq \mathbb{L}_{i-1}[x]/(f_i)$ and $f_i \in \mathbb{L}_{i-1}[x]$ is the minimal polynomial of some element $\vartheta_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_{i-1}$ over $\mathbb{L}_{i-1}$. If an embedding $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ extends φ, then the restrictions of ψ to the subfields $\mathbb{L}_i \subset \mathbb{K}$ form a sequence of embeddings $\psi_i : \mathbb{L}_i \hookrightarrow \mathbb{F}$, each of which extends the previous one. By Lemma 13.1, there are at most $\deg f_i = \deg \mathbb{L}_i/\mathbb{L}_{i-1}$ such extensions for each i. Therefore, there are at most $\prod_i \deg \mathbb{L}_i/\mathbb{L}_{i-1} = \deg \mathbb{K}/\Bbbk$ embeddings ψ extending φ. This upper bound is achieved if and only if every polynomial f_i^φ has exactly $\deg f_i$ distinct roots in $\mathbb{F}$. For every element $\vartheta \in \mathbb{K}$, there exists a tower (13.6) beginning with the adjunction of $\vartheta_1 = \vartheta$ at the bottom level. Thus, the existence of exactly $\deg \mathbb{K}/\Bbbk$ extensions of φ forces μ_ϑ^φ to be completely factorizable over $\mathbb{F}$ into a product of $\deg \mu_\vartheta$ distinct linear factors for all $\vartheta \in \mathbb{K}$. In particular, all μ_ϑ are separable. Conversely, if all elements $\vartheta \in \mathbb{K}$ are separable and the images μ_ϑ^φ of their minimal polynomials are the products of $\deg \mu_\vartheta$ linear factors,[8] then every polynomial f_i in every tower (13.6) is mapped by the embedding $\psi_{i-1} : \mathbb{L}_{i-1} \hookrightarrow \mathbb{F}$ to a completely factorizable separable polynomial in $\mathbb{F}[x]$, because f_i divides μ_{ϑ_i} in $\mathbb{L}_{i-1}[x]$. Therefore,

$$\varphi : \Bbbk \hookrightarrow \mathbb{F}$$

can be continued along such a tower in exactly $\deg \mathbb{K}/\Bbbk$ different ways. □

Exercise 13.7 Under the conditions of Proposition 13.1, let elements

$$\xi_1, \xi_2, \dots, \xi_m \in \mathbb{K}$$

generate the field $\mathbb{K}$ as a $\Bbbk$-algebra. Show that $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ admits exactly $\deg \mathbb{K}/\Bbbk$ extensions $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ if and only if every ξ_ν is separable and $\mu_{\xi_i}^\varphi$ splits completely in $\mathbb{F}[x]$ into a product of linear factors.

[8] Automatically distinct.

Proposition 13.2 *Let $\mathbb{K} \supset \Bbbk$ be an algebraic field extension, not necessarily finite. Then every embedding $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$ that acts identically on the subfield $\Bbbk$ is an automorphism of $\mathbb{K}$.*

Proof It is enough to check that $\varphi(\mathbb{K}) = \mathbb{K}$. Let $\vartheta \in \mathbb{K}$ have minimal polynomial $f \in \Bbbk[x]$ over $\Bbbk$. Since φ maps every root of f to a root of f, the equality $\varphi^m\vartheta = \varphi^n\vartheta$ holds for some $m > n$, where $\varphi^k = \varphi \circ \cdots \circ \varphi$ means the kth iteration of the map $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$. Then the injectivity of φ forces[9] $\vartheta = \varphi^{m-n}\vartheta \in \operatorname{im}\varphi$. □

13.3 Splitting Fields and Algebraic Closures

In this section we construct some special universal algebraic extensions of an arbitrary field $\Bbbk$. These universal extensions will be unique up to a nonunique (noncanonical) isomorphism that acts identically on $\Bbbk$.

Definition 13.1 (Splitting Field) Given a polynomial $f \in \Bbbk[x]$, a field $\mathbb{L}_f \supset \Bbbk$ is called a *splitting field* of f if f is a product of $\deg f$ linear factors in $\mathbb{L}_f[x]$ and for every field $\mathbb{F} \supset \Bbbk$ such that f is a product of $\deg f$ linear factors over $\mathbb{F}$, there exists an embedding $\mathbb{L}_f \hookrightarrow \mathbb{F}$ that is the identity over $\Bbbk$.

Example 13.3 (Splitting Field of a Cubic Polynomial) Let $f \in \Bbbk[x]$ be an irreducible cubic polynomial. We have seen in Example 13.1 on p. 296 that if the discriminant $D(f)$ is a square in $\Bbbk$, then the simple cubic extension $\mathbb{K} = \Bbbk[x]/(f)$ is a splitting field of f. If $D(f)$ is not a square in $\Bbbk$, then $D(f)$ is not a square even in $\mathbb{K}$, and a splitting field of f is provided by the simple quadratic extension of $\mathbb{K}$ by $\sqrt{D(f)}$. Note that the latter has degree 6 over $\Bbbk$.

Theorem 13.3 *Every polynomial $f \in \Bbbk[x]$ has a splitting field $\mathbb{L}_f$, and every two splitting fields are (noncanonically) isomorphic over*[10] *$\Bbbk$.*

Remark 13.1 Since all splitting fields of a given polynomial are isomorphic, we shall frequently refer to *the* splitting field of a polynomial. However, the reader should always keep in mind that given two splitting fields $\mathbb{L}' \supset \Bbbk \subset \mathbb{L}''$, there are in general many different isomorphisms $\mathbb{L}' \xrightarrow{\sim} \mathbb{L}''$ acting identically on $\Bbbk$.

Proof (of Theorem 13.3) Let $\mathbb{F} \supset \Bbbk$ be a finite extension such that f splits into a product of $\deg f$ linear factors[11] in $\mathbb{F}[x]$. Write $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{F}$ for the roots of f, and $\mathbb{L}_f \subset \mathbb{F}$ for the smallest[12] subfield containing $\Bbbk$ and all these roots. Then $\mathbb{L}_f$ is

[9] See Lemma 1.1 of Algebra I.

[10] That is, there exists an isomorphism between them acting on $\Bbbk$ identically.

[11] Such an extension exists by Theorem 3.1 of Algebra I.

[12] With respect to inclusions.

generated by $\alpha_1, \alpha_2, \dots, \alpha_m$ as a $\Bbbk$-algebra, and there exists a tower of simple field extensions

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \tag{13.7}$$

whereby some element $\vartheta \in \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ is adjoined at each level.[13] If f splits into a product of $\deg f$ linear factors over $\mathbb{F} \subset \Bbbk$, then by Lemma 13.2, the inclusion $\Bbbk \subset \mathbb{F}$ can be extended along the tower (13.7) to an embedding $\mathbb{L}_f \hookrightarrow \mathbb{F}$ that acts identically on $\Bbbk$, because the irreducible polynomials whose roots are adjoined on the levels of the tower divide ϑ and therefore are completely factorizable over $\mathbb{F}$ into linear factors. Hence, $\mathbb{L}_f$ is a splitting field of f. Given another splitting field $\mathbb{L}'_f$ of f, there exist embeddings $\varphi : \mathbb{L}_f \hookrightarrow \mathbb{L}'_f$ and $\varphi' : \mathbb{L}'_f \hookrightarrow \mathbb{L}_f$ provided by the definition of a splitting field. Since the compositions $\varphi \circ \varphi'$, $\varphi' \circ \varphi$ are bijective by Proposition 13.2, both embeddings have to be surjective. □

Example 13.4 (The Classification of Finite Fields Revisited) Every finite field $\mathbb{F}$ of characteristic p is a finite extension of the prime subfield $\mathbb{F}_p = \mathbb{Z}/(p) \subset \mathbb{F}$ and consists of $q = p^n$ elements for $n = \deg \mathbb{F}/\mathbb{F}_p = \dim_{\mathbb{F}_p} \mathbb{F}$. Since the nonzero elements of $\mathbb{F}$ form a multiplicative group of order $q - 1$, they are exactly the roots of the polynomial $x^{q-1} - 1 \in \mathbb{F}_p[x]$ in the field $\mathbb{F}$. Therefore, $\mathbb{F}$ is a splitting field of the polynomial $f(x) = x^q - x \in \mathbb{F}_p[x]$. This forces $\mathbb{F}$ to be the unique field of q elements up to a (noncanonical) isomorphism.

Definition 13.2 (Algebraic Closure) An algebraically closed algebraic extension $\overline{\Bbbk} \supset \Bbbk$ is called an *algebraic closure* of $\Bbbk$.

Theorem 13.4 *Every field $\Bbbk$ has an algebraic closure, unique up to a (noncanonical) isomorphism that acts identically on $\Bbbk$.*

Proof Given two algebraic closures $\mathbb{L}'$, $\mathbb{L}''$ of the field $\Bbbk$, then by Lemma 13.2 on p. 300, the embedding $\Bbbk \subset \mathbb{L}'$ can be extended to an embedding $\varphi' : \mathbb{L}' \hookrightarrow \mathbb{L}''$ that acts identically on $\Bbbk$. Symmetrically, there is an embedding $\varphi'' : \mathbb{L}'' \hookrightarrow \mathbb{L}'$ that acts identically on $\Bbbk$. Proposition 13.2 forces the compositions $\varphi' \circ \varphi''$, $\varphi'' \circ \varphi'$ to be bijective. Therefore, the embeddings φ', φ'' have to be surjective, and $\mathbb{L}' \simeq \mathbb{L}''$.

The proof of existence consists of two steps. Assume first that there exists an algebraically closed field $\mathbb{F} \supset \Bbbk$. Then we can put $\overline{\Bbbk}$ as the integral[14] closure of $\Bbbk$ in $\mathbb{F}$, which is a field by Proposition 10.3 on p. 229. Every polynomial $f \in \overline{\Bbbk}[x] \subset \mathbb{F}[x]$ has a root $\vartheta \in \mathbb{F}$, which is algebraic over $\overline{\Bbbk}$ and therefore algebraic over $\Bbbk$. This forces $\vartheta \in \overline{\Bbbk}$. Hence, $\overline{\Bbbk}$ is algebraically closed, i.e., is an algebraic closure of $\Bbbk$. It remains to show that an algebraically closed field $\mathbb{F} \supset \Bbbk$ exists. To begin with, let us construct a field $\mathbb{F}_1 \supset \Bbbk$ such that every polynomial $f \in \Bbbk[x]$ is a product of $\deg f$

[13] Note that k may be less than m, because the adjunction of a root may cause the appearance of several more roots.

[14] Or equivalently, algebraic.

linear factors in $\mathbb{F}_1[x]$. By Zermelo's theorem,[15] the set $\Bbbk[x]$ can be well ordered[16] by some order relation $f < g$.

Exercise 13.8 Use the transfinite induction principle[17] to show that for every $f \in \Bbbk[x]$, there exists a field $\mathbb{K}_f \supset \Bbbk$ such that f splits completely into a product of linear factors over $\mathbb{K}_f$, and $\mathbb{K}_f \subset \mathbb{K}_g$ for all $f < g$.

We put $\mathbb{F}_1 = \bigcup_{f \in \Bbbk[x]} \mathbb{K}_f$. Repeating the procedure leads to an infinite tower of fields

$$\Bbbk \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \cdots$$

such that every polynomial $f \in \mathbb{F}_i[x]$ is a product of $\deg f$ linear factors in $\mathbb{F}_{i+1}[x]$. This forces the union $\mathbb{F} = \bigcup_{i \in \mathbb{N}} \mathbb{F}_i$ to be an algebraically closed field containing $\Bbbk$. □

Corollary 13.2 *For every tower of finite field extensions $\mathbb{L}_1 \subset \mathbb{L}_2 \subset \mathbb{L}_3$, the extension $\mathbb{L}_1 \subset \mathbb{L}_3$ is separable if and only if the extensions $\mathbb{L}_1 \subset \mathbb{L}_2$, $\mathbb{L}_2 \subset \mathbb{L}_3$ are separable.*

Proof If $\mathbb{L}_3$ is separable over $\mathbb{L}_1$, then in particular, the subfield $\mathbb{L}_2$ is separable, and $\mathbb{L}_3$ is separable over $\mathbb{L}_2$, because the minimal polynomial of every element $\vartheta \in \mathbb{L}_3$ over $\mathbb{L}_2$ is a divisor of the separable minimal polynomial of ϑ over $\mathbb{L}_1$. Conversely, if the extensions $\mathbb{L}_1 \subset \mathbb{L}_2 \subset \mathbb{L}_3$ are separable, then by Proposition 13.1, the identical embedding of $\mathbb{L}_1$ into the algebraic closure $\mathbb{L}_1 \hookrightarrow \overline{\mathbb{L}}_1$ admits exactly $\deg \mathbb{L}_2/\mathbb{L}_1$ continuations $\mathbb{L}_2 \hookrightarrow \overline{\mathbb{L}}_1$, each of which has exactly $\deg \mathbb{L}_3/\mathbb{L}_2$ continuations

$$\mathbb{L}_3 \hookrightarrow \overline{\mathbb{L}}_1.$$

Since there are $\deg \mathbb{L}_2/\mathbb{L}_1 \cdot \deg \mathbb{L}_3/\mathbb{L}_2 = \deg \mathbb{L}_3/\mathbb{L}_1$ embeddings $\mathbb{L}_3 \hookrightarrow \overline{\mathbb{L}}_1$ extending the identical inclusion $\mathbb{L}_1 \hookrightarrow \overline{\mathbb{L}}_1$, Proposition 13.1 forces the extension $\mathbb{L}_1 \subset \mathbb{L}_3$ to be separable. □

13.4 Normal Extensions

An algebraic field extension $\Bbbk \subset \mathbb{K}$ is called *normal* if every irreducible polynomial $f \in \Bbbk[x]$ possessing a root in $\mathbb{K}$ splits completely over $\mathbb{K}$ into a product of linear factors.

Exercise 13.9 Convince yourself that every monic irreducible polynomial $f \in \Bbbk[x]$ possessing a root ϑ in an extension $\mathbb{K} \supset \Bbbk$ is the minimal polynomial of that ϑ over $\Bbbk$.

[15] See Problem 1.20 of Algebra I.

[16] See Sect. 1.4.2 of Algebra I.

[17] See Exercise 1.16 in Sect. 1.4.2 of Algebra I.

Thus, an algebraic extension $\Bbbk \subset \mathbb{K}$ is normal if and only if the minimal polynomials of all elements $\vartheta \in \mathbb{K}$ over $\Bbbk$ split completely in $\mathbb{K}[x]$ into products of linear factors.

Exercise 13.10 Check that every simple quadratic field extension is normal.

Lemma 13.3 *Let $\overline{\Bbbk} \supset \Bbbk$ be an algebraic closure of a field $\Bbbk$. An algebraic field extension $\Bbbk \subset \mathbb{K}$ is normal if and only if all embeddings $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ extending the inclusion $\Bbbk \subset \overline{\Bbbk}$ have the same image.*

Proof Fix one such an embedding $\varphi : \mathbb{K} \hookrightarrow \overline{\Bbbk}$, which exists by Lemma 13.2 on p. 300, and identify $\mathbb{K}$ with the subfield $\varphi(\mathbb{K}) \subset \overline{\Bbbk}$ by means of this embedding. Thus, we have a tower $\Bbbk \subset \mathbb{K} \subset \overline{\Bbbk}$. Every other embedding $\psi : \mathbb{K} \hookrightarrow \overline{\Bbbk}$ extending the inclusion $\Bbbk \subset \overline{\Bbbk}$ maps every element $\vartheta \in \mathbb{K}$ to a root of the minimal polynomial μ_ϑ of ϑ over $\Bbbk$. If all the roots of μ_ϑ in $\overline{\Bbbk}$ belong to $\mathbb{K}$ for every $\vartheta \in \mathbb{K}$, then we certainly have $\psi(\mathbb{K}) \subset \mathbb{K}$. Conversely, it follows from Lemma 13.2 that for every $\vartheta \in \mathbb{K}$ and every root ξ of the minimal polynomial $\mu_\vartheta \in \Bbbk[x]$, there exists an embedding of fields $\psi_{\vartheta,\xi} : \mathbb{K} \hookrightarrow \overline{\Bbbk}$ such that $\psi_{\vartheta,\xi}(\vartheta) = \xi$. If the images of all $\psi_{\vartheta,\xi}$ coincide with $\mathbb{K}$, all roots of μ_ϑ belong to $\mathbb{K} \subset \overline{\Bbbk}$ for all $\vartheta \in \mathbb{K}$. □

Lemma 13.4 *Let $\Bbbk \subset \mathbb{L} \subset \mathbb{K}$ be a tower of algebraic extensions of fields such that $\mathbb{K}$ is normal over $\Bbbk$. Then $\mathbb{K}$ is normal over $\mathbb{L}$ as well, whereas $\mathbb{L}$ is normal over $\Bbbk$ if and only if the image of every embedding $\mathbb{L} \hookrightarrow \mathbb{K}$ that acts identically on $\Bbbk$ coincides with $\mathbb{L}$*

Proof For every element $\vartheta \in \mathbb{K}$, the minimal polynomial of ϑ over $\mathbb{L}$ divides in $\mathbb{L}[x]$ the minimal polynomial of ϑ over $\Bbbk$. Thus, if the minimal polynomial of ϑ over $\Bbbk$ is completely factorizable in $\mathbb{K}[x]$ into linear factors, then the minimal polynomial of ϑ over $\mathbb{L}$ is, too. Therefore, $\mathbb{K}$ is normal over $\mathbb{L}$. The second statement of the lemma holds because of Lemma 13.3 and the following observation. Let

$$\overline{\Bbbk} \supset \mathbb{K} \supset \mathbb{L} \supset \Bbbk$$

be an algebraic closure of $\Bbbk$. Then the images of all embeddings $\mathbb{L} \hookrightarrow \overline{\Bbbk}$ that act identically on $\Bbbk$ lie in $\mathbb{K}$, since every such embedding can be extended to an embedding $\mathbb{K} \hookrightarrow \overline{\Bbbk}$, whose image is $\mathbb{K}$ if $\mathbb{K}$ is normal over $\Bbbk$. □

Caution 13.1 Given two normal field extensions $\mathbb{L} \supset \Bbbk$ and $\mathbb{F} \supset \mathbb{L}$, the resulting extension $\mathbb{F} \supset \Bbbk$ is not necessarily normal. For example, the simple quartic extension $\mathbb{Q}\left[\sqrt[4]{2}\right] = \mathbb{Q}[x]/(x^4 - 2) \supset \mathbb{Q}$ can obviously be decomposed into a tower of two quadratic extensions $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{2}\right] \subset \mathbb{Q}\left[\sqrt{\sqrt{2}}\right]$, each of which is normal by Exercise 13.10. However, the quartic field $\mathbb{Q}\left[\sqrt[4]{2}\right]$ is not normal over $\mathbb{Q}$, because its four embeddings into $\overline{\mathbb{Q}} \subset \mathbb{C}$ send the primitive element $x \pmod{x^4 - 2}$ to the fourth roots of 2 in $\mathbb{C}$, i.e., to $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$, where $\sqrt[4]{2}$ denotes the real positive root. The images of these embeddings form *two* different subfields of $\mathbb{C}$ linearly generated over $\mathbb{Q}$ by $1, \sqrt[4]{2}$ and by $1, i\sqrt[4]{2}$ respectively.

Proposition 13.3 *A finite field extension $\mathbb{K} \supset \Bbbk$ is normal if and only if $\mathbb{K}$ is a splitting field of some not necessarily irreducible polynomial $f \in \Bbbk[x]$.*

Proof Let $\mathbb{K}$ be normal over $\Bbbk$, and suppose $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{K}$ generate $\mathbb{K}$ as a $\Bbbk$-algebra. Write $f_i \in \Bbbk[x]$ for the minimal polynomial of α_i over $\Bbbk$. Then the product $f = \prod f_i$ is completely factorizable over $\mathbb{K}$ into linear factors, and it follows from Exercise 13.7 that $\mathbb{K}$ can be embedded into every field $\mathbb{L}$ over which f is a product of $\deg f$ linear factors. This forces $\mathbb{K}$ to be a splitting field of f. Conversely, if $\mathbb{K} \supset \Bbbk$ is a splitting field of a polynomial $f \in \Bbbk[x]$ and $\overline{\Bbbk} \supset \Bbbk$ is an algebraic closure of $\Bbbk$, then every embedding $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ that acts identically on $\Bbbk$ maps $\mathbb{K}$ isomorphically onto the subfield $\Bbbk[\alpha_1, \alpha_2, \dots, \alpha_k] \subset \overline{\Bbbk}$ spanned as a $\Bbbk$-algebra by all the roots $\alpha_1, \alpha_2, \dots, \alpha_k$ of f in $\overline{\Bbbk}$. Thus, $\mathbb{K}$ is normal by Lemma 13.3. □

13.5 Compositum

Let us fix an algebraic closure $\overline{\Bbbk}$ of a field $\Bbbk$. For every collection of subfields

$$\mathbb{K}_1, \mathbb{K}_2, \dots, \mathbb{K}_m \subset \overline{\Bbbk}$$

containing $\Bbbk$, the smallest subfield of $\overline{\Bbbk}$ containing all the fields $\mathbb{K}_\nu$ is called the *compositum* of the fields $\mathbb{K}_\nu$ and is denoted by $\mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_m$. It is linearly generated over $\Bbbk$ by the products $\vartheta_1\vartheta_2 \cdots \vartheta_m$, where $\vartheta_i \in \mathbb{K}_i$ for all i.

Exercise 13.11 Prove this last statement.

Proposition 13.4 *Let $\mathbb{F}, \mathbb{K} \subset \overline{\Bbbk}$ be two fields containing $\Bbbk$. If $\mathbb{K}$ is normal (respectively separable) over $\Bbbk$, then the compositum $\mathbb{K}\mathbb{F}$ is normal (respectively separable) over $\mathbb{F}$.*

Proof The embeddings $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\mathbb{F}} = \overline{\Bbbk}$ that act identically on $\mathbb{F} \subset \mathbb{K}\mathbb{F}$ are in bijection with the embeddings $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ that act identically on $\Bbbk \subset \mathbb{K}$, because every embedding $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ admits a unique $\mathbb{F}$-linear continuation $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$, and conversely, the restriction of every $\mathbb{F}$-linear embedding $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$ to $\mathbb{K}$ gives an embedding $\mathbb{K} \subset \mathbb{K}\mathbb{F}$. Thus, the statements follow from Lemma 13.3 and Proposition 13.1. □

Theorem 13.5 (Normal Closure) *Let $\mathbb{F} \supset \Bbbk$ be a finite separable field extension. There is a field $\mathbb{K} \supset \mathbb{F}$ normal and separable over $\Bbbk$ such that for every field $\mathbb{L} \supset \mathbb{F}$ normal and separable over $\Bbbk$, there is an embedding $\mathbb{K} \hookrightarrow \mathbb{L}$ that acts identically on $\mathbb{F}$. For every two such fields $\mathbb{K}$, $\mathbb{K}'$, there exists a noncanonical isomorphism $\mathbb{K} \xrightarrow{\sim} \mathbb{K}'$ that acts identically on $\mathbb{F}$.*

Proof Let $\overline{\Bbbk} \supset \Bbbk$ be an algebraic closure of $\Bbbk$, and $n = \deg \mathbb{F}/\Bbbk$. Put $\mathbb{K}$ as the compositum of all n distinct embeddings $\mathbb{F} \hookrightarrow \overline{\Bbbk}$ that act identically on $\Bbbk$. Then $\deg \mathbb{K}/\mathbb{F} \leqslant n$, and $\mathbb{K}$ is normal and separable over the fields $\mathbb{F}$, $\Bbbk$. For every normal separable extension $\mathbb{L} \supset \Bbbk$, every embedding $\mathbb{F} \hookrightarrow \mathbb{L}$ that acts identically on $\Bbbk$ certainly can be extended to an embedding $\mathbb{K} \hookrightarrow \mathbb{L}$. The last statement is established by the same argument as in Theorems 13.3 and 13.4. □

Definition 13.3 A field $\mathbb{K}$ satisfying the conditions of Theorem 13.5 is called a *normal closure* of the separable extension $\mathbb{F} \supset \Bbbk$.

