Ciências ULisboa
Faculdade de Ciências da Universidade de Lisboa

Algebra III

(Bachelor Programme || 2018-2019)

Fernando Silva

June 13, 2020

The latest version of this text is available on
http://webpages.fc.ul.pt/~fasilva/alg3-lm/alg3.pdf

This is a companion textbook for Algebra III, a course included in the undergraduate studies in Mathematics at *Faculdade de Ciências da Universidade de Lisboa*. It is not intended to be a stand-alone book. The main topics of Algebra III are polynomials and Galois theory.

This text was written for the school year 2016-2017 and revised in subsequent years. Initially, it was written in Portuguese, but latter the first three chapters were translated into English so that these chapters could be used as a reference for the Algebra course of the Master Programme in Mathematics. The Master Programme in Mathematics has regularly foreign students.

Students are assumed to be familiar with the language of set theory, to know the arithmetic of integers, and to have taken basic courses on linear algebra and abstract algebra. Occasionally, calculus and topology arguments are used. For reference, this text includes a review of some topics taught in previous courses. Other topics are also considered to be known from previous courses and students should review them as needed.

The symbol $\mathbb{N}$ denotes the set of positive integer numbers; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote, respectively, the sets of integer, rational, real and complex numbers. If X is a set, $|X|$ denotes its cardinality. If $z_1, \ldots, z_n \in \mathbb{Z}$, then $\gcd\{z_1, \ldots, z_n\}$ denotes the non-negative greatest common divisor of $z_1, \ldots, z_n$ and $\operatorname{lcm}\{z_1, \ldots, z_n\}$ denotes the non-negative least common multiple of $z_1, \ldots, z_n$.

Propositions without proofs or with incomplete proofs should be proved as exercises. The bibliography is on
http://webpages.fc.ul.pt/~fasilva/alg3-lm/

Contents

Chapter 0

Preliminaries

It is assumed that most of the topics in this chapter, but not all of them, have been taught in previous courses on Abstract Algebra. They are included for reference.

0.1 Modular arithmetic

Let $n \in \mathbb{N}$. We say that $k, l \in \mathbb{Z}$ are *congruent modulo* n and write $k \equiv l \bmod(n)$ if n divides $k - l$. Congruence modulo n is an equivalence relation. Denote the equivalence class of $k \in \mathbb{Z}$ by $\overline{k}$. Denote the set of all equivalence classes by $\mathbb{Z}_n$.

Proposition 0.1 *Let $n \in \mathbb{N}$.*

(a) *For every $k \in \mathbb{Z}$, $\overline{k} = \{k + zn : z \in \mathbb{Z}\}$.*

(b) *$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ and $|\mathbb{Z}_n| = n$.*

The operations

$$\begin{aligned} & + : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad (\overline{k}, \overline{l}) \mapsto \overline{k} + \overline{l} := \overline{k + l}, \\ \text{and} \qquad & \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad (\overline{k}, \overline{l}) \mapsto \overline{k}\,\overline{l} := \overline{kl}, \end{aligned}$$

are well-defined, that is, the images $\overline{k+l}$ and $\overline{kl}$ do not depend on the representatives k and l of $\overline{k}$ and $\overline{l}$, respectively. In fact, for all $k, k', l, l' \in \mathbb{Z}$,

$$\begin{aligned} \overline{k} = \overline{k'} \text{ and } \overline{l} = \overline{l'} \quad & \Rightarrow \quad k \equiv k' \bmod(n) \text{ and } l \equiv l' \bmod(n) \\ & \Rightarrow \quad n \mid k - k' \text{ and } n \mid l - l' \\ & \Rightarrow \quad n \mid (k - k') + (l - l') \text{ and } n \mid (k - k')l + k'(l - l') \\ & \Rightarrow \quad n \mid (k + l) - (k' + l') \text{ and } n \mid kl - k'l' \\ & \Rightarrow \quad k + l \equiv k' + l' \bmod(n) \text{ and } kl \equiv k'l' \bmod(n) \\ & \Rightarrow \quad \overline{k + l} = \overline{k' + l'} \text{ and } \overline{kl} = \overline{k'l'}. \end{aligned}$$

It is easy to see that these operations of addition and multiplication defined in $\mathbb{Z}_n$ inherit various properties of the corresponding operations in $\mathbb{Z}$.

Proposition 0.2 *Let $n \in \mathbb{N}$. Let $k, l, m \in \mathbb{Z}$.*

(a) $\overline{k} + \overline{l} = \overline{l} + \overline{k}, \quad \overline{k} + (\overline{l} + \overline{m}) = (\overline{k} + \overline{l}) + \overline{m}, \quad \overline{k} + \overline{0} = \overline{k}, \quad \overline{k} + \overline{-k} = \overline{0}.$

(b) $\overline{k}\,\overline{l} = \overline{l}\,\overline{k}, \quad \overline{k}(\overline{l}\,\overline{m}) = (\overline{l}\,\overline{k})\overline{m}, \quad \overline{k}\,\overline{1} = \overline{k}.$

(c) $\overline{k}(\overline{l} + \overline{m}) = \overline{k}\,\overline{l} + \overline{k}\,\overline{m}, \quad (\overline{k} + \overline{l})\overline{m} = \overline{k}\,\overline{m} + \overline{l}\,\overline{m}.$

0.2 Groups

A *semigroup* is a set G together with an associative binary operation $* : G \times G \to G$. *Associative* binary operation means that, for all $x, y, z \in G$, $(x*y)*z = x*(y*z)$. A semigroup, as defined above, is denoted by $(G, *)$ or just by the letter G when there is no ambiguity about the binary operation. A semigroup $(G, *)$ is said to be *Abelian* or *commutative* if $*$ is commutative, that is, for all $x, y \in G$, $x * y = y * x$.

A *monoid* is a semigroup $(G, *)$ such that $*$ has an *identity* $e \in G$, that is, for all $x \in G$, $x * e = e * x = x$. In a monoid, there is only one identity: if e, e' are two identities, then $e = e * e' = e'$.

A *group* is a monoid $(G, *)$ with an identity e such that each $x \in G$ has an *inverse* $x' \in G$, that is, $x * x' = x' * x = e$. In a group G, each $x \in G$ has only one inverse: if x', x'' are inverses of x, then $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$.

Usually, the binary operation in a group G is denoted by either $\cdot$ or $+$. In the first case, we say that the group is *multiplicative*, the operation is called *multiplication;* the *product* $x \cdot y$ is also denoted by xy; the identity is denoted by 1_G or 1; for every $x \in G$, the inverse of x is denoted by x^{-1}. For all $n \in \mathbb{N}$, $x \in G$, x^n is defined as the product $x \cdots x$ of x by itself n times ([1]); $x^0 := 1_G$ and $x^{-n} := (x^{-1})^n$.

When using the symbol $+$, we say that the group is *additive*, the operation is called *addition;* the identity is called *zero* and is denoted by 0_G or 0; for every $x \in G$, the inverse of x is denoted by $-x$. For all $n \in \mathbb{N}$, $x \in G$, nx is defined as the sum $x + \cdots + x$ of x by itself n times; $0x := 0_G$ and $(-n)x := n(-x)$. It is frequent to use the additive language when the group is Abelian.

A group with only one element is called *trivial.* Frequently, a trivial multiplicative group is represented by 1, while a trivial additive group is represented by 0. Note that we are using the same symbol for the identity and for a trivial group, what is an abuse of language. This ambiguity can usually be solved by the context.

In this first chapter, it is assumed that we are using the multiplicative language, unless otherwise stated.

[1] Recursively: $x^1 = x$ and $x^n = x \cdot x^{n-1}$, for every $n \geq 2$.

Proposition 0.3 *Let G be a (multiplicative) group. For all $x, y, z \in G$, $m, n \in \mathbb{Z}$,*

(a) $xy = xz \Rightarrow y = z, \;\; yx = zx \Rightarrow y = z,$

(b) $(x^{-1})^{-1} = x,$

(c) $(xy)^{-1} = y^{-1}x^{-1},$

(d) $x^m x^n = x^{m+n},$

(e) $(x^m)^n = x^{mn},$

(f) *if G is Abelian, then $(xy)^m = x^m y^m$.*

Proposition 0.4 *Let G be an additive group. For all $x, y, z \in G$, $m, n \in \mathbb{Z}$,*

(a) $x + y = x + z \Rightarrow y = z$ *and* $y + x = z + x \Rightarrow y = z,$

(b) $-(-x) = x,$

(c) $-(x + y) = (-y) + (-x),$

(d) $mx + nx = (m + n)x,$

(e) $m(nx) = (mn)x,$

(f) *if G is Abelian, then $m(x + y) = mx + my$.*

Group homomorphisms

In Algebra, a homomorphism is a map between two algebraic structures of the same kind that preserves all operations, relations and constants required in the definition of those algebraic structures.

A *homomorphism of semigroups* is a map $f : G \to H$, where G, H are semigroups, that preserves the binary operation, that is, for all $x, y \in G$, $f(xy) = f(x)f(y)$.

A *homomorphism of monoids* is a map $f : G \to H$, where G, H are monoids, that preserves the binary operation and the identity, that is, f is a homomorphism of semigroups and $f(1_G) = 1_H$.

A *homomorphism of groups* is a map $f : G \to H$, where G, H are groups, that preserves the binary operation, the identity and inverses, that is, f is a homomorphism of monoids and, for every $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

For these algebraic structures and others to be introduced in the future, a homomorphism $f : G \to H$ is called *monomorphism* if f is injective; *epimorphism* if f is surjective; *isomorphism* if f is bijective; *endomorphism* if $G = H$; *automorphism* if $G = H$ and f is bijective.

We say that two groups (respectively, semigroups, monoids) G and H are *isomorphic*, and write $G \cong H$, if there is an isomorphism $f : G \to H$.

It is easy to prove that, in any of the three cases above (semigroups, monoids, groups), the composition of homomorphisms is a homomorphism, the inverse of an isomorphism is an isomorphism and the map identity $\mathrm{id}_G : G \to G$, $x \mapsto x$, is an automorphism. It follows that the set $\operatorname{Aut} G$ of all automorphisms of a group (or semigroup, or monoid) G is always a group with the composition as its binary operation.

If G, H are groups (respectively, monoids), the function $G \to H$ that maps all $x \in G$ to the identity of H is a homomorphism of groups (respectively, monoids), called a *trivial homomorphism*.

Proposition 0.5 *Given two groups G, H, a map $f : G \to H$ is a homomorphism of groups if and only if, for all $x, y \in G$, $f(xy) = f(x)f(y)$.*

Proof ($\Rightarrow$) Trivial.

($\Leftarrow$) We have $f(1)f(1) = f(1 \cdot 1) = f(1)$. When we multiply both sides on the right (or on the left) by $f(1)^{-1}$, we get $f(1) = 1$. Let $x \in G$. Then $f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1$. Analogously $f(x^{-1})f(x) = 1$. Therefore $f(x^{-1}) = f(x)^{-1}$. ■

Note that a map $f : G \to H$, where G, H are monoids, may preserve products without preserving the identity. Consider a monoid $S = \{1, s\}$, where $1 \neq s$, 1 is the identity and $s^2 = s$. Then $f : S \to S$, $x \mapsto s$, preserves products but $f(1) \neq 1$.

Subgroups and cosets

Let G a group. A subset H of G is said to be a *subgroup* of G if $1 \in H$ and, for all $x, y \in H$, $xy \in H$ and $x^{-1} \in H$. The symbol $H \leq G$ means that H is a subgroup of G. The symbol $H < G$ means that H is a subgroup of G and $H \neq G$.

If H is a subgroup of a group G, then H is a group, with the restriction of the multiplication to $H \times H$ as the binary operation.

Let H be a subgroup of a group G. For every $x \in G$, let

$$Hx = \{hx : h \in H\} \quad \text{and} \quad xH = \{xh : h \in H\}.$$

The sets of the form Hx are called the *right cosets* of H in G. The sets of the form xH are called the *left cosets* of H in G.

A subgroup N of a group G is said to be *normal* if, for every $x \in G$, $Nx = xN$. The symbol $N \trianglelefteq G$ means that N is a normal subgroup of G. The symbol $N \triangleleft G$ means that N is a normal subgroup of G and $N \neq G$.

Given a group G, $\{1\}$ and G are always normal subgroups of G. The subgroup $\{1\}$ is called the *trivial subgroup* of G and is denoted by the symbol 1. A subgroup H of a group G is said to be *proper* if $H \neq G$.

Proposition 0.6 *A non-empty subset H of a group G is a subgroup of G if and only if, for all $x, y \in H$, $x^{-1}y \in H$.*

Proposition 0.7 *Let N be a subgroup of a group G. The following statements are equivalent.*

(a) $N \trianglelefteq G$.

(b) *For all* $x \in G$, $Nx \subseteq xN$.

(c) *For all* $x \in G$, $y \in N$, $x^{-1}yx \in N$.

Given a homomorphism of groups $f : G \to G'$, the *kernel* of f is

$$\ker f = f^{-1}(\{1\}) = \{x \in G : f(x) = 1\}.$$

Proposition 0.8 *Let $f : G \to G'$ be a homomorphism of groups.*

(a) *If $x \in G$ and $n \in \mathbb{Z}$, then $f(x^n) = f(x)^n$.*

(b) *If $H \leq G$, then $f(H) \leq G'$.*

(c) *If $H \trianglelefteq G$, then $f(H) \trianglelefteq f(G)$.*

(d) *If $H' \leq G'$, then $f^{-1}(H') \leq G$.*

(e) *If $H' \trianglelefteq G'$, then $f^{-1}(H') \trianglelefteq G$. In particular,* $\ker f \trianglelefteq G$.

(f) *f is injective if and only if* $\ker f = 1$.

Let H be a subgroup of a group G. It is said that $x, y \in G$ are *right congruent modulo H* if $xy^{-1} \in H$. It is said that $x, y \in G$ are *left congruent modulo H* if $x^{-1}y \in H$.

Proposition 0.9 *Let H be a subgroup of a group G.*

(a) *For all $x, y \in G$, $xy^{-1} \in H$ if and only if $Hx = Hy$.*

(b) *For all $x, y \in G$, $x^{-1}y \in H$ if and only if $xH = yH$.*

(c) *Right (respectively, left) congruence modulo H is an equivalence relation.*

(d) *The right (respectively, left) congruence modulo H class of $x \in G$ is the right coset Hx (respectively, left coset xH).*

Proposition 0.10 *Let H be a subgroup of a group G. Let $\mathcal{R}$ and $\mathcal{L}$ the sets the right cosets and left cosets, respectively, of H in G.*

(a) *The map*

$$\mathcal{R} \to \mathcal{L}, \quad Hx \mapsto x^{-1}H,$$

is well-defined and is bijective.

(b) *If G is finite, then for each $x \in G$, $|Hx| = |H| = |xH|$.* ([2])

[2] For students who studied transfinite cardinal numbers: these equalities are also valid for infinite groups.

Proof (a) The map is well-defined and injective: for all $x, y \in G$, $Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow yx^{-1} \in H \Leftrightarrow x^{-1}H = y^{-1}H$. Clearly the map is surjective. ■

With the notation of the previous proposition, let $[G : H] = |\mathcal{R}| = |\mathcal{L}|$. This cardinality is called the *index* of H in G.

Proposition 0.11 *Let H be a subgroup of a group G. If $[G : H] = 2$, then $H \trianglelefteq G$.*

Proof If $[G : H] = 2$, then H and $G \setminus H$ are the right and also the left cosets of H in G. As right and left cosets coincide, $H \trianglelefteq G$. ■

Proposition 0.12 [Lagrange theorem] *Let H be a subgroup of a finite group G. Then*

$$|G| = [G : H]|H| \quad (^3) \tag{1}$$

and $|H|$ divides $|G|$.

Proof Let $(x_i)_{i \in I}$ be a family of representatives of the left cosets of H in G, i. e., the cosets x_iH are all the left cosets of of H in G and $x_iH \neq x_jH$ whenever $i \neq j$. As the left cosets partition the set G, $|G| = \sum_{i \in I} |x_iH|$. By Proposition 0.10 (b), $|G| = |I||H| = [G : H]|H|$. ■

If X, Y are non-empty subsets of a group G, the product XY is defined by

$$XY = \{xy : x \in X, y \in Y\}.$$

Proposition 0.13 *Let H, K be subgroups of a finite group G. Then*

$$|HK||H \cap K| = |H||K|. \quad (^3)$$

Proof $HK = \bigcup_{x \in K} Hx$ is a union of right cosets of H. For all $x, y \in K$,

$$Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow xy^{-1} \in H \cap K \Leftrightarrow (H \cap K)x = (H \cap K)y.$$

It follows that the number of distinct cosets Hx, with $x \in K$, is equal to $[K : H \cap K]$. Therefore

$$|HK||H \cap K| = |\bigcup_{x \in K} Hx||H \cap K| = [K : H \cap K]|H||H \cap K| = |H||K|.$$

■

[3] For students who studied transfinite cardinal numbers: this equality is also valid for infinite groups.

Proposition 0.14 *Let H, N be subgroups of a group G.*

(a) *If $N \subseteq H$, then $N \leq H$.*

(b) *If $N \trianglelefteq G$ and $N \subseteq H$, then $N \trianglelefteq H$.*

(c) *HN is a subgroup of G if and only if $HN = NH$.*

(d) *If $N \trianglelefteq G$, then $H \cap N \trianglelefteq H$.*

(e) *If $N \trianglelefteq G$, then $N \trianglelefteq HN = NH \leq G$.*

(f) *If $N_1, \ldots, N_p$ are normal subgroups of G, then $N_1 \cdots N_p \trianglelefteq G$.*

Proof (c) Suppose that $HN \leq G$. Let $x = hn \in HN$, where $h \in H$ and $n \in N$. As $HN \leq G$, $n^{-1}h^{-1} = x^{-1} \in HN$. Thus $n^{-1}h^{-1} = h'n'$, for some $h' \in H$ and $n' \in N$. Then $x = (h'n')^{-1} = n'^{-1}h'^{-1} \in NH$. Hence $HN \subseteq NH$. To prove the other inclusion, let $x = nh \in NH$, where $n \in N$ and $h \in H$. Then $x^{-1} = h^{-1}n^{-1} \in HN$. As $HN \leq G$, $x \in HN$. Hence $NH \subseteq HN$.

Conversely, suppose that $HN = NH$. Clearly $1 \in HN$. Let $x, y \in HN$ and suppose that $x = hn$ and $y = h'n'$, for some $h, h' \in H$ and $n, n' \in N$. As $h^{-1}h'n' \in HN = NH$, $h^{-1}h'n' = n''h''$, for some $n'' \in N$ and $h'' \in H$. Then $x^{-1}y = n^{-1}h^{-1}h'n' = n^{-1}n''h'' \in NH = HN$. Hence $HN \leq G$.

(f) Suppose that $p = 2$. By (c) and (a), $N_1N_2 \leq G$. Let $g \in G$, $x \in N_1$, $y \in N_2$. Then $g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) \in N_1N_2$. Hence $N_1N_2 \trianglelefteq G$. It is easy to complete the proof by induction. ■

Quotient Groups

Let N be a normal subgroup of a group G. Let G/N be the set of all cosets $Nx = xN$ of N in G. In G/N, define a multiplication as follows:

$$G/N \times G/N \to G/N, \quad (xN, yN) \mapsto (xy)N. \tag{2}$$

Proposition *With the previous notation, the multiplication* (2) *is well-defined, that is, the image $(xy)N$ does not depend on the representatives x, y chosen in the cosets xN, yN, and, with it, G/N is a group with identity N. The inverse of a coset xN is $x^{-1}N$.*

If G is Abelian, then G/N is Abelian.

With the previous notation, the group G/N is said to be the *quotient group* of G by N.

Proof Suppose that $xN = wN$ and $yN = zN$. Let $g \in (xy)N$. Then $g = xyn$, for some $n \in \mathbb{N}$. As $yn \in yN = zN = Nz$, $yn = n'z$, for some $n' \in N$. As $xn' \in xN = wN = Nw$, $xn' = n''w$, for some $n'' \in N$. Then $g = xyn = xn'z = n''wz \in N(wz) = (wz)N$. Thus $(xy)N \subseteq (wz)N$. The other inclusion can be proved analogously. Hence $(xy)N = (wz)N$ and (2) is well-defined. ■

For every normal subgroup N of a group G, the map

$$p : G \to G/N, \quad x \mapsto xN,$$

is an epimorphism of groups called the *canonical epimorphism* from G to G/N.

Proposition 0.15 *Let G be a group, $N \trianglelefteq G$, and let $p : G \to G/N$ be the canonical epimorphism.*

(a) *For each subgroup H of G, $p(H) = HN/N$.*

(b) *For each subgroup S of G/N, $N \subseteq p^{-1}(S)$ and $S = p^{-1}(S)/N$.*

Proof (a) By Proposition 0.14 (e), $N \trianglelefteq HN$.

Let $p(h) \in p(H)$, where $h \in H$. As $h = h1 \in HN$, $p(h) = hN \in HN/N$. Thus $p(H) \subseteq HN/N$. To prove the other inclusion, let $xN \in HN/N$. As $x \in HN$, $x = hn$, for some $h \in H$ and $n \in N$. Then $xN = (hn)N = h(nN) = hN = p(h) \in p(H)$. Thus $HN/N \subseteq p(H)$.

(b) Let S be a subgroup of G/N. Let $p : G \to G/N$ be the canonical epimorphism. Then $H = p^{-1}(S)$ is a subgroup of G. For each $x \in N$, $p(x) = xN = N = 1_{G/N} \in S$ and $x \in p^{-1}(S) = H$. Thus $N \subseteq H$. By Proposition 0.14, $N \trianglelefteq H$. Let us prove that $S = H/N$.

Let $xN \in S$. As $p(x) = xN \in S$, $x \in p^{-1}(S) = H$. Thus $S \subseteq H/N$. Now let $xN \in H/N$, where $x \in H = p^{-1}(S)$. Then $xN = p(x) \in S$. Thus $H/N \subseteq S$. Hence $S = H/N$.

To prove the other inclusion, let H be a subgroup of G containing N. As $1 \in H$, $N = 1N \in H/N$. For all $x, y \in H$, as xy^{-1}, $(xN)(yN)^{-1} = (xN)(y^{-1}N) = (xy^{-1})N \in H/N$. Hence H/N is a subgroup of G/N. ■

Proposition 0.16 *Let N be a normal subgroup of a group G.*

(a) *The set of all subgroups of G/N is $\{H/N : N \leq H \leq G\}$.*

(b) *The set of all normal subgroups of G/N is $\{H/N : N \leq H \trianglelefteq G\}$.*

Proof (a) It follows from Proposition 0.15.

(b) Let H/N be a subgroup of G/N. Then

$$\begin{aligned} H/N \trianglelefteq G/N &\Leftrightarrow \forall y \in G, x \in N, (yN)^{-1}(xN)(yN) \in H/N \\ &\Leftrightarrow \forall y \in G, x \in N, (y^{-1}xy)N \in H/N \\ &\Leftrightarrow \forall y \in G, x \in N, y^{-1}xy \in H \Leftrightarrow H \trianglelefteq G. \end{aligned}$$ ■

Group isomorphism theorems

Proposition 0.17 [First isomorphism theorem] *Let $f : G \to H$ be a homomorphism of groups. The groups $G/\ker f$ and $f(G)$ are isomorphic. The map*

$$\Phi : \frac{G}{\ker f} \to f(G), \quad x(\ker f) \mapsto f(x),$$

is well-defined and is an isomorphism of groups.