13.6 Automorphisms of Fields and the Galois Correspondence

Given an field extension $\Bbbk \subset \mathbb{K}$, automorphisms of $\mathbb{K}$ acting identically on $\Bbbk$ are called automorphisms *over* $\Bbbk$ or *automorphisms of the extension* $\Bbbk \subset \mathbb{K}$. They form a group, denoted by

$$\operatorname{Aut}_{\Bbbk} \mathbb{K} \stackrel{\text{def}}{=} \{\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K} \mid \forall\, t \in \Bbbk \;\; \varphi(t) = t\}\,.$$

For a finite extension $\mathbb{K} \supset \Bbbk$, Proposition 13.1 on p. 301 implies the inequality

$$|\operatorname{Aut}_{\Bbbk} \mathbb{K}| \leqslant \deg \mathbb{K}/\Bbbk\,. \tag{13.8}$$

A finite extension $\mathbb{K} \supset \Bbbk$ is called a *Galois extension* if this inequality is in fact an equality. It follows from Proposition 13.1 that a finite field extension is a Galois extension if and only if it is normal and separable. The automorphism group of a Galois extension $\mathbb{K} \supset \Bbbk$ is called the *Galois group* and denoted by $\operatorname{Gal} \mathbb{K}/\Bbbk \stackrel{\text{def}}{=} \operatorname{Aut}_{\Bbbk} \mathbb{K}$. Let me stress that this notation always assumes that $\Bbbk \subset \mathbb{K}$ is a Galois extension.

Given an arbitrary group G of automorphisms $\mathbb{K} \xrightarrow{\sim} \mathbb{K}$ of a field $\mathbb{K}$, the G-invariant elements $t \in \mathbb{K}$ form a subfield of $\mathbb{K}$, denoted by

$$\mathbb{K}^G \stackrel{\text{def}}{=} \{t \in \mathbb{K} \mid \forall \varphi \in G \;\; \varphi(t) = t\}$$

and called the *field of G-invariants*. Note that $\mathbb{K}^G$ contains the prime subfield[18] of $\mathbb{K}$.

Theorem 13.6 *Let $\mathbb{K}$ be an arbitrary field, and G a finite group of automorphisms $\mathbb{K} \xrightarrow{\sim} \mathbb{K}$. Then the extension $\mathbb{K} \supset \mathbb{K}^G$ is a Galois extension of degree $|G|$, and $\operatorname{Gal} \mathbb{K}/\Bbbk = G$.*

Proof Given an element $\vartheta \in \mathbb{K}$, write $\vartheta_1, \vartheta_2, \dots, \vartheta_m \in \mathbb{K}$ for all the distinct elements of the G-orbit of $\vartheta = \vartheta_1$. Then the polynomial

$$f_\vartheta(x) = (x - \vartheta_1)(x - \vartheta_2)\cdots(x - \vartheta_m) \tag{13.9}$$

[18] It is isomorphic to $\mathbb{Q}$ for $\operatorname{char}(\Bbbk) = 0$, and to $\mathbb{F}_p = \mathbb{Z}/(p)$ for $\operatorname{char}(\Bbbk) = p > 0$; see Sect. 2.8.1 of Algebra I.

has its coefficients in $\mathbb{K}^G$. For every polynomial $h \in \mathbb{K}^G[x]$, the group G maps the roots of h to the roots of h. Therefore, G cannot act transitively on the roots of a product h_1h_2, where $h_i \in \mathbb{K}^G[x]$ and $\deg h_i > 0$ for $i = 1, 2$. This forces the polynomial (13.9) to be irreducible in $\mathbb{K}^G[x]$. Hence, f_ϑ is the minimal polynomial of ϑ over $\mathbb{K}^G$. Since f_ϑ splits in $\mathbb{K}[x]$ into a product of $\deg f_\vartheta$ distinct linear factors, the extension $\mathbb{K}^G \subset \mathbb{K}$ is algebraic, normal, and separable. Moreover, $\deg_{\mathbb{K}^G} \vartheta \leqslant |G|$ for all $\vartheta \in \mathbb{K}$. By Corollary 13.1, the extension $\mathbb{K}^G \subset \mathbb{K}$ is finite with $\deg \mathbb{K}/\mathbb{K}^G \leqslant |G|$. At the same time, $|G| \leqslant |\mathrm{Aut}_{\mathbb{K}^G} \mathbb{K}| \leqslant \deg \mathbb{K}/\mathbb{K}^G$, because $G \subset \mathrm{Aut}_{\mathbb{K}^G} \mathbb{K}$. This forces all the inequalities to be equalities, and $G = \mathrm{Aut}_{\mathbb{K}^G} \mathbb{K}$. □

Corollary 13.3 *For every finite field extension $\Bbbk \subset \mathbb{K}$ and subgroup $G \subset \mathrm{Aut}_\Bbbk \mathbb{K}$, the equalities $\mathbb{K}^G = \Bbbk$ and $|G| = \deg \mathbb{K}/\Bbbk$ are equivalent. If they hold, then $G = \mathrm{Aut}_\Bbbk \mathbb{K}$.*

Proof Applying Theorem 13.6 to the tower $\Bbbk \subset \mathbb{K}^G \subset \mathbb{K}$ leads to the equality $\deg \mathbb{K}/\mathbb{K}^G = |G|$, which immediately implies all the statements.

However, it is quite instructive to give a direct proof of Corollary 13.3 without using the primitive element theorem, Theorem 13.2 on p. 298, hidden within[19] Theorem 13.6. Such a proof follows below.

Let $|G| = \deg \mathbb{K}/\Bbbk$. The inequalities $|G| \leqslant \deg \mathbb{K}/\mathbb{K}^G \leqslant \deg \mathbb{K}/\Bbbk$ force

$$\deg \mathbb{K}/\mathbb{K}^G = \deg \mathbb{K}/\Bbbk = \deg \mathbb{K}/\mathbb{K}^G \cdot \deg \mathbb{K}^G/\Bbbk\,.$$

Therefore, $\deg \mathbb{K}^G/\Bbbk = 1$ and $\mathbb{K}^G = \Bbbk$. Conversely, let $\mathbb{K}^G = \Bbbk$. The same arguments as in the proof of Theorem 13.6 show that the extension $\mathbb{K} \supset \Bbbk$ is normal and separable. Therefore, the inclusion $\Bbbk \hookrightarrow \mathbb{K}$ allows exactly $\deg \mathbb{K}/\Bbbk$ extensions to automorphisms $\mathbb{K} \xrightarrow{\sim} \mathbb{K}$ over $\Bbbk$, i.e., $|\mathrm{Aut}_\Bbbk \mathbb{K}| = \deg \mathbb{K}/\Bbbk$. It remains to verify that $\mathrm{Aut}_\Bbbk \mathbb{K} = G$. For every $\vartheta \in \mathbb{K}$, the coefficients of the minimal polynomial f_ϑ of ϑ over $\Bbbk$ are $\mathrm{Aut}_\Bbbk \mathbb{K}$-invariant. This forces every automorphism $\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ over $\Bbbk$ to map ϑ to a root of f_ϑ. Moreover, as we have seen before formula (13.9), these roots form one orbit of G. We conclude that for every $\varphi \in \mathrm{Aut}_\Bbbk \mathbb{K}$ and every $\vartheta \in \mathbb{K}$, there exists $g \in G$ such that $g(\vartheta) = \varphi(\vartheta)$. Thus, for each $\varphi \in \mathrm{Aut}_\Bbbk \mathbb{K}$, the field $\mathbb{K}$, considered as a vector space over $\Bbbk$, splits into a finite union of vector subspaces $V_g = \{\vartheta \in \mathbb{K} \mid g(\vartheta) = \psi(\vartheta)\}$ taken for all $g \in G$. For an infinite field $\Bbbk$, this forces[20] $\mathbb{K}$ to coincide with some V_g, and therefore, $\varphi = g$. For a finite field $\Bbbk$, the field $\mathbb{K}$ is also finite and spanned as a $\Bbbk$-algebra by a generator ϑ of the cyclic multiplicative group $\mathbb{K}^*$. In this case, $\varphi = g$ for that $g \in G$ with $\varphi(\vartheta) = g(\vartheta)$. □

Example 13.5 (Field of Invariants for the Group of a Triangle) Consider the coordinate projective line $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ over an arbitrary field $\Bbbk$, on which the group

[19] The proof of Theorem 13.6 is based on Corollary 13.1 on p. 299, a direct corollary of Theorem 13.2.

[20] See Exercise 11.14 on p. 254.

of a triangle[21] $G = S_3$ acts by linear fractional automorphisms permuting the points $0 = (0:1)\,,\ 1 = (1:1)\,,\ \infty = (1:0)$. Namely, the identity map, the two cycles

$$\tau : 0 \mapsto 1 \mapsto \infty \mapsto 0\,, \quad \tau^{-1} : \infty \mapsto 1 \mapsto 0 \mapsto \infty\,,$$

and the three reflections σ_0, σ_1, σ_∞ marked by their fixed points 0, 1, ∞, act on the affine coordinate $t = t_0/t_1$ by the rules

$$\begin{aligned} &\mathrm{Id} : \ t \mapsto t\,, && \tau : \ t \mapsto 1/(1-t)\,, && \tau^{-1} : \ t \mapsto (t-1)/t\,, \\ &\sigma_0 : \ t \mapsto t/(t-1)\,, && \sigma_1 : \ t \mapsto 1/t\,, && \sigma_\infty : \ t \mapsto 1-t\,. \end{aligned} \tag{13.10}$$

The pullback of this action provides the field of rational functions $\mathbb{K} = \Bbbk(t)$ with the action of G by the rule $g : \varphi(t) \mapsto \varphi\left(g^{-1}(t)\right)$ for all $g \in G$, $\varphi \in \mathbb{K}$. The field of G-invariants $\mathbb{K}^G \subset \mathbb{K}$ consists of all rational functions $\varphi(t) \in \Bbbk(t)$ mapped to themselves under all six substitutions (13.10). By Theorem 13.6, the extension $\mathbb{K}^G \subset \mathbb{K}$ is a Galois extension of degree 6. We are going to write an explicit transcendence generator[22] for $\mathbb{K}^G$. If a function $\psi(t) = p(t)/q(t)$ is G-invariant, then every rational function of ψ is certainly G-invariant as well. Such functions form a subfield $\Bbbk(\psi) \subset \mathbb{K}^G$. The transcendence generator t of $\mathbb{K}$ over $\Bbbk$ is a root of the polynomial equation $\psi \cdot q(x) - p(x)$ with coefficients in $\Bbbk(\psi)$. Therefore, $\mathbb{K} \supset \Bbbk(\psi)$ is a finite extension of degree $\deg \mathbb{K}/\Bbbk(\psi) \leqslant \max(\deg p, \deg q)$.

Since the left-hand side of this inequality is divisible by $\deg \mathbb{K}/\mathbb{K}^G = 6$, we conclude that $\max(\deg p, \deg q) \geqslant 6$, and equality holds if and only if $\mathbb{K}^G = \Bbbk(\psi)$. A particular G-invariant function ψ with $\deg p, \deg q \leqslant 6$ is easily obtained from projective geometry. Choose a G-orbit $\alpha_1, \alpha_2, \dots, \alpha_m$ in $\mathbb{P}_1(\overline{\Bbbk})$ and write

$$f(t_0, t_1) = \prod_i \det(t, \alpha_i) \in \Bbbk[t_0, t_1]$$

for the homogeneous polynomial with simple zeros at the points α_i. Then the substitutions (13.10) transform f into polynomials with the same zeros. Since all these polynomials are proportional, $f(g^{-1}t) = \lambda(g) \cdot f(t)$ for all $g \in G$, where $\lambda : G \to \Bbbk^*$, $g \mapsto \lambda(g)$, is a multiplicative homomorphism, i.e., a 1-dimensional character of G. The group S_3 has exactly two such characters, coming from the trivial and sign representations. Hence, f either is completely G-invariant or is invariant under rotations and alternates sign under reflections. The three-point orbit 0, 1, ∞ provides us with the sign-alternating polynomial $p = t_0t_1(t_0 - t_1)$, whose square p^2 is completely G-invariant. The two-point orbit formed by the eigenvectors of the rotations[23] produces the G-invariant polynomial $q = t_0^2 - t_0t_1 + t_1^2$. The minimal

[21] See Example 12.4 of Algebra I.

[22] Recall that every subfield $\mathbb{F} \subset \Bbbk(t)$ strictly larger than $\Bbbk$ is isomorphic to $\Bbbk(f)$ for some $f \in \Bbbk(t)$ by Lüroth's theorem; see Theorem 10.4 on p. 238.

[23] Note that even if these eigenvectors are not defined over $\Bbbk$, the G-invariant polynomial with roots at these points has to lie in $\Bbbk[t_0, t_1]$.

Laurent monomial in p^2, q, having total degree zero[24] in $(t_0 : t_1)$, is

$$\psi(t) = \frac{p^2}{q^3} = \frac{t_0^2 t_1^2 \,(t_0 - t_1)^2}{\left(t_0^2 - t_0 t_1 + t_1^2\right)^3} = \frac{t^2(t-1)^2}{(t^2 - t + 1)^3}\,.$$

Since both numerator and denominator have degree at most 6, the equality $\mathbb{K}^G = \Bbbk(\psi)$ holds.

Exercise 13.12 Verify by direct computation that $\psi(t)$ goes to itself under all six substitutions (13.10).

Example 13.6 (Automorphisms and Embeddings of Finite Fields) Let $q = p^n$ for a prime $p \in \mathbb{N}$. Since the extension $\mathbb{F}_p \subset \mathbb{F}_q$ is finite, normal, and separable, we have $\left|\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q\right| = \deg \mathbb{F}_q/\mathbb{F}_p = n$. Write $F_p^0 = \mathrm{Id}$, F_p, F_p^2, … , F_p^{n-1} for iterations of the *Frobenius automorphism* $F_p : \vartheta \mapsto \vartheta^p$. They all are distinct, because an equality $F_p^k = F_p^m$ would force all the p^n elements of $\mathbb{F}_q$ to be roots of the polynomial $x^{p^k} - x^{p^m}$, which is impossible for $k, m < n$. We conclude that $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q$ is the cyclic group of order n generated by F_p. For every $k \mid n$, the cyclic subgroup $G_k \subset \mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q$ generated by F_p^k has order n/k, and the G_k-invariants are exactly the roots of the polynomial $x^{p^k} - x$. Therefore, $\mathbb{F}_q^{G_k} = \mathbb{F}_{p^k} \subset \mathbb{F}_{p^n}$ is a splitting field of the polynomial $x^{p^k} - x$, and $G_k \simeq \mathrm{Aut}_{\mathbb{F}_{p^k}} \mathbb{F}_{p^n}$. Every embedding $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^n}$ maps $\mathbb{F}_{p^k}$ isomorphically onto the subfield $\mathbb{F}_q^{G_k}$, because every element of $\mathbb{F}_{p^k}$ has to go to a root of the polynomial $x^{p^k} - x$. Altogether, there are exactly k such embeddings, and they form one orbit of the group $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^k}$ acting on the embeddings by right multiplication.

Exercise 13.13 Check that the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ equals the product of all monic polynomials irreducible over $\mathbb{F}_p$ whose degrees divide n.

Theorem 13.7 (Galois Correspondence) *Let $\Bbbk \subset \mathbb{K}$ be a finite Galois extension with Galois group $G = \mathrm{Aut}_{\Bbbk} \mathbb{K}$. Then there is a canonical bijection between the subgroups $H \subset G$ and the subfields $\mathbb{L} \subset \mathbb{K}$ such that $\Bbbk \subset \mathbb{L}$. It takes a subgroup $H \subset G$ to the subfield of H-invariants $\mathbb{K}^H \subset \mathbb{K}$. The inverse map sends a field $\mathbb{L}$ such that $\Bbbk \subset \mathbb{L} \subset \mathbb{K}$ to the subgroup $\mathrm{Aut}_{\mathbb{L}} \mathbb{K} \subset G$. Under this correspondence, the normal subgroups $H \lhd G$ are in bijection with the Galois extensions $\mathbb{L} \supset \Bbbk$ contained in $\mathbb{K}$, and $\mathrm{Gal}\, \mathbb{L}/\Bbbk \simeq G/H$ for every such Galois extension $\mathbb{L} \supset \Bbbk$.*

Proof Given a tower of fields $\Bbbk \subset \mathbb{L} \subset \mathbb{K}$, the extension $\mathbb{L} \subset \mathbb{K}$ is normal by Lemma 13.4 and separable by Corollary 13.2. Thus, $\mathbb{L} \subset \mathbb{K}$ is a Galois extension with Galois group $H = \mathrm{Aut}_{\mathbb{L}} \mathbb{K}$, and $|H| = \deg \mathbb{K}/\mathbb{L}$. Certainly, the group H is a

[24] The rational functions of $t = t_0/t_1$ are exactly those polynomials.

subgroup of $G = \mathrm{Aut}_{\Bbbk} \mathbb{K}$, and by Corollary 13.3, $K^H = \mathbb{L}$. This proves[25] the first statement, concerning the one-to-one correspondence between subgroups $H \subset G$ and subfields $\mathbb{L} \subset \mathbb{K}$ such that $\Bbbk \subset \mathbb{L}$. To prove the second statement, consider the action of $G = \mathrm{Gal}\, \mathbb{K}/\Bbbk$ on the subfields $\mathbb{L} \subset \mathbb{K}$ such that $\Bbbk \subset \mathbb{L}$. We have proved already that the centralizer $C_{\mathbb{L}} \stackrel{\text{def}}{=} \{g \in G \mid g|_{\mathbb{L}} = \mathrm{Id}_{\mathbb{L}}\} = \mathrm{Aut}_{\mathbb{L}} \mathbb{K}$ of every such $\mathbb{L}$ is the subgroup $H \subset G$ corresponding to $\mathbb{L}$. Since the extension $\mathbb{K} \supset \Bbbk$ is normal and separable, every embedding

$$\varphi : \mathbb{L} \hookrightarrow \mathbb{K} \tag{13.11}$$

over $\Bbbk$ can be extended to an automorphism $g : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ over $\Bbbk$. Therefore, $\varphi(\mathbb{L}) = g(\mathbb{L})$ for some $g \in G$, and the centralizer of $\varphi(\mathbb{L})$ in G is conjugate to H:

$$\mathrm{Aut}_{\varphi(\mathbb{L})} \mathbb{K} = C_{\varphi(\mathbb{L})} = C_{g(\mathbb{L})} = gC_{\mathbb{L}}g^{-1} = gHg^{-1} .$$

It follows from Lemma 13.4 and Corollary 13.2 that an extension $\mathbb{L} \supset \Bbbk$ is always separable. It is normal if and only if $\varphi(\mathbb{L}) = \mathbb{L}$ for all embeddings (13.11), which means that all subgroups conjugate to H coincide with H, i.e., that $H \lhd G$ is normal. In this case, the Galois group $\mathrm{Gal}\, \mathbb{K}/\Bbbk$ maps $\mathbb{L}$ to itself. This leads to a surjective homomorphism of groups $\mathrm{Gal}\, \mathbb{K}/\Bbbk \twoheadrightarrow \mathrm{Gal}\, \mathbb{L}/\Bbbk$ with kernel $\mathrm{Gal}\, \mathbb{K}/\mathbb{L}$. Therefore, $\mathrm{Gal}\, \mathbb{L}/\Bbbk = \big(\mathrm{Gal}\, \mathbb{K}/\Bbbk\big)/\big(\mathrm{Gal}\, \mathbb{K}/\mathbb{L}\big)$. □

Exercise 13.14 Convince yourself that the Galois correspondence reverses inclusions,

$$H \subset K \subset \mathrm{Gal}\, \mathbb{K}/\Bbbk \iff \mathbb{K}^H \supset \mathbb{K}^K \supset \Bbbk ,$$

and takes the intersection of subgroups $H_1 \cap H_2$ to the compositum $\mathbb{L}_1\mathbb{L}_2$ of corresponding fields $\mathbb{L}_1 = \mathbb{K}^{H_1}$, $\mathbb{L}_2 = \mathbb{K}^{H_2}$, and the intersection of fields $\mathbb{L}_1 \cap \mathbb{L}_2$ to the smallest subgroup of G containing the corresponding subgroups $H_1 = \mathrm{Aut}_{\mathbb{L}_1} \mathbb{K}$, $H_2 = \mathrm{Aut}_{\mathbb{L}_2} \mathbb{K}$.

Problems for Independent Solution to Chapter 13

Problem 13.1 Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

Problem 13.2 Is it true that **(a)** $\cos 36^\circ \in \mathbb{Q}(\sin 36^\circ)$? **(b)** $\sin 36^\circ \in \mathbb{Q}(\cos 36^\circ)$?

[25] Instead of Corollary 13.3, we could have used Theorem 13.6, which says that the extension $\mathbb{K}^H \subset \mathbb{K}$ is a Galois extension with Galois group H for every subgroup $H \subset G$.

Problem 13.3 Does the field $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$ coincide with
(a) $\mathbb{Q}\left(\sqrt{-2}\right)$? **(b)** $\mathbb{Q}(\sqrt{-1} + \sqrt{2})$?

Problem 13.4 Ascertain whether any of the following extensions $\mathbb{K} \supset \mathbb{Q}$ are Galois, and for those that are, compute $\operatorname{Gal} \Bbbk/\mathbb{Q}$:

(a) $\mathbb{K} = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) \subset \mathbb{R}$, $\sqrt{2}, \sqrt{3} \in \mathbb{R}$,
(b) $\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{1} + \sqrt[3]{2}\right) \subset \mathbb{C}$, $\sqrt[3]{1} \in \mathbb{C} \smallsetminus \mathbb{R}$, $\sqrt[3]{2} \in \mathbb{R}$,
(c) $\mathbb{K} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ is the splitting field of $x^7 - 5$.

Problem 13.5 For every field $\mathbb{K}$ from the previous problem, enumerate all the subfields $\mathbb{L} \subset \mathbb{K}$, determine which of the $\mathbb{L}$ are isomorphic, indicate which $\mathbb{L}$ are Galois extensions of $\mathbb{Q}$, and compute their Galois groups over $\mathbb{Q}$.

Problem 13.6 Find the dimension over $\mathbb{Q}$ of the $\mathbb{Q}$-linear span of the positive real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$.

Problem 13.7 Find the degree over $\mathbb{Q}$ of the splitting fields of the polynomials $x^4 - 2$ and $x^p - a$, where $p \in \mathbb{N}$ is prime and $a \in \mathbb{Q}$ has $\sqrt[p]{a} \notin \mathbb{Q}$.

Problem 13.8 Let $\mathbb{F} \supset \Bbbk$ be a finite Galois extension, and $G = \operatorname{Gal} \mathbb{F}/\Bbbk$. Prove that there exists an element $\vartheta \in \mathbb{F}$ whose G-orbit is a basis of $\mathbb{F}$ as a vector space over $\Bbbk$.

Problem 13.9 For every nonconstant polynomial $f \in \mathbb{Z}[x]$, prove that there exist infinitely many primes $p \in \mathbb{N}$ such that the reduction of f modulo p has a root in $\mathbb{F}_p$.

Problem 13.10 Prove that an algebraic closure $\overline{\mathbb{F}}_p \supset \mathbb{F}_p$ is achieved by the adjunction to $\mathbb{F}_p$ of all primitive roots of unity of all prime degrees different from p.

Problem 13.11 Let $p \in \mathbb{N}$ be prime, $q = p^n$ for some $n \in \mathbb{N}$, and $a \in \mathbb{F}_p^*$. Prove that the polynomial $x^p - x - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if $p \nmid n$.

Problem 13.12 Find all $n \in \mathbb{N}$ such that the polynomial $x^{2n} + x^n + 1$ is irreducible in $\mathbb{F}_2[x]$.

Problem 13.13 For every positive integer $n \not\equiv 2 \pmod 3$, ascertain whether the polynomial **(a)** $x^n - x + 1$, **(b)** $x^n + x + 1$, is irreducible over $\mathbb{Q}$.

Problem 13.14 (Invariants of the Dihedral Group) The dihedral group[26] D_n acts on the complex projective line $\mathbb{P}_1(\mathbb{C})$ with affine coordinate t, and on the field of rational functions $\mathbb{C}(t)$ by the rule $\tau : t \mapsto e^{2\pi i/n}t$, $\sigma : t \mapsto 1/t$, where τ and σ are the rotation and reflection generating D_n. Describe the field of invariants $\mathbb{C}(t)^{D_n}$.