Proof For all $x, y \in G$, $x \ker f = y \ker f \Leftrightarrow y^{-1}x \in \ker f \Leftrightarrow f(y^{-1}x) = 1 \Leftrightarrow f(y)^{-1}f(x) = 1 \Leftrightarrow f(x) = f(y)$. Thus Φ is a well-defined map and is injective. Clearly Φ is also surjective.

For all $x, y \in G$, $\Phi((x \ker f)(y \ker f)) = \Phi((xy) \ker f) = f(xy) = f(x)f(y) = \Phi(x \ker f)\Phi(y \ker f)$. Hence Φ is an isomorphism of groups. ∎

Proposition 0.18 [Second isomorphism theorem] *Let H be a subgroup of a group G. Let N be a normal subgroup of G. Then the groups $H/(H \cap N)$ and $(HN)/N$ are isomorphic. The map*

$$\Phi : \frac{H}{H \cap N} \to \frac{HN}{N}, \quad x(H \cap N) \mapsto xN,$$

is well-defined and is an isomorphism of groups.

Proof By Proposition 0.14, $H \cap N \trianglelefteq H$ and $N \trianglelefteq HN \leq G$. Prove that

$$\Psi : H \to \frac{HN}{N}, \quad x \mapsto xN,$$

is an epimorphism of groups and $\ker \Psi = H \cap N$. The conclusion follows from Proposition 0.17. ∎

Proposition 0.19 [Third isomorphism theorem] *Let K, L be normal subgroups of a group G such that $K \subseteq L$. The groups G/L and $(G/K)/(L/K)$ are isomorphic. The map*

$$\Phi : \frac{G}{L} \to \frac{G/K}{L/K}, \quad xL \mapsto (xK)(L/K),$$

is well-defined and is an isomorphism of groups.

Subgroup generated by a set. Cyclic groups

Proposition 0.20 *Let G be a group. Let $(H_i)_{i \in I}$ be a non-empty family of subgroups (respectively, normal subgroups) of G. Then $\bigcap_{i \in I} H_i$ is a subgroup (respectively, normal subgroup) of G.*

Let X be a subset of a group X. The intersection of all subgroups (respectively, normal subgroups) of G that contain X is called the *subgroup of G generated by X* (respectively, *normal subgroup of G generated by X*). The subgroup generated by X is denoted by $\langle X \rangle$. If $X = \{x_1, \ldots, x_n\}$ is finite, then $\langle X \rangle$ is also denoted by $\langle x_1, \ldots, x_n \rangle$; in this case, we also say that G is generated by $x_1, \ldots, x_n$. A group G is said to be *cyclic* if there is $x \in G$ such that $G = \langle x \rangle$.

The normal subgroup of G generated by X is also called the *normal closure* or the *conjugate closure* of X. Let $X^G = \{gxg^{-1} : g \in G, x \in X\}$.

Proposition 0.21 *Let X be a subset of a group X. The normal closure of X is equal to $\langle X^G \rangle = \langle X \rangle^G$.*

Proposition 0.22 *Let $f : G \to G'$ be a homomorphism of groups. If G is generated by a set $X \subseteq G$, then $f(G)$ is generated by $X' = \{f(x) : x \in X\}$. In particular, if G is cyclic, then $f(G)$ is cyclic.*

Proposition 0.23 *Let G be a group generated by $X \subseteq G$. If $X = \emptyset$, then $G = 1$. If $X \neq \emptyset$, then*

$$\begin{aligned} G &= \{x_1^{k_1} \cdots x_n^{k_n} : n \in \mathbb{N}, x_1, \ldots, x_n \in X, k_1, \ldots, k_n \in \{1, -1\}\}. \\ &= \{x_1^{k_1} \cdots x_n^{k_n} : n \in \mathbb{N}, x_1, \ldots, x_n \in X, k_1, \ldots, k_n \in \mathbb{Z}\}. \end{aligned}$$

In particular, if $X = \{x\}$, then $G = \{x^k : k \in \mathbb{Z}\}$.

Given a group G, the cardinality of G is called the *order* of the group. If x is an element of a group G, the order of the cyclic group $\langle x \rangle$ is also called the *order* of x and is denoted by $|x|$.

Proposition 0.24 *Let $n \in \mathbb{N}$. With the addition defined in Section* 0.1, *$\mathbb{Z}_n$ is an additive cyclic group of order n.*

Proof By the propositions in Section 0.1, $\mathbb{Z}_n$ is an additive group of order n. It is easy to see that $\mathbb{Z}_n = \langle \bar{1} \rangle$. ■

Proposition 0.25 *Let G be a cyclic group generated by $x \in G$.*

(a) *If there is a positive power of x equal to* 1 *and $n \in \mathbb{N}$ is the smallest positive integer such that $x^n = 1$, then,*

  (i) *for all $k \in \mathbb{Z}$, $x^k = 1 \Leftrightarrow n \mid k$,*

  (ii) *for all $k, l \in \mathbb{Z}$, $x^k = x^l$ if and only if $k \equiv l \bmod (n)$,*

  (iii) *$G = \langle x \rangle = \{1, x^1, \ldots, x^{n-1}\}$ and $n = |G| = |x|$,*

  (iv) *G is isomorphic to the additive group $\mathbb{Z}_n$.*

(b) *If G is infinite, then all powers x^k are different and G is isomorphic to the additive group $\mathbb{Z}$.*

(c) *G is finite if and only if there is $n \in \mathbb{N}$ such that $x^n = 1$.*

Proof (i) Suppose that $x^k = 1$, where $k \in \mathbb{Z}$. Then $k = nq + r$, for some $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$. Then $1 = x^k = (x^n)^q x^r = x^r$. By the minimality of n, $r = 0$. Therefore $n \mid k$.

Conversely, if $k = nq$, for some $q \in \mathbb{Z}$, then $x^k = (x^n)^q = 1$.

(ii) $x^k = x^l \Leftrightarrow x^{k-l} = 1 \Leftrightarrow n \mid k - l \Leftrightarrow k \equiv l \bmod (n)$.

(iii) Let $x^m \in G$, where $m \in \mathbb{Z}$. Then $m = nq + r$, where $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$. Then $x^m = (x^n)^q x^r = x^r$. Therefore $G \subseteq \{1, x^1, \ldots, x^{n-1}\}$.

The other inclusion is trivial. From (ii), the elements $1, x^1, \ldots, x^{n-1}$ are distinct and, therefore, $|G| = n$.

(iv) By (ii),

$$f : \mathbb{Z}_n \to G, \quad \overline{k} \mapsto x^k,$$

is a well-defined injective map. Clearly f is surjective. For all $k, l \in \mathbb{Z}$,

$$f(\overline{k} + \overline{l}) = f(\overline{k+l}) = x^{k+l} = x^k x^l = f(\overline{k}) f(\overline{l}).$$

(b) If there are $k > l$ such that $x^k = x^l$, then $x^{k-l} = 1$ and, by (a), G would be finite, a contradiction. It is easy to see that $\mathbb{Z} \to G$, $k \mapsto x^k$, is an isomorphism.

(c) follows from (a) and (b). ■

Proposition 0.26 *Let G be a group and $x \in G$.*

(a) *If $|x|$ is finite, then $|x|$ is the smallest positive integer n such that $x^n = 1$.*

(b) *If G is finite, then $x^{|G|} = 1$.*

Proof The first statement follows from the previous proposition. By Lagrange theorem, $|x| \mid |G|$. As $x^{|x|} = 1$, $x^{|G|} = 1$. ■

Lemma 0.27 *Let G be a cyclic group generated by $x \in G$. Let H be a non-trivial subgroup of G. Let k be the smallest positive integer such that $x^k \in H$ ([4]). Then $H = \langle x^k \rangle$.*

Proof Let $x^m \in H$, where $m \in \mathbb{Z}$. Then $m = kq + r$, where $q \in \mathbb{Z}$ and $r \in \{0, \ldots, k-1\}$. Then $x^m = (x^k)^q x^r$ and $x^r = (x^k)^{-q} x^m \in H$. By the minimality of k, $r = 0$. Then $x^m = (x^k)^q \in \langle x^k \rangle$. Therefore $H \subseteq \langle x^k \rangle$. As $x^k \in H$, the other inclusion is trivial. ■

Proposition 0.28 *Let G be a cyclic group.*

(a) *Every subgroup of G is cyclic.*

(b) *If G is finite, then, for every $d \mid |G|$, G has one, and only one, subgroup of order d.*

(c) *If G is infinite, then every non-trivial subgroup of G is infinite.*

Proof (a) follows from Lemma 0.27.

(b) Let $n = |G|$. Let $d \mid n$. If $d = 1$, then the trivial subgroup has order d and is the only subgroup of order d. Suppose that $d > 1$. Let $k = n/d$.

[4] As $H \neq 1$, there is $l \in \mathbb{Z} \setminus \{0\}$ such that $x^l \in H$. Then $x^l, x^{-l} \in H$, with either $l \in \mathbb{N}$ or $-l \in \mathbb{N}$. Therefore there is a positive power of x in H.

Then d is the smallest positive integer such that $(x^k)^d = 1$. By Proposition 0.25, $|\langle x^k \rangle| = d$.

Now let H be any subgroup of G of order d. Let l be the smallest positive integer such that $x^l \in H$. By Lemma 0.27, $H = \langle x^l \rangle$, $l \mid n$ and $d = |H| = n/l$. Then $l = n/d = k$. Therefore, $H = \langle x^k \rangle$.

(c) Let H be a non-trivial subgroup of G. By Lemma 0.27, $H = \langle x^k \rangle$, for some $k \in \mathbb{N}$. By Proposition 0.25, all powers of x^k are different. Therefore H is infinite.

■

Proposition 0.29 *Let G be a group and suppose that $x \in G$ has finite order. If $1 \leq k \mid |x|$, then $|x^k| = |x|/k$.*

Proof As $1 = x^{|x|} = (x^k)^{|x|/k}$, $|x^k|$ divides $|x|/k$. As $1 = (x^k)^{|x^k|} = x^{k|x^k|}$, $|x|$ divides $k|x^k|$ and $|x|/k$ divides $|x^k|$. Therefore $|x^k| = |x|/k$. ■

Products of groups

Proposition 0.30 *Let $G_1, \ldots, G_n$ be groups. In*

$$G = G_1 \times \cdots \times G_n = \{(x_1, \ldots, x_n) \in G : x_i \in G_i\},$$

define a multiplication as follows: for all $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in G$,

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

With this multiplication, G is a group. The group G is Abelian if and only if, for all $i \in \{1, \ldots, n\}$, G_i is Abelian.

With the previous notation, G is called the *product* of the groups $G_1, \ldots, G_n$.

Sums of subgroups of an additive Abelian group

Let G be an additive Abelian group.

If $(x_i)_{i \in I}$ is a non-empty family of elements of G and $S = \{i \in I : x_i \neq 0\}$ is finite, we call *sum of the family* $(x_i)_{i \in I}$ to the element

$$\sum_{i \in I} x_i := \sum_{i \in S} x_i \text{ when } S \neq \emptyset \quad \text{and} \quad \sum_{i \in I} x_i := 0 \text{ when } S = \emptyset.$$

If $(X_i)_{i \in I}$ is non-empty a family of non-empty subsets of G, then

$$\sum_{i \in I} X_i$$

represents the set of all sums of families $(x_i)_{i\in I}$, where, for each i, $x_i \in X_i$ and $S = \{i \in I : x_i \neq 0\}$ is finite. In particular, if $X_1, \dots, X_k$ is a finite family of non-empty subsets of G, then

$$X_1 + \cdots + X_k = \{x_1 + \cdots + x_k : \text{ for each } i,\ x_i \in X_i\}.$$

Note that the sum of subsets is commutative and associative: if $\emptyset \neq X, Y, Z \subseteq G$, then $X + Y = Y + X$ and $X + (Y + Z) = (X + Y) + Z$.

If $x \in G$, $\emptyset \neq Y \subseteq G$, then $x + Y$ represents the set

$$x + Y = \{x\} + Y = \{x + y : y \in Y\}.$$

Proposition Let $(G_i)_{i\in I}$ be a non-empty family of subgroups of an additive Abelian group G. Then $\sum_{i\in I} G_i$ is the subgroup of G generated by $\bigcup_{i\in I} G_i$.

Exercises

0.2.1 Let $n \in \mathbb{N}$. Prove that $\mathbb{Z}_n$ is an additive group and a multiplicative monoid. Prove that $\mathbb{Z}_n \setminus 0$ is a multiplicative monoid. Prove that $\mathbb{Z}_n$ is a multiplicative group if and only if n is a prime number. (This is already known from previous courses. Students should do the exercise to recall the argument.)

0.2.2 Let $k \in \mathbb{R}$. In $\mathbb{R}$, define a binary relation $\sim$ as follows: $x \sim y$ if and only if there is $n \in \mathbb{Z}$ such that $x - y = nk$.

(a) Prove that $\sim$ is an equivalence relation.

Denote the equivalence class of $x \in \mathbb{R}$ by $\overline{x}$ or by x is there is no risk of confusion. Denote the set of all equivalence classes by $\mathbb{R}_k$.

(b) Prove that the addition $+ : \mathbb{R}_k \times \mathbb{R}_k \to \mathbb{R}_k$, $(\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$, is well-defined and $\mathbb{R}_k$ is an Abelian group with this addition.

(c) Prove that $f : \mathbb{R} \to \mathbb{R}_0$, $x \mapsto \overline{x}$, is an isomorphism of additive groups.

(d) Suppose that $k \neq 0$. Prove that the additive groups $\mathbb{R}$ and $\mathbb{R}_k$ are not isomorphic.

(Hint: Show that $\mathbb{R}_k$ has an element w of order 2 and $\mathbb{R}$ has no elements of order 2, and note that, if $f : \mathbb{R}_k \to \mathbb{R}$ is an isomorphism, then $|f(w)| = |w| = 2$.)

(e) Suppose that $k \neq 0$. To avoid ambiguities, denote the class of x in $\mathbb{R}_1$ by $\widehat{x}$ and the class of x in $\mathbb{R}_k$ by $\overline{x}$.

Prove that $g : \mathbb{R}_1 \to \mathbb{R}_k$, $\widehat{x} \mapsto \overline{xk}$, is well-defined and is an isomorphism of additive groups.

0.2.3 Prove that $T = \{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of the multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus 0$. Prove that $f : \mathbb{R}_{2\pi} \to T$, $\overline{x} \mapsto e^{ix}$, is well-defined and is an isomorphism between the additive group $\mathbb{R}_{2\pi}$ and T.

0.2.4 Let G be a semigroup and $H \subseteq G$. Then H is said to be a *subsemigroup* of G if, for all $x, y \in H$, $xy \in H$. Show that H is a semigroup with the restriction of the multiplication to $H \times H$ as its binary operation.

0.2.5 Let G be a monoid and $H \subseteq G$. Then H is said to be a *submonoid* of G if, for all $x, y \in H$, $xy \in H$ and $1_G \in H$. Show that H is a monoid with the restriction of the multiplication to $H \times H$ and $1_H = 1_G$.

0.2.6 Let G be a group. An equivalence relation $\sim$ on G is said to be a *group congruence relation* if, for all $w, x, y, z \in G$, if $w \sim x$ and $y \sim z$, then $wy \sim xz$.

Let $\sim$ be a congruence relation on G. Prove that, for all $w, x \in G$, if $w \sim x$, then $w^{-1} \sim x^{-1}$. ([5])

Given $n \in \mathbb{N}$, note that the congruence modulo n on $\mathbb{Z}$ is a congruence relation on the additive group $\mathbb{Z}$.

0.2.7 Let G be a group.

(a) Let $\sim$ be a congruence relation on G and let $N_\sim$ be the equivalence class (frequently called *congruence class*) of 1.

Prove that $N_\sim \trianglelefteq G$.

(b) Let $N \trianglelefteq G$. It is said that $x, y \in G$ are *congruent modulo N* (and we write $x \sim_N y$) if $xy^{-1} \in N$.

Prove that $\sim_N$ is a congruence relation on G.

(c) Prove that (a) and (b) give a bijective correspondence between the set $\mathcal{C}$ of all congruences on G and the set $\mathcal{N}$ of all normal subgroups of G.

0.2.8 Let G be a set where a binary operation is defined. (The multiplicative notation will be used.) Prove that G is a group if and only if

(a) (associativity) for all $x, y, z \in G$, $(xy)z = x(yz)$,

(b) (existence of right identity) there is $e \in G$ such that, for every $x \in G$, $xe = x$,

(c) (existence of right inverses) and, for each $x \in G$, there is $x' \in G$ such that $xx' = e$.

0.2.9 Let G be a non-empty set where a binary operation is defined. (The multiplicative notation will be used.) Prove that G is a group if and only if the operation is associative and, for all $g, h \in G$, the equations $gx = h$ and $yg = h$ have solutions in G.
(Hint: ($\Leftarrow$) Fix $g \in G$. Choose $e \in G$ such that $ge = g$. Show that, for every $h \in G$, $he = h$. Apply Exercise 0.2.8.)

0.2.10 Prove that, if $a^2 = 1$, for all elements a of a group G, then G is Abelian.

0.2.11 Let G be a non-empty finite set with an associative binary operation such that, for all $a, b, c \in G$, $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. Prove that G is a group. Show that this conclusion may be false if G is infinite. (Hint: Apply Exercise 0.2.9.)

0.2.12 Let G be a finite group and let $K \leq H \leq G$. Prove that

$[G : K] = [G : H][H : K]$.

0.2.13 If $f : G \to H$ is a group homomorphism, H is Abelian and N is a subgroup of G containing $\ker f$, then $N \trianglelefteq G$.

[5] In abstract algebra, a congruence relation (or simply congruence) is an equivalence relation on an algebraic structure (such as a group, ring, or vector space) that is compatible with the structure in the sense that algebraic operations done with equivalent elements will yield equivalent elements.

0.2.14 If $f : G \to H$ is a homomorphism of groups, $N = \ker f$, and $K \leq G$, then $f^{-1}(f(K)) = KN$. Hence $f^{-1}(f(K)) = K$ if and only if $N \leq K$.

0.2.15 If $f : G \to H$ is a group homomorphism, $a \in G$, and $f(a)$ has finite order, then $|a|$ is infinite or $|f(a)|$ divides $|a|$.

0.2.16 Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. (Hint: Prove that $\mathbb{Q}$ is not cyclic and recall that $\mathbb{Z}$ is cyclic.)

0.2.17 Let G be a finite group. Prove that, if $a, b \in G$, then $|ab| = |ba|$.

0.2.18 If G is an Abelian group, then the set of all elements of G with finite order is a subgroup of G.

0.2.19 If H and K are subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

0.2.20 Let H, K, N be subgroups of a group G such that $H \leq K$, $H \cap N = K \cap N$ and $HN = KN$. Show that $H = K$.

0.2.21 Let G be a group of order $2n$, where n is odd. Prove that G has one and only one element of order 2.

0.2.22 Let H be a normal cyclic subgroup of a group G. Prove that every subgroup of H is normal in G.

0.2.23 Let H be a subgroup of a group G. Prove that $\operatorname{Core}_G H := \bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup of G contained in H. ($\operatorname{Core}_G H$ is called the *core* of H in G.)

0.2.24 Prove that, if G is a group of order 4, then either $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

0.3 Rings

A *ring* is a set R, with an addition $+ : R \times R \to R$ and a multiplication $\cdot : R \times R \to R$, such that:

- $(R, +)$ is an Abelian group;
- $(R, \cdot)$ is a monoid;
- the following distributive properties are satisfied: for all $a, b, c \in R$,

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc.$$

A ring is said to be *commutative* if the multiplication is commutative. A ring is said to be trivial if $R = 0$.

In some books, the definition of ring may be a bit different. Note that, according to this definition, all rings have identity for multiplication and it is not required that $1 \neq 0$.

Note that a ring R is trivial if and only if $1 = 0$.

An element a of a ring R is said to be *invertible* if there is $a^{-1} \in R$ (called *inverse* of a) such that $aa^{-1} = a^{-1}a = 1$. The invertible elements of a unit ring are also called *units*. It is easy to prove that an invertible element has a unique inverse.

A ring R is called a division ring if $R \neq 0$ and all non-zero elements of R are invertible. A commutative division ring is called a *field*.

Proposition 0.31 *Let R be a ring. For all $a, b, c \in R$,*

(a) $0a = a0 = 0$,

(b) $(-a)b = a(-b) = -(ab)$,

(c) $a(b-c) = ab - ac$, $(a-b)c = ac - bc$.

Proposition 0.32 *Let R be a ring, $a, b \in R$ and $n \in \mathbb{N}$. If $ab = ba$, then*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Ring homomorphisms

A map $f : R \to R'$, where R and R' are rings, is called a *homomorphism of rings* (or *ring homomorphism*) if it is a homomorphism of additive groups and a homomorphism of multiplicative monoids, that is, if for any $a, b \in R$,

- $f(a+b) = f(a) + f(b)$,
- $f(ab) = f(a)f(b)$,
- $f(1_R) = 1_{R'}$.

Proposition 0.33 *Let $f : R \to R'$ be a ring homomorphism. Then, for any $a, b \in R$,*

(a) $f(0_R) = 0_{R'}$,

(b) $f(-a) = -f(a)$,

(c) $f(a-b) = f(a) - f(b)$,

(d) *if a is invertible, then $f(a)$ is invertible and $(f(a))^{-1} = f(a^{-1})$.*

Proposition 0.34 *The composition of ring homomorphisms is a ring homomorphism. The inverse of a ring isomorphism is a ring isomorphism. The set of all automorphisms of a ring is a group with the composition.*

Subrings and ideals

A subset S of a ring R is called a *subring* of R if S is an additive subgroup of R (that is, $0_R \in S$ and $\forall b, d \in S$, $b - d \in S$), $1_R \in S$ and, for all $b, d \in S$, $bd \in S$.

A subset $\mathfrak{a}$ of a ring R is called:

- a *left ideal* of R if $\mathfrak{a}$ is an additive subgroup of R and, for all $r \in R$ and $a \in \mathfrak{a}$, $ra \in \mathfrak{a}$;
- a *right ideal* of R if $\mathfrak{a}$ is an additive subgroup of R and, for all $r \in R$ and $a \in \mathfrak{a}$, $ar \in \mathfrak{a}$;
- an *ideal* of R if $\mathfrak{a}$ is a left ideal and a right ideal of R.

If R is a division ring, then 0 and R are the unique left ideals (and the unique right ideals) of R.

Proposition 0.35 *Let S be a subring of a ring R. Then*

(a) $0_S = 0_R$ *and* $1_S = 1_R$.

(b) *The additive inverses of $b \in S$, in rings R and S, coincide.*

(c) *If $b \in S$ is invertible in S, then b is invertible in R and the two inverses coincide.*

(d) *S, with the restrictions of addition and multiplication to $S \times S$, is a ring.*

Proposition 0.36 *Let $f : R \to R'$ be a ring homomorphism.*

(a) *If S is a subring of R, then $f(S)$ is a subring of R',*

(b) *If $\mathfrak{a}$ is an ideal* (*respectively, left ideal; right ideal*) *of R and f is an epimorphism, then $f(\mathfrak{a})$ is an ideal* (*respectively, left ideal; right ideal*) *of R'.*

(c) *If S' is a subring of R', then $f^{-1}(S')$ is a subring of R.*

(d) *If $\mathfrak{a}$ is an ideal* (*respectively, left ideal; right ideal*) *of R', then $f^{-1}(\mathfrak{a})$ is an ideal* (*respectively, left ideal; right ideal*) *of R. In particular,* $\ker f = f^{-1}(\{0\})$ *is an ideal of R.*

(e) *f is injective if and only if* $\ker f = 0$.

Proposition 0.37 *Let $(B_i)_{i\in I}$ be a non-empty family of subrings* (*respectively, ideals; left ideals; right ideals*) *of a ring R.*

(a) $\bigcap_{i\in I} B_i$ *and* $\sum_{i\in I} B_i$ *are subrings* (*respectively, ideals; left ideals; right ideals*) *of R.*

(b) *If the family $(B_i)_{i\in I}$ is totally ordered by inclusion, then $\bigcup_{i\in I} B_i$ is a subring* (*respectively, ideal; left ideal; right ideal*) *of R.*

Subrings and ideals generated by a set

Let X be a subset of a ring R. The subring of R *generated by X* is the intersection of all subrings (respectively, ideals; left ideals; right ideals) of R that contain X.

Let R be a ring. If $X_1, \dots, X_k$ are non-empty subsets of R, then $X_1 \cdots X_n$ denotes the subset of R whose elements have the form

$$\sum_{i=1}^{n} a_{i,1} \cdots a_{i,k}, \quad \text{where} \quad n \in \mathbb{N}, a_{i,j} \in X_j, i \in \{1, \dots, n\}, j \in \{1, \dots, k\}.$$

Note that this product of subsets of R is associative. If $Y_1, \dots, Y_k$ are non-empty subsets or elements of R, and at least one of them is a subset of R, then $Y_1 \cdots Y_k$ denotes the set $X_1 \cdots X_n$, where $X_j = Y_j$, if Y_j is a subset of R, and $X_j = \{Y_j\}$, if Y_j is an element of R. In particular, if $x \in R$, then

$$Rx = R\{x\} = \{ax : a \in R\}$$

is the left ideal of R generated by $\{x\}$ and

$$RxR = R\{x\}R = \left\{ \sum_{i=1}^{n} a_i x b_i : n \in \mathbb{N}, a_i, b_i \in R, i \in \{1, \dots, n\} \right\}$$

is the ideal of R generated by $\{x\}$.

Proposition 0.38 *Let $\mathfrak{c}$ be a left ideal and let $\mathfrak{d}$ be a right ideal of a ring R. Let X be a non-empty subset of R. Then $\mathfrak{c}X$ is a left ideal of R and $\mathfrak{c}\mathfrak{d}$ and $\mathfrak{c}X\mathfrak{d}$ are ideals of R.*

Quotient rings

Let $\mathfrak{a}$ be an ideal of a ring R. In the additive group $R/\mathfrak{a}$, define a multiplication as follows: for all $x, y \in R$,

$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}.$$

It is easy to prove that this multiplication is well defined and, with it, the additive group $R/\mathfrak{a}$ is a ring, whose identity is $1_R + \mathfrak{a}$. The ring $R/\mathfrak{a}$ is called the *quotient ring* of R by $\mathfrak{a}$.

Proposition 0.39 *Let $\mathfrak{a}$ be an ideal of a ring R. The set of all subrings* (*respectively, ideals; left ideals; right ideals*) *of $R/\mathfrak{a}$ is*

$$\{S/\mathfrak{a} : S \textit{ is a subring } (\textit{respectively, ideal; left ideal; right ideal}) \\ \textit{of } R \textit{ and } \mathfrak{a} \subseteq S\}.$$

Proof Only for subrings. The proofs for ideals, left ideals and right ideals are analogous.

Let $\mathcal{S}$ be a subring of $R/\mathfrak{a}$. In particular, $\mathcal{S}$ is an additive subgroup of $R/\mathfrak{a}$. By Proposition 0.16, $\mathcal{S} = S/\mathfrak{a}$, for some additive subgroup S of R such that $\mathfrak{a} \subseteq S$. Let $x, y \in S$. Then $x + \mathfrak{a}, y + \mathfrak{a} \in S/\mathfrak{a} = \mathcal{S}$. As $\mathcal{S}$ is a subring of $R/\mathfrak{a}$, $xy + \mathfrak{a} = (x + \mathfrak{a})(y + \mathfrak{a}) \in \mathcal{S} = S/\mathfrak{a}$. Thus $xy \in S$. Analogously $1_R + \mathfrak{a} \in \mathcal{S} = S/\mathfrak{a}$ and $1_R \in S$. Therefore S is a subring of R.

To prove the other inclusion, let S be a subring of R such that $\mathfrak{a} \subseteq S$. Then S is an additive subgroup of R and, by Proposition 0.16, $S/\mathfrak{a}$ is an additive subgroup of $R/\mathfrak{a}$. For all $x, y \in S$, $xy \in S$ and $(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a} \in S/\mathfrak{a}$. Moreover $1_R \in S$ and $1_R + \mathfrak{a} \in S/\mathfrak{a}$. Therefore $S/\mathfrak{a}$ is a subring of $R\mathfrak{a}$. ■

Ring isomorphism theorems

Proposition 0.40 *Let $f : R \to R'$ be a ring homomorphism. The rings $R/\ker f$ and $f(R)$ are isomorphic. The map*

$$\Phi : \frac{R}{\ker f} \to f(R), \quad x + \ker f \mapsto f(x),$$

is a ring isomorphism.

Proof By Proposition 0.17, Φ is an isomorphism of additive groups. It is easy to conclude that Φ is a ring isomorphism. ■

Proposition 0.41 *Let $\mathfrak{a}, \mathfrak{b}$ be ideals of a ring R such that $\mathfrak{a} \subseteq \mathfrak{b}$. The rings $R/\mathfrak{b}$ and $(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ are isomorphic. The map*

$$\Psi : \frac{R}{\mathfrak{b}} \to \frac{R/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}}, \quad x + \mathfrak{b} \mapsto (x + \mathfrak{a}) + (\mathfrak{b}/\mathfrak{a}),$$

is a ring isomorphism.

Proposition 0.42 *Let S be a subring and $\mathfrak{a}$ an ideal of a ring R. Then $S + \mathfrak{a}$ is a subring of R, $\mathfrak{a}$ is an ideal of $S + \mathfrak{a}$, $S \cap \mathfrak{a}$ is an ideal of S and the rings $(S + \mathfrak{a})/\mathfrak{a}$ and $S/(S \cap \mathfrak{a})$ are isomorphic. The map*

$$\Omega : \frac{S}{S \cap \mathfrak{a}} \to \frac{S + \mathfrak{a}}{\mathfrak{a}}, \quad x + (S \cap \mathfrak{a}) \mapsto x + \mathfrak{a},$$

is a ring isomorphism.

Exercises

0.3.1 Which are the subrings and the ideals of the ring $\mathbb{Z}$ of the integer numbers?

0.4 Commutative rings

Proposition 0.43 *Let $n \in \mathbb{N}$.*

(a) *With the operations defined in Section* 0.1, *$\mathbb{Z}_n$ is a commutative ring isomorphic to the quotient ring $\mathbb{Z}/\mathbb{Z}n$.*

(b) *$\mathbb{Z}_n$ is a field if and only if n is a prime number.*

Proof (a) By Proposition 0.2, $\mathbb{Z}_n$ is a commutative ring. Prove that $\mathbb{Z}_n \to \mathbb{Z}/\mathbb{Z}n$, $\overline{k} \mapsto k + \mathbb{Z}n$, is a well-defined ring isomorphism.

(b) Suppose that n is prime. Let $\overline{x} \in \mathbb{Z}_n \setminus 0$. Prove that

$$f : \mathbb{Z}_n \to \mathbb{Z}_n, \quad \overline{y} \mapsto \overline{x}\,\overline{y} = \overline{xy}$$

is injective. As $\mathbb{Z}_n$ is finite, f is bijective. Then there is $\overline{y} \in \mathbb{Z}_n$ such that $\overline{x}\,\overline{y} = \overline{1}$, that is, $\overline{y}$ is an inverse of $\overline{x}$. Therefore $\mathbb{Z}_n$ is a field.

Conversely, suppose that n is not prime. If $n = 1$, then $|\mathbb{Z}_n| = 1$ and $\mathbb{Z}_n$ is not a field. If $n > 1$, then there are $x, y \in \{1, \ldots, n-1\}$ such that $n = xy$. It follows that $\overline{x}, \overline{y} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ and $\overline{x}\,\overline{y} = \overline{0}$. Therefore $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{\overline{0}\}$ is not a group and $\mathbb{Z}_n$ is not a field. ■

Field of fractions of an integral domain

A commutative ring R is called an *integral domain* if $R \neq 0$ and, for all $a, b \in R$, $ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$. If R is an integral domain, then, for all $a, b \in R, c \in R \setminus 0$, $ac = bc \Rightarrow a = b$. Fields are integral domains.

Let R be an integral domain. Let $R^* = R \setminus 0$. In $R \times R^*$, define an equivalence relation $\approx$ as follows:

$$(a, b) \approx (c, d) \Leftrightarrow ad = cb.$$

Let Q of the equivalence classes for this relation. If $(a, b) \in R \times R^*$, the equivalence class of (a, b) is represented as a fraction a/b. In Q, define an addition and a multiplication as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

It is easy to see that, with these operations, Q is a field, called the *field of fractions of* R. The map

$$i : R \to Q, \quad a \mapsto a/1,$$

is a ring monomorphism, which allows us to identify R with its image $i(R)$ and thus consider R as a subring of Q.

Polynomials in one variable

Let R be a commutative ring. Let X be a variable. Let $R[X]$ be the set of all sequences $(a_n)_{n \in \mathbb{N}_0}$ of elements of R such that $\{n \in \mathbb{N}_0 : a_n \neq 0\}$ is finite. Denote each $(a_n)_{n \in \mathbb{N}_0} \in R[X]$ by

$$\sum_{n \in \mathbb{N}_0} a_n X^n. \tag{3}$$

At this point, (3) does not represent a sum; it is just a symbol. Note that

$$\sum_{n \in \mathbb{N}_0} a_n X^n = \sum_{n \in \mathbb{N}_0} b_n X^n \quad \Leftrightarrow \quad \forall n \in \mathbb{N}_0,\ a_n = b_n. \tag{4}$$

In $R[X]$, define an addition and a multiplications as follows:

$$\left(\sum_{n\in\mathbb{N}_0} a_nX^n\right) + \left(\sum_{n\in\mathbb{N}_0} b_nX^n\right) = \sum_{n\in\mathbb{N}_0} (a_n + b_n)X^n, \tag{5}$$

$$\left(\sum_{r\in\mathbb{N}_0} a_rX^r\right)\left(\sum_{s\in\mathbb{N}_0} b_sX^s\right) = \sum_{n\in\mathbb{N}_0}\left(\sum_{r,s\in\mathbb{N}_0:rs=n} a_rb_s\right)X^n. \tag{6}$$

Proposition 0.44 *With the operations* (5) *and* (6), $R[X]$ *is a ring. The zero of* $R[X]$ *is* $(0, 0, 0, \dots)$ *and the identity of* $R[X]$ *is* $(1, 0, 0, \dots)$*.*

The elements of $R[X]$ are called polynomials in the variable X with coefficients in R.

The polynomials were introduced here as sequences of elements of R, but could have been introduced as other objects. The nature of the polynomials is not important, what is important is the way they operate. Whatever the way the ring of polynomials is introduced, polynomials must be represented by expressions of form (3), must satisfy (4) and addition and multiplication must be defined by (5) and (6).

Later, when studying polynomials in several variables, the polynomials will be introduced a little more complicated way because, among other things, we want that, if X and Y are distinct variables, then $R[X] \neq R[Y]$, what does not happen with the previous definition.

Let $a \in R$ e $k \in \mathbb{N}_0$. Then aX^k denotes the polynomial $(a_n)_{n\in\mathbb{N}_0}$ where $a_k = a$ and $a_j = 0$ whenever $j \neq k$; X^k denotes the polynomial $1X^k$; X also denotes the polynomial X^1; and a also denotes the polynomial aX^0.

With this notation, X^0 is the identity of $R[X]$, X^k is the kth power of X and aX^k is the product of the polynomial a by the polynomial X^k. Moreover, given a polynomial (3), there is $p \in \mathbb{N}_0$ such that, for $n \geq p$, $a_n = 0$ and

$$\sum_{n\in\mathbb{N}_0} a_nX^n = \sum_{n=0}^{p} a_nX^n = a_0 + a_1X + \cdots + a_pX^p,$$

where, on the right side, it is the sum of the polynomials $a, a_1X, \dots, a_pX^p$. Thus all operations suggested in (3) are real.

Extend the addition and order defined in $\mathbb{N}_0$ to $\{-\infty\} \cup \mathbb{N}_0$, according to the usual conventions: whatever $n \in \{-\infty\} \cup \mathbb{N}_0$,

$$n + (-\infty) = (-\infty) + n = -\infty, \quad -\infty \leq n.$$

Let $f = \sum a_nX^n \in R[X]$. If $f \neq 0$, the *degree* of f is the largest n such that $a_n \neq 0$. If $f = 0$, it is said that the *degree* of f is $-\infty$. The degree of f is denoted by $d(f)$.

Proposition 0.45 *For all $f, g \in R[X]$,*

(a) $d(f+g) \leq \max\{d(f), d(g)\}$,

(b) $d(fg) \leq d(f) + d(g)$,

(c) *if R is an integral domain, then $d(fg) = d(f) + d(g)$,*

(d) *if R is an integral domain, then $R[X]$ is also an integral domain.*

If $f \in R[X] \setminus 0$ is a polynomial in a single variable X and $d = d(f)$, then the coefficient of X^d in f is called the *leading coefficient* of f; if the leading coefficient of f is 1, it is said that f is a *monic polynomial.*

Division of polynomials

Proposition 0.46 *Let R be a commutative ring. If $f, g \in R[X]$, $g \neq 0$ and the leading coefficient of g is invertible, then there are unique polynomials $q, r \in R[X]$ such that $f = gq + r$ and $d(r) < d(g)$.*

Proof (Existence) By induction on $d(f)$. If $d(f) < d(g)$, take $q = 0$ and $r = f$. If $d(f) = d(g) = 0$, take $q = g^{-1}f$ and $r = 0$.

Suppose now that neither of the two previous cases occurs. Then $d(f) \geq 1$ and $d(f) \geq d(g)$. Suppose that $n = d(f)$, $m = d(g)$, $f = a_nX^n + \cdots + a_0$, $g = b_mX^m + \cdots + b_0$, $a_i, b_j \in R$. Let $f' = f - gb_m^{-1}a_nX^{n-m}$. Note that $d(f') < d(f)$. By the induction assumption, there are $q', r \in R[X]$ such that $f' = gq' + r$ and $d(r) < d(g)$. Thus

$$f = f' + gb_m^{-1}a_nX^{n-m} = g(q' + b_m^{-1}a_nX^{n-m}) + r.$$

(Unicity) Suppose that $f = gq+r = gq'+r'$, $d(r) < d(g)$ and $d(r') < d(g)$. Then $g(q-q') = r'-r$. Suppose that $q \neq q'$. As the leading coefficient of g is invertible, $d(g(q-q')) = d(g) + d(q-q') \geq d(g)$. On the other hand, $d(r'-r) < d(g)$, which is absurd. Hence $q = q'$ e $r' = r$. ■

Euclidean rings

The integral domain $\mathbb{Z}$ of the integers and the integral domain $F[X]$ of the polynomials in a variable X with coefficients in a field F are known to share a Euclidean division, as reproduced below.

Proposition 0.47 *Let $a, b \in \mathbb{Z}$, with $a \neq 0$. there are unique integer numbers q, r such that $b = aq + r$ and $0 \leq r < |a|$.*

Proposition 0.48 *Let F be a field and $f, g \in F[X]$, with $g \neq 0$. there are unique polynomials $q, r \in F[X]$ such that $f = gq + r$ and $d(r) < d(g)$.*

More generally, a commutative ring R is said to be *Euclidean* if there is a map $\delta : R \setminus 0 \to \mathbb{N}_0$ such that, for all $a, b \in R$,

- if $ab \neq 0$, then $\delta(a) \leq \delta(ab)$
- and, if $a \neq 0$, then there are $q, r \in R$ such that $b = aq + r$ and ($r = 0$ or $\delta(r) < \delta(a)$).

A Euclidean ring R is called *Euclidean domain* if it is a Euclidean ring and an integral domain.

The rings $\mathbb{Z}$ and $F[X]$ are examples of Euclidean domains. In $\mathbb{Z}$, $\delta(a) = |a|$. In $F[X]$, $\delta(f) = d(f)$. Other examples: a field F, with $\delta(a) = 0$; the ring of Gauss integers $\{a + ib : a, b \in \mathbb{Z}\}$, with $\delta(a + ib) = a^2 + b^2$.

Principal ideal rings

Let R be a commutative ring. An ideal $\mathfrak{a}$ of R is said to be *principal* if $\mathfrak{a}$ is generated by a set with a unique element.

It is said that R is a *principal ideal ring* if all the ideals of R are principal.

It is said that R is a *principal ideal domain* if it is a principal ideal ring and an integral domain.

Proposition 0.49 *If R is a Euclidean ring, then R is a principal ideal ring.*

Proof Let R be a Euclidean ring. Let $\mathfrak{a}$ be an ideal of R. If $\mathfrak{a} = 0$, then $\mathfrak{a}$ is generated by $\{0\}$. Suppose now that $\mathfrak{a} \neq 0$. Choose $x \in \mathfrak{a} \setminus 0$ so that $\delta(x)$ is minimal. Let $y \in \mathfrak{a}$. there are $q, r \in R$ such that $y = xq + r$ and ($r = 0$ or $\delta(r) < \delta(x)$). If $r \neq 0$, then $r = y - xq \in \mathfrak{a} \setminus 0$, which contradicts the choice of x. Thus $r = 0$ and $y = xq \in Rx$. Hence $\mathfrak{a} = Rx$. ■

Prime ideals and maximal ideals

Let R be a commutative ring.

An ideal $\mathfrak{p}$ of R is said to be *prime* if $\mathfrak{p} \neq R$ and, for all $a, b \in R$, $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

An ideal $\mathfrak{p}$ of R is said to be *maximal* if $\mathfrak{m} \neq R$ and $\mathfrak{m}$ is maximal in the set of all proper ideals of R.

Proposition 0.50 *Let $\mathfrak{a}$ be a proper ideal of a commutative ring R. Then there is a maximal ideal $\mathfrak{m}$ of R such that $\mathfrak{a} \subseteq \mathfrak{m} \subsetneqq R$.*

Proof Let B be the set of all proper ideals of R that contain $\mathfrak{a}$. Clearly $\mathfrak{a} \in B$. Let C be a non-empty chain of elements of B. By Proposition 0.37, $\mathfrak{d} = \bigcup_{\mathfrak{c} \in C} \mathfrak{c}$ is an ideal of R. For each $\mathfrak{c} \in C$, as $\mathfrak{c} \neq R$, $1 \notin \mathfrak{c}$. Therefore $1 \notin \mathfrak{d}$ and $\mathfrak{d} \neq R$. Thus $\mathfrak{d} \in B$.

By Zorn's lemma, B has a maximal element $\mathfrak{m}$. It is easy to conclude that $\mathfrak{m}$ is a maximal ideal of R that contains $\mathfrak{a}$. ■

Corollary 0.51 *If R is a non-trivial commutative ring, then R contains a maximal ideal.*

Proposition 0.52 *A non-trivial commutative ring R is a field if and only if 0 and R are the only ideals of R.*

Proof Let R be a field. Let $\mathfrak{a}$ be a non-trivial ideal of R. Let $x \in \mathfrak{a} \setminus 0$. Then $R = Rx^{-1}x \subseteq Rx \subseteq \mathfrak{a} \subseteq R$ and $\mathfrak{a} = R$.

Conversely suppose that 0 and R are the only ideals of a commutative ring R. For all $x \in R \setminus 0$, Rx is a non-trivial ideal of R; thus $R = Rx$ and there is $y \in R$ such that $1 = yx$. Therefore every element of $R \setminus 0$ has an inverse and R is a field. ■

Corollary 0.53 *Let $\mathfrak{m}$ be an ideal of a commutative ring R. The ring $R/\mathfrak{m}$ is a field if and only if $\mathfrak{m}$ is a maximal ideal of R.*

Proposition 0.54 *Let $\mathfrak{p}$ be an ideal of a commutative ring R.*

(a) *The ring $R/\mathfrak{m}$ is an integral domain if and only if $\mathfrak{m}$ is a prime ideal of R.*

(b) *If $\mathfrak{p}$ is maximal, then $\mathfrak{p}$ is prime.*

Divisibility in integral domains

Let R be an integral domain.

The set $U(R)$ of all units of R is a group with multiplication. If $a, b \in R$, $a \mid b$ means that a *divides* b, that is, there is $r \in R$ such that $b = ar$; $a \sim b$ means that a and b are *associates*, that is, $a \mid b$ and $b \mid a$.

An element $p \in R$ is said to be *prime* if $p \neq 0$, $p \notin U(R)$ and, for all $a, b \in R$, $p \mid ab \Rightarrow (p \mid a$ or $p \mid b)$. An element $p \in R$ is said to be *irreducible* if $p \neq 0$, $p \notin U(R)$ and, for all $a, b \in R$, $p = ab \Rightarrow (a \in U(R)$ or $b \in U(R))$.

Proposition 0.55 *Let R be an integral domain, $a, b \in R$ and $p \in R \setminus 0$.*

(a) *$a \mid b \Leftrightarrow bR \subseteq aR$.*

(b) *$a \sim b \Leftrightarrow bR = aR$.*

(c) *$\sim$ is an equivalence relation.*

(d) *$a \sim b$ if and only if there is $u \in U(R)$ such that $b = au$.*

(e) *p is a unit if and only if $pR = R$.*

(f) *If p is prime and $p \mid a_1 \cdots a_n$, then there is $i \in \{1, \ldots, n\}$ such that $p \mid a_i$.*

(g) *p is prime if and only if pR is a prime ideal of R.*

(h) *p is irreducible if and only if pR is maximal in the set of all proper principal ideals of R.*

(i) *If p is prime, then p is irreducible.*

(j) *If R is a principal ideal domain, then p is prime if and only if p is irreducible.*

Proof (j) Suppose that R is a principal ideal domain and p is irreducible. Let $a, b \in R$ and suppose that $p \mid ab$. Suppose that p does not divide b. Then $bR \not\subseteq pR$. Then $pR \subsetneqq pR + bR$. As $pR + bR$ is a principal ideal, it follows from de (h) that $R = pR + bR$. Then $1 = px + by$, for some $x, y \in R$. Then $a = apx + aby$. As $p \mid ab$, $p \mid a$. Hence p is prime. ■

Let R be an integral domain and $a_1, \ldots, a_n \in R$. It is said that $d \in R$ is a *greatest common divisor* of $a_1, \ldots, a_n$ if,

- for all $i \in \{1, \ldots, n\}$, $d \mid a_i$
- and, if, for all $i \in \{1, \ldots, n\}$, $e \mid a_i$, then $e \mid d$.