Problem 13.15 (Klein Forms) Let us identify the complex projective line $\mathbb{P}_1(\mathbb{C})$ with the unit sphere $S^2 = \left\{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\right\}$ in such a way

[26] Recall that we write D_n for the group of the regular n-gon, which has order $2n$; see Example 12.4 of Algebra I.

that the standard affine charts U_0, U_1 on $\mathbb{P}_1$ are provided by the projections of the sphere from its north and south poles $(0, 0, \pm 1)$ onto the equatorial plane[27] $z = 0$, which is identified with the complex plane $\mathbb{C} = \{x + iy\}$ in the usual way. Let M be a tetrahedron, cube, or dodecahedron inscribed in S^2, and let G denote the proper group[28] of M. Then G acts on $\mathbb{P}_1(\mathbb{C})$ by means of the rotations of the unit sphere provided by the rotations of M. Write $(t_0 : t_1)$ for the homogeneous coordinate on $\mathbb{P}_1(\mathbb{C})$ compatible with the standard charts just described. Then the linear fractional changes of coordinates provided by the projective transformations from G equip the polynomial ring $\mathbb{C}[t_0, t_1]$ and the field of rational functions $\mathbb{C}(t)$, $t = t_0/t_1$, with the action of G. Write $\varphi, \psi, \chi \in \mathbb{C}[t_0 : t_1]$ for the homogeneous polynomials with only simple roots, which are situated, respectively, at the vertices of M, at the projections to S^2 of the midpoints of edges of M, and at the projections to S^2 of the centers of faces of M. For every M, consider the following products constructed from φ, ψ, χ, where the lower indices of polynomials indicate their degrees in t_0, t_1:

$$\alpha_6 \overset{\text{def}}{=} \psi_6\,, \qquad \beta_8 \overset{\text{def}}{=} \varphi_4\chi_4\,, \qquad \gamma_{12} \overset{\text{def}}{=} \varphi_4^3\,, \qquad \text{for } M \text{ the tetrahedron}\,;$$

$$\alpha_8 \overset{\text{def}}{=} \varphi_8\,, \qquad \beta_{12} \overset{\text{def}}{=} \chi_6^2\,, \qquad \gamma_{18} \overset{\text{def}}{=} \chi_6\psi_{12}\,, \qquad \text{for } M \text{ the cube}\,;$$

$$\alpha_{12} \overset{\text{def}}{=} \chi_{12}\,, \qquad \beta_{20} \overset{\text{def}}{=} \varphi_{20}\,, \qquad \gamma_{30} \overset{\text{def}}{=} \psi_{30}\,, \qquad \text{for } M \text{ the dodecahedron}\,.$$

In each case, verify that the polynomials $\alpha, \beta, \gamma \in \mathbb{C}[t_0, t_1]$ are G-invariant, and describe the field of invariants $\mathbb{C}(x)^G$. Try to prove that the *ring* of invariants $\mathbb{C}[t_0, t_1]^G \subset \mathbb{C}[t_0, t_1]$ is isomorphic to $\mathbb{C}[\alpha, \beta, \gamma]/(f)$, where

$$f = \alpha_6^4 + \beta_8^3 + \gamma_{12}^2 \qquad \text{for the tetrahedron}\,;$$

$$f = \alpha_8^3\beta_{12} + \beta_{12}^3 + \gamma_{18}^2 \qquad \text{for the cube}\,;$$

$$f = \alpha_{12}^5 + \beta_{20}^3 + \gamma_{30}^2 \qquad \text{for the dodecahedron}\,.$$

Problem 13.16 Describe the field of invariants $\mathbb{C}(x_1, x_2, \dots, x_n)^G$ for

(a) $G = S_n$ acting by permutations of variables $(x_1, x_2, \dots, x_n)$,
(b) the cyclic subgroup $G \subset S_n$ generated by the long cycle $|1, 2, \dots, n\rangle$,
(c) the cyclic group G generated by the homothety $x_\nu \mapsto e^{2\pi i/n}x_\nu$, $1 \leqslant \nu \leqslant n$.

Problem 13.17 Let $G = \mathrm{PGL}_2(\mathbb{F}_q)$ and suppose the subgroups $P \subset G$, $N \subset P$ consist, respectively, of the transformations $t \mapsto at + b$, $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, and

---

[27]Note that this model of $\mathbb{P}_1(\mathbb{C})$ differs slightly from that used in Example 11.1 of Algebra I, where the sphere of diameter 1 was projected from the north and south poles onto the tangent planes drawn through the opposite poles.

[28]That is, bijections $M \xrightarrow{\sim} M$ induced by the orientation-preserving linear isometries $\mathbb{R}^3 \xrightarrow{\sim} \mathbb{R}^3$; see Sect. 12.3 of Algebra I.

$t \mapsto t + b$, $b \in \mathbb{F}_q$. Show that **(a)** $\mathbb{F}_q(t)^N = \mathbb{F}_q(t^q - t)$, **(b)** $\mathbb{F}_q(t)^P = \mathbb{F}_q\big((t^q - t)^{q-1}\big)$, **(c)** $\mathbb{F}_q(t)^G = \mathbb{F}_q\left(\frac{(t^{q^2}-t)^{q+1}}{(t^q-t)^{q^2+1}}\right)$.

Problem 13.18 Let $\operatorname{char} \Bbbk = p$, and let x, y be variables algebraically independent over $\Bbbk$. Compute $\deg \Bbbk(x, y)/\Bbbk(x^p, y^p)$ and show that there are infinitely many subfields $\mathbb{F} \subset \Bbbk(x, y)$ containing $\Bbbk$.

Problem 13.19 Let A be a Noetherian normal ring with field of fractions $K = Q_A$, and let $L \supset K$ be a finite separable field extension of K. Prove that the integral closure of A in L is a finitely generated A-module.

Problem 13.20 (Norm and Trace) Given a finite field extension $\mathbb{K} \supset \Bbbk$ and an element $\vartheta \in \mathbb{K}$, write $\chi_\vartheta(x) \in \Bbbk[x]$, $\operatorname{Sp}(\vartheta) \in \Bbbk$, and $N(\vartheta) \in \Bbbk$, respectively, for the characteristic polynomial, trace, and determinant of the $\Bbbk$-linear map

$$\vartheta : \mathbb{K} \to \mathbb{K}\,, \quad x \mapsto \vartheta x\,,$$

and call them the *characteristic polynomial*, *trace*, and *norm* of ϑ over $\Bbbk$. For a finite Galois extension $\Bbbk \subset \mathbb{K}$ with Galois group $G = \operatorname{Aut}_{\Bbbk} \mathbb{K}$, prove the following equalities: **(a)** $\chi_\vartheta(x) = \prod_{g\in G}(x - g\vartheta)$, **(b)** $\operatorname{Sp}(\vartheta) = \sum_{g\in G} g\vartheta$, **(c)** $N(\vartheta) = \prod_{g\in G} g\vartheta$.

Problem 13.21 Under the notation from the previous problem, show that:

(a) The *linear trace form* $\mathbb{K} \to \Bbbk$, $\vartheta \mapsto \operatorname{Sp}(\vartheta)$, vanishes identically in $\vartheta \in \mathbb{K}$ if and only if every element $\vartheta \in \mathbb{K} \smallsetminus \Bbbk$ is inseparable[29] over $\Bbbk$.

(b) The *bilinear trace form* $\mathbb{K} \times \mathbb{K} \to \Bbbk$, $(\vartheta_1, \vartheta_2) = \operatorname{Sp}(\vartheta_1\vartheta_2)$, is nondegenerate if and only if the extension $\mathbb{K} \supset \Bbbk$ is separable.

[29] In this case, the extension $\mathbb{K} \supset \Bbbk$ is called *purely inseparable*.

Chapter 14
Examples of Galois Groups

14.1 Straightedge and Compass Constructions

Let us identify the Euclidean coordinate plane $\mathbb{R}^2$ with the field $\mathbb{C}$ in the standard way.[1]

Exercise 14.1 Given the points $0,\ 1,\ a,\ b \in \mathbb{C}$, construct the points $a \pm b$, a/b, ab, and $\sqrt{a}$ using straightedge and compass.

It follows from Exercise 14.1 that for every tower of quadratic extensions

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L}\,, \tag{14.1}$$

where $\mathbb{L} \subset \mathbb{C}$ and $\mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big]$ for some $a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2$, every point $\zeta \in \mathbb{L}$ can be constructed by straightedge and compass if the points $0, 1 \in \mathbb{C}$ are given. The converse is also true. More precisely, given the points $0, 1 \in \mathbb{C}$, a point $\zeta \in \mathbb{C}$ can be constructed by straightedge and compass only if ζ lies in some subfield $\mathbb{L} \subset \mathbb{C}$ arrived at by a tower of quadratic extensions (14.1) such that every intermediate field $\mathbb{L}_i$ of the tower goes to itself under complex conjugation $z \mapsto \bar{z}$. This is verified by induction as follows.

For two distinct points $a, b \in \mathbb{C}$, write $\ell_{a,b}$ for the line joining them and $C_{a,b}$ for the circle centered at a with radius $|b - a|$. The construction of ζ by straightedge and compass splits into several steps, each of which produces a new point, namely $p = \ell_{a,b} \cap \ell_{c,d}$, $p = \ell_{a,b} \cap C_{c,d}$, or $p = C_{a,b} \cap C_{c,d}$, from some already constructed points a, b, c, d. We put $\mathbb{L}_1 = \mathbb{Q}\big[\sqrt{-1}\big]$ and assume inductively that a, b, c, d belong to a field $\mathbb{L} \subset \mathbb{C}$ achieved by a tower (14.1) and mapped to itself by complex conjugation. Then $p = \ell_{a,b} \cap \ell_{c,d}$ is a rational function of a, b, c, d, and therefore lies in $\mathbb{L}$. The intersections $\ell_{a,b} \cap C_{c,d}$ and $C_{a,b} \cap C_{c,d}$ can be found by solving the

[1] See Section 3.5.1 of Algebra I.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5_14

quadratic equation $f(t) = 0$ obtained by substituting[2] $z = a + (b - a) \cdot t$ in the equation for $C_{c,d}$,

$$(z - c)(\overline{z} - \overline{c}) = (d - c)\left(\overline{d} - \overline{c}\right) ,$$

and moving all terms to the left-hand side. In the case of the intersection $\ell_{a,b} \cap C_{c,d}$, the quadratic trinomial f has two real roots, whereas for the intersection $C_{a,b} \cap C_{c,d}$, it has two roots lying on the unit circle $\mathrm{U}_1 \subset \mathbb{C}$. Substitution of these roots into the parametric equation $z = a + (b - a) \cdot t$ gives the required intersection points and shows that p belongs to the splitting field of f. Since complex conjugation maps $\mathbb{L}$ to itself, the coefficients of f are real and belong to $\mathbb{L}$. Therefore, the roots of f lie either in $\mathbb{L}$ or in the quadratic extension $\mathbb{L}' \supset \mathbb{L}$ whose basis over $\mathbb{L}$ is formed by the roots of f. Since the roots are either both real or complex conjugate to each other, the field $\mathbb{L}'$ is mapped to itself under complex conjugation. This completes the inductive step.

The Galois correspondence from Theorem 13.7 on p. 310 gives an easy and effective characterization of the fields $\mathbb{L} \subset \mathbb{C}$ appearing as the top levels of the towers (14.1), as well as of those elements $\vartheta \in \mathbb{C}$ that can be constructed with straightedge and compass.

Proposition 14.1 *A finite Galois extension $\mathbb{K} \supset \Bbbk$ is contained in a field $\mathbb{L} \supset \Bbbk$ obtained by a tower of quadratic extensions*

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L} , \qquad (14.2)$$

with $\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{a_i}]$, $a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2$, if and only if $\deg \mathbb{K}/\Bbbk = 2^n$ *for some* $n \in \mathbb{N}$.

Proof If $\mathbb{K} \subset \mathbb{L}$ for $\mathbb{L}$ from (14.2), then $\deg \mathbb{K}/\Bbbk$ divides $\deg \mathbb{L}/\Bbbk = 2^m$, and therefore, $\deg \mathbb{K}/\Bbbk = 2^n$ for some $n \leqslant m$. Conversely, let $\deg \mathbb{K}/\Bbbk = |\mathrm{Gal}\, \mathbb{K}/\Bbbk| = 2^n$. Hence, $G = \mathrm{Gal}\, \mathbb{K}/\Bbbk$ is a finite 2-group. Every composition factor[3] of a 2-group has to be a 2-group. By Proposition 13.6 from Algebra I, the only simple 2-group is $\mathbb{Z}/(2)$. Therefore, the Jordan–Hölder series of G looks like

$$G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{e\} , \qquad (14.3)$$

where $G_{i+1} \lhd G_i$ and $G_i/G_{i+1} \simeq \mathbb{Z}/(2)$ for all i. Under the Galois correspondence,[4] this series of subgroups produces a tower of quadratic extensions leading directly to the field $\mathbb{K}$:

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{n-1} \subset \mathbb{L}_n = \mathbb{K} ,$$

where $\mathbb{L}_i = \mathbb{K}^{G_i}$. □

[2] The parametric equation $z = a + (b - a) \cdot t$ defines the line $\ell_{a,b}$ as t runs through $\mathbb{R}$, and defines the circle $C_{a,b}$ as t runs through the unit circle $\mathrm{U}_1 \subset \mathbb{C}$.

[3] See Section 13.3 of Algebra I.

[4] See Theorem 13.7 on p. 310.

Exercise 14.2 Give a straightforward construction of the subgroups (14.3) without reference to the Jordan–Hölder theorem.

Theorem 14.1 *A complex root of an irreducible polynomial* $f(x) \in \mathbb{Q}[x]$ *can be constructed by straightedge and compass starting from the points* $0,\ 1 \in \mathbb{C}$ *if and only if the degree of the splitting field of* f *over* $\mathbb{Q}$ *is a power of two. In this case, every root of* f *can be constructed by straightedge and compass.*

Proof Write $\mathbb{K} \subset \mathbb{C}$ for the splitting field of f. Then $\mathbb{K} \supset \mathbb{Q}$ is a finite Galois extension by Proposition 13.3. For $\deg \mathbb{K}/\mathbb{Q} = 2^m$, we have seen in the proof of Proposition 14.1 that $\mathbb{K}$ can be achieved by quadratic extensions (14.1), and therefore, every element of $\mathbb{K}$ can be constructed by straightedge and compass. Conversely, let a root ϑ of f be constructible by straightedge and compass. Then the simple extension $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ is contained in some field $\mathbb{L} \subset \mathbb{C}$ from (14.1). Let $\vartheta' \in \mathbb{K}$ be another root of f, and $\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ an automorphism sending ϑ to ϑ'. Then φ maps the subfield $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ to the subfield $\mathbb{Q}[\vartheta'] \subset \mathbb{C}$. The embedding

$$\varphi|_{\mathbb{Q}[\vartheta]} : \mathbb{Q}[\vartheta] \hookrightarrow \mathbb{C}\,, \quad \vartheta \mapsto \vartheta',$$

can be extended to an embedding $\overline{\varphi} : \mathbb{L} \hookrightarrow \mathbb{C}$ that coincides with φ on the subfield $\mathbb{Q}[\vartheta] \subset \mathbb{L}$ and maps the tower (14.1) to the tower

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1' \subset \mathbb{L}_2' \subset \cdots \subset \mathbb{L}_{m-1}' \subset \mathbb{L}_m' = \mathbb{L}'\,, \tag{14.4}$$

where $\mathbb{L}_{i+1}' = \mathbb{L}_i'\big[\sqrt{a_i'}\big]$ with $a_i' = \overline{\varphi}(a_i) \in \mathbb{L}_i' \smallsetminus \big(\mathbb{L}_i'\big)^2$. Since $\vartheta' \in \mathbb{L}'$, the root ϑ' is also constructible by straightedge and compass. The compositum $\mathbb{L}\mathbb{L}'$ contains the roots ϑ, ϑ' and can be achieved by a tower of quadratic extensions, because it is obtained from $\mathbb{L}$ by the successive adjunction of elements $a_1', a_2', \dots, a_m'$ whose degrees over the corresponding subfields $\mathbb{L},\ \mathbb{L}\mathbb{L}_1',\ \dots,\ \mathbb{L}\mathbb{L}_{m-1}'$ are at most two. Proceeding by induction, we construct a tower of quadratic extensions containing all the roots of f, and therefore $\mathbb{K}$. By Proposition 14.1, $\deg \mathbb{K}/\mathbb{Q}$ is a power of two. □

Corollary 14.1 *A number* $\zeta \in \mathbb{C}$ *can be constructed by straightedge and compass starting from the points* $0,\ 1 \in \mathbb{C}$ *only if* ζ *is algebraic over* $\mathbb{Q}$ *and* $\deg_{\mathbb{Q}} \zeta = 2^n$ *for some* $n \in \mathbb{N}$.

Proof Since the simple extension $\mathbb{Q}[\zeta]$ is contained in the splitting field of the minimal polynomial for ζ, the degree of ζ over $\mathbb{Q}$ divides the degree of that splitting field. □

Example 14.1 (Trisection of an Angle) The angle $\pi/3$ cannot be subdivided into three equal angles $\pi/9$ by straightedge and compass. Indeed, such a possibility would allow the construction of the number $\zeta = \cos(\pi/9)$, which is a root of the polynomial[5] $4x^3 - 3x - 1/2$. Since this polynomial has no rational roots, it is irreducible over $\mathbb{Q}$, and therefore proportional to the minimal polynomial of ζ. Thus, $\deg_{\mathbb{Q}} \zeta = 3$, in contradiction to Corollary 14.1.

Example 14.2 (Doubling of the Cube) The edge of a cube whose volume is twice the volume of a given cube cannot be constructed by straightedge and compass, because such a construction would allow the construction of a root of the polynomial $x^3 - 2$, which is irreducible over $\mathbb{Q}$.

Example 14.3 (Regular 7-gon) The regular 7-gone also cannot be constructed by straightedge and compass, because otherwise, one could construct the seventh root of unity $\zeta = e^{2\pi i/7}$, whose minimal polynomial[6] $\Phi_7(x) = (x^7 - 1)/(x - 1)$ has degree 6.

14.1.1 Effect of Accessory Irrationalities

The problem of straightedge and compass construction can be modified by assuming that some other points $\zeta_1, \zeta_2, \dots, \zeta_n \in \mathbb{C}$ are initially given besides the points 0, 1. In this case, every point of the field $\mathbb{F} = \mathbb{Q}(\zeta_1, \zeta_2, \dots, \zeta_n) \subset \mathbb{C}$ is constructible, and we can assume that the given points form a subfield $\mathbb{F} \subset \mathbb{C}$, not necessarily algebraic over $\mathbb{Q}$. The elements of $\mathbb{F}$ are called *accessory irrationalities*. Everything said above remains valid after replacement of $\mathbb{Q}$ by an arbitrary accessory subfield $\mathbb{F} \subset \mathbb{C}$. Namely, given all the elements of $\mathbb{F}$, a number $\zeta \in \mathbb{C}$ is constructible by straightedge and compass if and only if ζ is absorbed by a finite tower of quadratic extensions of the field $\mathbb{F}$. The latter is equivalent to the fact that ζ is algebraic over $\mathbb{F}$ and the splitting field of the minimal polynomial of ζ over $\mathbb{F}$ has degree 2^m for some $m \in \mathbb{N}$. This may happen only if $\deg_{\mathbb{F}} \zeta$ is a power of two.

Exercise 14.3 Prove all these statements.

In the most general setup, the effect of accessory irrationalities on Galois extensions is described by the next claim.

Proposition 14.2 (Accessory Irrationalities Theorem) *Let $\mathbb{F}, \mathbb{K} \supset \Bbbk$ be fields contained in a common algebraically closed field $\mathbb{L}$. If the extension $\mathbb{K} \supset \Bbbk$ is a finite Galois extension, then the extension $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ is a finite Galois extension as well, and the Galois group* $\operatorname{Gal} \mathbb{F}\mathbb{K}/\mathbb{F}$ *is isomorphic to the subgroup* $H_{\mathbb{F}\cap\mathbb{K}} \subset \operatorname{Gal} \mathbb{K}/\Bbbk$ *associated with the intermediate subfield $\Bbbk \subset \mathbb{F}\cap\mathbb{K} \subset \mathbb{K}$ under the Galois correspondence for the extension $\Bbbk \subset \mathbb{K}$.*

Proof By Proposition 13.3, $\mathbb{K} \subset \mathbb{L}$ is the splitting field of some separable polynomial $f \in \Bbbk[x]$. As a $\Bbbk$-algebra, $\mathbb{K}$ is generated by the roots $\vartheta_1, \vartheta_2, \dots, \vartheta_n \in \mathbb{L}$

[5] Obtained from the relation $\cos(3\varphi) = 4\cos\varphi - 3\cos^2\varphi$ for $\varphi = \pi/9$.

[6] Recall that the cyclotomic polynomial $\Phi_p(x)$ is irreducible for prime $p \in \mathbb{N}$ by Eisenstein's criterion; see Example 5.9 of Algebra I.

of f. The same roots generate the compositum $\mathbb{F}\mathbb{K}$ as an algebra over $\mathbb{F}$. By Proposition 13.4, the extension $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ is normal and separable, i.e., a finite Galois extension. This forces $\mathbb{F}\mathbb{K}$ to be the splitting field for f over $\mathbb{F}$. Automorphisms of $\mathbb{K}$ over $\Bbbk$ and automorphisms of $\mathbb{F}\mathbb{K}$ over $\mathbb{F}$ preserve the polynomial f and map the set of roots $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ to itself. Since this set generates both $\mathbb{K}$ over $\Bbbk$ and $\mathbb{F}\mathbb{K}$ over $\mathbb{F}$, every automorphism is uniquely determined by its action on the roots of f. Thus, the Galois groups $\operatorname{Gal}\mathbb{K}/\Bbbk$, $\operatorname{Gal}\mathbb{F}\mathbb{K}/\mathbb{F}$ are naturally embedded in the permutation group $\operatorname{Aut}\{\vartheta_1, \vartheta_2, \dots, \vartheta_n\} \simeq S_n$. The group $\operatorname{Gal}\mathbb{K}/\Bbbk$ consists of the permutations of $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ that can be extended to $\Bbbk$-algebra endomorphisms of $\mathbb{K} = \Bbbk[\vartheta_1, \vartheta_2, \dots, \vartheta_n]$. The group $\operatorname{Gal}\mathbb{F}\mathbb{K}/\mathbb{F}$ consists of the permutations that can be extended to $\mathbb{F}$-algebra endomorphisms. Since $\Bbbk \subset \mathbb{F}$, every $\mathbb{F}$-linear endomorphism is automatically $\Bbbk$-linear. Therefore, the second group is a subgroup of the first. It is formed by all transformations $g : \Bbbk[\vartheta_1, \vartheta_2, \dots, \vartheta_n] \to \Bbbk[\vartheta_1, \vartheta_2, \dots, \vartheta_n]$ from $\operatorname{Gal}\mathbb{K}/\Bbbk$ that are $\mathbb{F}$-linear. The latter means that g acts identically on $\mathbb{F} \cap \mathbb{K}$. $\square$

14.2 Galois Groups of Polynomials

Given a separable polynomial $f \in \Bbbk[x]$, its splitting field $\mathbb{L}_f$ is a finite Galois extension of $\Bbbk$ by Proposition 13.3. The Galois group $\operatorname{Gal}\mathbb{L}_f/\Bbbk$ is called the *Galois group of f over* $\Bbbk$ and denoted by $\operatorname{Gal} f/\Bbbk$. Since all the coefficients of f are Galois invariant, every automorphism $\psi \in \operatorname{Gal} f/\Bbbk$ acts on the roots $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ of f as a permutation, and this permutation uniquely determines ψ, because $\mathbb{L}_f$ is generated by $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ as a $\Bbbk$-algebra. Therefore, the Galois group $\operatorname{Gal} f/\Bbbk$ can be canonically embedded into the group $\operatorname{Aut}\{\vartheta_1, \vartheta_2, \dots, \vartheta_n\}$. A permutation of the roots belongs to $\operatorname{Gal} f/\Bbbk$ if and only if it respects all the algebraic relations among the roots. This can be formalized as follows.