It is said that $m \in R$ is a *least common multiple* of $a_1, \ldots, a_n$ if,

- for all $i \in \{1, \ldots, n\}$, $a_i \mid m$
- and, if, for all $i \in \{1, \ldots, n\}$, $a_i \mid k$, then $m \mid k$.

With the above notation, if $d \in R$ is a greatest common divisor of $a_1, \ldots, a_n$, then the greatest common divisors of $a_1, \ldots, a_n$ are the associates of d. Analogously, if $m \in R$ is a least common multiple of $a_1, \ldots, a_n$, then the least common multiples of $a_1, \ldots, a_n$ are the associates of m.

Proposition 0.56 *Let R be a principal ideal domain and $a_1, \ldots, a_n \in R$.*

(a) *$d \in R$ is greatest common divisors of $a_1, \ldots, a_n$ if and only if $dR = a_1R + \cdots + a_nR$.*

(b) *$m \in R$ is a least common multiple of $a_1, \ldots, a_n$ if and only if $dR = a_1R \cap \cdots \cap a_nR$.*

Unique factorization domain

An integral domain R is called a *unique factorization domain* if the following two conditions are satisfied:

- every non-zero non-unit element of R can be written as a product of irreducible elements
- and, if $p_1 \cdots p_t = q_1 \cdots q_s$, where $s, t \in \mathbb{N}$ and $p_1, \ldots, p_t, q_1, \ldots, q_s \in R$ are irreducible, then $t = s$ and there is a bijective map $\pi : \{1, \ldots, t\} \to \{1, \ldots, t\}$ such that, for each $i \in \{1, \ldots, t\}$, $p_i \sim q_{\pi(i)}$.

Notation 0.57 Let R be a unique factorization domain. Later, we use the following notation.

Choose a set $\mathcal{R}$ of representatives of the equivalence classes of the relation $\sim$ as follows: $0 \in \mathcal{R}$; the class of the units is represented by 1; in each class of irreducible elements, we choose a representative in some way; in each of the remaining classes we choose the only element that is a product of irreducible elements previously chosen.

The resulting set $\mathcal{R}$ is a multiplicative monoid. It is easy to see that, if $a, b \in \mathcal{R}$ and $0 \neq a \mid b$, then $b/a \in \mathcal{R}$.

Denote by $\mathcal{I}$ the set of all irreducible elements that belong to $\mathcal{R}$.

When $R = \mathbb{Z}$, the ring of integers, we choose for $\mathcal{R}$ the set of all non-negative integers.

When $R = F[X]$, where F is a field, we choose for $\mathcal{R}$ the set formed by 0 and by all monic polynomials.

Thus, if a is a non-zero non-unit element of R, then

$$a = up_1^{r_1} \cdots p_t^{r_t},$$

where $u \in U(R)$, $p_1, \ldots, p_t$ are distinct elements of $\mathcal{I}$ and $r_1, \ldots, r_t \in \mathbb{N}$; moreover, the elements $u, t, p_1, \ldots, p_t, r_1, \ldots, r_t$ are unique up to the order of the factors $p_1^{r_1}, \ldots, p_t^{r_t}$.

Let $a_1, \ldots, a_n \in R \setminus 0$. Then

$$\begin{aligned} a_1 &= u_1 p_1^{r_{1,1}} \cdots p_t^{r_{1,t}}, \\ &\vdots \\ a_n &= u_n p_1^{r_{n,1}} \cdots p_t^{r_{n,t}}, \end{aligned}$$

where $u_1, \ldots, u_n \in U(R)$, $p_1, \ldots, p_t$ are distinct elements of $\mathcal{I}$ and the elements $r_{i,j}$ are non-negative integers.

Proposition 0.58 *With this notation,*

(a) $a_1 \mid a_2$ *if and only if, for each* $i \in \{1, \ldots, t\}$, $r_{1,i} \leq r_{2,i}$,

(b) $p_1^{\nu_1} \cdots p_t^{\nu_t} \in \mathcal{R}$, *where* $\nu_j = \min\{r_{1,j}, \ldots, r_{n,j}\}$, *is a greatest common divisor of* $a_1, \ldots, a_n$,

(c) $p_1^{\mu_1} \cdots p_t^{\mu_t} \in \mathcal{R}$, *where* $\mu_j = \max\{r_{1,j}, \ldots, r_{n,j}\}$, *is a least common multiple of* $a_1, \ldots, a_n$,

With the previous notation, $\gcd\{a_1, \ldots, a_n\}$ denotes $p_1^{\nu_1} \cdots p_t^{\nu_t}$ which is the unique greatest common divisor of $a_1, \ldots, a_n$ in $\mathcal{R}$. Analogously, $\mathrm{mmc}\{a_1, \ldots, a_n\}$ denotes $p_1^{\mu_1} \cdots p_t^{\mu_t}$.

Proposition 0.59 *Let R be a unique factorization domain. For all $b, a_1, \ldots, a_n \in R$, $\gcd\{ba_1, \ldots, ba_n\} \sim b\gcd\{a_1, \ldots, a_n\}$.*

Proposition 0.60 *Let R be a unique factorization domain. For every $p \in R$, p is prime if and only if p is irreducible.*

Lemma 0.61 *Let R be a principal ideal domain. For every chain of ideals $a_1R \subseteq a_2R \subseteq \cdots$ there is $p \in \mathbb{N}$ such that, for each $n \geq p$, $a_pR = a_nR$.*

Proof By Proposition 0.37, $\bigcup_{n\in\mathbb{N}} a_nR$ is an ideal of R. As R is a principal ideal domain, $\bigcup_{n\in\mathbb{N}} a_nR = bR$, for some $b \in R$. there is $p \in \mathbb{N}$ such that $b \in a_pR$. For each $n \geq p$, $bR \subseteq a_pR \subseteq a_nR \subseteq bR$ and $a_pR = a_nR$.

■

Lemma 0.62 *Let R be a principal ideal domain. If a is a non-zero non-unit element of R, then there is an irreducible element $p \in R$ such that $p \mid a$.*

Proof With a view to a contradiction, suppose that $a_1 = a$ does not have an irreducible divisor. As a_1 is a reducible non-unit, $a_1 = a_2b$, where a_2, b are non-units. Then a_2 is a non-unit and a_1, a_2 are not associates. As $a_2 \mid a_1$ and a_1 does not have irreducible divisors, a_2 does not have irreducible divisors. Therefore, a_2 also has a non-unit non-associate divisor a_3. By repeating this argument, we construct a sequence $(a_n)_{n\in\mathbb{N}}$ such that, for each n, a_{n+1} is a non-associate divisor of a_n. Then $a_1R \subsetneqq a_2R \subsetneqq \cdots$, which contradicts the previous lemma. ■

Proposition 0.63 *If R is a principal ideal domain, then R be a unique factorization domain.*

Proof (Existence of factorization) Let a be a non-zero non-unit element of R. With a view to a contradiction, suppose that $a_1 = a$ cannot be written as a product of irreducible elements. By the previous lemma, there is an irreducible element p_1 that divides a_1. Then $a_1 = p_1a_2$, where $a_2 \in R$ is reducible, non-zero, non-unit and a_2 cannot be written as a product of irreducible elements. Then $a_2 = p_2a_3$, where p_2 is irreducible. By repeating this argument, we construct a sequence $(p_n)_{n\in\mathbb{N}}$ of irreducible elements and a sequence $(a_n)_{n\in\mathbb{N}}$ of elements of R such that, for each n, $a_n = p_na_{n+1}$. Then $a_1R \subsetneqq a_2R \subsetneqq \cdots$, which contradicts Lemma 0.61.

(Unicity of factorization) Suppose that $p_1 \cdots p_t = q_1 \cdots q_s$, where $p_1, \ldots, p_t, q_1, \ldots, q_s$ are irreducible. The proof is by induction on $\mu = \min\{t, s\}$.

By Proposition 0.55 (j), p_t is prime and, therefore, p_t divides one of the elements $q_1, \ldots, q_s$. Without loss of generality, suppose that $p_t \mid q_s$. As q_s is irreducible and p_t is a non-unit, $p_t \sim q_s$. Then $q_s = up_t$, for some $u \in U(R)$.

Suppose that $\mu = 1$. Without loss of generality, suppose that $t = 1$. Then $1 = uq_1 \cdots q_{s-1}$. If $s > 1$, then q_1 would be a unit, a contradiction. Hence $s = 1$ and the proof is complete in this case.

Suppose that $t > 1$. Then $p_1 \cdots p_{t-1} = q'_1 \cdots q'_{s-1}$, where $q'_1 = uq_1$ and $q'_i = q_i$ for each $i \in \{2, \ldots, s-1\}$. By the induction assumption, $t = s$ and there is a bijective map $\pi : \{1, \ldots, t-1\} \to \{1, \ldots, t-1\}$ such that $p_i \sim q'_{\pi(i)} \sim q_{\pi(i)}$ for each $i \in \{1, \ldots, t-1\}$. It is easy to complete the proof.

■

Unique factorization of polynomials

Let R be a unique factorization domain. The content of a polynomial $f \in R[X] \setminus 0$ is the greatest common divisor of the coefficients of f that belongs to $\mathcal{R}$ ([6]). The content of f is denoted by $C(f)$. A polynomial $f \in R[X]$ is said to be *primitive* if $C(f) = 1$.

Lemma 0.64 *Let R be a unique factorization domain. Let $a, b \in R \setminus 0$ and $f, g \in R[X] \setminus 0$.*

(a) *$C(af) \sim aC(f)$. Se $a \in \mathcal{R}$, $C(af) = aC(f)$.*

(b) *There is a primitive polynomial $f' \in R[X]$ such that $f = C(f)f'$.*

(c) *If f and g are primitive and $af = bg$, then $a \sim b$.*

Proof (a) Suppose that $f = c_nX^n + \cdots + c_0$. Then

$$C(af) = \gcd\{ac_0, \ldots, ac_n\} \sim a \gcd\{c_0, \ldots, c_n\} = aC(f).$$

As $\mathcal{R}$ is a multiplicative monoid, if $a \in \mathcal{R}$, then $C(af) = aC(f)$.

(b) As $C(f)$ divides all coefficients of f, $f = C(f)f'$, for some $f' \in R[X]$. By (a), $C(f) = C(f)C(f')$. Hence $C(f') = 1$ and f' is primitive.

(c) $a = aC(f) \sim C(af) = C(bg) \sim bC(g) = b$. ■

Lemma 0.65 [Gauss] *Let R be a unique factorization domain and $f, g \in R[X] \setminus 0$. Then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.*

Proof First, let us prove that the product of primitive polynomials is primitive. Let $f = a_nX^n + \cdots + a_0$, $g = b_mX^m + \cdots + b_0 \in R[X]$ be primitive polynomials. Then

$$fg = \sum_{k=0}^{n+m} c_kX^k, \quad \text{where} \quad c_k = \sum_{i+j=k} a_ib_j.$$

With a view to a contradiction, suppose that fg is not primitive. Then there is an irreducible element p of R that divides all coefficients c_k. As f is primitive, p does not divide all coefficients of f. Let s be the smallest index such that p does not divide a_s. Analogously, let t be the smallest index such that p does not divide b_t. As p divides the elements $a_0, \ldots, a_{s-1}, b_0, \ldots, b_{t-1}$ and

$$p \mid c_{s+t} = a_0b_{s+t} + \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t}b_0,$$

it follows that $p \mid a_sb_t$. As p is prime, $p \mid a_s$ or $p \mid b_t$, which is a contradiction. Hence fg is primitive.

[6] The set $\mathcal{R}$ was introduced in page 26.

Now the general case. By the previous lemma, there are polynomials $f', g' \in R[X]$ such that $f = C(f)f'$ and $g = C(g)g'$. By the first part of this proof, $C(f'g') = 1$. By the previous lemma,

$$C(fg) = C(C(f)f'C(g)g') = C(f)C(g)C(f'g') = C(f)C(g). \qquad \blacksquare$$

Lemma 0.66 *If R is an integral domain, $U(R[X]) = U(R)$.*

If R is not an integral domain, the above lemma may be false. For example, $2X + 1 \in U(\mathbb{Z}_4[X])$, because $(2X + 1)^2 = 1$, but $2X + 1 \notin U(\mathbb{Z}_4)$.

Lemma 0.67 *Let R be an integral domain. An element $a \in R$ is irreducible in R if and only a it is irreducible in $R[X]$.*

Proof Suppose that $a \in R$ is irreducible in R. Suppose that $a = fg$, where $f, g \in R[X]$. As $0 = d(a) = d(f)+d(g)$, $0 = d(f) = d(g)$ and $f, g \in R$. As a is irreducible in R, $f \in U(R) = U(R[X])$ ou $g \in U(R) = U(R[X])$. Hence a is irreducible in $R[X]$.

The reciprocal statement is also easy to prove. $\blacksquare$

Lemma 0.68 *Let R be a unique factorization domain and let Q be the field of fractions of R.*

(a) *If $g \in Q[X] \setminus 0$, then there are $a/b \in Q \setminus 0$ and a primitive polynomial $g' \in R[X]$ such that $g = (a/b)g'$.*

(b) *If $f \in R[X]$ is primitive, then f is irreducible in $R[X]$ if and only if f is irreducible in $Q[X]$.*

Proof (a) Let b be an element of $R \setminus 0$ such that $bg \in R[X]$. By Lemma 0.64, there is a primitive polynomial $g' \in R[X]$ such that $bg = ag'$, where $a = C(bg)$.

(b) Let $f \in R[X]$ be a primitive polynomial. Suppose that f is irreducible in $R[X]$. Suppose that $f = gh$, where $g, h \in Q[X]$. By (a), $g = (a/b)g'$ and $h = (c/d)h'$, where $a/b, c/d \in Q$ and $g', h' \in R[X]$ are primitive. Thus $bdf = acg'h'$ and

$$bd = bdC(f) \sim C(bdf) = C(acg'h') \sim acC(g'h') = ac.$$

Let u be a unit of R such that $ac = ubd$. Then $f = ug'h'$. As f is irreducible in $R[X]$, $ug' \in U(R[X]) = U(R)$ or $h' \in U(R[X]) = U(R)$. Then $g = (a/b)g' \in Q \setminus 0 = U(Q[X])$ or $h = (c/d)h' \in Q \setminus 0 = U(Q[X])$. Hence f is irreducible in $Q[X]$.

Conversely, suppose that f is irreducible in $Q[X]$. suppose that $f = gh$, where $g, h \in R[X]$. As f is irreducible in $Q[X]$, $g \in U(Q[X]) = U(Q) = Q \setminus 0$ or $h \in U(Q[X]) = Q \setminus 0$. Then $g \in R \setminus 0$ or $h \in R \setminus 0$. If $g \in R \setminus 0$, then $1 = C(f) = C(gh) \sim gC(h)$, which implies that $g \in U(R) = U(R[X])$. Analogously, if $h \in R \setminus 0$, then $h \in U(R[X])$. Hence f is irreducible in $R[X]$.

$\blacksquare$

Proposition 0.69 *Let R be a unique factorization domain. If $f \in R[X]$ is irreducible and $d(f) > 0$, then f is primitive.*

Proof If $f \in R[X]$ is not primitive and $d(f) > 0$, then $f = C(f)f'$, where $C(f)$ and f' are non-units. Hence f is reducible. ■

Proposition 0.70 *If F is a field, then $F[X]$ is a unique factorization domain.*

Proof As noted on page 23, $F[X]$ is a Euclidean domain. By Proposition 0.49, $F[X]$ is a principal ideal domain. By Proposition 0.63, $F[X]$ is a unique factorization domain. ■

Proposition 0.71 *If R is a unique factorization domain, then $R[X]$ is also a unique factorization domain.*

Proof Let Q be the field of fractions of R. Let f be a non-zero non-unit element of $R[X]$.

Case 1. Suppose that $d(f) = 0$.

(Factorization existence) As R is a unique factorization domain, $f = p_1 \cdots p_t$, where $p_1, \dots, p_t$ are irreducible in R. By Lemma 0.67, $p_1, \dots, p_t$ are also irreducible in $R[X]$.

(Factorization unicity) Suppose that $f = p_1 \cdots p_t = q_1 \cdots q_s$, where $p_1, \dots, p_t, q_1, \dots, q_s$ are irreducible in $R[X]$. As $d(f) = 0$, $p_1, \dots,$ $p_t, q_1,$ $\dots, q_s$ also have degree 0 and, therefore, belong to R. By Lemma 0.67, $p_1, \dots, p_t, q_1, \dots, q_s$ are irreducible in R. As R is a unique factorization domain, $t = s$ and there is a bijective map $\pi : \{1, \dots, t\} \to \{1, \dots, t\}$ such that, for each $i \in \{1, \dots, t\}$, p_i and $q_{\pi(i)}$ are associates in R. Clearly p_i and $q_{\pi(i)}$ are also associates in $R[X]$.

Caso 2. Suppose that $d(f) > 0$.

(Factorization existence) By Lemma 0.64, $f = cf'$, where $c = C(f)$ and $f' \in R[X]$ is primitive. As $Q[X]$ is a unique factorization domain, $f' = q_1 \cdots q_t$, where $q_1, \dots, q_t$ are irreducible in $Q[X]$. By Lemma 0.68, for each $i \in \{1, \dots, t\}$, there are $a_i/b_i \in Q$ and a primitive polynomial $p_i \in R[X]$ such that $q_i = (a_i/b_i)p_i$. Thus q_i and p_i are associates in $Q[X]$ and, therefore, p_i is also irreducible in $Q[X]$. By Lemma 0.68, p_i is irreducible in $R[X]$. On the other hand, $b_1 \cdots b_t f' = a_1 \cdots a_t p_1 \cdots p_t$. By Lemma 0.64 (c), $b_1 \cdots b_t$ and $a_1 \cdots a_t$ are associates in R. Thus there is $u \in U(R)$ such that $a_1 \cdots a_t = ub_1 \cdots b_t$. Then $f' = up_1 \cdots p_t$ and $f = cup_1 \cdots p_t$.

Suppose that $cu \in U(R)$. Then $f = (cup_1)p_2 \cdots p_t$ is a decomposition of f as a product of irreducible elements of $R[X]$.

Suppose that $cu \notin U(R)$. As R is a unique factorization domain, $cu = c_1 \cdots c_k$, where $c_1, \dots, c_k$ are irreducible in R. By Lemma 0.67, $c_1, \dots, c_k$

are also irreducible in $R[X]$. Thus $f = c_1 \cdots c_k p_1 \cdots p_t$ is a decomposition of f as a product of irreducible elements of $R[X]$.

(Factorization unicity) Suppose that

$$f = c_1 \cdots c_k p_1 \cdots p_t = d_1 \cdots d_l q_1 \cdots q_s$$

are decompositions of f as two products of irreducible elements of $R[X]$, where $k, l \geq 0$, $c_1, \ldots,\ c_k, d_1, \ldots, d_l$ have degree 0, $t, s > 0$ e $p_1, \ldots, p_t, q_1, \ldots, q_s$ have degree greater than 0. By Proposition 0.69, $p_1 \cdots p_t, q_1 \cdots q_s$ are primitive. By Lemma 0.64, $c_1 \cdots c_k$ and $d_1 \cdots d_l$ are associates in R, where $c_1 \cdots c_k = 1$ if $k = 0$, and $d_1 \cdots d_l = 1$ if $l = 0$. Thus $k = 0$ if and only if $l = 0$. Suppose that $k > 0$. As R is a unique factorization domain, $k = l$ and there is a bijective map $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ such that, for each $i \in \{1, \ldots, k\}$, c_i and $d_{\sigma(i)}$ are associates in R and, therefore, there is $u \in U(R)$ such that $d_1 \cdots d_l = uc_1 \cdots c_k$. Then

$$p_1 \cdots p_t = uq_1 \cdots q_s.$$

By Lemma 0.68, $p_1, \ldots, p_t, q_1, \ldots, q_s$ are irreducible in $Q[X]$. As $Q[X]$ is a unique factorization domain, $t = s$ and there is a bijective map $\pi : \{1, \ldots, t\} \to \{1, \ldots, t\}$ such that, for each $j \in \{1, \ldots, k\}$, p_j and $q_{\pi(j)}$ are associates in $Q[X]$. Let $j \in \{1, \ldots, k\}$. there is $a_j/b_j \in Q \setminus 0 = U(Q[X])$ such that $q_{\pi(j)} = (a_j/b_j)p_j$. Then $b_j q_{\pi(j)} = a_j p_j$ and, by Lemma 0.64, b_j and a_j are associates in R. Then $a_j/b_j \in U(R) = U(R[X])$. Hence p_j and $q_{\pi(j)}$ are associates in $R[X]$. ■

Theorem 0.72 [Eisenstein criterion] *Let R be a unique factorization domain Let Q be the field of fractions of R. Let*

$$f = a_n X^n + \cdots + a_0 \in R[X], \quad \textit{where} \quad n = d(f) \geq 1.$$

If there is an irreducible element p in R such that

$$p \nmid a_n, \quad p \mid a_i, \ \textit{for}\ i \in \{0, 1, \ldots, n-1\}, \quad \textit{and} \quad p^2 \nmid a_0,$$

then f is irreducible in $Q[X]$. Moreover, if f is primitive, then f is irreducible in $R[X]$.

Proof First suppose that f is primitive. Let us prove that f is irreducible in $R[X]$. Suppose that $f = gh$, where $g, h \in R[X]$. As $1 = C(f) = C(g)C(h)$, $1 = C(g) = C(h)$ and g, h are primitive.

With a view to a contradiction, suppose that

$$\begin{aligned} g &= b_r X^r + \cdots + b_0, \quad \text{where} \quad r = d(g) \geq 1, \\ h &= c_s X^s + \cdots + c_0, \quad \text{where} \quad s = d(h) \geq 1. \end{aligned}$$

As $p \mid a_0 = b_0c_0$, $p \mid b_0$ or $p \mid c_0$. Without loss of generality, suppose that $p \mid b_0$. As $p^2 \nmid a_0 = b_0c_0$, $p \nmid c_0$. As g is primitive, p does not divide all coefficients of g. Let k be the lowest index such that $p \nmid b_k$. Then

$$p \mid a_k = b_0c_k + \cdots + b_{k-1}c_1 + b_kc_0$$

As $p \mid b_0, \ldots, p \mid b_{k-1}$, $p \mid b_kc_0$. As p is prime $p \mid b_k$ or $p \mid c_0$, which is a contradiction. Hence $d(g) = 0$ or $d(h) = 0$.

As g and h are primitive, $g \in U(R)$ or $h \in U(R)$. Hence f is irreducible in $R[X]$. By Lemma 0.68, f is irreducible in $Q[X]$.

Now consider the general case. There is a primitive polynomial $f' = a'_nX^n + \cdots + a'_0 \in R[X]$ such that $f = C(f)f'$. For each i, $a_i = C(f)a'_i$. As $p \nmid a_n$, $p \nmid C(f)$. As $p \nmid a_n$, $p \nmid a'_n$. For each $i \in \{0, 1, \ldots, n-1\}$, as $p \mid a_i$ and $p \nmid C(f)$, $p \mid a'_i$. As $p^2 \nmid a_0$, $p^2 \nmid a'_0$. By the previous case, f' is irreducible in $Q[X]$. As f and f' are associates in $Q[X]$, f is also irreducible in $Q[X]$. ■

Exercises

0.4.1 Show that $\mathbb{Z}_4$ is a Euclidean ring but is not a Euclidean domain.

0.4.2 Let F be a field. Prove that $R = F^{2\times 2}$, the ring of 2×2 matrices with entries in F, has only two ideals: 0 e R. Conclude that R is a principal ideal ring but is not an integral domain. ([7])

0.4.3 Let S be a subset of a commutative ring R such that $0 \notin S$. Prove that the set of all ideals of R disjoint from S has a maximal element.

[7] A non-trivial ring R with only two ideals is said to be *simple*. In general, if D is a division ring and $n \in \mathbb{N}$, then $D^{n\times n}$ is simple.

Chapter 1

Groups

1.1 Group actions. Cauchy theorem

An *action* of a group G on a set X is a map

$$G \times X \to X, \quad (g, x) \mapsto gx, \tag{1.1}$$

such that, for all $g, h \in G$, $x \in X$, $g(hx) = (gh)x$ and $1x = x$ ([1]).

Given an action (1.1) and $x \in X$, the *orbit* of x, $O(x)$, and the *stabilizer* of x, $S(x)$, are defined by

$$O(x) = \{gx : g \in G\}, \qquad S(x) = \{g \in G : gx = x\}.$$

Note that the orbits are the equivalence classes for an equivalence relation $\sim$ defined on X as follows: $x \sim y \Leftrightarrow \exists g \in G : y = gx$.

Examples 1.1 1. The multiplication in a group G is an action of G on G.

2. If V is a vector space over a field K, then $K^* = K \setminus \{0\}$ is a multiplicative group and the scalar multiplication $K^* \times V \to V$, $(\lambda, v) \mapsto \lambda v$, is an action of K^* on V.

Proposition 1.2 [Orbit-stabilizer theorem] *Given an action* (1.1) *and $x \in X$, $S(x)$ is a subgroup of G. Let $\mathcal{L}$ be the set of all left cosets of $S(x)$ in G. Then*

$$\mathcal{L} \to O(x), \quad gS(x) \mapsto gx, \tag{1.2}$$

is a well-defined bijective aplication and $[G : S(x)] = |O(x)|$. If G is finite, $|O(x)|$ divides $|G|$.

[1] If G is an additive group, we should write $g(hx) = (g + h)x$ and $0x = x$

Proof As $1x = x$, $1 \in S(x)$. Let $g, h \in S(x)$. Then $gx = x$ and $hx = x$. It follows that

$$(gh)x = g(hx) = gx = x \quad \text{and} \quad g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1x = x.$$

Therefore $gh, g^{-1} \in S(x)$ and $S(x)$ is a subgroup of G. For all $g, h \in G$,

$$gS(x) = hS(x) \Leftrightarrow h^{-1}g \in S(x) \Leftrightarrow (h^{-1}g)x = x \Leftrightarrow gx = hx.$$

Thus (1.2) is a well-defined injective map. Clearly (1.2) is also surjective. Therefore $[G : S(x)] = |O(x)|$. ■

Conjugacy, centralizer, normalizer and center

Let G be a group. Recall that $x, y \in G$ are said to be *conjugate* in G if there is $g \in G$ such that $y = gxg^{-1}$. Note that conjugacy is an equivalence relation in G. The equivalence classes are called the *conjugacy classes* of G. Also note that

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1}, \tag{1.3}$$

is an action of G on G. The orbits associated with this action are the conjugacy classes of G and the stabilizer of $x \in G$ is

$$C_G(x) = \{g \in G : gx = xg\}.$$

The group $C_G(x)$ is called the *centralizer* of x in G. The following result follows from the orbit-stabilizer theorem (Proposition 1.2).

Proposition 1.3 *Let G be a finite group. The cardinality of the conjugacy class of $x \in G$ is equal to $[G : C_G(x)]$ and divides $|G|$.*

Proposition 1.4 *A subgroup N of a group G is normal if and only if N is a union of conjugacy classes of G.*

Proof ($\Rightarrow$) For each $x \in G$, let K_x be the conjugacy class of x. Let $x \in N$. Let $gxg^{-1} \in K_x$, where $g \in G$. As $N \trianglelefteq G$, $gxg^{-1} \in N$. Then $K_x \subseteq N$. Therefore $\bigcup_{x \in N} K_x \subseteq N$. The other inclusion is trivial.

Prove the converse. ■

Now let $\mathcal{G}$ be the set of all subgroups of a group G. Two subgroups $K, L \in \mathcal{G}$ are said to be *conjugate* in G if there is $g \in G$ such that

$$L = gKg^{-1} \; (= \{gxg^{-1} : x \in K\}).$$

Now conjugacy is an equivalence relation in $\mathcal{G}$ and

$$G \times \mathcal{G} \to \mathcal{G}, \quad (g, K) \mapsto gKg^{-1},$$

is an action of G on $\mathcal{G}$. The equivalence classes for conjugacy and the orbits of this action coincide. In this case, the stabilizer of $K \in \mathcal{G}$ is

$$N_G(K) = \{g \in G : gK = Kg\}.$$

The group $N_G(K)$ is called the *normalizer* of K in G.

Proposition 1.5 *Let K be a subgroup of a finite group G. The cardinality of the conjugacy class of K is equal to $[G : N_G(K)]$ and divides $|G|$.*

Given a subgroup K of a group G, we call *centralizer* of K in G to

$$C_G(K) = \{g \in G : gx = xg, \text{ for all } x \in K\}.$$

The centralizer $C_G(K)$ is equal to the intersection of the centralizers of its elements and, therefore, $C_G(K)$ is a subgroup of G. Note that the centralizer of $x \in G$ coincides with the centralizer of the subgroup of G generated by x.

Proposition 1.6 *Let K be a subgroup of a group G.*

(a) $C_G(K) \leq N_G(K) \leq G$.

(b) *$K \trianglelefteq N_G(K)$ and $N_G(K)$ is the largest subgroup of G containing K as a normal subgroup.*

(c) *If $L \leq N_G(K)$, then $KL = LK \leq G$.*

Proposition 1.7 *Let K, L be subgroups of a group G. If K, L are conjugate in G, then $N_G(K), N_G(L)$ are conjugate in G.*

Proof. Suppose that $L = gKg^{-1}$, for some $g \in G$. Then $y \in N_G(L) \Leftrightarrow yL = Ly \Leftrightarrow ygKg^{-1} = gKg^{-1}y \Leftrightarrow g^{-1}ygK = Kg^{-1}yg \Leftrightarrow g^{-1}yg \in N_G(K) \Leftrightarrow y \in gN_G(K)g^{-1}$. Therefore $N_G(L) = gN_G(K)g^{-1}$. ■

We call *center* of a group G to

$$Z(G) = \{x \in G : gx = xg, \text{ for all } g \in G\} = C_G(G).$$

Proposition 1.8 *Let G be a group.*

(a) *G is Abelian if and only if $G = Z(G)$.*

(b) *$x \in Z(G)$ if and only if the conjugacy class of x is $\{x\}$.*

(c) $Z(G) \trianglelefteq G$.

Now let G be a finite group. By the previous proposition, $Z(G)$ is the union of the conjugacy classes of G with only one element. Let $K_1, \dots, K_r$ be the conjugacy classes with cardinality greater than 1. As G is the disjoint union of its conjugacy classes,

$$|G| = |Z(G)| + |K_1| + \cdots + |K_r|. \tag{1.4}$$

This equality is called the *class equation* of G.

Cauchy theorem

Proposition 1.9 *Let p be a positive prime number. Let G be a finite group such that $|G|$ is a power of p. Suppose that G acts on a finite set X. Let*

$$F = \{x \in X : \forall g \in G, gx = x\}.$$

F is called the set of the fixed points for this action. Then $|X| \equiv |F| \pmod{p}$.

Proof Let $x \in X$. The orbit $O(x) = \{gx : g \in G\}$ has a unique element if and only if $x \in F$. Hence $|F|$ is the number of orbits with exactly one element. Let $O(x_1), \ldots, O(x_n)$ be the orbits with more than one element. For each $i \in \{1, \ldots, n\}$, $|O(x_i)| = [G : S(x_i)] = |G|/|S(x_i)| \mid |G|$. As $|G|$ is a power of p and $|O(x_i)| \neq 1$, $p \mid |O(x_i)|$. As $|X| = |F| + |O(x_1)| + \cdots + |O(x_n)|$, $|X| \equiv |F| \pmod{p}$. ■

Theorem 1.10 [Cauchy theorem] *Let G be a finite group and let p be a positive prime number that divides $|G|$. Then G has an element of order p.*

Proof Let $m = |G|$ and

$$\begin{aligned} S &= \{(a_1, \ldots, a_p) \in G^p : a_1 \cdots a_p = 1\} \\ &= \{(a_1, \ldots, a_{p-1}, a_{p-1}^{-1} \cdots a_1^{-1}) : a_1, \ldots, a_{p-1} \in G\}. \end{aligned}$$

Clearly $|S| = m^{p-1}$. As $1 < p \mid m$, $p \mid m^{p-1}$. Thus $|S| = m^{p-1} \equiv 0 \pmod{p}$.

Note that, if $(a_1, \ldots, a_p) \in S$, then, for each $k \in \{0, 1, \ldots, p-1\}$,

$$a_{k+1}a_{k+2} \cdots a_p a_1 a_2 \cdots a_k = (a_k^{-1} \cdots a_1^{-1})(a_1 \cdots a_p)(a_1 \cdots a_k) = 1$$

and $a_{k+1} \cdots a_p a_1 \cdots a_k \in S$. Prove that the function $\mathbb{Z}_p \times S \to S$, that maps $(\overline{k}, (a_1, \ldots, a_p))$, where $k \in \{0, 1, \ldots, p-1\}$, to $(a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$, is an action of the additive group $\mathbb{Z}_p$ on S. Note that the set of the fixed points for this action is

$$\begin{aligned} F &= \{(a_1, \ldots, a_p) \in S : \forall k \in \{0, \ldots, p-1\}, \overline{k}(a_1, \ldots, a_p) = (a_1, \ldots, a_p)\}. \\ &= \{(a, \ldots, a) \in G^p : a^p = 1\}. \end{aligned}$$

Clearly $(1, \ldots, 1) \in F$ and $|F| \neq 0$. By the previous proposition and the first paragraph of this proof, $|F| \equiv |S| \equiv 0 \pmod{p}$. Thus $1 < p \mid |F|$ and there is $a \in G \setminus 1$ such that $a^p = 1$. Then $1 < |a| \mid p$. As p is prime positive, $|a| = p$. ■

Exercises

1.1.1 Let p be a positive prime number. A group in which the order of each element is a power of p is called a p-group.

Prove that a finite G is a p-group if and only if $|G|$ is a power of p. (Hint: Use Lagrange and Cauchy theorems.)

1.2 Finite subgroups of the multiplicative group of a field

Proposition 1.11 *Let G be a group and suppose that $x, y \in G$ have finite relatively prime orders. Then*

(a) $\langle x\rangle \cap \langle y\rangle = 1$.

(b) *If $xy = yx$, then $|xy| = |x||y|$.*

(c) *If $y_1, \ldots, y_t \in G$ and, for all $i, j \in \{1, \ldots, t\}$ with $i \neq j$, $|y_i|, |y_j|$ are finite relatively prime and $y_iy_j = y_jy_i$, then $|y_1 \cdots y_t| = |y_1| \cdots |y_t|$.*

Proof (a) Let $z \in \langle x\rangle \cap \langle y\rangle$. By Lagrange theorem, $|z| \mid \gcd\{|x|, |y|\} = 1$. Then $z = 1$.

(b) As $xy = yx$, $(xy)^{|x||y|} = (x^{|x|})^{|y|}(y^{|y|})^{|x|} = 1$. Therefore $|xy| \mid |x||y|$. Let $r = |xy|$. Then $1 = (xy)^r = x^ry^r$. Then $x^r = y^{-r} \in \langle x\rangle \cap \langle y\rangle = 1$. Then $|x| \mid r$ and $|y| \mid r$. As $|x|, |y|$ are relatively prime, $|x||y| \mid r = |xy|$.

(c) Follows from (b) with an induction argument. ■

The *exponent* of a finite group G is defined as the positive lower common multiple of the orders of its elements. Denote the exponent of G by $e(G)$. It follows from Lagrange theorem that $e(G) \mid |G|$.

Proposition 1.12 *If G is a finite Abelian group, then there is $x \in G$ such that $|x| = e(G)$.*

Proof The case $G = 1$ is trivial. Suppose that $G \neq 1$. Suppose that $e(G) = p_1^{r_1} \cdots p_t^{r_t}$, where $p_1, \ldots, p_t$ are distinct positive prime numbers and $r_1, \ldots, r_t \in \mathbb{N}$.

Let $i \in \{1, \ldots, t\}$. From the definition of $e(G)$, it follows that there is $x_i \in G$ such that $|x_i| = p_i^{r_i}n_i$, where $n_i \in \mathbb{N}$ and $\gcd\{p_i, n_i\} = 1$. Let $y_i = x_i^{n_i}$. By Proposition 0.29, $|y_i| = p_i^{r_i}$. By Proposition 1.11 (c), $|y_1 \cdots y_t| = |y_1| \cdots |y_t| = e(G)$. ■

Proposition 1.13 *Let F be a field. Every finite subgroup G of the multiplicative group $F^* = F \setminus \{0\}$ is cyclic.*

Proof Let $e = e(G)$. For every $x \in G$, $|x| \mid e$ and, therefore, $x^e = 1$. Thus every element of G is a root of the polynomial $X^e - 1 \in F[X]$. As $X^e - 1$ has at most e roots in F, $|G| \leq e$. As $e \mid |G|$, $e = |G|$. By Proposition 1.12, G is cyclic. ■

1.3 Permutation groups

Let X be a set. A bijective map $X \to X$ is called a *permutation* of X. Let $\mathrm{Sym}\, X$ be the set of all permutations of X. With the composition, $\mathrm{Sym}\, X$ is a group, called the *symmetric group* on X. The subgroups of symmetric groups are called *permutation groups.*

Proposition 1.14 [Cayley theorem] *Every group is isomorphic to a permutation group.*

Proof Let G be a group. For every $x \in G$,

$$\pi(x) : G \to G, \quad y \mapsto xy,$$

is a permutation of the set G. The map

$$\pi : G \to \mathrm{Sym}\, G, \quad x \mapsto \pi(x).$$

is a monomorphism of groups. Therefore $G \cong \pi(G) \leq \mathrm{Sym}\, G$. ■

Representations by permutations

A *representation by permutations* of a group G is a homomorphism from G to a symmetric group $\mathrm{Sym}\, X$. An injective representation is said to be *faithful.* Note that, in other words, Cayley theorem says that every group has a faithful representation by permutations.

Proposition 1.15 *Let G be a group and let X be a set.*

(a) *Let $G \times X \to X$ be an action of G on X. Then, for every $g \in G$,*

$$f(g) : X \to X, \quad x \mapsto gx,$$

is a permutation of X; and the map

$$f : G \to \mathrm{Sym}\, X, \quad g \mapsto f(g),$$

is a representation.

(b) *Let $f : G \to \mathrm{Sym}\, X$ be a representation. Then*

$$G \times X \to X, \quad (g, x) \mapsto f(g)(x),$$

is an action of G on X.

(c) (a) *and* (b) *give a bijective correspondence between the set of all group actions of G on X and the set of all group representations $G \to \mathrm{Sym}\, X$.*

Generally, the word representation can be used to designate other homomorphisms of a group G to a more concrete group, with additional structure, which we hope will be easier to understand. Representations also appear when studying other mathematical structures.

The finite symmetric and alternating groups

Let $n \in \mathbb{N}$. The symmetric group on $N = \{1, \ldots, n\}$ is denoted by S_n and is called the *symmetric group* of degree n. The group S_n has order $n!$.

Let $i_1, \ldots, i_r$, where $1 \leq r \leq n$, be distinct elements of N. The permutation $(i_1, \ldots, i_r) : N \to N$, defined by

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1 \text{ and } j \mapsto j \text{ if } j \notin \{i_1, \ldots, i_r\},$$

is called a *cycle of length* r or an r-cycle. Note that $(i_1, \ldots, i_r)^{-1} = (i_r, \ldots, i_1)$. A 2-cycle is called a *transposition.* If $\sigma \in S_n$, let

$$S(\sigma) = \{k \in \{1, \ldots, n\} : \sigma(k) \neq k\}.$$

Clearly, if $r \geq 2$, $S((i_1, \ldots, i_r)) = \{i_1, \ldots, i_r\}$ and $S((i_1)) = \emptyset$. Two permutations $\sigma, \tau \in S_n$ are said to be *disjoint* if $S(\sigma) \cap S(\tau) = \emptyset$.

Proposition 1.16 *If two permutations $\sigma, \tau \in S_n$ are disjoint, then $\sigma\tau = \tau\sigma$.*

Proposition 1.17 *Every permutation in $S_n \setminus 1$ is the product of disjoint cycles of length at least 2. This factorization is unique up to the order of the factors.*

Lemma 1.18 *If $p \in \mathbb{N}$ is odd and $\tau_1, \ldots, \tau_p \in S_n$ are transpositions, then $1 \neq \tau_1 \cdots \tau_p$.*

Proof By induction on p. Suppose that $\tau_p = (a, b)$. If $p = 1$, then $1(a) = a \neq b = \tau_1(a)$ and $1 \neq \tau_1$.. Suppose that $p > 1$ and $p \in \mathbb{N}$ is odd. Let

$$m = |\{j \in \{1, \ldots, p\} : a \in S(\tau_j)\}|.$$

The proof continues by induction on m. If $m = 1$, then $a = (\tau_1 \cdots \tau_{p-1})(a)$, $1(a) = a \neq b = (\tau_1 \cdots \tau_p)(a)$ and $1 \neq \tau_1 \cdots \tau_p$. Suppose that $m > 1$. Let q be the largest $j \in \{1, \ldots, p-1\}$ such that $a \in S(\tau_j)$.

The proof continues by induction on $\mu = p - q$. If $\mu = 1$, then $\tau_{p-1} = \tau_q = (a, c)$. If $b = c$, then $\tau_{p-1} = \tau_p$ and, by the induction assumption on p, $1 \neq \tau_1 \cdots \tau_{p-2} = \tau_1 \cdots \tau_p$. If $b \neq c$, then $\tau_{p-1}\tau_p = (a, c)(a, b) = (a, b, c) = (b, c)(a, c)$ and, by the induction assumption on m, $1 \neq \tau_1 \cdots \tau_{p-2}(b, c)(a, c) = \tau_1 \cdots \tau_p$. Finally, suppose that $\mu > 1$. Then $q < p - 1$ and $\tau_{q+1} = (d, e)$, where $a \notin \{d, e\}$. If $c \notin \{d, e\}$, then τ_q, τ_{q+1} are disjoint and commute and, by the induction assumption on μ, $1 \neq \tau_1 \cdots \tau_{q-1}\tau_{q+1}\tau_q\tau_{q+2} \cdots \tau_p = \tau_1 \cdots \tau_p$. If $c \in \{d, e\}$, suppose, without loss of generality, that $c = d$; then, by the induction assumption on μ, $1 \neq \tau_1 \cdots \tau_{q-1}(c, e)(a, e)\tau_{q+2} \cdots \tau_p = \tau_1 \cdots \tau_p$. ■

Proposition 1.19 *If $n \geq 2$, then every permutation $\sigma \in S_n$ is a product of transpositions. The number of transpositions in any such factorization of σ is always even or always odd.*

Proof If $(i_1, \dots, i_r)$ is a cycle of lenght $r \geq 2$, then

$$(i_1, \dots, i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_2). \tag{1.5}$$

As every $\sigma \in S_n \setminus 1$ is a product of cycles with length at least 2, it follows that σ is a product of transpositions. Moreover $1 = (1, 2)(1, 2)$.

If $\sigma = \tau_1 \cdots \tau_p = \rho_1 \cdots \rho_q$ are two fatorizations of a permutation σ as product of transpositions, then $1 = \tau_p^{-1} \cdots \tau_1^{-1} \rho_1 \cdots \rho_q$. By the previous lemma, $p + q$ is even. Then p, q are both even or both odd. ■

A permutation $\sigma \in S_n$ is said to be *even* if it can be written as a product of an even number of transpositions; otherwise, it is said do be *odd.*

By (1.5), a cycle of odd length is even and a cycle of even length is odd.

Proposition 1.20 *The set A_n of all even permutations in S_n is a normal subgroup of S_n of index* 2.

The group A_n is called the *alternating group* of degree n.

Conjugation in S_n

Proposition 1.21 *Let $\sigma \in S_n$. Then*

$$\sigma = (s_{1,1}, \dots, s_{1,j_1}) \cdots (s_{k,1}, \dots, s_{k,j_k}), \tag{1.6}$$

where $\{1, \dots, n\} = \{s_{1,1}, \dots, s_{1,j_1}, \dots, s_{k,1}, \dots, s_{k,j_k}\}$, $j_1 + \cdots + j_k = n$ *and* $j_1 \leq \cdots \leq j_k$.

Proof If $\sigma = 1$, $1 = (1)(2) \cdots (n)$. Suppose that $\sigma \neq 1$. By Proposition 1.17, $\sigma = \tau_1 \cdots \tau_p$, where $\tau_1, \cdots, \tau_p$ are disjoint cycles of lenght at least 2. As disjoint cycles commute, we may assume that the sequence of lengths of $\tau_1, \cdots, \tau_p$ is nonincreasing. Suppose that $\{1, \dots, n\} \setminus \bigcup_{j \in \{1, \dots, p\}\}} S(\tau_j)$ has q elements $i_1, \dots, i_q$. Then $\sigma = (i_1) \cdots (i_q) \tau_1 \cdots \tau_p$ is the prescribed factorization. ■

With the notation of the last proposition, the sequence $(j_1, \dots, j_k)$ is called the *cycle type* (em português *tipo de ciclos*) of σ. From the unicity in Proposition 1.17, it follows that σ has a unique cycle type.

Proposition 1.22 *Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle type.*

Proof Suppose that $\sigma, \tau \in S_n$ are conjugate. Let g be an element of S_n such that $\tau = g \sigma g^{-1}$. Suppose that (1.6) is a factorization of σ as a product of disjoint cycles as described in Proposition 1.21. Suppose that

$$g = \begin{pmatrix} s_{1,1} & \cdots & s_{1,j_1} & \cdots & s_{k,1} & \cdots & s_{k,j_k} \\ t_{1,1} & \cdots & t_{1,j_1} & \cdots & t_{k,1} & \cdots & t_{k,j_k} \end{pmatrix}. \tag{1.7}$$

Then

$$\tau = (t_{1,1}, \ldots, t_{1,j_1}) \cdots (t_{k,1}, \ldots, t_{k,j_k}), \tag{1.8}$$

and, therefore, σ, τ have the same cycle type.

Conversely suppose that σ, τ have the same cycle type. Suppose that (1.6) and (1.8) are factorizations of σ and τ, respectively, as described in Proposition 1.21. Let g be the permutation (1.7). Then $\tau = g\sigma g^{-1}$. ■

Simple alternating groups

A group G is said to be *simple* if it is non-trivial and 1 and G are its only normal subgroups.

The alternating groups A_1 and A_2 are not simple, since they are trivial; A_3 is simple, since it has prime order and, by Lagrange theorem, 1 and A_3 are its only subgroups; A_4 is not simple, since $1 \neq K \lhd A_4$, where

$$K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

We will prove that A_n is simple for $n \geq 5$. This is the proof in [Hungerford-2].