Let $\overline{\Bbbk} \supset \Bbbk$ be an algebraic closure of $\Bbbk$. Then the splitting field $\mathbb{L}_f \subset \overline{\Bbbk}$ coincides with the image of the evaluation homomorphism

$$\operatorname{ev}_{\vartheta_1,\vartheta_2,\dots,\vartheta_n} : \Bbbk[t_1, t_2, \dots, t_n] \to \overline{\Bbbk}, \quad \psi \mapsto \psi(\vartheta_1, \vartheta_2, \dots, \vartheta_n)\,. \tag{14.5}$$

Its kernel $I_\Bbbk(\vartheta) \stackrel{\text{def}}{=} \ker \operatorname{ev}_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$ consists of all polynomial relations among the roots of f, i.e., of those $\psi \in \Bbbk[t_1, t_2, \dots, t_n]$ that vanish at the point $\vartheta = (\vartheta_1, \vartheta_2, \dots, \vartheta_n) \in \mathbb{A}^n(\overline{\Bbbk})$. A permutation of variables $g : t_i \mapsto t_{g(i)}$ can be factorized through the endomorphism of the quotient algebra $\mathbb{L}_f = \Bbbk[t_1, t_2, \dots, t_n]/I_\Bbbk(\vartheta)$ if and only if g maps the relation ideal $I_\Bbbk(\vartheta)$ to itself. Thus,

$$\operatorname{Gal} f/\Bbbk \simeq \{g \in S_n \mid \forall \psi \in I_\Bbbk(\vartheta)\ \ \psi^g \in I_\Bbbk(\vartheta)\}\ , \tag{14.6}$$

where $\psi^g(t_1, t_2, \dots, t_n) \stackrel{\text{def}}{=} \psi\left(t_{g(1)}, t_{g(2)}, \dots, t_{g(n)}\right)$. Formula (14.6) was originally introduced by Évariste Galois as the definition of the group of a polynomial.

Caution 14.1 The inclusion of the Galois group $\mathrm{Gal}\, f/\Bbbk$ into the standard symmetric group $S_n = \mathrm{Aut}\{1, 2, \dots, n\}$ provided by the formula (14.6) is *not* canonical and depends on the choice of bijection between the roots $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ and the independent variables $x_1, x_2, \dots, x_n$ in the evaluation map (14.5).

Proposition 14.3 *The affine algebraic variety $V(I_\Bbbk(\vartheta)) \subset \mathbb{A}^n\left(\overline{\Bbbk}\right)$ consists of*

$$m = \deg \mathbb{L}_f/\Bbbk = |\,\mathrm{Gal}\, f/\Bbbk|$$

distinct points $\left(\vartheta_{g(1)}, \vartheta_{g(2)}, \dots, \vartheta_{g(n)}\right)$, in bijection with the elements $g \in \mathrm{Gal}\, f/\Bbbk$ and forming one orbit of the action of $\mathrm{Gal}\, f/\Bbbk \subset S_n$ on $\mathbb{A}^n$ by permutations of coordinates.

Proof Let $f = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. Write $e_i(t_1, t_2, \dots, t_n)$ for the elementary symmetric polynomials. Note that $e_i(t_1, t_2, \dots, t_n) - (-1)^i a_i \in I_\Bbbk(\vartheta)$, because

$$e_i(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = (-1)^i a_i$$

by the Viète formulas. For every point $a = (\alpha_1, \alpha_2, \dots, \alpha_n) \in V(I_\Bbbk(\vartheta))$, the equalities

$$e_i(\alpha_1, \alpha_2, \dots, \alpha_n) = (-1)^i a_i$$

force $(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = f(x) = (x - \vartheta_1)(x - \vartheta_2) \cdots (x - \vartheta_n)$. Hence,

$$(\alpha_1, \alpha_2, \dots, \alpha_n) = \left(\vartheta_{g(1)}, \vartheta_{g(2)}, \dots, \vartheta_{g(n)}\right)$$

for some $g \in S_n$. If $g \notin \mathrm{Gal}\, f/\Bbbk$, then there exists some $\psi \in I_\Bbbk(\vartheta)$ such that $\psi^g \notin I_\Bbbk(\vartheta)$, and $\psi(\alpha_1, \dots, \alpha_n) = \psi\left(\vartheta_{g(1)}, \dots, \vartheta_{g(n)}\right) = \psi^g(\vartheta_1, \dots, \vartheta_n) \neq 0$, in contradiction to the assumption that $a \in V(I_\Bbbk(\vartheta))$. Therefore, $V(I_\Bbbk(\vartheta))$ is contained in the Galois orbit of ϑ. Conversely,

$$\psi\left(\vartheta_{g(1)}, \vartheta_{g(2)}, \dots, \vartheta_{g(n)}\right) = \psi^g(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = 0$$

for all $g \in \mathrm{Gal}\, f/\Bbbk$, $\psi \in I_\Bbbk(\vartheta)$, because $\psi^g \in I_\Bbbk(\vartheta)$ in this case. Thus, the Galois orbit of ϑ is contained in $V(I_\Bbbk(\vartheta))$. ◻

Exercise 14.4 Show that a separable polynomial $f \in \Bbbk[x]$ is irreducible if and only if the Galois group $\mathrm{Gal}\, f/\Bbbk$ acts transitively on the roots of f.

14.2.1 Galois Resolution

Let $\mathbb{L}_f \supset \Bbbk$ be a splitting field of a separable polynomial

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \Bbbk[x]\,.$$

Write $\vartheta_1, \vartheta_2, \ldots, \vartheta_n \in \mathbb{L}_f$ for the roots of f and consider the linear homogeneous form

$$\psi = \vartheta_1 t_1 + \vartheta_2 t_2 + \cdots + \vartheta_n t_n \in \mathbb{L}_f[t_1, t_2, \ldots, t_n]\,. \tag{14.7}$$

The polynomial

$$F(t_1, \ldots, t_n) = \prod_{\sigma \in S_n} \psi^\sigma(t_1, \ldots, t_n) = \prod_{\sigma \in S_n} \left(\vartheta_1 t_{\sigma(1)} + \cdots + \vartheta_n t_{\sigma(n)}\right)\,, \tag{14.8}$$

of degree $n!$, is called the *Galois resolution* of f. Combining the factors obtained by means of the permutations σ lying in the same coset hG of the Galois group $G = \mathrm{Gal}\, f/\Bbbk \subset S_n$ allows us to rewrite (14.8) as

$$F(t_1, \ldots, t_n) = \prod_{h \in S_n/G} F_h(t_1, \ldots, t_n)\,, \tag{14.9}$$

where

$$\begin{aligned} F_h(t_1, \ldots, t_n) &= \prod_{g \in G} \left(\vartheta_1 t_{hg(1)} + \cdots + \vartheta_n t_{hg(n)}\right) \\ &= \prod_{g \in G} \left(\vartheta_{g^{-1}(1)} t_{h(1)} + \cdots + \vartheta_{g^{-1}(n)} t_{h(n)}\right) = \prod_{g \in G} g\left(\psi^h\right)\,. \end{aligned} \tag{14.10}$$

Here the linear form $\psi^h \in \mathbb{L}_f[t_1, t_2, \ldots, t_n]$ is obtained from ψ by the permutation h of variables $t_1, \ldots, t_n$, and $g\left(\psi^h\right)$ is obtained from ψ^h by applying the automorphism $g : \mathbb{L}_f \xrightarrow{\sim} \mathbb{L}_f$ to the coefficients of ψ^h. Since all the linear forms $g\left(\psi^h\right)$ in the product (14.10) are distinct and form one orbit of the Galois group, every polynomial F_h has coefficients in $\Bbbk$ and is irreducible over $\Bbbk$. Therefore, $F \in \Bbbk[t_1, t_2, \ldots, t_n]$, and formula (14.9) gives the irreducible factorization of F in $\Bbbk[t_1, t_2, \ldots, t_n]$. Since the irreducible factors of F form one orbit of the S_n-action on $\Bbbk[t_1, t_2, \ldots, t_n]$ by permutations of variables, the Galois group $G = \mathrm{Gal}\, f \subset S_n$ coincides with the stabilizer of the factor F_e and is conjugate to the stabilizer of every other irreducible factor F_h.

Proposition 14.4 *The Galois group* $\mathrm{Gal}\, f/\Bbbk$ *of a separable polynomial* $f \in \Bbbk[x]$ *is isomorphic to the group of all permutations of* $t_1, t_2, \ldots, t_n$ *preserving some factor* F_h *in the irreducible factorization of the Galois resolution of* f *in* $\Bbbk[t_1, t_2, \ldots, t_n]$.

□

14.2.2 Reduction of Coefficients

Let $\Bbbk = \mathbb{Q}$ and let

$$f = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$$

be a monic polynomial with integer coefficients. We fix a prime $p \in \mathbb{N}$ and write

$$\overline{f} = x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_{n-1}x + \overline{a}_n \in \mathbb{F}_p[x]$$

for the polynomial with the reduced, modulo p, coefficients $\overline{a}_i = a_i \pmod p \in \mathbb{F}_p$.

Theorem 14.2 *If the polynomial $\overline{f} \in \mathbb{F}_p[x]$ is separable, then there exists an injective group homomorphism*

$$\mathrm{Gal}\,\overline{f}/\mathbb{F}_p \hookrightarrow \mathrm{Gal}\,f/\mathbb{Q}\,.$$

Proof Since the roots $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ of f are integral over $\mathbb{Z}$, all the coefficients of every polynomial F_h in the irreducible decomposition (14.9) belong to the ring of integers $O \subset \mathbb{L}_f$. This forces the coefficients of each polynomial $F_h \in \mathbb{Q}[t_1, t_2, \ldots, t_n]$ to be integers. Thus, the irreducible factorization (14.9) occurs in $\mathbb{Z}[t_1, t_2, \ldots, t_n]$. Reducing all the coefficients modulo p leads to the factorization

$$\overline{F}(t_1, t_2, \ldots, t_n) = \prod_{h \in S_n/G} \overline{F}_h(t_1, t_2, \ldots, t_n)\,. \tag{14.11}$$

in $\mathbb{F}_p[t_1, t_2, \ldots, t_n]$.

Exercise 14.5 Verify that the quotient ring $A \overset{\text{def}}{=} O/(p)$ is an $\mathbb{F}_p$-algebra.

Write $\overline{\vartheta}_i = \vartheta_i \pmod p$ for the class of the root ϑ_i in the $\mathbb{F}_p$-algebra $A = O/(p)$. Since $\overline{f}$ is separable over $\mathbb{F}_p$, it splits in $A[t]$ into a product $\overline{f}(x) = \prod\bigl(x - \overline{\vartheta}_i\bigr)$ of $\deg f$ distinct linear factors.

Exercise 14.6 Check that the $\mathbb{F}_p$-subalgebra of A generated by the roots of $\overline{f}$ is a splitting field of $\overline{f}$ over $\mathbb{F}_p$.

This forces the polynomial $\overline{F} \in \mathbb{F}_p[t_1, t_2, \ldots, t_n]$ to be the Galois resolution (14.8) for the polynomial $\overline{f} \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. By Proposition 14.4, the Galois group $\mathrm{Gal}\,\overline{f}/\mathbb{F}_p$ can be identified with the group of permutations of the variables t_i that preserve some factor P from the irreducible factorization of $\overline{F}$ in $\mathbb{F}_p[t_1, t_2, \ldots, t_n]$. The polynomial P divides the modulo p reduction $\overline{F}_h$ of some factor F_h from the irreducible decomposition of F in $\mathbb{Z}[t_1, t_2, \ldots, t_n]$. Let us identify the Galois group $\mathrm{Gal}\,f/\mathbb{Q}$ with the group of permutations of the t_i that preserve F_h. Since every permutation $\sigma \in S_n \smallsetminus \mathrm{Gal}\,f/\mathbb{Q}$ transforms F_h to another factor $F_{h'} \neq F_h$, it cannot, in particular, transform the irreducible factor P of $\overline{F}_h$ in $\mathbb{F}_p[t_1, t_2, \ldots, t_n]$ to itself. Therefore, $\mathrm{Gal}\,f/\mathbb{Q} \supset \mathrm{Gal}\,\overline{f}/\mathbb{F}_p$. □

Corollary 14.2 *Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial, and $\overline{f} \in \mathbb{F}_p[x]$ its reduction modulo p. If*

$$\overline{f} = q_1 q_2 \cdots q_m$$

for irreducible polynomials $q_1, q_2, \dots, q_m \in \mathbb{F}_p[x]$ of degrees $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_m$, then the Galois group $\mathrm{Gal}\, f/\mathbb{Q}$*, considered as a subgroup of the permutation group of the roots of f, contains a permutation of cyclic type $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$.*

Proof The splitting field of $\overline{f}$ over $\mathbb{F}_p$ is a finite field with a cyclic[7] Galois group G over $\mathbb{F}_p$. Since G acts transitively on the roots of each irreducible polynomial q_i, the generator of G acts on the roots of $\overline{f}$ by a permutation of cyclic type λ. By Theorem 14.2, this permutation belongs to $\mathrm{Gal}\, f/\mathbb{Q}$ as well. ◻

Example 14.4 (Quintic Polynomial with Galois Group S_5) Let us compute the Galois group of the polynomial $f(x) = x^5 - x - 1$ over $\mathbb{Q}$. Consider the irreducible factorizations of $\overline{f}$ in $\mathbb{F}_2[x]$ and in $\mathbb{F}_3[x]$. Every nontrivial factorization of f contains a factor of degree at most 2. By Exercise 13.13, the product of all monic irreducible polynomials of degree at most 2 in $\mathbb{F}_p[x]$ equals $x^{p^2} - x$. The Euclidean algorithm shows that $\mathrm{GCD}\left(x^5 - x - 1\,,\, x^4 - x\right) = x^2 + x + 1$ over $\mathbb{F}_2$ and $\mathrm{GCD}\left(x^5 - x - 1\,,\, x^9 - x\right) = 1$ over $\mathbb{F}_3$. Thus, $\overline{f}$ is irreducible in $\mathbb{F}_3[x]$, whereas $\overline{f} = (x^2 + x + 1) \cdot \left(x^3 + x^2 + 1\right)$ in $\mathbb{F}_2[x]$. By Corollary 14.2, the Galois group $\mathrm{Gal}\, f/\mathbb{Q}$ contains a cycle of length 5 and a permutation of cyclic type $(3, 2)$, the cube of which is a transposition. Since a cycle of length 5 and a transposition generate the whole symmetric group S_5, we conclude that $\mathrm{Gal}\, f/\mathbb{Q} \simeq S_5$. It will follow from Theorem 14.5 on p. 330 that the roots of $x^5 - x - 1$ cannot be expressed through the rational numbers by means of the four arithmetic operations and radicals of positive integer degree.

14.3 Galois Groups of Cyclotomic Fields

The field $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$, which is generated as a $\mathbb{Q}$-algebra by the primitive nth root of unity

$$\zeta_n \stackrel{\text{def}}{=} e^{2\pi i/n} \in \mathbb{C}\,, \tag{14.12}$$

is called the *nth cyclotomic field*. This is the smallest subfield in $\mathbb{C}$ containing the multiplicative group of all nth roots of unity $\boldsymbol{\mu}_n \subset \mathbb{C}$. Equivalently, it can be described as the splitting field of the separable polynomial $x^n - 1 \in \mathbb{Q}[x]$ within $\mathbb{C}$. Hence, the nth cyclotomic field is the Galois extension of $\mathbb{Q}$. Every automorphism

[7] See Example 13.6 on p. 310.

$\sigma \in \operatorname{Gal} \mathbb{Q}[\zeta_n]/\mathbb{Q}$ maps the generator ζ_n of $\boldsymbol{\mu}_n$ to some other generator of $\boldsymbol{\mu}_n$, that is, acts by the rule $\sigma : \zeta_n \mapsto \zeta_n^{m(\sigma)}$ for some invertible element $m(\sigma) \in (\mathbb{Z}/(n))^*$ of the residue class ring $\mathbb{Z}/(n)$. This leads to the homomorphic embedding of the Galois group of the nth cyclotomic field into the multiplicative group of invertible residue classes in $\mathbb{Z}/(n)$,

$$\operatorname{Gal} \mathbb{Q}[\zeta_n]/\mathbb{Q} \hookrightarrow \left(\mathbb{Z}/(n)\right)^*, \quad \sigma \mapsto m(\sigma). \tag{14.13}$$

Write $R_n \stackrel{\text{def}}{=} \{\zeta_n^m \mid \operatorname{GCD}(n,m) = 1\} \subset \boldsymbol{\mu}_n$ for the set of all primitive nth roots of unity. Since the Galois group $\operatorname{Gal} \mathbb{Q}[\zeta_n]/\mathbb{Q}$ maps R_n to itself, the coefficients of the *nth cyclotomic polynomial*

$$\Phi_n(x) \stackrel{\text{def}}{=} \prod_{\xi \in R_n} (x - \xi)$$

are Galois invariant, that is, rational and therefore integers, because all the complex roots of unity are integral over $\mathbb{Z}$. Thus, $\Phi_n \in \mathbb{Z}[x]$. For example,

$$\begin{aligned}
\Phi_2(x) &= x + 1\,, \\
\Phi_3(x) &= (x - \omega)\left(x - \omega^2\right) = x^2 + x + 1\,, \\
\Phi_4(x) &= (x - i)\,(x + i) = x^2 + 1\,, \\
\Phi_5(x) &= \left(x^5 - 1\right)/(x - 1) = x^4 + x^3 + x^2 + x + 1\,, \\
\Phi_6(x) &= (z - \zeta_6)\left(x - \zeta_6^{-1}\right) = x^2 - x + 1\,, \\
&\dots
\end{aligned}$$

In particular, the nth cyclotomic field $\mathbb{Q}[\zeta_n] \subset \mathbb{C}$ can be characterized as the splitting field of the nth cyclotomic polynomial $\Phi_n \in \mathbb{Z}[x]$, and

$$\operatorname{Gal} \mathbb{Q}[\zeta_n]/\mathbb{Q} = \operatorname{Gal} \Phi_n\,.$$

14.3.1 Frobenius Elements

For every prime $p \nmid n$, the polynomial $x^n - 1$ is separable over $\mathbb{F}_p$. The reduction $\overline{\Phi}_n$ of Φ_n modulo p is also separable over $\mathbb{F}_p$, because $\overline{\Phi}_n$ divides $x^n - 1$ in $\mathbb{F}_p[x]$. Therefore, the mapping $\xi \mapsto \overline{\xi} = \xi \pmod{p}$ establishes a bijection between the set of complex primitive roots of unity $R_n \subset O \subset \mathbb{Q}[\zeta_n] \subset \mathbb{C}$ and the set of roots of the reduced cyclotomic polynomial in the splitting field of $\overline{\Phi}_n$ over $\mathbb{F}_p$, which is generated as an $\mathbb{F}_p$-algebra by the residue classes $\overline{\xi} \in O/(p)$ of the complex roots of unity ξ in the quotient algebra of the ring of integers $O \subset \mathbb{Q}[\zeta_n]$ by the principal ideal $(p) \subset O$. Since this splitting field is finite, it is a finite Galois extension of $\mathbb{F}_p$ with cyclic Galois group generated by the Frobenius endomorphism[8]

$$F_p : \overline{\xi} \mapsto \overline{\xi}^p .$$

By Theorem 14.2, the Galois group $\mathrm{Gal}\,\Phi_n/\mathbb{Q}$ contains a permutation $\sigma \in \mathrm{Aut}\,R_n$ of the complex primitive roots such that $\overline{\sigma(\xi)} = \overline{\xi}^p$. Therefore, the multiplicative group automorphism

$$F_p : \boldsymbol{\mu}_n \xrightarrow{\sim} \boldsymbol{\mu}_n , \quad \xi \mapsto \xi^p , \tag{14.14}$$

can be extended to an automorphism of the cyclotomic field $\mathbb{Q}[\zeta_n]$ over $\mathbb{Q}$. This extension is called the *p-Frobenius element* in the Galois group of the cyclotomic field. Thus, for all prime integers $p \nmid n$, the Frobenius automorphisms $F_p \in \mathrm{Gal}\,\overline{\Phi}_n/\mathbb{F}_p$ are *canonically* included in the Galois group $\mathrm{Gal}\,\Phi_n/\mathbb{Q}$. Moreover, every complex primitive root $\zeta_n^m \in R_n$, $\mathrm{GCD}(m,n) = 1$, can be obtained by applying the Frobenius elements to the initial root $\zeta_n = e^{2\pi i/n}$. Namely, if $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, then $\zeta_n^m = F_{p_1}^{m_1} F_{p_2}^{m_2} \cdots F_{p_k}^{m_k} \zeta_n$. In particular, the Galois group $\mathrm{Gal}\,\Phi_n/\mathbb{Q}$ acts transitively on the roots of Φ_n. Hence, Φ_n is irreducible over $\mathbb{Q}$. Thus, Φ_n is the minimal polynomial of ζ_n over $\mathbb{Q}$.

Proposition 14.5 *The embedding* (14.13) *is a group isomorphism, i.e.,*

$$\mathrm{Gal}\,\Phi_n \simeq \big(\mathbb{Z}/(n)\big)^* .$$

In particular, $\deg \mathbb{Q}[\zeta_n]/\mathbb{Q} = \varphi(n)$ *is* Euler's function.

Proof Since the Galois group $\mathrm{Gal}\,\Phi_n$ acts transitively on the roots of Φ_n, the inequality $\big|\mathrm{Gal}\,\Phi_n\big| \geqslant \deg \Phi_n = \varphi(n) = \big|\big(\mathbb{Z}/(n)\big)^*\big|$ holds. □

Example 14.5 (Gaussian Sum) Let $p > 2$ be a rational prime. If a subgroup $H \subset \mathbb{F}_p^*$ has index two, then H contains all nonzero squares in $\mathbb{F}_p$, because

$$\xi^2 H = \xi H \cdot \xi H = H$$

in the quotient group $\mathbb{F}_p^*/H \simeq \mathbb{Z}/(2)$. This forces H to coincide with the multiplicative group of quadratic residues[9] modulo p. Therefore, the Galois group of the cyclotomic field contains a unique subgroup of index two, and the isomorphism $m : \mathrm{Gal}\,\Phi_n \xrightarrow{\sim} \mathbb{F}_p^*$ from formula (14.13) on p. 324 maps this subgroup isomorphically onto the multiplicative group of quadratic residues. By the Galois correspondence,

[8]See Example 13.6 on p. 310 and the proof of Corollary 14.2 on p. 323.

[9]Compare with Section 3.6.3 of Algebra I.

there exists a unique quadratic extension $\mathbb{Q} \subset \mathbb{K}$ contained in the cyclotomic field $\mathbb{Q}[\zeta_p]$. The field $\mathbb{K}$ is spanned over $\mathbb{Q}$ by the complex number

$$\vartheta = \sum_{\substack{\sigma\in\operatorname{Gal}\Phi_n:\\ m(\sigma)\in\mathbb{F}_p^{*2}}} \sigma(\zeta_p) - \sum_{\substack{\sigma\in\operatorname{Gal}\Phi_n:\\ m(\sigma)\notin\mathbb{F}_p^{*2}}} \sigma(\zeta_p) = \sum_{m=1}^{p-1} \left[\frac{m}{p}\right] \cdot \zeta_p^m\,, \tag{14.15}$$

where

$$\left[\frac{m}{p}\right] \overset{\text{def}}{=} \begin{cases} 0 & \text{for } m \pmod p = 0\,, \\ 1 & \text{for } m \pmod p \in \mathbb{F}_p^2 \smallsetminus 0\,, \\ -1 & \text{for } m \pmod p \notin \mathbb{F}_p^2\,, \end{cases}$$

is the *Legendre–Jacobi symbol.*[10] Indeed, the sum (14.15) is invariant under the action of the subgroup $\mathbb{F}_p^{*2} \subset \operatorname{Gal}\Phi_n$, and it alternates sign under the action of all other automorphisms of the cyclotomic field. The sum (14.15) is known as a *Gaussian sum*.

Exercise 14.7 Verify that $\sqrt{(-1)^{(p-1)/2}p} \in \mathbb{Q}[\vartheta]$ for all rational primes $p > 2$, and write an explicit expression for this square root in terms of the complex pth roots of unity.

14.4 Cyclic Extensions

Let $\Bbbk$ be an arbitrary field. An element $\zeta \in \Bbbk$ is called a *primitive mth root of unity* if $\zeta^m = 1$ and $\zeta^i \neq 1$ for $0 < i < m$. If the field $\Bbbk$ contains such a primitive root ζ, then the multiplicative group of roots of the binomial $x^m - 1$ in $\Bbbk$ has order m and is generated by ζ. Hence, the polynomial $x^m - 1$ is separable and completely factorizable over $\Bbbk$ in this case. Therefore, $m \nmid \operatorname{char}(\Bbbk)$, and every polynomial

$$x^d - a \in \Bbbk[x]$$

of degree $d \mid m$ is separable over $\Bbbk$ as well. We write $\boldsymbol{\mu}_m \subset \Bbbk^*$ for the cyclic multiplicative group of mth roots of unity in $\Bbbk$. The generators of $\boldsymbol{\mu}_m$ are exactly the primitive mth roots. We also write

$$\Bbbk^{*s} = \{\alpha^s \mid \alpha \in \Bbbk^*\}$$

for the multiplicative group of all the proper nonzero sth powers in $\Bbbk$.