Lemma 1.23 *Let r, s be distinct elements of $\{1, \ldots, n\}$, with $n \geq 3$. The alternating group A_n is generated by*

$$\{(r, s, k) : k \in \{1, \ldots, n\} \setminus \{r, s\}\}. \tag{1.9}$$

Proof The case $n = 3$ is trivial, since $A_3 = \langle (1,2,3) \rangle$.

Suppose that $n > 3$. A permutation $\sigma \in S_n$ belongs to A_n if and only if it can be written as a product of 2-cycles with an even number of factors. Therefore, the set of all products of two distinct 2-cycles generates A_n. That is,

$$\{(a,b)(c,d), (a,b)(a,c) : a, b, c, d \text{ are distinct elements of } \{1, \ldots, n\}\}$$

generates A_n. As

$$(a,b)(c,d) = (a,c,b)(a,c,d) \text{ and } (a,b)(a,c) = (a,c,b),$$

A_n is generated by the 3-cycles. After fixing r and s, any 3-cycle is of one of the forms

$$(r,s,a), (r,a,s), (r,a,b), (s,a,b), (a,b,c),$$

where a, b, c are distinct elements of $\{1, \ldots, n\}$. As $(r,a,s) = (r,s,a)^2$, $(r,a,b) = (r,s,b)(r,s,a)^2$, $(s,a,b) = (r,s,b)^2(r,s,a)$ and

$$(a,b,c) = (r,s,a)^2(r,s,c)(r,s,b)^2(r,s,a),$$

A_n is generated by (1.9). ■

Lemma 1.24 *If N is a normal subgroup of A_n and N contains a 3-cycle, then $N = A_n$.*

Proof Suppose that $(r, s, a) \in N$. Then, for any $k \in \{1, \dots, n\} \backslash \{r, s, a\}$,

$$(r, s, k) = ((a, k)(r, s))^{-1}(r, s, a)^2(a, k)(r, s) \in N.$$

By Lemma 1.23, $N = A_n$. ■

Proposition 1.25 *For every $n \geq 5$, A_n is simple.*

Proof Let N be a non-trivial normal subgroup of A_n. Choose $\sigma \in N \backslash 1$. Suppose that $\sigma = c_1 \cdots c_t$, where $c_1, \dots, c_t$ are disjoint cycles, each c_i is an r_i-cycle and $r_1 \geq \cdots \geq r_t > 1$.

Case 1. *Suppose that $r_1 \geq 4$.* Let $\tau = c_2 \cdots c_t$. To simplify the notation, suppose, without loss of generality, that $c_1 = (1, 2, \dots, r)$. Let $\delta = (1, 2, 3) \in A_n$. As $N \trianglelefteq A_n$,

$$\begin{aligned} N \ni \sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(r, r-1, \dots, 2, 1)(1, 2, 3)(1, 2, \dots, r-1, r)\tau(3, 2, 1) \\ &= (1, 3, r). \end{aligned}$$

By Lemma 1.24, $N = A_n$.

Case 2. *Suppose that $t \geq 2$, $r_1 = r_2 = 3$.* Let $\tau = c_3 \cdots c_t$. To simplify the notation, suppose, without loss of generality, that $c_1 = (1, 2, 3)$ and $c_2 = (4, 5, 6)$. Let $\delta = (1, 2, 4) \in A_n$. As $N \trianglelefteq A_n$,

$$\begin{aligned} N \ni \sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(6, 5, 4)(3, 2, 1)(1, 2, 4)(1, 2, 3)(4, 5, 6)\tau(4, 2, 1) \\ &= (1, 4, 2, 6, 3). \end{aligned}$$

By Case 1, $N = A_n$.

Case 3. *Suppose that $t \geq 2$, $r_1 = 3$ and $r_2 = 2$.* Let $\tau = c_2 \cdots c_t$. Note that τ is the product of disjoint 2-cycles and $\tau^2 = 1$. To simplify the notation, suppose, without loss of generality, that $c_1 = (1, 2, 3)$. Then

$$N \ni \sigma^2 = (1, 2, 3)\tau(1, 2, 3)\tau = (1, 2, 3)(1, 2, 3) = (1, 3, 2).$$

By Lemma 1.24, $N = A_n$.

Case 4. *Suppose that $t = 1$ and $r_1 = 3$.* By Lemma 1.24, $N = A_n$.

Case 5. *Suppose that $r_1 = 2$.* As $\sigma \in A_n$, $t \geq 2$. Let $\tau = c_3 \cdots c_t$. Without loss of generality, suppose that $c_1 = (1, 2)$ and $c_2 = (3, 4)$ Then $\tau^2 = 1$. Let $\delta = (1, 2, 3) \in A_5$. Then

$$N \ni \sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(1, 2)(3, 4)(1, 2, 3)(1, 2)(3, 4)\tau(3, 2, 1) = (1, 3)(2, 4).$$

Let $\zeta = (1, 3)(2, 4) \in N$ and $\xi = (1, 3, 5) \in A_n$. Then

$$N \ni \zeta(\xi\zeta\xi^{-1}) = (1, 3, 5).$$

By Lemma 1.24, $N = A_n$.

In any case, $N = A_n$. Therefore A_n is simple. ■

Dihedral groups

Let $n \geq 3$. We call *dihedral group* of degree n, denoted by D_n ([2]), to the subgroup of S_n generated by x, y, where

$$\begin{aligned} &x = (1, n-1)(2, n-2) \cdots ((n-1)/2, (n+1)/2), \quad \text{if } n \text{ is odd}, \\ &x = (1, n-1)(2, n-2) \cdots ((n-2)/2, (n+2)/2), \quad \text{if } n \text{ is even}, \\ &y = (1, 2, \ldots, n). \end{aligned}$$

Proposition 1.26 *Let $n \geq 3$.*

(a) *D_n is generated by two elements x, y satisfying*

$$|x| = 2, \quad |y| = n \quad \textit{and} \quad xy = y^{-1}x. \tag{1.10}$$

(b) *If a group G is generated by two elements x, y satisfying* (1.10), *then $|G| = 2n$, and $G \cong D_n$.*

Proof The details are left as exercises.
(b) Using (1.10), deduce that

$$G = \{y^i x^j : i \in \{0, \ldots, n-1\}, j \in \{0, 1\}\} = \langle y \rangle \langle x \rangle. \tag{1.11}$$

If $x \in \langle y \rangle$, then $xy = y^{-1}x$ would imply that $y^2 = 1$, what is impossible because $|y| = n \geq 3$. Then $x \notin \langle y \rangle$. Prove that $|G| = 2n$.

If H is another group generated by two elements w, z satisfying (1.10), with x replaced by w and y replaced by z, then

$$H = \{z^i w^j : i \in \{0, \ldots, n-1\}, j \in \{0, 1\}\}.$$

It is not hard to see that $G \to H$, $y^i x^j \mapsto z^i w^j$, is an isomorphism of groups. ■

The quaternion group Q_8

We call *quaternion group* to the subgroup Q_8 of S_8 generated by $x = (1, 2, 3, 4)(5, 6, 7, 8)$ and $y = (1, 5, 3, 7)(2, 8, 4, 6)$.

Proposition 1.27 (a) *Q_8 is generated by two elements x, y satisfying*

$$|x| = |y| = 4, \quad x^2 = y^2 \quad \textit{and} \quad yx = x^3 y. \tag{1.12}$$

(b) *If a group G is generated by two elements x, y satisfying* (1.12), *then $G = \langle x \rangle \langle y \rangle$, $|G| = 8$, and $G \cong Q_8$.*

Proof Prove (b) by adapting the proof of Proposition 1.26. ■

[2] Alternative notation: in some publications, the dihedral group of degree n is represented by D_{2n}.

Exercises

1.3.1 Show that A_4 has no subgroup of order 6. ([3])

1.3.2 Show that $\langle(1,2)(3,4)\rangle \trianglelefteq \langle(1,2)(3,4)\rangle\langle(1,3)(2,4)\rangle \trianglelefteq A_4$ and $\langle(1,2)(3,4)\rangle$ is not normal in A_4. So the relation $\trianglelefteq$ is not always transitive.

1.4 Solvable groups

A group G is said to be *solvable* if there is a finite chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that, for each $i \in \{1,\ldots,n\}$, G_i/G_{i-1} is Abelian.

Proposition 1.28 *Let G be a group, $H \le G$ and $N \trianglelefteq G$.*

(a) *If G is solvable, then H and G/N are solvable.*

(b) *If N and G/N are solvable, then G is solvable.*

Proof (a) Suppose that G is solvable and

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

where, for each $i \in \{1,\ldots,n\}$, G_i/G_{i-1} is Abelian.

For each $i \in \{0,\ldots,n\}$, let $H_i = G_i \cap H$. Let $i \in \{1,\ldots,n\}$. For each $y \in H_i$, $yH_{i-1} = yG_{i-1} \cap yH = G_{i-1}y \cap Hy = H_{i-1}y$. Thus $H_{i-1} \trianglelefteq H_i$ and

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H.$$

Note that $G_{i-1} \trianglelefteq G_i$ and $G_i \cap H \le G_i$. By Proposition 0.14 (c), $G_{i-1} \trianglelefteq G_{i-1}(G_i \cap H) \le G_i$. By Proposition 0.18, the second isomorphism theorem,

$$\frac{H_i}{H_{i-1}} = \frac{G_i \cap H}{G_{i-1} \cap (G_i \cap H)} \cong \frac{G_{i-1}(G_i \cap H)}{G_{i-1}} \le \frac{G_i}{G_{i-1}}.$$

As G_i/G_{i-1} is Abelian, H_i/H_{i-1} is also Abelian. Hence H is solvable.

Let $p : G \to G/N$, $g \mapsto gN$, be the canonical epimorphism. Then

$$1 = p(G_0) \trianglelefteq p(G_1) \trianglelefteq \cdots \trianglelefteq p(G_n) = G/N.$$

Prove that, for each $K \le G$, $p(K) = KN/N$.

Let $i \in \{1,\ldots,n\}$. As

$$\frac{p(G_i)}{p(G_{i-1})} = \frac{G_iN/N}{G_{i-1}N/N} \cong \frac{G_iN}{G_{i-1}N} = \frac{G_i(G_{i-1}N)}{G_{i-1}N} \cong \frac{G_i}{G_i \cap G_{i-1}N}$$
$$\cong \frac{G_i/G_{i-1}}{(G_i \cap G_{i-1}N)/G_{i-1}}$$

[3] We have seen that finite cyclic groups satisfy Proposition 0.28 (b), a converse of Lagrange theorem. This exercise shows that this converse is not always true.

and G_i/G_{i-1} is Abelian, we deduce that $p(G_i)/p(G_{i-1})$ is also Abelian. Hence G/N is solvable.

(b) Suppose that N and G/N are solvable,

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = N,$$

where, for each $i \in \{1, \ldots, m\}$, N_i/N_{i-1} is Abelian, and

$$\{N\} = G_0/N \trianglelefteq G_1/N \trianglelefteq \cdots \trianglelefteq G_n/N = G/N,$$

where, for each $i \in \{1, \ldots, n\}$,

$$\frac{G_i/N}{G_{i-1}/N} \cong \frac{G_i}{G_{i-1}}$$

is Abelian. As

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

G is solvable. ■

Proposition 1.29 *If $f : G \to H$ is a homomorphism of groups and G is solvable, then $f(G)$ is solvable.*

Proof By Proposition 1.28, $G/\ker f$ is solvable. As $G/\ker f \cong f(G)$, $f(G)$ is also solvable. ■

Recall that a group G is said to be *simple* if it is non-trivial and 1 and G are its only normal subgroups.

Examples 1.30 1. Every Abelian group is solvable.

2. If G is a simple non-Abelian group, then G is not solvable. By Proposition 1.25, for $n \geq 5$, the alternating group A_n is not solvable.
3. The symmetric group S_3 is solvable: $1 \trianglelefteq A_3 \trianglelefteq S_3$, where A_3 ($\cong \mathbb{Z}_3$) and S_3/A_3 ($\cong \mathbb{Z}_2$) are Abelian.
4. S_4 is solvable: if $K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, then $1 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$, where K ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2$), A_4/K ($\cong \mathbb{Z}_3$) and S_4/A_4 ($\cong \mathbb{Z}_2$) are Abelian. Note that $K \trianglelefteq S_4$ because $K \leq S_4$ and K is a union of conjugacy classes of S_4 (cf. Proposition 1.4). As $K \leq A_4 \leq S_4$, K is also normal in A_4.
5. For $n \geq 5$, as S_n contains the non-solvable group A_n, S_n is also non-solvable.

Exercises

1.4.1 Let G and H be solvable groups. Prove that the product $G \times H$ is solvable. (See the definition of products of groups in page 12.)

1.5 Linear groups

Let V be a vector space over a field F. Let $\mathrm{GL}\, V$ be the set of the linear automorphisms of V. With the composition, $\mathrm{GL}\, V$ is a group, called the *general linear group* of V. The set $\mathrm{GL}_n F$ of the $n \times n$ invertible matrices over F is a group, with the usual multiplication, called the *general linear group* of degree n over F. The subgroups of $\mathrm{GL}\, V$ and $\mathrm{GL}_n F$ are called *linear groups* ([4]).

A *linear representation* of a group G is a homomorphism from G to a group $\mathrm{GL}\, V$, where V is a vector space. A *linear representation by matrices* of a group G is a homomorphism from G to a group $\mathrm{GL}_n F$, where F is a field. Linear representations are particularly important, as they bring the Linear Algebra tools to Group Theory.

Example 1.31 Let G be a group and let V be a vector space. Then $f : G \to \mathrm{GL}\, V$, $g \mapsto \mathrm{id}_V$, is a representation, called a *trivial* representation.

Example 1.32 Let V be a vector space over a field F with dimension $n \in \mathbb{N}$. Let $B = \{b_1, \ldots, b_n\}$ be a basis of V.

Let $\sigma \in S_n$. From Linear Algebra ([5]), there is a unique isomorphism f_σ of V such that, for all $k \in \{1, \ldots, n\}$, $f_\sigma(b_k) = b_{\sigma(k)}$. Then $f : S_n \to \mathrm{GL}\, V$, $\sigma \mapsto f_\sigma$, is a faithful (that is, injective) representation.

Frequently, groups emerging from other areas of Mathematics or from Physics have a topology such that the binary multiplication and the inverse are continuous maps. These groups are called *topological groups*. In these cases, it may be more useful to consider *continuous linear representations* to *topological linear groups*.

Example 1.33 Let $\mathbb{C}^*$ be the multiplicative group of all non-zero complex numbers. The set T of all complex numbers with modulus equal to 1 is a subgroup of $\mathbb{C}^*$, called the *circle group*:

$$T = \{e^{2\pi i x} : x \in \mathbb{R}\} = \{e^{2\pi i x} : x \in [0, 1)\}. \tag{1.13}$$

The map

$$f : T \to \mathrm{GL}_2 \mathbb{R}, \quad e^{2\pi i x} \mapsto \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix},$$

is a faithful representation of the circle group T. With the topology induced by the usual toplogy in $\mathbb{C}$, T is a topological group. With the topology induced by the usual toplogy in $\mathbb{R}^{2\times 2}$, $\mathrm{GL}_2 \mathbb{R}$ is a topological group. Moreover f is continuous.

[4] When $\mathrm{GL}\, V$ (or $\mathrm{GL}_n F$) also has a topological structure, as it is the case when $F \in \{\mathbb{R}, \mathbb{C}\}$, the name *linear group* may be reserved for closed subgroups, since they are especially relevant in that context.

[5] The following facts are known from Linear Algebra: given $u_1, \ldots, u_n \in V$, there is a unique linear endomorphism f of V such that, for all $k \in \{1, \ldots, n\}$, $f(b_k) = u_k$; this endomorphism f is an isomorphism if and only if $\{u_1, \ldots, u_n\}$ is a basis of V.

Exercises

1.5.1 The quotient of the additive group $\mathbb{R}$ by its subgroup $\mathbb{Z}$ is

$$\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} : x \in \mathbb{R}\} = \{x + \mathbb{Z} : x \in [0, 1)\}.$$

If T is the circle group introduced in (1.13), then

$$T \to \mathbb{R}/\mathbb{Z}, \quad e^{2\pi i x} \mapsto x + \mathbb{Z},$$

is an isomorphism.

1.5.2 Let Q_8 be the quaternion group introduced in page 43. Prove that there is one and only one faithful representation $Q_8 \to \mathrm{GL}_2 \mathbb{C}$ such that

$$x \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad y \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

1.5.3 Let Q_8 be the quaternion group introduced in page 43. Prove that there is one and only one faithful representation $Q_8 \to \mathrm{GL}_2(\mathbb{Z}_3)$ such that

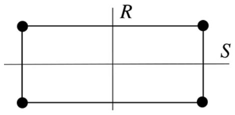
$$x \mapsto \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad y \mapsto \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}.$$

1.6 Symmetry groups

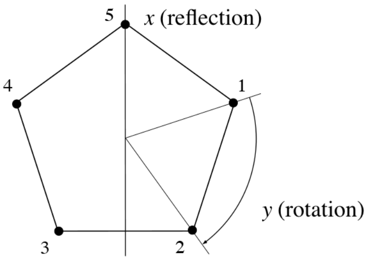
Symmetry groups

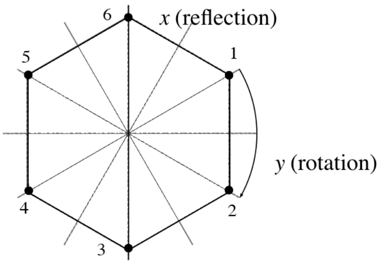
Let S be a subset (called a geometric figure) of the n-dimensional Euclidean space E_n. A symmetry of S is a bijective transformation $T : E_n \to E_n$ that preserves lengths (and, consequentely, sends straight lines to straight lines and preserves measures of angles) and satisfies $T(S) = S$. The set of all symmetries of S, together with the composition, is a group, called the *symmetry group* of S.

The symmetries of a rectangle that is not a square are the identity, two reflections R, S and their composition RS which is a rotation. These symmetries constitute an Abelian group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.



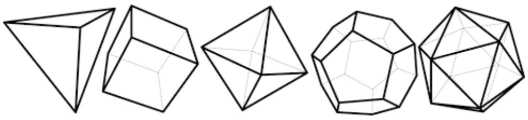
The symmetry group G_n of a regular n-sided polygon in E_2 is generated by a reflection x and a rotation y satisfying (1.10), and, therefore, is isomorphic to the dihedral group D_n.





The symmetries of a regular tetrahedron in E_3 constitute a group isomorphic to S_4. To justify this, observe that any transposition of the four vertices of the tetrahedron can be obtained by a symmetry and, therefore, any permutation of the vertices can be obtained by a symmetry.

Students can find more details and, in particular, the symmetry groups of the other Platonic solids in [Cameron, p. 140–144].



In the previous examples, the symmetry groups are finite, but many geometric figures, as the sphere, have infinite symmetry groups.

Symmetry groups of bilinear forms

Let F be a field. Let $V = F^{n\times 1}$, the vector space of column vectors with n coordinates. Let $(e_1, \ldots, e_n)$ be the canonical basis of V. Let $\beta : V \times V \to F$ be a bilinear form. Then, for all $u, v \in V$,

$$\beta(u, v) = u^T Bv, \quad \text{where } B = [b_{i,j}] \in F^{n\times n}, b_{i,j} = \beta(e_i, e_j).$$

The matrix B is called the matrix of the bilinear form β (relative to the canonical basis).

An invertible matrix $P \in \mathrm{GL}_n F$ is said to be a *symmetry* of β (or is said to *preserve* β; or is said to be an *automorphism* of β) if,

$$\forall u, v \in V, \quad \beta(Pu, Pv) = \beta(u, v), \tag{1.14}$$

that is,

$$\forall u, v \in V, \quad u^T P^T BPv = u^T Bv, \tag{1.15}$$

It is easy to see that (1.15) is equivalent to $P^T BP = B$. It is also easy to see that the set

$$A(\beta) = \{P \in \mathrm{GL}_n F : P^T BP = B\}$$

of all symmetries of β is a subgroup of $\mathrm{GL}_n F$.

Now let $F = \mathbb{C}$. With the notation used above, let $\beta : V \times V \to \mathbb{C}$ be a *sesquilinear* form. Sesquilinear form means that, for all $a \in \mathbb{C}$, $u, u', v, v' \in V$,

$$\begin{aligned} \beta(u + u', v) &= \beta(u, v) + \beta(u', v), \quad \beta(au, v) = \overline{a}\beta(u, v), \\ \beta(u, v + v') &= \beta(u, v) + \beta(u, v'), \quad \beta(u, av) = a\beta(u, v). \end{aligned}$$

Then, for all $u, v \in V$,

$$\beta(u, v) = u^* Bv, \ (^6) \quad \text{where } B = [b_{i,j}] \in \mathbb{C}^{n \times n}, b_{i,j} = \beta(e_i, e_j).$$

The matrix B is called the matrix of the sesquilinear form β (relative to the canonical basis). A *symmetry* of β is defined as any matrix $P \in \mathrm{GL}_n \mathbb{C}$ satisfying (1.14). Now (1.14) is equivalent to $P^* BP = B$. The set

$$A(\beta) = \{P \in \mathrm{GL}_n \mathbb{C} : P^* BP = B\}$$

of all symmetries of β is a subgroup of $\mathrm{GL}_n \mathbb{C}$.

Matrix Lie groups

Following [Hall, p. 4], a *matrix Lie group* is any subgroup G of a general linear group $\mathrm{GL}_n \mathbb{C}$ such that, for every sequence $(A_k)_{k \in \mathbb{N}}$ of matrices in G, if $(A_k)_{k \in \mathbb{N}}$ converges to some matrix $A \in \mathrm{GL}_n \mathbb{C}$, then $A \in G$.

Consider in $\mathrm{GL}_n \mathbb{C}$ the topology induced by the usual topology in $\mathbb{C}^{n \times n}$. The definition means that a subgroup G of $\mathrm{GL}_n \mathbb{C}$ is a matrix Lie group if and only if it is a closed subset of $\mathrm{GL}_n \mathbb{C}$.

The general linear group $\mathrm{GL}_n \mathbb{C}$ is a matrix Lie group, since it is closed in $\mathrm{GL}_n \mathbb{C}$.

The real general linear group $\mathrm{GL}_n \mathbb{R}$ is also a matrix Lie group. Let $(A_k)_{k \in \mathbb{N}}$ be a sequence of real invertible matrices converging to $A \in \mathrm{GL}_n \mathbb{C}$. Then $(A_k)_{k \in \mathbb{N}}$ is a Cauchy sequence. As $\mathbb{R}^{n \times n}$ is a complete space, $(A_k)_{k \in \mathbb{N}}$ converges in $\mathbb{R}^{n \times n}$. Hence A is a real matrix. As A is invertible, $A \in \mathrm{GL}_n \mathbb{R}$. Therefore $\mathrm{GL}_n \mathbb{R}$ is closed in $\mathrm{GL}_n \mathbb{C}$.

The set

$$\mathrm{SL}_n \mathbb{C} = \{A \in \mathrm{GL}_n \mathbb{C} : \det A = 1\}$$

is a subgroup of $\mathrm{GL}_n \mathbb{C}$ called the *special linear group*. As

$$d : \mathrm{GL}_n \mathbb{C} \to \mathbb{C}, \quad A \mapsto \det A,$$

is a continuous function and $\{1\}$ is closed in $\mathbb{C}$, $\mathrm{SL}_n \mathbb{C} = d^{-1}(\{1\})$ is closed in $\mathrm{GL}_n \mathbb{C}$. Therefore $\mathrm{SL}_n \mathbb{C}$ is a matrix Lie group.

The *real special linear group*

$$\mathrm{SL}_n \mathbb{R} = \{A \in \mathrm{GL}_n \mathbb{R} : \det A = 1\} = \mathrm{GL}_n \mathbb{R} \cap \mathrm{SL}_n \mathbb{C}$$

[6] $u^* = \overline{u}^T$, the conjugate transpose of u.

is also a matrix Lie group.

Let $F \in \{\mathbb{R}, \mathbb{C}\}$. Recall that a matrix $B \in F^{n\times n}$ is said to be *symmetric* if $B^T = B$; *Hermitian* if $B^* = B$; *antisymmetric* if $B^T = -B$; *orthogonal* if $B^T B = BB^T = I_n$; *unitary* if $B^* B = BB^* = I_n$.

Using the notation introduced above, let $\beta : V \times V \to F$ be a bilinear form and let B be its matrix. The function

$$\phi : \mathrm{GL}_n F \to F^{n\times n}, \quad P \mapsto P^T BP - B,$$

is continuous and, therefore, $A(\beta) = \phi^{-1}(\{0\})$ is closed in $\mathrm{GL}_n F$. As $\mathrm{GL}_n F$ is closed in $\mathrm{GL}_n \mathbb{C}$, $A(\beta)$ is closed in $\mathrm{GL}_n \mathbb{C}$. Hence $A(\beta)$ is a matrix Lie group. Analogously, if $F = \mathbb{C}$ and $\beta : V \times V \to \mathbb{C}$ is a sesquilinear form, then $A(\beta)$ is a matrix Lie group. Some of these groups appear as symmetry groups in Physics.

Using the notation above, a bilinear form β is said to be *symmetric* if its matrix B is symmetric; β is said to be *antisymmetric* if its matrix B is antisymmetric. Usually, the group of symmetries of a symmetric bilinear form is said to be an *orthogonal* group and the group of symmetries of an antisymmetric bilinear form is said to be a *symplectic* group.

If the bilinear form β has matrix I_n, then $A(\beta)$ is the group of all orthogonal $n \times n$ matrices over F and is denoted by $\mathrm{O}_n F$. Note that, if $F = \mathbb{R}$ and β has matrix I_n, then β is the usual inner product in $\mathbb{R}^n$.

The space-time of special relativity is $\mathbb{R}^4$. The bilinear form β with matrix $B = \mathrm{diag}(1, 1, 1, -1)$ is used to measure it, replacing the inner product. In this case, $A(\beta)$ is called the *Lorentz group*.

If a bilinear form β has matrix

$$B = \begin{bmatrix} 0 & I_k \\ -I_k & 0 \end{bmatrix},$$

then the symplectic group $A(\beta)$ is denoted by $\mathrm{Sp}_{2k}F$. Its elements are called *symplectic matrices*.

If $F = \mathbb{C}$ and a sesquilinear form β has matrix I_n, then $A(\beta)$ is denoted by $\mathrm{U}_n \mathbb{C}$. These groups are called *unitary groups*.

The matrix Lie group $\mathrm{SO}_n = \mathrm{SL}_n \mathbb{R} \cap \mathrm{O}_n \mathbb{R}$ is called the *special orthogonal group* and $\mathrm{SU}_n = \mathrm{SL}_n \mathbb{C} \cap \mathrm{U}_n \mathbb{C}$ is called the *special unitary group*. In Example 1.33, the image of the faithful representation f is SO_2. SO_2 is also isomorphic to the group of rotations of $\mathbb{R}^2$. SO_3 is isomorphic to the group of rotations of $\mathbb{R}^3$. In Particle Physics, SU_2 arises in the electroweak interaction and SU_3 in quantum chromodynamics.

Chapter 2

Modules, algebras, and polynomials

2.1 Modules

Let R be a ring. A *left module* over R (or, simply, left R-module) is an additive Abelian group M with a map, called *scalar multiplication,*

$$R \times M \to M, \quad (a, x) \mapsto ax, \tag{2.1}$$

such that, for all $a, b \in R$, $x, y \in M$,

(M$_1$) $a(x + y) = ax + ay$,

(M$_2$) $(a + b)x = ax + bx$,

(M$_3$) $(ab)x = a(bx)$,

(M$_4$) $1x = x$.

Analogously, a *right R-module* is an additive Abelian group with a scalar multiplication

$$M \times R \to M, \quad (x, a) \mapsto xa,$$

such that, for all $a, b \in R$, $x, y \in M$, (M$'_1$) $(x + y)a = xa + ya$, (M$'_2$) $x(a + b) = xa + xb$, (M$'_3$) $x(ab) = (xa)b$, (M$'_4$) $x1 = x$.

In any case, if M is an R-module, R is said to be the *ring of scalars* of M.

A left R-module M can be represented by ${}_RM$ if this is convenient to clarify which is the ring of scalars. Analogously, a right R-module M can be represented by M_R.

Left modules and right modules have analogous properties. Thus, unless otherwise stated, we study only left modules and the word 'module' means 'left module'.

Remark 2.1 Suppose that R is a commutative ring. If M is a left R-module, it is easy to see that M can be turned into a right module by defining that the right scalar product of $x \in M$ by $a \in R$ is equal to the left scalar product of a by x. Analogously a right module over a commutative ring can be turned into a left module.

This remark shows that, when the ring of scalars is commutative, left modules and right modules can be viewed as the same mathematical objects, the only difference being the representation of the scalar product.

In general, this remark is not true if the ring of scalars is non-commutative.

Examples 2.2 1. If V is a vector space over a field F, then V is an F-module. In general, the modules over a division ring D are called vector spaces over D.

2. A ring R is a left module over itself with the usual operations. This module is called the *left regular module*. Analogously, R is a right module over itself, called the *right regular module*.

3. Let R be a ring. The set $R^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in R\}$ is an R-module with the operations defined as follows:
for all $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in R^n$ and $c \in R$,

$$\begin{aligned} (a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n), \\ c(a_1, \ldots, a_n) &= (ca_1, \ldots, ca_n). \end{aligned}$$

4. Let G be an additive Abelian group. Then G is a module over the ring of the integers $\mathbb{Z}$. The scalar product of elements of $\mathbb{Z}$ by elements of G is defined in the usual way: for all $n \in \mathbb{N}$, $x \in G$, nx is the sum $x + \cdots + x$ of x by itself n times; $0x := 0_G$ and $(-n)x := n(-x)$. See Proposition 0.4.

5. Let G be an additive Abelian group and suppose that there is $n \in \mathbb{N}$ such that, for all $x \in G$, $nx = 0$. Then G is a $\mathbb{Z}_n$-module with the scalar multiplication $\mathbb{Z}_n \times G \to G$, $(\bar{k}, x) \mapsto kx$.

6. Let $\phi : S \to R$ be a homomorphism of rings. Let M be an R-module. Then M is an S-module with the scalar multiplication

$$S \times M \to M, \quad (s, x) \mapsto \phi(s)x.$$

Proposition 2.3 *Let M be a module over a ring R. Then, for all $a, b \in R$, $x, y \in M$,*

(a) $0x = a0 = 0$.

(b) $(-a)x = a(-x) = -(ax)$.

(c) $a(x - y) = ax - ay$.

(d) $(a - b)x = ax - bx$.

Proof (a) $0x = (0+0)x = 0x + 0x$. Then $0 = 0x$. Analogously $0 = a0$.

(b) $0 = 0x = (a + (-a))x = ax + (-a)x$, which shows that $(-a)x = -(ax)$. Analogously $a(-x) = -(ax)$.

(c) $a(x - y) = a(x + (-y)) = ax + a(-y) = ax + (-ay) = ax - ay$.

The proof of (d) is analogous to the proof of (c). ■

Module homomorphisms

A map $f : M \to M'$, where M and M' are left modules over a ring R, is called a module *homomorphism* or *linear map* if it is a homomorphism of additive groups and, for all $a \in R$, $x \in M$, $f(ax) = af(x)$. The definition of homomorphism of right modules is analogous.

Proposition 2.4 *A map $f : M \to M'$, where M and M' left modules over a ring R, is a module homomorphism if and only if, for all $a \in R$, $x, y \in M$, $f(x + y) = f(x) + f(y)$ and $f(ax) = af(x)$.*

Proof It follows from Proposition 0.5. ■

It is easy to prove that the composition of homomorphisms (of modules) is a homomorphism, the inverse of an isomorphism is an isomorphism and the set of all automorphisms of an R-module M, denoted by $\operatorname{Aut}_R M$, is a subgroup of $\operatorname{Aut} M$, the group of all automorphisms of the additive Abelian group M.

Remark 2.5 Let $f : M \to M'$ be a module homomorphism. As f is a homomorphism of additive Abelian groups, for all $x, y \in M$,

(a) $f(0_M) = 0_{M'}$,

(b) $f(-x) = -f(x)$,

(c) $f(x - y) = f(x) - f(y)$,

(d) f is a monomorphism if and only if $\ker f = 0$. ([1])

Submodules

Let M be a module over a ring R. It is said that a subset N of M is a *submodule* of M if N is an additive subgroup of M (that is, $0 \in N$ and, for all $x, y \in N$, $x - y \in N$) and, for all $a \in R$ and $x \in N$, $ax \in N$. It is easy to prove that, if N is a submodule of an R-module M, then N is an R-module with the restrictions of the operations to N.

It is said that a module M is *simple* or *irreducible* if $M \neq 0$ and 0 and M are the only submodules of M.

[1] Recall that $\ker f$ was defined when studying groups. With the additive language, $\ker f = \{x \in M : f(x) = 0\}$.

If R is a ring, then the submodules of the regular module ${}_R R$ are the left ideals of R.

Proposition 2.6 *Let $f : M \to M'$ be a module homomorphism.*

(a) *If S is a submodule of M, then $f(S)$ is a submodule of M',*

(b) *If S' is a submodule of M', then $f^{-1}(S')$ is a submodule of M.*
In particular, $\ker f$ *is a submodule of M.*

Proposition 2.7 *Let $(N_i)_{i\in I}$ be a non-empty totally ordered family of submodules of a module M. Then*

$$\bigcup_{i\in I} N_i$$

is a submodule of M.

Proposition 2.8 *Let $(N_i)_{i\in I}$ be a non-empty family of submodules of a module M. Then*

$$\bigcap_{i\in I} N_i$$

is a submodule of M.

Submodule generated by a set

Let X be a subset of a module M over a ring R. The intersection of all submodules of M that contain X is called the *submodule of M generated by X*. Thus the submodule of M generated by X is the smallest submodule of M that contains X. It is said that M is *cyclic* if there is $x \in M$ such that M is generated by $\{x\}$. A *linear combination* of X is any element of the form

$$a_1x_1 + \cdots + a_nx_n, \tag{2.2}$$

where $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$, $x_1, \ldots, x_n \in X$.

If $\emptyset \neq A \subseteq R$ and $\emptyset \neq X \subseteq M$, then

$$AX := \{a_1x_1 + \cdots + a_nx_n : n \in \mathbb{N}, a_1, \ldots, a_n \in A, x_1, \ldots, x_n \in X\}.$$

In particular, RX is the set of all linear combinations of X. If $a \in R$, then aX denotes the set $\{a\}X = \{ax : x \in X\}$. If $x \in M$, então Ax denotes the set $A\{x\} = \{ax : a \in A\}$.

Proposition 2.9 *Let X be a non-empty subset of a module M. Then RX is the submodule of M generated by X.*

Proposition 2.10 *Let $(N_i)_{i\in I}$ be a non-empty family of submodules of a module M. Then*

$$\sum_{i\in I} N_i$$

is the submodule of M generated by $\bigcup_{i\in I} N_i$.

Quotient module

Let S be a submodule of a module M over a ring R. In the additive quotient group M/S, define a scalar multiplication as follows: for all $a \in R$ and $x \in M$,

$$a(x+S) = (ax) + S.$$

It is easy to prove that this scalar multiplication is well defined and, with it, the additive group M/S is an R-module. This module M/S is called the *quotient module* of M by S. The map

$$p : M \to M/S, \quad x \mapsto x + S,$$

is an module epimorphism called the *canonical epimorphism* from M to M/S. The map

$$i : S \to M, \quad x \mapsto x,$$

is a module monomorphism called *inclusion* from S to M.

Proposition 2.11 *Let S be a submodule of a module M. The set of all submodules of M/S is*

$$\{N/S : N \textit{ is a submodule of } M \textit{ and } S \subseteq N\}.$$

Proposition 2.12 *Let $f : M \to M'$ be a module homomorphism. The modules $M/\ker f$ and $f(M)$ are isomorphic and*

$$\Phi : \frac{M}{\ker f} \to f(M), \quad x + \ker f \mapsto f(x),$$

is a module isomorphism.

Proof By Proposition 0.17, Φ is an isomorphism of additive groups. Suppose that M, M' are modules over a ring R. For all $a \in R$ and $x \in M$, $\Phi(a(x+\ker f)) = \Phi((ax)+\ker f) = f(ax) = af(x) = a\Phi(x+\ker f)$. ■

Proposition 2.13 *Let S, T be submodules of a module M such that $S \subseteq T$. The modules M/T and $(M/S)/(T/S)$ are isomorphic and*

$$\Psi : \frac{M}{T} \to \frac{M/S}{T/S}, \quad x + T \mapsto (x+S) + (T/S),$$

is a module isomorphism.

Proposition 2.14 *Let S and T be submodules of a module M. The modules $(S+T)/T$ and $S/(T \cap S)$ are isomorphic and*

$$\Omega : \frac{S}{T \cap S} \to \frac{S+T}{T}, \quad x + (T \cap S) \mapsto x + T,$$

is a module isomorphism.

Free modules

Let M be a module over a ring R.

It is said that a subset X of M is *linearly independent* if, for all $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$, $x_1, \ldots, x_n \in X$, where $x_1, \ldots, x_n$ are distinct,

$$a_1x_1 + \cdots + a_nx_n = 0 \ \Rightarrow \ a_1 = \cdots = a_n = 0.$$

In particular, $\emptyset$ is a linearly independent subset of M. Every subset of a linearly independent set is also a linearly independent set.

A subset B of M is called a *basis* of M if it generates M and is linearly independent. If M has a basis, it is said that M is *free*.

Examples 2.15 1. A trivial module $M = 0$ is free and $\emptyset$ is a basis of M.

2. Let R be a ring. The regular module ${}_RR$ (respectively, R_R) is free and $\{1\}$ is one of its bases.
3. If R is a ring and $n \in \mathbb{N}$, then

   $$\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$$

   is a basis of ${}_RR^n$ (respectively, R^n_R) called the *canonical basis* of this module.
4. We know, from elementary Algebra Linear courses, that every finitely generated vector space over a field is free. The non-finitely generated vector spaces are also free. To justify this assertion, take any vector space V and, using the Zorn lemma, prove that V has a maximal linearly independent subset X; then prove that X generates V.
5. If G is a finite non-trivial additive Abelian group, then G is not free as $\mathbb{Z}$-module. To justify this assertion, suppose that a finite non-trivial additive Abelian group G is free and that B is one of its bases. If either $B = \emptyset$ or $B = \{0\}$, then the group G generated by B would be trivial, a contradiction. Thus $B \neq \emptyset$, $B \neq \{0\}$ and there is $b \in B \setminus \{0\}$. As G is finite, there is $n \in \mathbb{Z} \setminus 0$ such that $nb = 0$, which contradicts the linear independence of B.
6. A free module can have bases with different cardinalities. For example, if $R = 0$ is a trivial ring, then $\emptyset$ and $\{0\}$ are basis of a trivial R-module $M = 0$.

Exercises

2.1.1 Let R be a ring, $\mathfrak{a}$ a left ideal of R, M a left R-module and $\emptyset \neq X \subseteq M$. Prove that $\mathfrak{a}X$ is a submodule of M.

2.1.2 Prove that, if S, T, U are submodules of a module M and $U \subseteq S$, then $S \cap (T + U) = (S \cap T) + U$.

2.1.3 Let K and L be submodules of a module M. Prove that $K \cup L$ is a submodule of M if and only if $K \subseteq L$ or $L \subseteq K$.

2.1.4 Let M be a module over a ring R and $\mathfrak{a}$ an ideal of R. Prove that $M/\mathfrak{a}M$ is an $(R/\mathfrak{a})$-module with the scalar multiplication

$$\frac{R}{\mathfrak{a}} \times \frac{M}{\mathfrak{a}M} \to \frac{M}{\mathfrak{a}M}, \quad (r + \mathfrak{a}, x + \mathfrak{a}M) \mapsto (r + \mathfrak{a})(x + \mathfrak{a}M) := rx + \mathfrak{a}M.$$

In particular, when $\mathfrak{a}M = 0$, M is an $(R/\mathfrak{a})$-module with the scalar multiplication

$$R/\mathfrak{a} \times M \to M, \quad (r + \mathfrak{a}, x) \mapsto (r + \mathfrak{a})x := rx.$$

In this case, the submodules of the R-module M coincidem with the submodules of the $(R/\mathfrak{a})$-module M.

2.1.5 Let R be a principal ideal domain and let $p \in R$ be irreducible. We already know that Rp is a maximal ideal of R and R/Rp is a field. Let M be an R-module and

$$M_p = \{x \in M : px = 0\}.$$

Prove that M_p is a submodule of M and is a vector space over R/Rp with the scalar multiplication

$$R/Rp \times M_p \to M_p \quad (r + Rp, x), \mapsto (r + Rp)x := rx.$$

2.1.6 Let $\mathfrak{a}$ be a proper ideal of a ring R. Prove that the left R-module $R/\mathfrak{a}$ is free if and only if $\mathfrak{a} = 0$.

2.1.7 Let M be a module over a ring R and $X \subseteq M$. Prove that:

(a) X is a basis of M if and only if every element of M can be written in a unique way as a linear combination of X. ([2])

(b) If there is $x \in X$ such that x is a linear combination of $X \setminus \{x\}$, then X is linearly dependent.

(c) In the regular module $\mathbb{Z}$, $\{2, 3\}$ is linearly dependent, but 2 is not a linear combination of $\{3\}$ and 3 is not a linear combination of $\{2\}$.

(d) If R is a division ring and X is linearly dependent, then there is $x \in X$ such that x is a linear combination of $X \setminus \{x\}$.

2.2 Rings and modules of matrices and operators

Matrices

Let R be a ring.

A matrix of size $n \times m$, where $n, m \in \mathbb{N}$, with entries in R is any map

$$\{1, \dots, n\} \times \{1, \dots, m\} \to R, \quad (i, j) \mapsto a_{i,j}. \tag{2.3}$$

[2] "y can be written in a unique way as a linear combination of X" means that y is a linear combination of X and, for all families $(a_x)_{x \in X}$ and $(c_x)_{x \in X}$ of elements of R such that $\{x \in X : a_x \neq 0\}$ and $\{x \in X : c_x \neq 0\}$ are finite, $y = \sum_{x \in X} a_x b = \sum_{x \in X} c_x b \Rightarrow \forall x \in X \; a_x = c_x$.

We will use the usual language of matrices known from elementary linear algebra. In particular, a matrix (2.3) is represented by a rectangular array with n rows and m columns:

$$\begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{bmatrix}$$

or, briefly, by $[a_{i,j}]$. The identity matrix of order n is denotes by I_n. The set of all matrices of size $n \times m$ with entries in R is denoted by $R^{n\times m}$. Matrix operations are also defined as usual:

Addition: if $A = [a_{i,j}], B = [b_{i,j}] \in R^{n\times m}$, then $A + B \in R^{n\times m}$ has its entry (i, j) equal to $a_{i,j} + b_{i,j}$.

Left scalar multiplication: if $r \in R$ and $A = [a_{i,j}] \in R^{n\times m}$, then $rA \in R^{n\times m}$ has its entry (i, j) equal to $ra_{i,j}$.

Right scalar multiplication: if $r \in R$ and $A = [a_{i,j}] \in R^{n\times m}$, then $Ar \in R^{n\times m}$ has its entry (i, j) equal to $a_{i,j}r$.

Multiplication: if $A = [a_{i,k}] \in R^{n\times p}$ and $B = [b_{k,j}] \in R^{p\times m}$, then $AB \in R^{n\times m}$ has its entry (i, j) equal to $\sum_{k=1}^{p} a_{i,k}b_{k,j}$.

Transpose: if $A = [a_{i,j}] \in R^{n\times m}$, then $A^T \in R^{m\times n}$ has its entry (j, i) equal to $a_{i,j}$.

Proposition 2.16 *Let R be a ring. Let $A, A' \in R^{n\times p}$, $B, B' \in R^{p\times q}$, $C \in R^{q\times m}$. Then*

(a) $(AB)C = A(BC)$,

(b) $I_nA = A = AI_p$,

(c) $(A + A')B = AB + A'B$,

(d) $A(B + B') = AB + AB'$.

Proposition 2.17 *Let R be a ring.*

(a) $R^{n\times m}$ *is a left R-module and is a right R-module.*

(b) $R^{m\times m}$ *is a ring.*

(c) $R^{n\times m}$ *is a left $R^{n\times n}$-module and is a right $R^{m\times m}$-module.*

Rings and modules of homomorphisms

Let G and H be additive Abelian groups. Let $\mathrm{Hom}(G, H)$ be the set of all homomorphisms of groups $G \to H$. The set $\mathrm{Hom}(G, G)$ is also represented by $\operatorname{End} G$.

In $\mathrm{Hom}(G, H)$, define an addition as follows: for all $f, g \in \mathrm{Hom}(G, H)$, $f + g$ is the function $G \to H$ that maps each $x \in G$ to $f(x) + g(x)$.

Proposition 2.18 *Let G and H be additive Abelian groups. The sum of homomorphisms of groups is a homomorphism of groups. With this addition,* $\mathrm{Hom}(G, H)$ *is an Abelian group.*

Proposition 2.19 *Let G be an additive Abelian group. With the addition and the composition,* $\operatorname{End} G$ *is a ring. The identity of* $\operatorname{End} G$ *is the identity map* $\mathrm{id}_G : G \to G$, $x \mapsto x$.

Now let M and N be left modules over a ring R. For all $a \in R$, $f \in \mathrm{Hom}(M, N)$, the product of a by f is defined as the map $af : M \to N$, $x \mapsto af(x)$.

Proposition 2.20 *Let M and N be left modules over a ring R. The product of $a \in R$ by $f \in \mathrm{Hom}(M, N)$ is a homomorphism of groups. With this scalar multiplication, the additive group* $\mathrm{Hom}(M, N)$ *is an R-module.*

With the previous notation, $\mathrm{Hom}_R(M, N)$ denotes the set of all homomorphisms of R-modules $M \to N$. The set $\mathrm{Hom}_R(M, M)$ is also denoted by $\operatorname{End}_R M$.

Proposition 2.21 *Let M and N be left modules over a commutative ring R. The product of $a \in R$ by $f \in \mathrm{Hom}(M, N)$ is a homomorphism of R-modules* ([3]). *Moreover,* $\mathrm{Hom}_R(M, N)$ *is a submodule of* $\mathrm{Hom}(M, N)$.