Theorem 14.3 *Let $\Bbbk$ be an arbitrary field containing a primitive mth root of unity, and $a \in \Bbbk^*$. Then the binomial $f(x) = x^m - a$ has cyclic Galois group over $\Bbbk$,*

[10] See the discussion after formula (3.22) of Algebra I.

and the irreducible factorization of f *in* $\Bbbk[x]$ *has the form* $f = g_1 g_2 \cdots g_k$*, where* $g_i(x) = x^n - b_i$*. The numbers* $k, n \in \mathbb{N}$ *satisfy the conditions*

$$kn = m, a \in \Bbbk^{*k}, |\,\mathrm{Gal} f/\Bbbk| = n\,.$$

In particular, f *is irreducible if and only if* $n = m$*, and this means that the quotient algebra* $\Bbbk[x]/(f)$ *is a splitting field of* f*.*

Proof Let $\overline{\Bbbk} \supset \Bbbk$ be an algebraic closure, and $\alpha \in \overline{\Bbbk}$ a root of f. Then the roots of f in $\overline{\Bbbk}$ are in bijection with the group $\boldsymbol{\mu}_m \subset \Bbbk$ and are equal to $\xi\alpha$, $\xi \in \boldsymbol{\mu}_m$. If a permutation $g \in \mathrm{Gal} f/\Bbbk$ maps α to $g(\alpha) = \vartheta_g \cdot \alpha$ for some $\vartheta_g \in \boldsymbol{\mu}_m$, then g acts on every root of f as multiplication by ϑ_g, because $g(\xi\alpha) = \xi g(\alpha) = \xi\vartheta_g\alpha = \vartheta_g\xi\alpha$. This leads to a monomorphism of groups

$$\mathrm{Gal} f/\Bbbk \hookrightarrow \boldsymbol{\mu}_m\,, \quad g \mapsto \vartheta_g = g(\alpha)/\alpha\,. \tag{14.16}$$

Since $\boldsymbol{\mu}_m$ is a cyclic group, the image $G \subset \boldsymbol{\mu}_m$ of the homomorphism (14.16) is a cyclic subgroup generated by a primitive nth root of unity ζ for some $n \mid m$. Therefore, $G = \boldsymbol{\mu}_n \subset \boldsymbol{\mu}_m$. The cosets $\boldsymbol{\mu}_n\xi \subset \boldsymbol{\mu}_m$ are in bijection with the orbits of the Galois group action on the roots of f. Hence, the cosets $\boldsymbol{\mu}_n\xi$ are in bijection with the irreducible factors $f_\xi(x) \stackrel{\text{def}}{=} \prod_{\nu=0}^{n-1}(x - \zeta^\nu\xi\alpha)$ of the binomial f in $\Bbbk[x]$.

Exercise 14.8 Verify that $f_\xi(x) = x^n - \xi^n\alpha^n$.

Since $f_\xi \in \Bbbk[x]$, its constant term b_ξ is equal to $\xi^n\alpha^n \in \Bbbk$. Therefore, the element

$$c = b_\xi/\xi^n = \alpha^n$$

lies in $\Bbbk$ and does not depend on ξ. Thus, the irreducible factorization of f in $\Bbbk[x]$ has the form $x^m - a = \prod_{\xi\in\boldsymbol{\mu}_m/\boldsymbol{\mu}_n}\left(x^n - b_\xi\right)$, and the constant term of f can be written as $a = \alpha^m = c^k \in \Bbbk^{*k}$ for $k = m/n$. As a byproduct, we conclude that f is irreducible if and only if $n = m$. In this case, the embedding (14.16) becomes an isomorphism, and the quotient algebra $\Bbbk[x]/(f)$ becomes a field containing all the roots $\xi \cdot x \pmod f$ of the binomial f. □

Exercise 14.9 Under the assumptions of Theorem 14.3, show that the splitting fields of two binomials $x^m - a$, $x^m - b$ coincide within $\overline{\Bbbk}$ if and only if $a = b^r c^m$ for some $c \in \Bbbk$ and $r \in \mathbb{N}$ coprime to m.

Definition 14.1 (Cyclic Extensions) A finite Galois extension $\mathbb{K} \supset \Bbbk$ is called *cyclic of order m* if the Galois group $\mathrm{Gal}\,\mathbb{K}/\Bbbk$ is cyclic of order m.

Theorem 14.4 *Let* $\Bbbk$ *be an arbitrary field containing a primitive mth root of unity. Then the cyclic extensions of* $\Bbbk$ *of degree m are exhausted by the splitting fields of irreducible binomials* $x^m - a \in \Bbbk[x]$*, i.e., by the simple extensions* $\Bbbk\left[\sqrt[m]{a}\right]$*.*

Proof Let $\mathbb{K} \subset \Bbbk$ be a cyclic extension of degree m with Galois group $G = \mathrm{Gal}\,\mathbb{K}/\Bbbk$ generated by an automorphism $\sigma \in \mathrm{Aut}_{\Bbbk}\,\mathbb{K}$ of order m, and let $\zeta \in \Bbbk$ be a primitive

mth root of unity. Consider the following $\Bbbk$-linear endomorphism of the field $\mathbb{K}$:

$$L_{\zeta,\sigma} \stackrel{\text{def}}{=} \sum_{i=0}^{m-1} \zeta^i \sigma^i : \vartheta \mapsto \sum_{i=0}^{m-1} \zeta^i \sigma^i(\vartheta)\,.$$

Since the automorphisms $\sigma^0 = \mathrm{Id}, \sigma, \sigma^2, \dots, \sigma^{m-1}$ constitute distinct multiplicative characters of the abelian group[11] $\mathbb{K}^*$ over the field $\mathbb{K}$, they are linearly independent[12] over $\mathbb{K}$ in the vector space of all functions $\mathbb{K}^* \to \mathbb{K}$. Therefore, the endomorphism $L_{\zeta,\sigma}$ is nonzero.

Exercise 14.10 Check that $\sigma L_{\zeta,\sigma} = \zeta^{-1} L_{\zeta,\sigma}$.

The equality $\left(\sigma - \zeta^{-1}\right) L_{\zeta,\sigma} = 0$ forces the image of $L_{\zeta,\sigma}$ to be in the ζ^{-1}-eigenspace of the automorphism σ. Hence, there exists a nonzero element $\alpha \in \mathbb{K}$ such that $\sigma(\alpha) = \zeta^{-1}\alpha$. The Galois orbit of α consists of m distinct elements $\sigma^i(\alpha) = \zeta^{-i}\alpha$, $0 \leqslant i \leqslant m-1$, the roots of the binomial $f(x) = x^m - \alpha^m$. This forces f to be irreducible with coefficients in $\Bbbk$.

Exercise 14.11 Check by direct computation that the constant term of f is Galois invariant.

We conclude that the simple extension $\Bbbk[\alpha] \simeq \Bbbk[x]/(f)$ is the splitting field of f contained in $\mathbb{K}$. Since the fields $\Bbbk[\alpha]$ and $\mathbb{K}$ have the same degree m over $\Bbbk$, they coincide. $\square$

Exercise 14.12* (Kummer Isomorphism) Let $\Bbbk$ be an arbitrary field, and $\overline{\Bbbk} \supset \Bbbk$ an algebraic closure of $\Bbbk$. Show that there exists a well-defined isomorphism of abelian groups

$$\Bbbk^*/\Bbbk^{*m} \simeq \mathrm{Hom}_{Ab}\left(\mathrm{Gal}\,\overline{\Bbbk}/\Bbbk, \boldsymbol{\mu}_m\right)$$

mapping a class $a \pmod{\Bbbk^{*m}}$ to the homomorphism of abelian groups

$$\mathrm{Gal}\,\overline{\Bbbk}/\Bbbk \to \boldsymbol{\mu}_m\,, \quad \sigma \mapsto \sigma\left(\sqrt[m]{a}\right)/\sqrt[m]{a}\,.$$

14.5 Solvable Extensions

A finite group G is called *solvable* if all the composition factors[13] of G are exhausted by the cyclic simple groups $\mathbb{Z}/(p)$ for some prime $p \in \mathbb{N}$. Given a field $\Bbbk$ of characteristic zero, a finite Galois extension $\mathbb{K} \supset \Bbbk$ is called *solvable* if the Galois group $\mathrm{Gal}\,\mathbb{K}/\Bbbk$ is solvable.

---

[11] See Sect. 5.4.2 on p. 111.

[12] In addition to the already cited Sect. 5.4.2, see Exercise 5.15 on p. 112.

[13] See Section 13.3.1 of Algebra I.

Lemma 14.1 *A finite group G is solvable if and only if there exists a decreasing series of subgroups*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{e\} \tag{14.17}$$

such that $G_{i+1} \lhd G_i$ and the quotient G_i/G_{i+1} is abelian for all $0 \leqslant i < m$.

Proof By definition, a composition series of a solvable group satisfies the condition of the lemma. Conversely, given a series (14.17), a composition series for G can be constructed by taking a composition series of every quotient G_i/G_{i+1},

$$G_i/G_{i+1} = H_{i,0} \supset H_{i,1} \supset H_{i,2} \supset \cdots \supset H_{i,m_i-1} \supset H_{i,m_i} = \{e\}\,, \tag{14.18}$$

and replacing the fragment $G_i \supset G_{i+1}$ in (14.17) by the preimage of the chain (14.18) under the factorization map $G_i \twoheadrightarrow G_i/G_{i+1}$, that is, by

$$G_i \supset H_{i,1}G_{i+1} \supset H_{i,2}G_{i+1} \supset \cdots \supset H_{i,m_i-1}G_{i+1} \supset G_{i+1}\,.$$

Since the composition factors of every abelian group $G_{i+1} \lhd G_i$ are exhausted by the simple abelian groups $\mathbb{Z}/(p)$, the resulting composition factors of G are also exhausted by the groups $\mathbb{Z}/(p)$. □

Lemma 14.2 *All the subgroups and quotient groups of a solvable group are solvable. Conversely, if a group G has a solvable normal subgroup $N \lhd G$ with solvable quotient G/N, then G is solvable.*

Proof Let G possess a decreasing series of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{e\} \tag{14.19}$$

satisfying the conditions of Lemma 14.1. Intersecting this series with an arbitrary subgroup $H \subset G$ leads to a chain

$$H = G_0 \cap H \supset G_1 \cap H \supset G_2 \cap H \supset \cdots \supset G_{m-1} \cap H \supset G_m \cap H = H$$

of subgroups in H with quotients $(G_i \cap H)\,/\,(G_{i+1} \cap H) \simeq ((G_i \cap H) \cdot G_{i+1})\,/G_{i+1}$, which are subgroups of the abelian groups G_i/G_{i+1}, and therefore are abelian as well. Symmetrically, for every quotient group G/H, applying the factorization homomorphism $\pi : G \twoheadrightarrow G/H$ to the chain (14.19) leads to the chain

$$\frac{G}{H} = \frac{G_0}{H} \supset \frac{G_1}{G_1 \cap H} \supset \frac{G_2}{G_2 \cap H} \supset \cdots \supset \frac{G_{m-1}}{G_{m-1} \cap H} \supset \frac{G_m}{G_m \cap H} = \{e\}$$

in G/H with factors

$$\frac{G_i/(G_i \cap H)}{G_{i+1}/(G_{i+1} \cap H)} \simeq \frac{G_i}{G_{i+1}(G_i \cap H)} \simeq \frac{G_i/G_{i+1}}{(G_i \cap H)/(G_{i+1} \cap H)}\,,$$

which are the quotient groups of the abelian groups G_i/G_{i+1}, and therefore are abelian too.

Conversely, given a solvable normal subgroup $N \lhd G$ with solvable quotient G/N, a chain (14.19) for the quotient group G/N is lifted to G along the factorization map $G \twoheadrightarrow G/N$ to the chain

$$G = G_0N \supset G_1N \supset G_2N \supset \cdots \supset G_{m-1}N \supset G_mN = N$$

with quotients

$$\frac{G_iN}{G_{i+1}N} \simeq \frac{G_iN/N}{G_{i+1}N/N} \simeq \frac{G_i}{G_{i+1}(N \cap G_i)} \simeq \frac{G_i/G_{i+1}}{(G_i \cap N)/(G_{i+1} \cap N)},$$

which are abelian for the same reason as above. Extending this chain by the chain (14.19) for the subgroup N,

$$N = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_{m-1} \supset N_n = \{e\},$$

we get the required chain (14.19) for G. □

Theorem 14.5 *Let $\Bbbk$ be a field of characteristic zero, and $f \in \Bbbk[x]$ an irreducible polynomial. If some root of f admits an expression through the elements of $\Bbbk$ by means of addition, subtraction, multiplication, division, and extraction of nth roots for arbitrary $n \in \mathbb{N}$, then the Galois group* $\operatorname{Gal} f/\Bbbk$ *is solvable. In this case, all the roots of f can be expressed in radicals through the elements of $\Bbbk$.*

Proof Let $\overline{\Bbbk} \supset \Bbbk$ be an algebraic closure of $\Bbbk$, and $\mathbb{K} \subset \overline{\Bbbk}$ the splitting field of f. A root $\alpha \in \overline{\Bbbk}$ of the polynomial f can be expressed in radicals if and only if α belongs to some field $\mathbb{L} \subset \overline{\Bbbk}$ achieved by a finite tower of simple extensions

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_m = \mathbb{L}, \tag{14.20}$$

where $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/\left(x^{k_i} - a_i\right)$ for some $a_i \in \mathbb{L}_i$ such that the polynomial $x^{k_i} - a_i$ is irreducible over $\mathbb{L}_i$. We will prove the theorem by constructing a Galois extension $\mathbb{L}' \supset \Bbbk$ with solvable Galois group $\operatorname{Gal}\mathbb{L}'/\Bbbk$ such that $\mathbb{L} \subset \mathbb{L}'$. This forces the splitting field $\mathbb{K}$ to be a subfield of $\mathbb{L}'$ normal over $\Bbbk$, and in accordance with the Galois correspondence, the Galois group

$$\operatorname{Gal}\mathbb{K}/\Bbbk = \frac{\operatorname{Gal}\mathbb{L}'/\Bbbk}{\operatorname{Gal}\mathbb{L}'/\mathbb{K}}$$

is solvable by Lemma 14.2, as the quotient group of a solvable group. We will construct $\mathbb{L}'$ by a step-by-step extension of the tower (14.20) to the tower

$$\Bbbk \subset \mathbb{L}'_0 \subset \mathbb{L}'_1 \subset \mathbb{L}'_2 \subset \cdots \subset \mathbb{L}'_m = \mathbb{L}' \tag{14.21}$$

such that $\mathbb{L}_i \subset \mathbb{L}'_i$ and every $\mathbb{L}'_i$ is a Galois extension of $\Bbbk$. At the first step, we put

$$\mathbb{L}'_0 \subset \overline{\Bbbk}$$

as the splitting field of the polynomial $x^N - 1$ with N sufficiently large that $\mathbb{L}'_0$ contains a primitive kth root of unity for all k appearing as the degrees of radicals in the expression of α. It follows from Proposition 14.5 and Proposition 13.4 that the extension $\Bbbk \subset \mathbb{L}'_0$ is a Galois extension with abelian Galois group. Assume that the field $\mathbb{L}'_i$ is already constructed, and put $\mathbb{L}'_{i+1} \subset \overline{\Bbbk}$ as the splitting field of the polynomial

$$\prod_{\sigma \in \mathrm{Gal}\,\mathbb{L}'_i/\Bbbk} \left(x^{k_i} - \sigma(a_i)\right) \in \mathbb{L}'_i[x]\,.$$

Since the coefficients of this polynomial are invariant under the action of the Galois group $\mathrm{Gal}\,\mathbb{L}'_i/\Bbbk$, they actually belong to $\Bbbk$, and therefore, $\mathbb{L}'_{i+1} \supset \Bbbk$ is a finite Galois extension containing the field $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/\left(x^{k_i} - a_i\right)$. Note that the field $\mathbb{L}'_{i+1}$ can be obtained from the previous field $\mathbb{L}'_i$ by the sequential adjunction of roots of irreducible binomials $x^n - a$ with $a \in \mathbb{L}'_i$. By Theorem 14.3, every such adjunction leads to a cyclic Galois extension.

After m steps, we get a normal separable field $\mathbb{L}' \supset \Bbbk$, obtained from $\Bbbk$ by sequential Galois extensions each with an abelian Galois group. The Galois correspondence provides the Galois group $\mathrm{Gal}\,\mathbb{L}'/\Bbbk$ with a decreasing series of subgroups satisfying the conditions of Lemma 14.1. Hence, the Galois group $\mathrm{Gal}\,\mathbb{L}'/\Bbbk$ is solvable. □

Remark 14.1 The assumption $\mathrm{char}(\Bbbk) = 0$ can be weakened to the requirement that $\mathrm{char}(\Bbbk)$ divide the degree of no radical appearing in the expression for the root. The above proof works in this case as well.

14.5.1 Generic Polynomial of Degree n

Let $\mathbb{F}$ be an arbitrary field, and $\Bbbk = \mathbb{F}(a_1, a_2, \dots, a_n)$ the field of rational functions in n variables $a_1, a_2, \dots, a_n$ algebraically independent over $\mathbb{F}$. The polynomial

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \Bbbk[x] \tag{14.22}$$

is called the *generic polynomial* of degree n over $\mathbb{F}$, because specializing the coefficients of F to concrete values in $\mathbb{F}$ allows one to produce every polynomial $f \in \mathbb{F}[x]$. In particular, every formula expressing the roots of F through the elements of $\Bbbk$ expresses the roots of a particular polynomial $f \in \mathbb{F}[x]$ in terms of the elements of $\mathbb{F}$, as does the well-known formula

$$x_\pm = \frac{p \pm \sqrt{p^2 - 4q}}{2}$$

for the roots of the generic quadratic polynomial $x^2 + px + q \in \mathbb{F}(p, q)[x]$. It follows from Example 14.4 on p. 323 that for $\mathbb{F} = \mathbb{Q}$, there is no formula expressing the roots of the generic fifth-degree polynomial in terms of the coefficients by means of the four arithmetic operations and radicals of arbitrary degree.

Let us describe the Galois group $\operatorname{Gal} F/\Bbbk$ for an arbitrary n over a field $\mathbb{F}$. Write $t_1, t_2, \dots, t_n$ for the roots of F in its splitting field $\mathbb{K} \supset \Bbbk$. Since $\mathbb{K}$ is algebraic over $\Bbbk$, it follows from Corollary 10.4 on p. 237 that a transcendence basis of $\mathbb{K}$ over $\mathbb{F}$ can be chosen among the roots $t_1, t_2, \dots, t_n$, which generate $\mathbb{K}$ as an $\mathbb{F}$-algebra.[14] The inequality $\operatorname{tr}\deg_{\mathbb{F}} \mathbb{K} \geqslant \operatorname{tr}\deg_{\mathbb{F}} \Bbbk = n$ forces this transcendence basis to be the whole collection $t_1, t_2, \dots, t_n$. Thus, the roots $t_1, t_2, \dots, t_n$ are algebraically independent over $\mathbb{F}$. In particular, they are all distinct. Hence, the generic polynomial F is separable, and $\mathbb{K} \simeq \mathbb{F}(t_1, t_2, \dots, t_n)$ is a finite Galois extension of $\Bbbk = \mathbb{F}(a_1, a_2, \dots, a_n)$. Since every permutation of the independent variables $t_1, t_2, \dots, t_n$ can be extended to a unique automorphism of the field $\mathbb{F}(t_1, t_2, \dots, t_n)$ over $\mathbb{F}$, we conclude that $\operatorname{Gal} \mathbb{K}/\Bbbk = S_n$, $\deg \mathbb{K}/\Bbbk = n!$, and $\mathbb{F}(t_1, t_2, \dots, t_n)^{S_n} = \mathbb{F}(a_1, a_2, \dots, a_n)$.

Exercise 14.13 Verify that the subfield of A_n-invariants $\mathbb{K}^{A_n} \subset \mathbb{K}$ is the quadratic extension of $\Bbbk$ by the element $\sqrt{D(f)} = \prod_{1 \leqslant i < j \leqslant n} (t_i - t_j)$.

For $n \geqslant 5$, the composition factors of S_n are the simple normal subgroup $A_n \lhd S_n$ and the group $\mathbb{Z}/(2) = S_n/A_n$ of order two. Therefore, S_n is not solvable for $n \geqslant 5$. By Theorem 14.5, the generic polynomial equation of degree $n \geqslant 5$ cannot be solved in radicals over a field $\mathbb{F}$ of characteristic zero. This fact is known as the *Abel–Ruffini theorem*.

14.5.2 Solvability of Particular Polynomials

The absence of a formula for expressing the roots of a generic polynomial F in terms of the coefficients of F in radicals certainly does not forbid the existence of such an expression for particular polynomials $f \in \mathbb{F}[x]$.

Theorem 14.6 *Let $\Bbbk$ be an arbitrary field of characteristic zero, and $f \in \Bbbk[x]$ a monic irreducible polynomial. If the Galois group* $\operatorname{Gal} f/\Bbbk$ *is solvable, then every root of f can be expressed in radicals in terms of the elements of $\Bbbk$.*

[14] Note that $a_1, a_2, \dots, a_n$ are polynomials in $t_1, t_2, \dots, t_n$ by Viète's theorem.

Proof Fix an algebraic closure $\overline{\Bbbk} \supset \Bbbk$, and write $\mathbb{K} \subset \overline{\Bbbk}$ for the splitting field of f, and $\mathbb{L} \subset \overline{\Bbbk}$ for the extension of $\Bbbk$ by a primitive root of unity of degree $n = |\operatorname{Gal} \mathbb{K}/\Bbbk|$. Then all elements of $\mathbb{L}$ can be expressed in radicals through the elements of $\Bbbk$. Since $\mathbb{K} \supset \Bbbk$ is a solvable Galois extension, it follows from Proposition 13.4 on p. 306 and Theorem 13.5 on p. 306 that the extension $\mathbb{LK} \supset \mathbb{L}$ is a solvable Galois extension as well, because the Galois group $\operatorname{Gal} \mathbb{LK}/\mathbb{L}$ is a subgroup of the solvable group $\operatorname{Gal} \mathbb{K}/\Bbbk$. A composition series

$$\operatorname{Gal} \mathbb{LK}/\mathbb{L} = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{e\}$$

with simple factors $G_i/G_{i+1} \simeq \mathbb{Z}/(p_i)$ forces the compositum $\mathbb{LK}$ to be obtained from $\mathbb{L}$ by a sequence of cyclic simple extensions. By Theorem 14.4, every such extension is obtained by the adjunction of a radical. Therefore, all elements of $\mathbb{LK} \supset \mathbb{K}$ can be expressed in radicals through the elements of $\Bbbk$. □

Remark 14.2 The assumption $\operatorname{char}(\Bbbk) = 0$ can be weakened to the requirement that $\operatorname{char}(\Bbbk)$ differ from the prime orders of the Jordan–Hölder factors of the Galois group $\operatorname{Gal} f/\Bbbk$. The previous proof works in this case as well.

Problems for Independent Solution to Chapter 14

Problem 14.1 Let $\Bbbk$ be a field with $\operatorname{char} \Bbbk \neq 2$, and $f \in \Bbbk[x]$ an irreducible polynomial. Show that the discriminant[15] $D(f)$ is in $\Bbbk^2$ if and only if the Galois group $\operatorname{Gal} f/\Bbbk$ contains only even permutations of the roots of f.

Problem 14.2 Find the Galois groups over $\mathbb{Q}$ for the following polynomials: **(a)** $x^3 - 3x + 1$, **(b)** $x^3 + 2x + 1$, **(c)** $x^4 + 1$, **(d)** $x^4 + x^2 + 1$, **(e)** $x^4 - 5x^2 + 6$, **(f)** $x^4 + 2x^2 + x + 3$, **(g)** $x^4 + x^2 + x + 1$.

Problem 14.3 Find the Galois group of the polynomial $x^3 - x - 1$ over the field $\mathbb{Q}\big[\sqrt{-23}\big]$.

Problem 14.4 Give an explicit example of an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree six with Galois group $\operatorname{Gal} f/\mathbb{Q} \simeq S_6$.

Problem 14.5 Is there a finite extension of $\mathbb{Q}$ containing infinitely many roots of unity?

Problem 14.6 Find all $n \in \mathbb{N}$ for which there exists a complex primitive nth root of unity with quadratic minimal polynomial over $\mathbb{Q}$.

Problem 14.7 Enumerate all the roots of unity in the field $\mathbb{Q}\big[\sqrt{-5}\big]$.

Problem 14.8 Express $\sqrt[5]{1}$ in quadratic radicals.

[15] See Problem 12.3 on p. 291 and Example 13.1 on p. 296.

Problem 14.9 Express $\sqrt{13}$ in terms of $e^{2\pi i/13} \in \mathbb{C}$.

Problem 14.10 (Gaussian Construction) Construct a regular 17-gon with straightedge and compass.

Problem 14.11 For every prime $p \in \mathbb{N}$ and $a \in \mathbb{Q}^* \smallsetminus \mathbb{Q}^{*p}$, show that the Galois group of the polynomial $x^p - a$ over $\mathbb{Q}$ is isomorphic to the group of affine automorphisms of the line $\mathbb{A}^1$ over $\mathbb{F}_p$.

Problem 14.12 Show that $\mathbb{Q}\left[\sqrt{p}\right] \subset \mathbb{Q}\left[e^{2\pi i/4p}\right]$ for every prime $p \equiv 3 \pmod 4$.

Problem 14.13 Show that every quadratic extension of $\mathbb{Q}$ can be embedded into some cyclotomic field.

Problem 14.14 (Quadratic Reciprocity Revisited) [16] Let $p, q > 2$ be rational primes, $q^* = (-1)^{(q-1)/2}q$, $\mathbb{K} = \mathbb{Q}[x]/\left(x^2 - q^*\right)$. Write $O \subset \mathbb{K}$ for the ring of integers,[17] and $[z]_p$ for the residue class $z \pmod p$ of an element $z \in O$ in the quotient ring $O/(p)$.

(a) Show that the following three statements are equivalent:

(1) $[q^*]_p$ is a proper square in $\mathbb{F}_p^2$.
(2) $O/(p) \simeq \mathbb{F}_p \oplus \mathbb{F}_p$.
(3) The Frobenius endomorphism $F_p : \vartheta \mapsto \vartheta^p$ acts identically on $O/(p)$.

(b) If the above three conditions fail, describe the $\mathbb{F}_p$-algebra $O/(p)$ and the Frobenius endomorphism $F_p : O/(p) \to O/(p)$, $\vartheta \mapsto \vartheta^p$.

(c) Construct an embedding of $\mathbb{K}$ into the qth cyclotomic field[18] $\varphi : \mathbb{K} \hookrightarrow \mathbb{Q}\left[\sqrt[q]{1}\right]$ such that the multiplicative endomorphism $F_{p,\mathbb{C}} : \mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^p$, maps $\varphi(O)$ to itself and admits a well-defined reduction modulo (p), which coincides with the Frobenius endomorphism $F_p : O/(p) \to O/(p)$, $\vartheta \mapsto \vartheta^p$.

(d) Write an explicit expression for $\sqrt{q^*}$ in terms of the complex qth roots of unity and clarify the effect of the endomorphism $F_{p,\mathbb{C}}$ on both sides of this expression.

(e) Prove the *quadratic reciprocity law*

$$\left[\frac{p}{q}\right] \cdot \left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

where $\left[\frac{q}{p}\right]$ means the *Legendre–Jacobi symbol* from Example 14.5 on p. 325.

Problem 14.15 Let $\Bbbk \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ be a maximal field with respect to inclusions such that $\sqrt[3]{5} \notin \Bbbk$. Does $\Bbbk$ admit a noncyclic finite Galois extension?

---

[16] See Section 3.6.3 of Algebra I and compare this problem with Problems 3.38 and 9.7 from Algebra I.

[17] That is, the integral closure of $\mathbb{Z}$ in $\mathbb{K}$.

[18] See Sect. 14.3 on p. 323.

Hints to Some Exercises

Exercise 1.1 Let $U \subset V_1 \otimes V_2 \otimes \cdots \otimes V_n$ be the K-linear span of tensor monomials. Check that the universal multilinear map $\tau : V_1 \times V_2 \times \cdots \times V_n \to V_1 \otimes V_2 \otimes \cdots \otimes V_n$ takes values within U, and the resulting map $\tau : V_1 \times V_2 \times \cdots \times V_n \to U$ is universal too. Then use 1.1.

Exercise 1.2 One should check that $v_1 \otimes v_2 \otimes \cdots \otimes v_n \neq 0$ as soon as all $v_i \neq 0$, and that the replacement $v_i \mapsto \lambda_i v_i$ with $\lambda_i \in \Bbbk$ changes $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ by a proportional tensor. The second follows immediately from the multilinearity of the tensor product: $(\lambda_1 v_1) \otimes (\lambda_2 v_2) \otimes \cdots \otimes (\lambda_n v_n) = \prod \lambda_i \cdot v_1 \otimes v_2 \otimes \cdots \otimes v_n$. To see the first, include every vector v_i in some basis of V_i. Then $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ is a basis vector in the basis of $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ described in Theorem 1.1 on p. 6. A similar argument proves the injectivity of the Segre map. Namely, given two collections of vectors

$$u_1, u_2, \ldots, u_n \quad \text{and} \quad w_1, w_2, \ldots, w_n, \quad u_i, w_i \in V_i,$$

such that u_j and w_j are not proportional in V_j for some j, then u_j, w_j can be included as two different basis vectors in some basis of V_j. Therefore, $u_1 \otimes u_2 \otimes \cdots \otimes u_n$ and $w_1 \otimes w_2 \otimes \cdots \otimes w_n$ are two different basis vectors in some basis of $V_1 \otimes V_2 \otimes \cdots \otimes V_n$.

Exercise 1.3 If $\operatorname{rk} F = 1$, then $\operatorname{im} F \subset W$ has dimension 1 and is spanned by some nonzero vector $w \in W$ uniquely up to proportionality determined by F. Hence, F acts on every vector $u \in U$ by the rule $F(u) = \xi(u) \cdot w$ for some $\xi \in U^*$ uniquely determined by F and w. Note that $\xi \in \operatorname{Ann} \ker F$ spans the 1-dimensional subspace $\operatorname{Ann} \ker F \subset U^*$.

Exercise 1.4 Since the Segre map $\mathbb{P}_1 \times \mathbb{P}_1 \xrightarrow{\sim} S$ is bijective and takes the coordinate lines on $\mathbb{P}_1 \times \mathbb{P}_1$ to the lines on S, all incidence relations among the latter lines are the same as between the first on $\mathbb{P}_1 \times \mathbb{P}_1$. Every line $\ell \subset S$ lies within $S \cap T_pS$, where T_pS is the tangent plane to S at an arbitrary point $p \in \ell$. Since the conic $S \cap T_pS$ is exhausted by the pair of lines from different families crossing at p, the line ℓ has to be one of those two lines.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5

Exercise 1.5 Verify that the map $K \times V \to V$, $(\lambda, v) \mapsto \lambda v$, is the universal bilinear map.

Exercise 1.6 The linearity is checked as follows:

$$\varphi\left(\lambda(u_x)_{x\in X} + \mu(w_x)_{x\in X}\right) = \varphi\left((\lambda u_x + \mu w_x)_{x\in X}\right) = \sum_{x\in X} \varphi_x\left(\lambda u_x + \mu w_x\right)$$

$$= \sum_{x\in X} \left(\lambda\varphi_x(u_x) + \mu\varphi_x(w_x)\right) = \lambda\varphi\left((u_x)_{x\in X}\right) + \mu\varphi\left((w_x)_{x\in X}\right),$$

where all the sums are well defined, because all but finitely many summands vanish.

Exercise 2.1 Use the same arguments as in 1.1 on p. 3.

Exercise 2.3 Let $E \sqcup R \sqcup S \sqcup T$ be a basis in V such that E is a basis in $U \cap W$, $E \sqcup R$ is a basis in U, $E \sqcup S$ is a basis in W. Identify $V^{\otimes n}$ with the noncommutative polynomial ring in the basis vectors. Then $U^{\otimes n}$ is the linear span of the monomials constructed from the basis vectors from $E \sqcup R$, whereas $W^{\otimes n}$ is the linear span of the monomials constructed out of the basis vectors from $E \sqcup S$. Their intersection is the linear span of the monomials constructed from the basis vectors from E.

Exercise 2.4 For every $x, y \in I$, the product $(a + x)(b + y)$ is equal to

$$ab + (ay + xb + xy) \equiv ab \pmod{I}.$$

Note that for just left or right ideals, this may fail.

Exercise 2.5 By the universal property of tensor algebras, for every $\Bbbk$-algebra A and linear map $f : V \to A$, there exists a unique algebra homomorphism $\widetilde{f} : \mathsf{T}V \to A$ such that

$$\widetilde{f}(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = f(v_1) \cdot f(v_2) \cdots f(v_n).$$

It is factorized through the quotient map $\mathsf{T}V \twoheadrightarrow \mathsf{T}/\mathcal{I}_{\text{sym}} \simeq SV$ if and only if $\widetilde{f}$ annihilates all the differences $u \otimes w - w \otimes u$, which means that $f(u)f(w) = f(w)f(u)$ for all $u, w \in V$, and this certainly holds in the commutative algebra A. The last statement of the exercise is verified exactly as in the proof of 1.1 on p. 3.

Exercise 2.6 $\dim S^n V = \binom{n+d-1}{d-1}$. This is the number of nonnegative integer solutions $(m_1, m_2, \dots, m_d)$ of the linear equation $m_1 + m_2 + \cdots + m_d = n$, i.e., the number of sequences formed by n ones placed in a row with $d - 1$ barriers separating the ones into d groups (some of which may be empty).

Exercise 2.7 The same argument as in 1.1 on p. 3.

Exercise 2.8 Over every field $\Bbbk$, the sums are expressed through the proper squares as $u \otimes w + w \otimes u = (u + w) \otimes (u + w) - u \otimes u - w \otimes w$. If $\operatorname{char} \Bbbk \neq 2$, then the converse expression $v \otimes v = (v \otimes v + v \otimes v)/2$ is also possible.

Exercise 2.9 Modify the arguments used in 2.5 on p. 27.

Exercise 2.10 For the first statement, modify the proof of 2.3 on p. 28. For the second, use the argument from 1.1 on p. 3.

Exercise 2.11 Relations (a), (b) are obvious (both sums consist of $n!$ equal summands). In (c), each of the two sums can be separated into two disjoint parts: the sum over all even permutations and the sum over all odd permutations, both of which consist of the same summands but taken with opposite signs. To prove (d) and (e), note that for all $h \in S_n$, left multiplication by $h : S_n \to S_n$, $g \mapsto g' = hg$, is bijective, and therefore,

$$h\Big(\sum_{g\in S_n} g(t)\Big) = \sum_{g\in S_n} hg(t) = \sum_{g'\in S_n} g'(t),$$

$$h\Big(\sum_{g\in S_n} \operatorname{sgn}(g)\cdot g(t)\Big) = \operatorname{sgn}(h)\cdot \sum_{g\in S_n} \operatorname{sgn}(hg)\cdot hg(t) = \operatorname{sgn}(h)\cdot \sum_{g'\in S_n} \operatorname{sgn}(g)\cdot g'(t).$$

Hence, $h(\operatorname{sym}_n(t)) = \operatorname{sym}_n(t)$ and $h(\operatorname{alt}_n(t)) = \operatorname{sgn}(h)\cdot \operatorname{alt}_n(t)$.

Exercise 2.12 $n^3 - \binom{n+2}{3} - \binom{n}{3} = \frac{2}{3}\left(n^3 - n\right)$.

Exercise 2.13 Direct computations using formula (2.18) on p. 32.

Exercise 2.15 The same arguments as in the proof of the multinomial expansion formula from Example 1.2 of Algebra I.

Exercise 2.17 Since the rule is linear in v, f, g, it is enough to check it for $v = e_i$, $f = x_1^{m_1}\cdots x_d^{m_d}$, $g = x_1^{k_1}\cdots x_d^{k_d}$. In this case, it follows directly from the definition of polar map.

Exercise 2.18 Use induction on $n = \deg f$ and the equality

$$\widetilde{f}(v_1, x, \dots, x) = \frac{1}{n}\cdot \partial_{v_1} f(x).$$

Exercise 2.21 Similar to 2.17.

Exercise 2.22 Let $e_1, e_2, \dots, e_m$ be a basis in U. If $\omega \notin \Lambda^m U$, then the expansion of ω as a linear combination of basis monomials e_I contains a monomial whose index I differs from the whole of $1, 2, \dots, m$. Let $k \notin I$. Then $e_k \wedge \omega \neq 0$, because the basis monomial $e_{\{k\}\sqcup I}$ appears in $e_k \wedge \omega$ with a nonzero coefficient. Conversely, if $\omega \in \Lambda^m U$, then $\omega = \lambda \cdot e_1 \wedge e_2 \wedge \cdots \wedge e_m$ and $e_i \wedge \omega = 0$ for all i.

Exercise 2.25 Let $U_1 \neq U_2$. Choose a basis of V consisting of the basis in $U_1 \cap U_2$, its complements to the bases in U_1, U_2, and some other vectors. Then $\Lambda^k U_1$ and $\Lambda^k U_2$ are represented by distinct basis monomials of $\Lambda^k V$.

Exercise 2.26 The relations $w = e \cdot A_w^t$, $u = e \cdot A_u^t$, $w = u \cdot C_{uw}$, where e, u, w are the row matrices whose elements are the corresponding basis vectors, force $A_w^t = A_u^t C_{uw}$.

Exercise 3.3 In both polynomials Δ_δ and $\prod_{i<j}(x_i - x_j)$, the lexicographically highest monomial is $x_1^{n-1}x_2^{n-2}\cdots x_{n-1}$, and it appears with the coefficient 1.

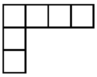
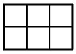
Exercise 3.4 For $n > \ell(\lambda)$, the matrix $\left(h_{\lambda_i+j-i}\right)$ has the block form $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ with a square upper unitriangular matrix of size $\ell(\lambda)+1$ in the right bottom corner.

Exercise 4.1 The stable matching between the ith and $(i+1)$th columns is established as follows. All balls of the ith column are initially considered free. Looking bottom up through the balls β of the $(i+1)$th column, we match β with the topmost free ball situated strictly lower than b in the ith column; if there are no such balls, b is declared to be free. The operation L_i either moves one of the topmost free balls of the $(i+1)$th column to the left neighbor cell, or does nothing if there are no free balls in the $(i+1)$th column. The operation R_i moves one of the lowest free balls of the ith column to the right, or does nothing if the ith column has no free balls.

Exercise 4.3 The arrays are

$$\begin{array}{|c|c|c|}\hline 0&0&2\\\hline 2&1&0\\\hline 1&1&0\\\hline 1&0&0\\\hline\end{array} \quad\text{and}\quad \begin{array}{|c|c|c|}\hline 1&1&0\\\hline 0&1&2\\\hline 0&3&0\\\hline 4&0&0\\\hline\end{array}.$$

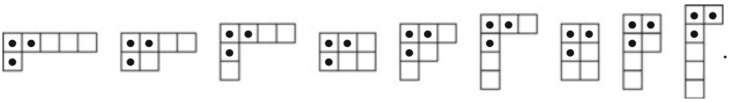
Exercise 4.5 To establish the DU-invariance of the difference $M' \setminus M''$ of DU-sets M', M'', consider an array $a' \in M' \setminus M''$. If $D_j a' \in M''$, then D_j effectively acts on a', and therefore $a' = U_j D_j a'$ must be in M''.

Exercise 4.7 The diagrams  and  are $\trianglerighteq$-incompatible.

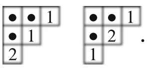
Exercise 4.8 Answers: $s_{(1)} \cdot s_{(1,1)} = s_{(2,1)} + s_{(1,1,1)}$,

$$s_{2,1}^2 = s_{4,2} + s_{2,2,1,1} + s_{4,1,1} + s_{3,1,1,1} + s_{3,3} + s_{2,2,2} + 2s_{3,2,1}.$$

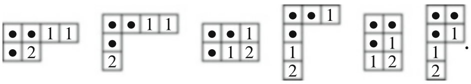
In the latter computations, there are nine ways to add three cells to $\lambda = (2,1)$:



The two outermost diagrams do not allow an admissible filling by $1, 1, 2$. The symmetric diagram allows two admissible fillings



Every remaining diagram admits the unique filling



Exercise 4.9 When we calculate $s_\lambda \cdot e_k$, we add k new cells to λ and fill them with the distinct numbers $1, 2, \ldots, k$. If two added cells fall in the same row, then the

Young tableau and the Yamanouchi word constraints contradict each other. In the computation of $s_\lambda \cdot h_k$, we fill the k added cells with k units. No two of them can appear in the same column because of the Young tableau constraint.

Exercise 5.1 By the universal property of basis,[1] the maps of sets $R \to B$ are in bijection with the linear maps $\mathbb{R} \otimes \Bbbk \to B$. By the universal property of tensor algebras,[2] the latter linear maps are in one-to-one correspondence with the algebra homomorphisms $A_R \to B$. Uniqueness is established by the same standard arguments as in Lemma 1.1 on p. 3.

Exercise 5.2 For all $w \in W$ and $u \in U$, the congruence

$$f(w+u) = fw + fu \equiv fw \pmod U$$

holds if $fu \in U$ for all $u \in U$.

Exercise 5.4 An upper bound of a chain in $\mathcal{S}'$ is provided by the union of all modules in the chain.

Exercise 5.5 Statements (a) and (b) are obvious. In (c), the inclusions

$$R\ker f \subset \ker f$$

and $R\,\mathrm{im} f \subset \mathrm{im} f$ for $f \in \mathrm{Hom}_R(W_1, W_2)$ are verified as follows. If $\varphi(v) = 0$, then $\varphi(fv) = f\varphi(v) = f(0) = 0$ for all $f \in R$. If $v = \varphi(u)$, then $fv = f\varphi(u) = \varphi(fu)$ for all $g \in R$.

Exercise 5.7 $\varphi\psi = \sum_{\alpha,\beta} \iota_\alpha \varphi_{\alpha\beta} \pi_\beta \circ \sum_{\mu,\nu} \iota_\mu \varphi_{\mu\nu} \pi_\nu = \sum_{\alpha,\nu} \iota_\alpha p_{\alpha\nu} \pi_\nu$, where

$$p_{\alpha\nu} = \sum_\eta \varphi_{\alpha\eta} \psi_{\eta\nu},$$

because

$$\pi_\beta \iota_\mu = \begin{cases} \mathrm{Id}_{V_\eta} & \text{for } \beta = \mu = \eta, \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 5.8 Since for two vectors $v, w \in V$ there exists a linear map $\varphi : V \to V$ sending v to w, the algebra $\mathrm{Ass}(R) = \mathrm{End}_\Bbbk(V)$ acts transitively on V. However, if $U \subsetneq W$ is a proper nonzero R-invariant subspace, then $\mathrm{Ass}(R)U \subset U$. This contradicts the transitivity.

Exercise 5.11 Since the assignment $g : \varphi \mapsto g\varphi g^{-1}$ is linear in φ, its coincidence with $\varrho^* \otimes \lambda$ can be checked only on the decomposable tensors $\varphi = \xi \otimes w$, where

[1] See Sect. 14.1.1 of Algebra I.

[2] See Proposition 2.1 on p. 21.

$\xi \in U^*$, $w \in W$. By definition, $\varrho^* \otimes \lambda(g)$ takes such a φ to

$$\varrho(g^{-1})^*\xi \otimes \lambda(g)w = (\xi \circ g^{-1}) \otimes (gw).$$

This linear operator sends each vector $u \in U$ to

$$\xi(g^{-1}u) \cdot gw = g\left(\xi(g^{-1}u) \cdot w\right) = g \circ (\xi \otimes w) \circ g^{-1}(u).$$

Exercise 5.12 Take $R = \{g\}$; note that every eigenvector spans a simple R-module of dimension one; and use Theorem 5.1 on p. 102.

Exercise 5.15 Let $\lambda_1\psi_1 + \lambda_2\psi_2 + \cdots + \lambda_n\psi_n = 0$ with $\lambda_\nu \in \Bbbk$ a shortest nontrivial linear relation between homomorphisms $\psi_\nu : G \to \Bbbk^*$. This forces all $\lambda_i \neq 0$. Fix an element $h \in G$ such that $\psi_1(h) \neq \psi_2(h)$. Since

$$\sum_i \lambda_i\psi_i(h)\psi_i(g) = \sum_i \lambda_i\psi_i(hg) = 0$$

for all $g \in G$, we get another linear relation on $\psi_1, \psi_2, \dots, \psi_n$ with coefficients $\lambda_i \cdot \psi_i(h)$. Subtracting this relation from the first multiplied by $\psi_1(h)$ leads to a shorter relation on ψ_2, ψ_3, ..., ψ_n in which ψ_2 appears with the coefficient $\lambda_2(\psi_1(h) - \psi_2(h)) \neq 0$.

Exercise 5.17 Take $\Bbbk = \mathbb{F}_2$, $G = \mathbb{Z}/(2)$, $V = \Bbbk^2$, and let the elements $[0], [1] \in G$ act by the linear operators with matrices

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Check that $U^2 = E$, $V^G = \Bbbk e_1$, and V is indecomposable, because U has just one eigenvector.

Exercise 5.21 If $v = \sum x_i e_i$ is nonzero modulo e, then $x_i \neq x_j$ for some $i \neq j$, and therefore $v - \sigma_{ij}v = (x_i - x_j)(e_i - e_j)$, where $\sigma_{ij} \in S_n$ is the transposition of i, j. This forces *all* the differences $e_i - e_j$, $i \neq j$, to lie within the linear span of the orbit $S_n v$.

Exercise 5.22 Compare with Exercise 2.13 on p. 33.

Exercise 5.23 Split the eight vertices of the cube into two quadruples forming a pair of centrally symmetric regular tetrahedra T_1, T_2 whose edges are the diagonals of the faces of the cube. Let U_{cube} and U_{tet} be the representations of S_4 in $\mathbb{R}^3$ by means of the proper group of the cube and the complete group of the tetrahedron T_1. Then the subgroup of even permutations $A_4 \subset S_4$ is represented in U_{cube} by the rotations of the cube that map T_1 to itself, that is, by the proper subgroup in the complete group of T_1. Every odd permutation $g \in S_n$ is represented in U_{cube} by a rotation of the cube mapping T_1 to T_2. Followed by the central symmetry, that is, multiplied by $\operatorname{sgn}(g)$, it takes T_1 to itself by a nonproper transformation from the complete group of the regular tetrahedron. Thus, $U_{\text{cube}} \otimes \operatorname{sgn} \simeq U_{\text{tet}}$. If $U_{\text{cube}} = V_1 \oplus V_2$, then

$U_{\text{tet}} = (V_1 \otimes \text{sgn}) \oplus (V_2 \otimes \text{sgn})$. However, U_{tet} is irreducible by Exercise 5.21 on p. 120.

Exercise 5.24 Show that every nonzero linear form $\varphi \in \text{Sym}^n(W)^*$ does not vanish identically on all of $w^{\otimes n}$. To this end, choose a basis $e_1, e_2, \dots, e_d$ in W, and let $w = \sum x_i e_i$ and $\varphi\big(e_{[m_1 m_2 \dots m_d]}\big) = a_{m_1 m_2 \dots m_d} \in \Bbbk$. Then

$$\varphi\left(w^{\otimes n}\right) = \sum_{m_1 m_2 \dots m_d} a_{m_1 m_2 \dots m_d} x_1^{m_1} x_2^{m_2} \cdots x_d^{m_d}.$$

Since $\Bbbk$ is infinite, this polynomial vanishes identically if and only if all its coefficients $a_{m_1 m_2 \dots m_d}$ are equal to 0.

Exercise 5.25 Let ψ be a linear form on $\text{Sym}^n(W)$ such that all $w^{\otimes n}$ with $F(w) \neq 0$ lie in the hyperplane $\text{Ann}\,\psi$. The function $G(w) = \psi(w^{\otimes})$ is a homogeneous polynomial of degree n on W. Since the product $F \cdot G$ is the zero function on W, it is the zero polynomial. This forces G to be the zero polynomial, because the polynomial F is not zero. Hence, $\psi(w^{\otimes}) \equiv 0$ for all $w \in W$. This contradicts Aronhold's principle.

Exercise 6.1 Since $\text{im}\,AB \subset \text{im}\,A = \text{im}(a \otimes \alpha) = \Bbbk \cdot a$, the trace $\text{tr}(AB)$ is equal to $AB(a) = a \cdot \alpha(b \cdot \beta(a)) = \alpha(b) \cdot \beta(a)$.

Exercise 6.2

$$(ga, b) = \text{tr}(L_{gab}) = \text{tr}(L_g \circ (L_a \circ L_b)) = \text{tr}((L_a \circ L_b) \circ L_g) = \text{tr}(L_{abg}) = (a, bg),$$

because $\text{tr}(AB) = \text{tr}(BA)$. If $I \subset \Bbbk[G]$ is a left ideal, then $I^\perp \subset \Bbbk[G]$ is an abelian subgroup, and for every $u \in I^\perp$, $x \in \Bbbk[G]$, $b \in I$, the equalities $(b, ux) = (xb, u) = 0$ hold, because $xb \in I$. Thus, $bx \in I^\perp$.

Exercise 6.3 In the bottom row are the traces of the identity map, axial symmetry, and rotation by 120°. The eigenvalues of these maps are, respectively, $(1, 1)$, $(1, -1)$, and (ω, ω^2), where $\omega^2 + \omega + 1 = 0$.

Exercise 6.4 Use the eigenvalues to compute the traces.

Exercise 6.5 Fix a basis of V consisting of eigenvectors of $\varrho(g)$ and write $\lambda_1, \lambda_2, \dots, \lambda_n$ for their eigenvalues. Then $\text{tr}\left(\Lambda^k \varrho(g)\right) = e_k(\lambda_1, \lambda_2, \dots, \lambda_n)$ and $\text{tr}\left(S^k \varrho(g)\right) = h_k(\lambda_1, \lambda_2, \dots, \lambda_n)$, where e_k and h_k are the elementary and complete symmetric polynomials. At the same time,

$$\det(1 + t\,\varrho(g)) = \prod(1 + \lambda_i t) = E(t)\,,$$
$$\det{}^{-1}(1 - t\,\varrho(g)) = \prod(1 - \lambda_i t)^{-1} = H(t)\,,$$

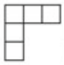
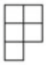
are the generating functions for these polynomials.

Exercise 6.6 In terms of $\Bbbk[G]$, the (commutative) multiplication of functions in $\Bbbk^G$ gives

$$\Big(\sum_{g\in G} x_g g\Big)\cdot\Big(\sum_{g\in G} y_g g\Big) = \sum_{g\in G}(x_g y_g)g\,,$$

whereas the (noncommutative) multiplication in $\Bbbk[G]$ takes a pair of functions $\varphi, \psi : G \to \Bbbk$ to their *convolution* $\varphi * \psi : G \to \Bbbk$, $g \mapsto \sum_{pq=g} \varphi(p)\psi(q)$.

Exercise 6.7 The group A_5 has one trivial irreducible representation of dimension 1, two irreducible representations of dimension 3 by the proper dodecahedral group,[3] and one 4-dimensional representation by the proper group of the regular simplex. Since $|\operatorname{Cl}(A_5)| = 5$ and $|A_5| = 60$, there should be one more irreducible representation, of dimension 5, in addition to those already listed, and its character should be orthogonal to all the other irreducible characters:

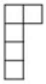
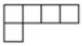
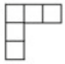
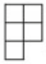
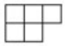
conjugacy class				$\lvert 12345\rangle$	$\lvert 21345\rangle$
its cardinality	1	20	15	12	12
values of characters:					
trivial	1	1	1	1	1
dodecahedral-1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
dodecahedral-2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
simplicial	4	1	0	-1	-1
5-dimensional	5	-1	1	0	0

Try to describe the 5-dimensional irreducible representation explicitly by means of the isomorphism $A_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ from Problem 12.33 of Algebra I. Besides the trivial and sign representations in dimension 1 and the simplicial representation Δ in dimension 4, the symmetric group S_5 has irreducible representations $\operatorname{sgn}\otimes\Delta$ and $\Lambda^2\Delta$ of dimensions 4 and 6. The symmetric square of the simplicial representation splits as $S^2\Delta = \operatorname{sgn}\oplus\Delta\oplus\zeta$, where ζ is an irreducible representation of dimension 5 provided by the action of $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$ on the harmonic quadruples of points[4]

[3] Different from each other by the composition with the outer automorphism of A_5 provided by conjugation by a transposition.

[4] Recall that an ordered quadruple of distinct points $a, b, c, d \in \mathbb{P}_1$ is called *harmonic* if the cross ratio $[a, b, c, d]$ equals -1, i.e., b is the midpoint of cd in the affine chart with $a = \infty$ (see Sect. 11.6 of Algebra I). Since every ordered triple of points is uniquely completed by the fourth point to the harmonic quadruple, and the same quadruple arises in this way from four different triples, there are altogether $\binom{6}{2}/4 = 5$ harmonic quadruples of points in $\mathbb{P}_1(\mathbb{F}_5)$. The tautological action of $\mathrm{PGL}_2(\mathbb{F}_5)$ on these quadruples gives an isomorphism $\mathrm{PGL}_2(\mathbb{F}_5) \xrightarrow{\sim} S_5$.

in $\mathbb{P}_1(\mathbb{F}_5)$. Thus, the complete table of irreducible characters of S_5 looks like this:

conjugacy class							
its cardinality	1	10	30	20	15	20	24
values of characters:							
trivial	1	1	1	1	1	1	1
sign, sgn	1	-1	-1	1	1	-1	1
simplicial, Δ	4	2	0	1	0	-1	-1
$\Delta \otimes \mathrm{sgn}$	4	-2	0	1	0	1	-1
$\Lambda^2\Delta$	6	0	0	0	-2	0	1
$\zeta \subset S^2\Delta$	5	1	-1	-1	1	1	0
$\zeta \otimes \mathrm{sgn}$	5	-1	1	-1	1	-1	0

Exercise 6.8 Fix some bases $u_1, u_2, \dots, u_n$ in U and $w_1, w_2, \dots, w_m$ in W. The component $\Lambda^\alpha U \otimes \Lambda^\beta W \subset \Lambda^k(U \oplus W)$ is spanned by the basis monomials $u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_\alpha} \wedge w_{j_1} \wedge w_{j_2} \wedge \cdots \wedge w_{j_\beta}$.

Exercise 6.11 For every extension $A \subset B$ of associative $\Bbbk$-algebras with unit, the canonical B-linear map $B \otimes_A A \to B$, which corresponds to the A-linear inclusion $A \hookrightarrow B$, is an algebra isomorphism.

Exercise 6.12 For every G-module M, there are canonical isomorphisms

$$\begin{aligned}\mathrm{Hom}_G(W \otimes \mathrm{ind}\, V, M) &\simeq \mathrm{Hom}_G(\mathrm{ind}\, V, W^* \otimes M) \simeq \mathrm{Hom}_H(V, \mathrm{res}(W^* \otimes M)) \\ &\simeq \mathrm{Hom}_H(V, \mathrm{res}(W)^* \otimes \mathrm{res}(M)) \simeq \mathrm{Hom}_H(\mathrm{res}(W) \otimes V, \mathrm{res}(M))\,.\end{aligned}$$

Therefore, the module $W \otimes \mathrm{ind}\, V$ has the universal property from Proposition 6.3 on p. 141 written for $\mathrm{res}(W) \otimes V$, M in the roles of V, W. By Exercise 6.9 on p. 142, this forces $W \otimes \mathrm{ind}\, V \simeq \mathrm{ind}\big((\mathrm{res}\, W) \otimes V\big)$.

Exercise 6.15 Fix representatives $\{g_1, g_2, \dots, g_r\}$ for the cosets of G/H. Then

$$G = g_1 H \sqcup c \dots \sqcup g_r H = H g_1^{-1} \sqcup \cdots \sqcup H g_r^{-1}\,,$$

and every H-linear operator $\varphi : \Bbbk[G] \to V$ is uniquely determined by the s vectors $v_\nu = \varphi\left(g_\nu^{-1}\right) \in V$, because $\varphi\left(h g_\nu^{-1}\right) = h v_\nu$ for all $h \in H$. Hence,

$$\dim \mathrm{Hom}_H(\Bbbk[G], V) = [G : H] \cdot \dim V = \dim \Bbbk[G] \otimes_{\Bbbk[H]} V\,.$$

The Fourier transform maps an H-linear operator $\varphi : g_\nu^{-1} \mapsto v_\nu$ to the tensor

$$\frac{1}{|G|}\sum_{g\in G} g^{-1} \otimes_{\Bbbk[H]} \varphi(g) = \frac{1}{|G|}\sum_{\nu}\sum_{h\in H} g_\nu h^{-1} \otimes_{\Bbbk[H]} \varphi\left(hg_\nu^{-1}\right)$$
$$= \frac{|H|}{|G|}\sum_{\nu} g_\nu v_\nu \in \bigoplus_{\nu} g_\nu V\,.$$

This tensor equals zero if and only if all v_ν are equal to 0. Thus, the Fourier transform is injective on $\mathrm{Hom}_H(\Bbbk[G], V)$ and therefore bijective for dimensional reasons.

Exercise 7.4 To prove transitivity, write $T \succ_a U$ if $T \succ U$ and the maximal element in different cells of T, U equals a. Let $T \succ_a U$ and $U \succ_b W$. Then $T \succ_a W$ for $a \geqslant b$, and $T \succ_b W$ for $a \leqslant b$.

Exercise 7.5 For all $q \in R_T$, $p \in C_U$, the strict inequality $pU \succ qT$ holds. By Lemma 7.1, there exists a transposition $\tau \in R_U \cap C_T$. The computation from formula (7.12) on p. 159 shows that $c_T\{U\} = 0$.

Exercise 7.6 Let $H' = \psi(H)$, $H'' = \varphi(H)$, and $g_i'H'$, $1 \leqslant i \leqslant r$, be the distinct left cosets of H'. Then $g_i''H''$, $1 \leqslant i \leqslant r$, with $g_i'' = gg_i'g^{-1}$ are the distinct left cosets of H'', and the conjugation map $\mathrm{Ad}_g : x \mapsto gxg^{-1}$ takes $g_i'H'$ to $g_i''H_i''$ bijectively and transfers the right multiplication by $h' \in H'$ in $g_i'H'$ to the right multiplication by $ghg^{-1} \in H''$ in $g_i''H_i''$. Therefore, the G-linear isomorphism between $\Bbbk[G] \otimes_{\Bbbk[H']} V = \sum_i g_i'V$ and $\Bbbk[G] \otimes_{\Bbbk[H'']} V = \sum_i g_i'V$ is well defined by the assignment $g' \otimes v \mapsto \mathrm{Ad}_g(g') \otimes v$.

Exercise 7.8 Every difference $\eta_i - \eta_j$ divides the determinant in the polynomial ring $\mathbb{Z}[\eta_1, \eta_2, \dots, \eta_n]$, because the determinant vanishes for $\eta_i = \eta_j$. Thus, $\prod_{i<j}(\eta_i - \eta_j)$ divides the determinant as well. Comparison of the lexicographically leading terms shows that the result of division equals 1.

Exercise 7.9 Use induction on λ_1 to show that the product of the hook lengths for all cells in a Young diagram λ is equal to $\prod_i \eta_i!/\prod_{i<j}(\eta_i - \eta_j)$, where $\eta = \lambda + \delta$. During the induction step, remove the first column and take into account that the hook lengths of the cells in the first column are $\eta_i - n + \ell$, where $\ell = \ell(\lambda)$ is the length of λ (the total number of rows). Then use the Frobenius formula from Corollary 7.7 on p. 169.

Exercise 8.5 The first statement obviously holds for the decomposable (that is, of rank one) operators $U \to W$; the second follows from the Jacobi identity.

Exercise 8.6 The line $E + tA$ touches the quadric $\det X = 1$ at the point E if and only if the quadratic trinomial $\det(E + tA) - 1 = \det(A) \cdot t^2 + \mathrm{tr}(A) \cdot t$ has a double root at zero.

Exercise 8.8 If $V = \Bbbk\cdot e_1 \oplus \Bbbk\cdot e_2 \oplus \cdots \oplus \Bbbk\cdot e_n$, then $\overline{\Bbbk} \otimes V \simeq \overline{\Bbbk}\cdot e_1 \oplus \overline{\Bbbk}\cdot e_2 \oplus \cdots \oplus \overline{\Bbbk}\cdot e_n$ by the distributivity isomorphism from Proposition 1.3 on p. 12.

Exercise 8.9 This is a version of the Jacobi identity:

$$\begin{aligned}\mathrm{ad}_{[X,Y]}(Z) &= [[X,Y],Z] - [Z,[X,Y]] = [X,[Y,Z]] + [Y,[Z,X]] \\ &= \mathrm{ad}_X\,\mathrm{ad}_Y(Z) - \mathrm{ad}_Y\,\mathrm{ad}_X(Z)\,.\end{aligned}$$

Exercise 8.10 This follows from the previous exercise and the Jacobi identity for the commutators in an associative algebra.

Exercise 8.15 Let W be an $\mathfrak{sl}_2$-module. The identification of $\Lambda^2 W$ with the space of skew-symmetric bilinear forms on W^* maps a decomposable bivector $u \wedge v \in \Lambda^2 W$ to the form[5]

$$W^* \times W^* \to \Bbbk\,, \quad \varphi, \psi \mapsto \frac{1}{2}\big(\langle\, u\,,\varphi\,\rangle\,\langle\, w\,,\psi\,\rangle - \langle\, u\,,\psi\,\rangle\,\langle\, w\,,\varphi\,\rangle\big)\,,$$

where $\langle\, *\,,*\,\rangle$ means the contraction between vectors and covectors. Check that this identification transfers the action of an element $Z \in \mathfrak{sl}_2$ on $\Lambda^2 W$ by the Leibniz rule

$$u \wedge v \mapsto (Zu) \wedge v + u \wedge (Zv)$$

to the action of Z on the space of bilinear forms on W^* by the rule

$$\omega(\varphi,\psi) \mapsto Z\omega(\varphi,\psi) = \omega(Z\varphi,\psi) + \omega(\varphi,Z\psi)\,,$$

where $Z\varphi$, $Z\psi$ mean the actions of Z on W^* in accordance with formula (8.2) on p. 175.

Exercise 9.2 Let an order-preserving map $\varphi : [n] \to [m]$ be factorized as

$$\varphi = \partial_m^{m-\alpha}\,\partial_{m-1}^{m-\alpha-1} \cdots \partial_{\alpha+1}^{j_1} s_\alpha^{i_{n-\alpha}} \cdots s_{n-2}^{i_2} s_{n-1}^{i_1}\,, \tag{14.1}$$

with $i_1 < i_2 < \cdots < i_{n-\alpha}$ and $j_1 < j_2 < \cdots < j_{m-\alpha}$, and let the collections $k_1, k_2, \dots, k_\alpha$ and $\ell_0, \ell_1, \dots, \ell_\alpha$ be complementary to $i_1, i_2, \dots, i_{n-\alpha}$ and $j_1, j_2, \dots, j_{m-\alpha}$ respectively. Then φ maps the elements $0, \dots, k_1$ to ℓ_0, $k_1+1, \dots, k_2$ to $\ell_1, \dots$, $k_\alpha+1, \dots, n$ to ℓ_α, and this assignment completely determines the map φ. Thus, every $\varphi \in \mathrm{Hom}_\Delta([n],[m])$ has the unique factorization (14.1), and therefore, the arrows (9.3)–(9.5) generate the algebra $\mathbb{Z}[\Delta]$. Verify the relations

$$\partial_{n+1}^j \partial_n^i = \partial_{n+1}^i \partial_n^{j-1} \quad \text{for } i<j\,, \qquad s_n^j s_{n+1}^i = s_n^i s_{n+1}^{j+1} \quad \text{for } i \leqslant j\,,$$

$$s_{n-1}^j \partial_n^i = \begin{cases} \partial_{n-1}^i s_{n-2}^{j-1} & \text{for } i<j\,,\\ e_{n-1} & \text{for } i = j, j+1\,,\\ \partial_{n-1}^{i-1} s_{n-2}^j & \text{for } i > j+1\,,\end{cases}$$

[5] See Sect. 2.6 on p. 45.

and prove that they allow us to rewrite every word consisting of the letters ∂_n^i, s_m^j in the form given on the right-hand side of (14.1). This forces every polynomial relation on the letters ∂_n^i, s_m^j in $\mathbb{Z}[\Delta]$ to fall in the two-sided ideal generated by the above relations.

Exercise 9.6 The typical answer "$\ln|x| + C$, where C is an arbitrary constant" is *incorrect*. Actually, C is a section of the *constant sheaf* $\mathbb{R}^{\sim}$ over the open set $\mathbb{R}\setminus\{0\}$.

Exercise 9.10 Expand the definitions of equivalence of categories and isomorphism of functors.

Exercise 9.11 The functor $h_{\Bbbk}$ is quasi-inverse to itself, because of the canonical isomorphism $V^{**} \xrightarrow{\sim} V$. A quasi-inverse to the functor $h_{[1]} : \Delta_{\text{big}}^{\text{opp}} \to \nabla_{\text{big}}$ is the functor $h_{[1]} : \nabla_{\text{big}}^{\text{opp}} \to \Delta_{\text{big}}$ from Example 9.11 on p. 196.

Exercise 9.13 An element $a \in F(A)$ corresponds to the natural transformation $f_X : \text{Hom}(A,X) \to F(X)$ that sends an arrow $\varphi : A \to X$ to the value of the map $F(\varphi) : F(A) \to F(X)$ at the element a. The inverse correspondence takes a natural transformation f to the value of the map $f_A : h^A(A) \to F(A)$ at the identity endomorphism $\text{Id}_A \in h^A(A)$. This is verified by means of the following commutative diagram provided by every arrow $\varphi : A \to X$:

$$\begin{tikzcd} h^A(A) = \text{Hom}(A,A) \arrow[r, "h^A(\varphi)"] \arrow[d, "f_A"'] & \text{Hom}(A,X) = h^A(X) \arrow[d, "f_X"] \\ F(A) \arrow[r, "F(\varphi)"] & F(X) \end{tikzcd} \tag{14.2}$$

Its upper horizontal map sends Id_A to φ, and therefore $f_X(\varphi) = F(\varphi)\big(f_A(\text{Id}_A)\big)$.

Exercise 9.18 Use the universal property of the tensor product of $\mathbb{Z}$-modules and the fact that for every pair of ring homomorphisms $\varphi : A \to C$, $\psi : B \to C$, the map $A \times B \to C$, $(a,b) \mapsto \varphi(a)\psi(b)$, is $\mathbb{Z}$-bilinear.

Exercise 9.19 Use the universal property of free groups and Proposition 13.2 from Algebra I.

Exercise 9.20 See Lemma 14.1 from Algebra I.

Exercise 9.28 In $\mathcal{S}et$ and $\mathcal{T}op$, $\mathbb{I} = \varnothing$, whereas $\mathbb{T}$ is the one-point set. The categories $\mathcal{A}b$, $\mathcal{M}od_K$, R-$\mathcal{M}od$, $\mathcal{G}rp$, $\mathcal{C}mr$ have the zero objects, whose underlaying group is exhausted by the identity element, i.e., the zero abelian group, the zero module, the trivial group, and the zero ring. In the category $\mathcal{P}re\mathcal{S}h(X)$ of presheaves of sets on a topological space X, the initial object $\mathbb{I}$ is the empty presheaf with the empty sets of sections over all open sets, whereas $\mathbb{T}$ is the constant presheaf provided by the one-point set. The category of presheaves of abelian groups has the zero element, the constant presheaf provided by the zero group.

Exercise 9.29 The coproduct of an arbitrary family of spaces X_ν is still their disjoint union, where every X_ν appears with its original topology. The topology on the product $P = \prod X_\nu$ should be the coarsest one for which all the canonical maps

$P \to X_\nu$ are continuous. It is called the *Tikhonov topology* or the *product topology*, and its base of open sets consists of products $\prod U_\nu$, where $U_\nu \subset X_\nu$ and $U_\nu \neq X_\nu$ for only finitely many ν.

Exercise 9.30 In dealing with coequalizers, use the fact that every map $\xi : Y \to Z$ provides Y with the equivalence relation $R_\xi = \{(y_1, y_2) \mid \xi(y_1) = \xi(y_2)\}$, and a map $\xi' : Y \to Z'$ is factorized as $\xi' = \eta \circ \xi$ for some $\eta : Z \to Z'$ if and only if $R_\xi \subset R_{\xi'}$.

Exercise 9.33 Given a diagram of groups $G \xleftarrow{\xi} K \xrightarrow{\eta} H$, the amalgamated product $G *_K H = G*H/N$ is the quotient of the free product[6] $G*H$ by the smallest normal subgroup N containing all the products $\xi(k)\eta^{-1}(k)$, $k \in K$. A diagram of commutative rings $A \xleftarrow{\xi} K \xrightarrow{\eta} B$ equips A, B with K-algebra structures. The pushforward $A \otimes_K B$ is the tensor product over K from Sect. 9.5.1 on p. 206, that is, the quotient of the tensor product of abelian groups $A \otimes B$ by the subgroup generated by all the differences $(ka)\otimes b - a \otimes (kb)$ with $a \in A$, $b \in B$, $k \in K$. The multiplication in $A \otimes_K B$ is defined by the rule $(a_1 \otimes_K b_1) \cdot (a_2 \otimes_K b_2) \overset{\text{def}}{=} (a_1 a_2) \otimes_K (b_1 b_2)$.

Exercise 9.34 Reflexivity and symmetry are obvious. To prove transitivity, let $x_\alpha \sim x_\beta \sim x - \gamma$. Then there exists a (not necessarily commutative) diagram in $\mathcal{F}$,

$$\begin{tikzcd}
& & \varepsilon & & \\
& & \delta \arrow[u, "\xi"] & & \\
& \eta \arrow[ur, "\psi_{\delta\eta}"] & & \zeta \arrow[ul, "\psi_{\delta\zeta}"'] & \\
\alpha \arrow[ur, "\varphi_{\eta\alpha}"] & & \beta \arrow[ul, "\varphi_{\eta\beta}"'] \arrow[ur, "\varphi_{\zeta\beta}"] & & \gamma \arrow[ul, "\varphi_{\zeta\gamma}"']
\end{tikzcd}$$

such that $x_\eta = X(\varphi_{\eta\alpha})\, x_\alpha = X(\varphi_{\eta\beta})\, x_\beta = x_\eta$ and $x_\zeta = X(\varphi_{\zeta\beta})\, x_\beta = X(\varphi_{\zeta\gamma})\, x_\gamma = x_\zeta$ in $\mathcal{S}et$, whereas $\xi\psi_{\delta\eta}\varphi_{\eta\beta} = \xi\psi_{\delta\zeta}\varphi_{\zeta\beta}$ in $\mathrm{Hom}_{\mathcal{F}}(\beta, \varepsilon)$. Write $\varkappa$ for the arrow on the both sides of the latter equality. Then $X(\varepsilon\psi_{\delta\eta}\varphi_{\eta\alpha})\, x_\alpha = X(\varkappa)x_\beta = X(\varepsilon\psi_{\delta\zeta}\varphi_{\zeta\gamma})\, x_\gamma$, which means that $x_\alpha \sim x_\gamma$. Checking the universal property is straightforward.

Exercise 9.35 For every $s, t \in S$, the arrows $s : t \to ts$ and $t : s \to st$ have the common target $ts = st$. If $as = bs$, then the arrows $as : s \mapsto as^2$ and $bs : s \mapsto as^2$ are equal.

Exercise 10.1 It is enough to construct such a ring $C \supset B$ for one monic polynomial $f \in B[x]$ of positive degree. Under these assumptions, the quotient ring

[6] See Example 9.14 on p. 204.

$D = B[x]/(f)$ contains B as the subring formed by the residue classes of constant polynomials. Write $\vartheta \in D$ for the residue class $x \pmod f$. Then $f(\vartheta) = 0$, and therefore f is divisible by $(x - \vartheta)$ in $D[x]$. The quotient of this division is a monic polynomial of degree $\deg f - 1$. Induction on $\deg f$ allows one to construct a ring $C \supset D$ over which the quotient becomes completely factorizable. (Compare with the proof of Theorem 3.1 from Algebra I.)

Exercise 10.2 Since ξ is algebraic over $\mathbb{Q}$, it satisfies a polynomial equation $a_0\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0$ with integer coefficients $a_i \in \mathbb{Z}$. Then $\zeta = a_0\xi$ is integral over $\mathbb{Z}$, because $\zeta^n = -a_1 \cdot \zeta^{n-1} - a_0a_2 \cdot \zeta^{n-2} - \cdots - a_0^{n-1}a_n$.

Exercise 10.3 If z is integral over $\mathbb{Z}$, then in every basis of O_K over $\mathbb{Z}$, which simultaneously is a basis of K over $\mathbb{Q}$, multiplication by $\mathbb{Z}$ has an integer matrix. Conversely, if multiplication by z has an integer matrix $Z \in \mathrm{Mat}_d(\mathbb{Z})$, then z is a root of the monic polynomial $\det(tE - Z) \in \mathbb{Z}[t]$ by the Cayley–Hamilton theorem.

Exercise 10.5 If $\mathbb{Q}\left[\sqrt{d_1}\right] \simeq \mathbb{Q}\left[\sqrt{d_2}\right]$, then

$$d_2 = \left(a + b\sqrt{d_1}\right)^2 = a^2 + d_1b^2 + 2ab\sqrt{d_1}$$

for some $a, b \in \mathbb{Q}$, and therefore, $ab = 0$ and $a^2 + d_1b^2 = d_2$. This forces $a = 0$, $b = 1$, $d_1 = d_2$.

Exercise 10.8 Since this submodule of $\mathbb{Q}$ has no torsion, it is free of finite rank, and its submodule spanned by q^n inherits this property.

Exercise 10.9 Show that $(\chi_W, \chi_W)_{G^n} = (\chi_V, \chi_V)_G^n$.

Exercise 11.1 An algebra homomorphism $\varphi : \mathrm{Spec_m}\, \Bbbk[x_1, x_2, \dots, x_n] \to \Bbbk$ is uniquely determined by the images of generators $p_i = \varphi(x_i) \in \Bbbk$. Mapping

$$\varphi \mapsto (p_1, p_2, \dots, p_n)$$

establishes the required bijection. Note that this means that every maximal ideal in $\Bbbk[x_1, x_2, \dots, x_n]$ is generated by some n linear forms $x_i - p_i, p_i \in \Bbbk$, $1 \leqslant i \leqslant n$, and the equality of ideals $(x_1 - p_1, \dots, x_n - p_n) = (x_1 - q_1, \dots, x_n - q_n)$ is equivalent to the equality of points $(p_1, p_2, \dots, p_n) = (q_1, q_2, \dots, q_n)$ in the affine space $\Bbbk^n$.

Exercise 11.2 If $a^n = 0$ and $b^m = 0$, then $(a + b)^{m+n-1} = 0$ and $(ca)^n = 0$ for all c.

Exercise 11.3 Since $A/\mathfrak{p}$ has no zero divisors for all prime $\mathfrak{p} \subset A$, every factorization map $A \twoheadrightarrow A\mathfrak{p}$ by a prime $\mathfrak{p}$ annihilates all the nilpotents. Thus, $\mathfrak{n}(A) \subset \bigcap \mathfrak{p}$. Conversely, let $a \in A$ be nonnilpotent. Then all nonnegative integer powers a^m form the multiplicative system A. Write $A[a^{-1}]$ for the localization[7] by this system. This is a nonzero ring.[8] The full preimage of every prime ideal[9]

[7]See Sect. 4.1.1 of Algebra I.

[8]Which may be a field.

[9]Which is zero if $A[a^{-1}]$ is a field.

$\mathfrak{m} \subset A[a^{-1}]$ under the canonical homomorphism $A \to A[a^{-1}]$ is a prime ideal of A that does not contain a.

Exercise 11.5 The homomorphisms $\Bbbk[X] \times \Bbbk[Y] \twoheadrightarrow \Bbbk$ are in bijection with the pairs of homomorphisms $\Bbbk[X] \twoheadrightarrow \Bbbk$, $\Bbbk[Y] \twoheadrightarrow \Bbbk$. One of many ways of thinking about the second question is to assume that $n \leqslant m$ and realize X, Y by explicit equations within two different hyperplanes $\mathbb{A}^m \times \{a\}$, $\mathbb{A}^m \times \{b\}$, $a \neq b$, in the affine space $\mathbb{A}^{m+1} = \mathbb{A}^m \times \mathbb{A}^1$. Then take all pairwise products of these equations (including those linear equations that cut the hyperplanes $\mathbb{A}^m \times \{a\}$, $\mathbb{A}^m \times \{b\}$ out of $\mathbb{A}^{m+1}$).

Exercise 11.6 Since $(a_1a_2) \otimes (b_1b_2)$ is linear in each of four elements, the prescription $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) \stackrel{\text{def}}{=} (a_1a_2) \otimes (b_1b_2)$ can be extended to a $\Bbbk$-bilinear map $(A \otimes B) \times (A \otimes B) \to A \otimes B$ that provides $A \otimes B$ with a commutative associative binary operation (it is enough to verify both properties on decomposable tensors). The required universal properties of maps $A \xrightarrow{\alpha} A \otimes B \xleftarrow{\beta} B$ follow from the universal properties of the tensor product of vector spaces. Namely, for every two homomorphisms $\varphi : A \to C$, $\psi : B \to C$ of $\Bbbk$-algebras with unit, the bilinear map $A \times B \to C$, $(a, b) \mapsto \varphi(a) \cdot \psi(b)$, can be uniquely passed through the tensor product $A \otimes B$.

Exercise 11.7 Take the union of the equations $f_\nu(x) = 0$, $g_\mu(y) = 0$, each considered as an equation on the whole set of coordinates (x, y) in $\mathbb{A}^n \times \mathbb{A}^m$.

Exercise 11.8 The equalities (a), (b), (c), and the inclusions

$$V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ) \subset V(I) \cup V(J)$$

in (d) follow immediately from the definitions. Note that the coincidence $V(I \cap J) = V(IJ)$ is equivalent to the equality of radicals $\sqrt{I \cap J} = \sqrt{IJ}$, which can be easily verified independently.

Exercise 11.9 Let $X \subset \mathbb{A}^n, f \in \Bbbk[x_1, x_2, \dots, x_n]$. If $V(f) = X$, then $f \in I(X)$, and therefore, the class of f in $\Bbbk[X]$ equals zero. If $V(f) = \varnothing$, then the ideal spanned in $\Bbbk xn$ by f and $I(X)$ has empty zero set and therefore contains the unit. Hence, $1 \equiv fg \pmod{I(X)}$ for some $g \in \Bbbk[x_1, x_2, \dots, x_n]$. Thus, the classes of f and g are inverse to each other in $\Bbbk[X]$.

Exercise 11.10 Otherwise, we would have $X = (X \smallsetminus U) \cup V(f - g)$. More scientifically, this holds because f and g are continuous and U is dense.

Exercise 11.11 $Y = (Y \cap Z) \cup \overline{Y \smallsetminus Z}$, where the first subset of Y is proper by the assumption.

Exercise 11.14 Let $V = U_1 \cup U_2 \cup \cdots \cup U_m$. For every i, choose a nonzero linear form $\xi_i \in V^*$ annihilating U_i. Then $f = \prod_{i=1}^m \xi_i \in S^m V^*$ is the nonzero polynomial on V that evaluates to zero at every point of $\mathbb{A}(V)$. This is impossible over an infinite ground field.

Exercise 11.16 Both rings consist of the same fractions considered modulo the same equivalences of fractions.

Exercise 11.17 Use the open covering $U = \bigcup \mathcal{D}(x_i)$ and Proposition 11.6.

Exercise 11.18 Every intersection $I \cap I(X_i)$ is a proper vector subspace of I, because if $I \subset I(X_\nu)$, then $X_\nu \subset \bigcup_{i \neq j}(X_i \cap X_j)$, and therefore $X_\nu \subset X_i \cap X_j$ for some $i \neq j$, although such inclusions are forbidden. If the $\Bbbk$-linear span of $I \cap \Bbbk[X]^\circ$ is proper too, then I splits into a finite union of proper vector subspaces.

Exercise 11.21 Let $A = \Bbbk[X]$, $B = \Bbbk[Y]$. The inclusion $\varphi^* : B \hookrightarrow A$ provides A with the structure of a finitely generated B-algebra. This allows us to rewrite A as $A \simeq B[x_1, x_2, \dots, x_m]/J$. Then $\psi^* : B[x_1, x_2, \dots, x_m] \twoheadrightarrow A$ is the quotient homomorphism, and $\pi^* : B \hookrightarrow B[x_1, x_2, \dots, x_m]$ is the inclusion of constants into the polynomial ring.

Exercise 11.22 Put $B = \Bbbk[Z]$, $A = \varphi^*(\Bbbk[Y]) \simeq \Bbbk[Y]$ (recall that $\varphi^* : \Bbbk[Y] \hookrightarrow \Bbbk[Z]$ is injective, because φ is dominant).

Exercise 12.2 If $x_i x_j \neq 0$, then $t_{j,\nu} = x_\nu/x_j = (x_\nu : x_i)\,/\,\big(x_j : x_i\big) = t_{i,\nu}/t_{i,j}$ (for $\nu = i$, we put $t_{i,i} = 1$). Therefore, $\varphi_{ji}^* : t_{j,\nu} \mapsto t_{i,\nu}/t_{i,j}$. The homomorphism

$$\Bbbk\left[\mathcal{D}\left(t_{i,j}\right)\right] \to \Bbbk\left[\mathcal{D}\left(t_{j,i}\right)\right]$$

inverse to φ_{ji}^* acts by the same rule $t_j^{(i)} \mapsto 1/t_i^{(j)}$, $t_{i,\nu} \mapsto t_{j,\nu}/t_{j,i}$.

Exercise 12.3 Every such W has a unique basis $w_1, w_2, \dots, w_k$ projected onto

$$e_{i_1},\ e_{i_2},\ \dots,\ e_{i_k}\,.$$

Write x_W for the matrix formed by the coordinates of vectors $w_1, w_2, \dots, w_k$ written in rows. Then $s_I\,(x_W) = E$.

Exercise 12.5 Note that the elements of the $k \times m$ matrix $s_J^{-1}\,(\varphi_I(t)) \cdot \varphi_I(t)$ are rational functions of the elements of the matrix t with denominators equal to $\det s_J\,(\varphi_I(t))$. In particular, they are all regular in $\mathcal{D}\,(\det s_J\,(\varphi_I(t)))$.

Exercise 12.6 This follows from the definition of regular function and Remark 11.3 on p. 255.

Exercise 12.9 The definition of $\varkappa$ can be rewritten as

$$(x_0 : x_1 : x_2) \mapsto (x_1 x_2 : x_0 x_2 : x_0 x_1)\,.$$

This makes clear that $\varkappa$ is undefined only at the points $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$ and takes all values except for these points.

Exercise 12.10 Given a homogeneous polynomial $\overline{f}(x_0, x_1, \dots, x_n)$, write

$$Z(f) \subset \mathbb{P}_n$$

for the set of its zeros. In the notation of Example 12.1 on p. 266, the intersection $Z(f) \cap U_i$ is described in terms of the affine coordinates t_i within the chart U_i by the polynomial equation $\overline{f}\,(t_{i,0}, \dots, t_{i,i-1}, 1, t_{i,i+1}, \dots, t_{i,n}) = 0$.

Exercise 12.12 Use the Segre embedding $\mathbb{P}_{n_1} \times \mathbb{P}_{n_2} \times \cdots \times \mathbb{P}_{n_m} \hookrightarrow \mathbb{P}_N$ described in Example 2.8 on p. 50 and analyzed in more detail in Example 2.8 on p. 50.

Exercise 12.14 If $A \subset B$ and $B \supset C$ are two integral extensions of commutative rings, then the extension $A \subset C$ is integral as well by Proposition 10.1 on p. 228.

Exercise 12.16 Let $X_1, X_2 \subset X$ be two closed irreducible subsets, and $U \subset X$ an open set such that both intersections $X_1 \cap U$, $X_2 \cap U$ are nonempty. Then $X_1 = X_2$ if and only if $X_1 \cap U = X_2 \cap U$, because $X_i = \overline{X_i \cap U}$.

Exercise 12.17 Check that the product of finite surjections $X \to \mathbb{A}^n$, $Y \to \mathbb{A}^m$ gives the finite surjection $X \times Y \to \mathbb{A}^n \times \mathbb{A}^m$.

Exercise 12.18 Chose some basis in H and write the coordinates of the basis vectors together with the coordinates of a variable point $p \in \mathbb{P}_n$ as the rows of an $(n-d+1)\times(n+1)$-matrix. Then the condition $p \in H$ is equivalent to the vanishing of all the minors of maximal degree $n-d+1$ in this matrix, which are quadratic bilinear polynomials in the homogeneous coordinates of p and the Plücker coordinates.[10]

Exercise 12.20 The set $\Gamma \subset \mathbb{P}_{N_0} \times \cdots \times \mathbb{P}_{N_n} \times \mathbb{P}_n$ is given by the equations

$$f_0(p) = f_1(p) = \cdots = f_n(p) = 0$$

in $f_i \in \mathbb{P}_{N_i}$ and $p \in \mathbb{P}_n$, linear and homogeneous in each f_i and homogeneous of degrees d_i in p.

Exercise 12.21 Take $n+1$ hyperplanes having one common point and exponentiate their (linear) equations in the prescribed degrees.

Exercise 12.22 Consider the product $\mathbb{P}_{n_1} \times \mathbb{P}_{n_2} \times \cdots \times \mathbb{P}_{n_m}$ and write

$$x^{(i)} = \left(x_0^{(i)} : x_1^{(i)} : \cdots : x_{n_i}^{(i)}\right)$$

for the set of homogeneous coordinates in the ith factor $\mathbb{P}_{n_i}$. Modify the proof of Lemma 12.1 on p. 273 to show that every closed submanifold

$$Z \subset \mathbb{P}_1 \times \mathbb{P}_2 \times \cdots \times \mathbb{P}_m$$

can be described by an appropriate system of global polynomial equations

$$f_\nu\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right) = 0\,,$$

homogeneous in every group of variables $x^{(i)}$. Then assume that Z is irreducible of codimension 1, show that there exists an irreducible polynomial

$$q\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right)$$

vanishing on Z, and use a dimensional argument to check that $Z = Z(q)$ is the zero set of q. Finally, use the strong Nullstellensatz to show that for irreducible polynomials q_1, q_2, the equality $Z(q_1) = Z(q_2)$ forces q_1, q_2 to be proportional.

[10]Recall that they equal the highest-degree minors of the transition matrix from some basis in H to the standard basis in V; see Example 12.5 on p. 272.

Exercise 12.23 Identify $\mathrm{Gr}(2,4)$ with the Plücker quadric $P \subset \mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$ by sending a line $(a,b) \subset \mathbb{P}_3$ to the point $a \wedge b \in \mathbb{P}_5$. The line (a,b) lies on the surface $V(f) \subset \mathbb{P}_3$ if and only if the polynomial f vanishes identically on the linear span of vectors a, b, which is the linear support of the Grassmannian polynomial $a \wedge b$ and coincides with the image of the map $V^* \to V$, $\xi \mapsto \xi \llcorner (a \wedge b)$, contracting a covector $\xi \in V^*$ with the first tensor factor of $(a \otimes b - b \otimes a)/2 \in \mathrm{Alt}^2 V$. Verify that the identical vanishing of the function $\xi \mapsto f(\xi \llcorner (a \wedge b))$ can be expressed by a system of bihomogeneous equations in the coefficients of f and the Plücker coordinates x_{ij} of the bivector $a \wedge b = \sum_{0 \leqslant i < j \leqslant 3} x_{ij} e_i \wedge e_j$.

Exercise 13.5 By Gauss's lemma, it is enough to check that f is irreducible in the ring $\mathbb{F}_p[t][x]$. Apply the Eisenstein criterion modulo the prime element $t \in \mathbb{F}_p[t]$.

Exercise 13.6 Every chain $\mathbb{L}_\nu$ in S is bounded above by the union $\bigcup_\nu \mathbb{L}_\nu$.

Exercise 13.8 For the minimal $f_* \in \Bbbk[x]$, put $\mathbb{K}_f$ as the splitting field of f over $\Bbbk$. Assume that $\mathbb{K}_g$ exists for all $g < f$, and put $\mathbb{K}_f$ as the splitting field of f over the field $\bigcup_{g<f} \mathbb{K}_g$.

Exercise 13.11 The linear span of the products $\vartheta_1\vartheta_2 \cdots \vartheta_m$ is a $\Bbbk$-algebra without zero divisors algebraic over $\Bbbk$. Therefore, it is a field by Proposition 10.3 on p. 229.

Exercise 13.13 The roots of the polynomial $x^{p^n} - x$ in the field $\mathbb{F}_{p^n}$ split into a disjoint union of orbits of the Galois group $G = \mathrm{Aut}\,\mathbb{F}_{p^n} \simeq \mathbb{Z}/(n)$. The length m of every such orbit $\alpha_1, \alpha_2, \ldots, \alpha_m$ divides n by the orbit length formula,[11] and the product $\prod(x - \alpha_i)$ is a monic irreducible polynomial with coefficients in $\mathbb{F}_{p^n}^G = \mathbb{F}_p$. Since the polynomial $x^{p^n} - x$ is separable, we conclude that its irreducible decomposition in $\mathbb{F}_p[x]$ consists of distinct monic irreducible factors whose degrees divide n. On the other hand, a monic irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree m divides $x^{p^n} - x$ if and only if g has a root in the splitting field $\mathbb{F}_{p^n}$ of the polynomial $x^{p^n} - x$. The latter is equivalent to the existence of an embedding $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$. Such an embedding exists if and only if $m \mid n$.

Exercise 14.1 Since addition, multiplication, subtraction, division, and taking square roots in $\mathbb{C}$ is completely reduced to the same operations applied separately to the real and imaginary parts, which can be constructed by straightedge and compass, and since a complex number can be recovered from its real and imaginary parts with straightedge and compass, the numbers a, b can be assumed to be real. Then $a \pm b$ are constructed straightforwardly, while the constructions of a/b, ab, and $\sqrt{a} = \sqrt{1 \cdot a}$ require a segment of length 1 and are shown in Figs. 14.1, 14.2, and 14.3.

[11] See Proposition 12.2 of Algebra I.

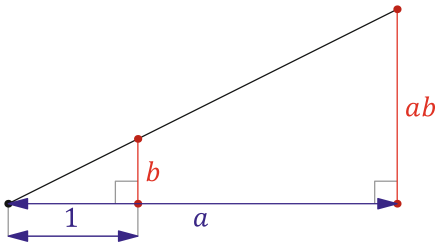


Fig. 14.1 Construction of ab

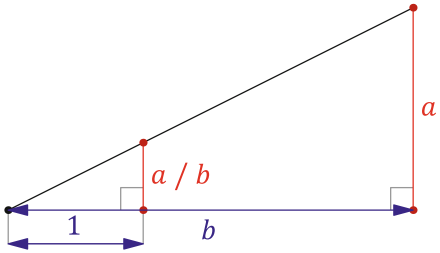


Fig. 14.2 Construction of a/b

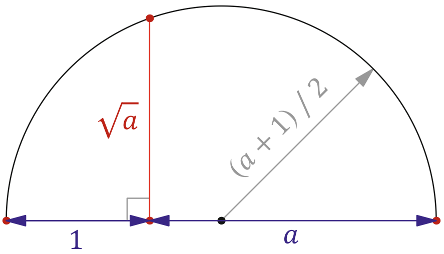


Fig. 14.3 Construction of $\sqrt{a}$

Exercise 14.2 Let $|G| = 2^n$. Use induction on n. By Proposition 13.6 from Algebra I, G has a nontrivial center $C \lhd G$, which is a normal abelian 2-subgroup. Use the description of abelian groups from Theorem 14.5 of Algebra I to construct a series of abelian groups

$$C = C_0 \supset C_1 \supset \cdots \supset C_{k-1} \supset C_k = \{e\}$$

with $C_i/C_{i+1} \simeq \mathbb{Z}/(2)$. By induction, the quotient group G/C admits a filtration

$$G/C = Q_0 \supset Q_1 \supset \cdots \supset Q_{\ell-1} \supset Q_\ell = \{e\}$$

with $Q_{i+1} \lhd Q_i$ and $Q_i/Q_{i+1} \simeq \mathbb{Z}/(2)$. Combining the filtrations on C and G/C leads to the filtration

$$G = CQ_0 \supset CQ_1 \supset \cdots \supset CQ_{\ell-1} \supset C \supset C_1 \supset \cdots \supset C_{k-1} \supset C_k = \{e\},$$

where $CQ_i \subset G$ are the preimages of the subgroups $Q_i \subset G/C$ under the factorization epimorphism $G \twoheadrightarrow G/C$. Then

$$CQ_i/CQ_{i+1} \simeq (CQ_i/C)\,/\,(CQ_{i+1}/C) \simeq Q_{i+1}/Q_i \simeq \mathbb{Z}/(2).$$

Exercise 14.3 Just repeat all the previous proofs word for word, replacing $\mathbb{Q}$ by $\mathbb{F}$, or use Proposition 14.2 on p. 318.

Exercise 14.4 Let the roots $\{\vartheta_1, \vartheta_2, \dots, \vartheta_k\} \subset \{\vartheta_1, \vartheta_2, \dots, \vartheta_n\}$ form a Galois orbit. Then the coefficients of the polynomial $g(x) = (x-\vartheta_1)(x-\vartheta_2)\cdots(x-\vartheta_k)$ are Galois invariant, and therefore $g \in \Bbbk[x]$. This forces f to be the product of polynomials g constructed from all the Galois orbits. Conversely, if f is nontrivially factorizable in $\Bbbk[x]$, then the Galois group sends the roots of every factor to the roots of the same factor, and therefore, its action on the roots of f is not transitive.

Exercise 14.6 A splitting field $\mathbb{L}_{\overline{f}}$ for $\overline{f}$ over $\mathbb{F}_p$ can be constructed as a tower of simple extensions,

$$\mathbb{F}_p = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L}_{\overline{f}},$$

every level of which is obtained from the previous one by adjunction of a root ϑ of the polynomial $\overline{f}$. Since $\overline{f}$ splits in $A[t]$ into a product of distinct linear factors, the tautological inclusion $\mathbb{F}_p \hookrightarrow A$ can be extended along the tower to an $\mathbb{F}_p$-algebra homomorphism $\mathbb{L}_{\overline{f}} \to A$. It is injective, because $\mathbb{L}_{\overline{f}}$ is a field, and its image coincides with the $\mathbb{F}_p$-subalgebra of A generated by the roots of $\overline{f}$.

Exercise 14.8 Since $x^n - 1 = \prod_{\nu=0}^{n-1}(x - \zeta^\nu)$, all the elementary symmetric polynomials e_i with $1 \leqslant i \leqslant n-1$ vanish on the successive powers of ζ, i.e., $e_i\left(\zeta^0, \zeta^1, \dots, \zeta^{n-1}\right) = 0$. This forces all the coefficients of f_ξ except for the leading coefficient and constant term[12] to vanish as well:

$$e_i\left(\zeta^0\xi\alpha, \zeta^1\xi\alpha, \dots, \zeta^{n-1}\xi\alpha\right) = \xi^i\alpha^i e_i\left(\zeta^0, \zeta^1, \dots, \zeta^{n-1}\right) = 0.$$

Exercise 14.11 $\sigma(\alpha^m) = \sigma(\alpha)^m = \zeta^{-m}\alpha^m = \alpha^m$.

[12] Which are obviously equal to 1 and $-\xi^n\alpha^n$ respectively.

References

[DK] Danilov, V.I., Koshevoy, G.A.: Arrays and the Combinatorics of Young Tableaux, *Russian Math. Surveys* 60:2 (2005), 269–334.

[Fu] Fulton, W.: *Young Tableaux with Applications to Representation Theory and Geometry*. Cambridge University Press, 1997.

[FH] Fulton, W., Harris, J.: *Representation Theory: A First Course*, Graduate Texts in Mathematics. Cambridge University Press, 1997.

[Mo] Morris, S. A.: *Pontryagin Duality and the Structure of Locally Compact Abelian Groups*, London Math. Society LNS 29. Cambridge University Press, 1977.

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5

Index

A.L. Gorodentsev, *Algebra II*, DOI 10.1007/978-3-319-50853-5