Proposition 2.22 *If M is a module over a ring R, then* $\operatorname{End}_R M$ *is a subring of* $\operatorname{End} M$.

Proposition 2.23 *Let M be a module over a ring R. Let $S = \operatorname{End}_R M$. The additive group M is an S-module with the scalar multiplication*

$$S \times M \to M, \quad (f, x) \mapsto fx := f(x).$$

Other examples of rings and modules of operators

Example 2.24 Let U, V, W be normed vector spaces over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Denote by $\mathcal{B}(U, V)$ the set of all continuous linear maps $U \to V$. Recall that a linear map $f : U \to V$ is continuous if and only if there is $\mu \in \mathbb{R}^+$ such that, for all $u \in U$, $||f(u)|| \leq \mu ||u||$. Using this characterization of continuous linear maps, it is easy to deduce that, for all $a \in \mathbb{F}$, $f, f' \in \mathcal{B}(U, V)$, $g \in \mathcal{B}(V, W)$,

$$af \in \mathcal{B}(U, V), \quad f + f' \in \mathcal{B}(U, V), \quad gf \in \mathcal{B}(U, W), \quad \mathrm{id}_U \in \mathcal{B}(U, U).$$

It is easy to conclude that

[3] Assuming that R is not commutative, give an example that shows that the product af is not always a homomorphism of R-modules.

- $\mathcal{B}(U, V)$ is a vector subspace of $\mathrm{Hom}_{\mathbb{F}}(U, V)$ over the field $\mathbb{F}$,
- $\mathcal{B}(U, U)$ is a subring of $\mathrm{End}_{\mathbb{F}}\, U$,
- $\mathcal{B}(U, V)$ is a right module over $\mathcal{B}(U, U)$,
- $\mathcal{B}(U, V)$ is a left module over $\mathcal{B}(V, V)$,

taking the composition as scalar multiplication.

Example 2.25 Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Let $C^\infty(\mathbb{F})$ be the set of functions $f : \mathbb{F} \to \mathbb{F}$ that have derivatives of all orders. In $C^\infty(\mathbb{F})$, define an addition and a scalar multiplication as follows: for all $f, g \in C^\infty(\mathbb{F})$, $a \in \mathbb{F}$,

$$\begin{aligned} f + g : \mathbb{F} \to \mathbb{F}, &\quad x \mapsto f(x) + g(x), \\ af : \mathbb{F} \to \mathbb{F}, &\quad x \mapsto af(x). \end{aligned}$$

With these operations, $C^\infty(\mathbb{F})$ is a vector space over $\mathbb{F}$.

As the composition of any two maps belonging to $C^\infty(\mathbb{F})$ also belongs to $C^\infty(\mathbb{F})$, it is easy to deduce that $C^\infty(\mathbb{F})$ is a ring with the addition defined above and the composition.

For each polynomial $p = b_n X^n + \cdots + b_1 X + b_0 \in \mathbb{F}[X]$, let

$$\overline{p} = p\left(\frac{d}{dx}\right) : C^\infty(\mathbb{F}) \to C^\infty(\mathbb{F}), \quad f \mapsto b_n \frac{d^n f}{dx^n} + \cdots + b_1 \frac{df}{dx} + b_0 f. \tag{2.4}$$

For the convenience of notation, we can write

$$\overline{p}(f) = \sum_{k=0}^{n} b_n \frac{d^k f}{dx^k},$$

if we agree that the operator "derivative of order 0," d^0/dx^0, is the identity $\mathrm{id}_{C^\infty(\mathbb{F})}$. The maps of the form (2.4) are linear.

Proof that $\overline{p}$ repects the sum (The proof that $\overline{p}$ respects the scalar product is analogous.) Let $f, g \in C^\infty(\mathbb{F})$. For all $x \in \mathbb{F}$,

$$\begin{aligned} \overline{p}(f+g)(x) &= \left(\sum_{k=0}^{n} b_n \frac{d^k(f+g)}{dx^k}\right)(x) = \sum_{k=0}^{n} b_n \frac{d^k(f+g)}{dx^k}(x) \\ &= \sum_{k=0}^{n} b_n \left(\frac{d^k f}{dx^k}(x) + \frac{d^k g}{dx^k}(x)\right) = \sum_{k=0}^{n} b_n \frac{d^k f}{dx^k}(x) + \sum_{k=0}^{n} b_n \frac{d^k g}{dx^k}(x) \\ &= \overline{p}(f)(x) + \overline{p}(g)(x) = (\overline{p}(f) + \overline{p}(g))(x). \end{aligned}$$

Thus $\overline{p}(f+g) = \overline{p}(f) + \overline{p}(g)$. ■

In

$$\mathcal{D} = \{\overline{p} : p \in \mathbb{F}[X]\},$$

define an addition and a scalar multiplication as follows: for all $p, q \in \mathbb{F}[X]$, $a \in \mathbb{F}$,

$$\begin{aligned} \overline{p} + \overline{q} : C^\infty(\mathbb{F}) \to C^\infty(\mathbb{F}), &\quad f \mapsto \overline{p}(f) + \overline{q}(f), \\ a\overline{p} : C^\infty(\mathbb{F}) \to C^\infty(\mathbb{F}), &\quad f \mapsto a\overline{p}(f). \end{aligned}$$

With these operations, $\mathcal{D}$ is a vector space over $\mathbb{F}$ and

$$\mathbb{F}[X] \to \mathcal{D}, \quad p \mapsto \overline{p},$$

is an isomorphism of vector spaces.

Moreover, for all $p, q \in \mathbb{F}[X]$,

$$\overline{p}\,\overline{q} = \overline{pq},$$

where, on the left side, $\overline{p}\,\overline{q}$ is the composition of the functions $\overline{p}$ and $\overline{q}$, and, on the right side, pq is the product of the polynomials p and q. With the addition defined above and the composition, $\mathcal{D}$ is a commutative ring isomorphic to $\mathbb{F}[X]$.

Finally, the additive Abelian group $C^\infty(\mathbb{F})$ is a $\mathcal{D}$-module with the scalar multiplication

$$\mathcal{D} \times C^\infty(\mathbb{F}) \to C^\infty(\mathbb{F}), \quad (\overline{p}, f) \mapsto \overline{p}(f).$$

Exercises

2.2.1 Let M be a left module over a ring R. Prove that the additive group $\mathrm{Hom}_R(M, R)$ is a right R-module with the scalar multiplication defined as follows: if $f \in \mathrm{Hom}_R(M, R)$ and $a \in R$, then $fa : M \to R$ is the function that maps each $x \in M$ to $f(x)a$. (The right R-module $\mathrm{Hom}_R(M, R)$ is called the *dual module* of M.)

2.3 Algebras over commutative rings

Let R be a commutative ring. An *algebra* over R or *R-algebra* is a set B with an addition $(+ : B \times B \to B)$, a multiplication $(\cdot : B \times B \to B)$ and a scalar multiplication $(\cdot : R \times B \to B)$ such that B is a ring, B is an R-module and, for all $a \in R$, $b, d \in B$,

$$a(bd) = (ab)d = b(ad).$$

An algebra is said to be *commutative* if the multiplication is commutative.

A *subalgebra* of an R-algebra B is a subset S of B that is both a subring of the ring B and a submodule of the module B. If S is a subalgebra of an R-algebra B, then, by restricting the operations from B to S, S is an R-algebra.

An *ideal* of an R-algebra B is a subset $\mathfrak{a}$ of B that is both an ideal of the ring B and a submodule of the module B. If $\mathfrak{a}$ is an ideal of an R-algebra B, then $B/\mathfrak{a}$ is an R-algebra with the operations defined in the usual way.

Let $(S_i)_{i\in I}$ is a non-empty family of subalgebras of an algebra B. We have seen that $\bigcap_{i\in I} S_i$ is both a subring and a submodule of B. Hence $\bigcap_{i\in I} S_i$ is a subalgebra of B.

Given a subset X of an algebra B, we call *subalgebra of B generated by X* to the intersection of all subalgebras of B that contain X. The subalgebra of B generated by X is the smallest subalgebra of B that contains X.

Analogously, the intersection of a non-empty family of ideals of an algebra B is an ideal of B. Given a subset X of an algebra B, we call *ideal of B generated by X* to the intersection of all ideals of B that contain X. The ideal of B generated by X is the smallest ideal of B that contains X.

A map $\phi : B \to D$, where B and D are R-algebras, is called a *homomorphism of R-algebras* if it is both a homomorphism of rings and a homomorphism of R-modules.

Examples 2.26 In the following examples, R is a commutative ring.

1. With the usual operations, $R^{n\times n}$ is an R-algebra.
2. If M is an R-module, then $\operatorname{End}_R M$ is an R-algebra.
3. Let B be a ring. The *center* of B is
$$Z(B) = \{b \in B : \forall d \in B, bd = db\}.$$
The center of B is a commutative subring of B.

   Suppose that R is a subring of B contained in $Z(B)$. With the usual operations, B is an R-algebra.
4. Let X be a set and B an R-algebra. In the set $F(X, B)$ of the functions from X to B, define an addition, a multiplication and a scalar multiplication as follows: for all $\phi, \psi \in F(X, B)$, $a \in R$,
$$\begin{aligned} \phi + \psi : X \to B, &\quad x \mapsto \phi(x) + \psi(x),\\ \phi\psi : X \to B, &\quad x \mapsto \phi(x)\psi(x),\\ a\phi : X \to B, &\quad x \mapsto a\psi(x). \end{aligned}$$
With these operations, $F(X, B)$ is an R-algebra.
5. In example 2.24, $\mathcal{B}(U, U)$ is an $\mathbb{F}$-algebra. In example 2.25, $C^\infty(\mathbb{F})$ is an $\mathbb{F}$-algebra, and $\mathcal{D}$ is an $\mathbb{F}$-álgebra.

The algebra of the quaternions

An algebra B is said to be a *division algebra* if B is a division ring. An algebra B over a field F is said to be *finite dimensional* if B is a finite dimensional vetor space over F. It is easy to verify that, with the usual operations, $\mathbb{R}$ and $\mathbb{C}$ are finite dimensional division algebras over $\mathbb{R}$. A theorem due to Frobenius states that, up to isomorphism, the only finite-dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and the algebra of the quaternions described below.

Proposition 2.27 (a) *There is a real division algebra* $\mathbb{H}$ *of dimension* 4 (*as a vector space over* $\mathbb{R}$) *with a basis* $\{1, i, j, k\}$ *such that*

$$i^2 = j^2 = k^2 = ijk = -1. \tag{2.5}$$

(b) *Given such an algebra* $\mathbb{H}$,

$$Q = \{1, -1, i, -i, j, -j, k, -k\} \tag{2.6}$$

is a multiplicative group isomorphic to the quaternion group Q_8 *introduced in page* 43.

(c) *Such an algebra* $\mathbb{H}$ *is unique up to isomorphism and is called the* real algebra of the quaternions *and the elements of* $\mathbb{H}$ *are called* quaternions.

Proof Suppose that H is a non-trivial real algebra and that $\{1, i, j, k\}$ is a linearly independent subset of H with cardinality equal to 4 that satisfies (2.5). Then $Q = \{1, -1, i, -i, j, -j, k, -k\}$ is a subset of H with cardinality equal to 8. By doing the math, we deduce that Q is closed for products and has the following multiplication table.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(2.7)

It is easy to conclude that Q is a multiplicative group. Let $x = i$ and $y = j$. Then (1.12) is satisfied and, by Proposition 1.27, $Q \cong Q_8$, which proves (b).

(a) Let $\mathbb{H}$ be the subspace of the real space $\mathbb{R}^{4\times 4}$ with basis $B = \{1, i, j, k\}$, where

$$1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \ j = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \ k = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

It is easy to see that (2.5) is satisfied. By the previous paragraph, $Q = \{1, -1, i, -i, j, -j, k, -k\}$ is a multiplicative group with table (2.7). It follows that the product of two elements $x, y \in \mathbb{H}$, which are linear combinations of B, is also a linear combination of B and $xy \in \mathbb{H}$. It follows that $\mathbb{H}$ is a subring of $\mathbb{R}^{4\times 4}$ and, therefore, a subalgebra of $\mathbb{R}^{4\times 4}$. It is easy to check that each $x = a + bi + cj + dk \in \mathbb{H} \setminus 0$, where $a, b, c, d \in \mathbb{R}$, has inverse

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

Hence $\mathbb{H}$ is a division algebra.

(c) Given any such algebra $\mathbb{H}$, $Q = \{1, -1, i, -i, j, -j, k, -k\}$ is a multiplicative group with table (2.7). The multiplication in $\mathbb{H}$ is uniquely determined by this table. It follows that the algebra $\mathbb{H}$ is unique up to isomorphism. ■

Banach algebras

A real or complex algebra B is said to be a *Banach algebra* if it is a Banach space, $\|1\| = 1$ and, for all $a, b \in B$, $\|ab\| \le \|a\|\|b\|$. The last condition implies that the multiplication is continuous. The theory of Banach algebras is a large area in functional analysis.

Example 2.28 If $x = a + bi + cj + dk \in \mathbb{H}$, then the non-negative real number $|x| = \sqrt{a^2 + b^2 + c^2 + d^2}$ is called the *absolute value* of x. $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ are real Banach algebras with the norm given by the absolute value.

Example 2.29 Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Let X be a set. Let $B(X, \mathbb{F})$ be the set of all bounded functions $X \to \mathbb{F}$ ([4]). Then $B(X, \mathbb{F})$ is a subalgebra of $F(X, \mathbb{F})$ (see Example 2.26.4). With the supremum norm, $B(X, \mathbb{F})$ is a Banach algebra.

Example 2.30 Let U, V be normed spaces over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. In $\mathcal{B}(U, V)$ (see Example 2.24), define the *operator norm*, induced by the norms of U and V, as follows: for each $f \in \mathcal{B}(U, V)$,

$$\|f\| = \sup_{x \in U \setminus 0} \frac{\|f(x)\|}{\|x\|} = \max_{x \in U \setminus 0} \frac{\|f(x)\|}{\|x\|}.$$

It is known from the Topology course that, if V is a Banach space, then $\mathcal{B}(U, V)$ is a Banach space with the operator norm. (See also [Fabian&al, Proposition 1.27].) Therefore, if V is a Banach space, then $\mathcal{B}(V, V)$ is a Banach algebra.

[4] Recall that $f : X \to \mathbb{F}$ is bounded if there is $M \in \mathbb{R}^+$ such that, for all $x \in X$, $|f(x)| \le M$.

Example 2.31 Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. In the algebra of matrices $\mathbb{F}^{n\times n}$, define the *operator norm* as follows: for each $A \in \mathbb{F}^{n\times n}$,

$$\|A\| = \sup_{x\in\mathbb{F}^{n\times 1}\setminus 0} \frac{\|Ax\|}{\|x\|} = \max_{x\in\mathbb{F}^{n\times 1}\setminus 0} \frac{\|Ax\|}{\|x\|}.$$

Then $\mathbb{F}^{n\times n}$ is a Banach algebra.

Example 2.32 Let V be a normed space over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Let M be a closed subspace of V. It is not difficult to prove that

$$V/M \to \mathbb{R}, \quad x + M \mapsto \|x + M\| := \inf_{y\in x+M} \|y\| = \inf_{m\in M} \|x + m\|,$$

is a norm in the quotient space V/M, called the *quotient norm*. The closed nature of M is required to prove that $\|x + M\| = 0 \Rightarrow x + M = M$ but is not required to prove the other axioms of normed spaces.

It is more difficult to prove that, if V is a Banach space and M a closed subspace of V, then V/M is a Banach space. For a proof, see [Fabian&al, Proposition 1.35]. Consequently, if V is a Banach algebra and M is a closed ideal of V, then V/M is a Banach algebra.

Exercises

2.3.1 Enounce and prove the three theorems of isomorphism for algebras over commutative rings.

2.3.2 Let $\mathfrak{a}$ be an ideal of an algebra B over a commutative ring R. Describe the set of the subalgebras of $B/\mathfrak{a}$. Describe the set of the ideals of $B/\mathfrak{a}$. Justify.

2.3.3 Let A be a non-trivial (i. e., $A \neq 0$) algebra over a field F. Prove that $\phi : F \to A$, $\lambda \mapsto \lambda 1_A$, is a monomorphism of F-algebras.

2.3.4 Let R be a commutative ring. Let $\phi : R \to B$ be a homomorphism of rings such that $\operatorname{im}\phi \subseteq Z(B)$. Prove that the ring B is an R-algebra with the scalar multiplication $R \times B \to B$, $(r, b) \mapsto \phi(r)b$.

2.3.5 Let B be an algebra over a commutative ring R. Prove that $\phi : R \to B$, $a \mapsto a1_B$, is a homomorphism of rings such that $\operatorname{im}\phi \subseteq Z(B)$.

2.4 Monoid algebras

Let R be a commutative ring. Let G be a multiplicative monoid. Let $R[G]$ be the set of all maps $\alpha : G \to R$ such that

$$\{g \in G : \alpha(g) \neq 0\}$$

is finite. Define an addition and a scalar multiplication as follows: for all $\alpha, \beta \in R[G]$, $a \in R$,

$$\begin{aligned} \alpha + \beta : G \to R, &\quad g \mapsto \alpha(g) + \beta(g), \\ a\alpha : G \to R, &\quad g \mapsto a\alpha(g). \end{aligned}$$

Proposition 2.33 *With these operations, $R[G]$ is an R-module. The zero of $R[G]$ is the function that maps each $g \in G$ to 0_R.*

Given $a \in R$ and $g \in G$, define $ag \in R[G]$ as follows:

$$ag : G \to R, \quad g \mapsto a \quad \text{and, for all } h \neq g, \quad h \mapsto 0.$$

It is easy to see that ag is equal to the scalar product of $a \in R$ by $1g \in R[G]$.

Let $\alpha \in R[G]$. For each $h \in G$,

$$\alpha(h) = (\alpha(h)h)(h) = \sum_{g \in G} (\alpha(g)g)(h) = \left(\sum_{g \in G} \alpha(g)g \right)(h).$$

Thus α can be written as a sum of elements of the form ag:

$$\alpha = \sum_{g \in G} \alpha(g)g.$$

With this notation, the addition and the scalar multiplication defined above can be described by the following formulas: for all $\alpha, \beta \in R[G]$, $a \in R$,

$$\alpha + \beta = \sum_{g \in G} (\alpha(g) + \beta(g))g, \tag{2.8}$$

$$a\alpha = \sum_{g \in G} (a\alpha(g))g. \tag{2.9}$$

Next, let us define a multiplication in $R[G]$ so that the R-module $R[G]$ becomes an R-algebra and the map

$$i : G \to R[G], \quad g \mapsto 1g, \tag{2.10}$$

becomes a monomorphism of monoids. Suppose such a multiplication exists. Then, for all $\alpha, \beta \in R[G]$,

$$\begin{aligned}
\alpha\beta &= \left(\sum_{k \in G} \alpha(k)k \right) \left(\sum_{l \in G} \beta(l)l \right) = \sum_{k,l \in G} (\alpha(k)k)(\beta(l)l) \\
&= \sum_{k,l \in G} (\alpha(k)(1k))(\beta(l)(1l)) = \sum_{k,l \in G} (\alpha(k)\beta(l))((1k)(1l)) \\
&= \sum_{k,l \in G} (\alpha(k)\beta(l))(1(kl)) = \sum_{g \in G} \sum_{\substack{k,l \in G \\ kl = g}} (\alpha(k)\beta(l))(1g) \\
&= \sum_{g \in G} \left(\sum_{\substack{k,l \in G \\ kl = g}} \alpha(k)\beta(l) \right)(1g) = \sum_{g \in G} \left(\sum_{\substack{k,l \in G \\ kl = g}} \alpha(k)\beta(l) \right) g.
\end{aligned}$$

Therefore, if such a multiplication exists, it must be defined by

$$\alpha\beta = \left(\sum_{k\in G}\alpha(k)k\right)\left(\sum_{l\in G}\beta(l)l\right) = \sum_{g\in G}\left(\sum_{\substack{k,l\in G\\ kl=g}}\alpha(k)\beta(l)\right)g. \tag{2.11}$$

Proposition 2.34 *With the addition defined by* (2.8), *the scalar multiplication defined by* (2.9) *and the multiplication defined by* (2.11), $R[G]$ *is an* R*-algebra, the map* i (2.10) *is a monomorphism of monoids, and the map*

$$j : R \to R[G], \quad a \mapsto a1, \tag{2.12}$$

is a monomorphism of rings. The monoid G *is Abelian if and only if the algebra* $R[G]$ *is commutative.*

The monomorphisms i and j allow us to identify G and R with their images in $R[G]$. Thus, if $g \in G$ and $a \in R$, $i(g) = 1g$ is represented by g and $j(a) = a1$ is represented b a. With this notation, ag is the scalar product of $a \in R$ by $g \in R[G]$ and is also the product of $a, g \in R[G]$.

Note that

$$R[G] = \left\{\sum_{g\in G} a_g g : \forall g \in G, a_g \in R\right\}$$

is the set of all linear combinations of G. Thus G generates the R-module $R[G]$. On the other hand,

$$\sum_{g\in G} a_g g = 0 \;\Rightarrow\; \forall g \in G, a_g = 0,$$

whereby G is linearly independent. Hence G is a basis of the R-module $R[G]$ and this module is free.

Proposition 2.35 *Let* B *be an* R*-algebra and* $h : G \to B$ *a homomor*phism of monoids. There is a unique homomorphism of R-algebras $\psi : R[G] \to B$ that extends h, that is, for all $g \in G$, $\psi(g) = h(g)$.

$$\begin{tikzcd} G \arrow[r, "i"] \arrow[dr, "h"'] & R[G] \arrow[d, "\psi"] \\ & B \end{tikzcd}$$

Proof If such a homomorphism ψ exists, then, whatever $\alpha \in R[G]$,

$$\psi(\alpha) = \psi\left(\sum_{g\in G}\alpha(g)g\right) = \sum_{g\in G}\alpha(g)\psi(g) = \sum_{g\in G}\alpha(g)h(g),$$

which proves unicity. It is easy to prove that

$$\psi : R[G] \to B, \quad \alpha \mapsto \sum_{g\in G}\alpha(g)h(g),$$

is a homomorphism of R-algebras that extends h. ■

Representations and modules

The definition of linear representation of a group was introduced in Section 1.5. More generally, a linear representation of a group G is any homomorphism of groups $G \to \operatorname{Aut}_R M$, where $\operatorname{Aut}_R M$ is the group of all automorphisms of a module M over a commutative ring R. Throughout this section, "representation" means "linear representation".

Proposition 2.36 *Let G be a group and let R be a commutative ring. There is a faithful (that is, injective) representation $f : G \to \operatorname{Aut}_R R[G]$.*

Proof Let $g \in G$. Prove that

$$f_g : R[G] \to R[G], \quad \sum_{x \in G} a_x x \mapsto \sum_{x \in G} a_x (gx),$$

is an automorphism of the R-module $R[G]$. Prove that

$$f : G \to \operatorname{Aut}_R R[G], \quad g \mapsto f_g,$$

is a faithful representation. ■

When representations by permutations of a group G were introduced in page 38, it was remarked that, given a set X, there is a bijective correspondence between representations $G \to \operatorname{Sym} X$ and actions of G on X. This correspondence allows us to carry problems about representations by permutations to the language of actions and vice versa. Representations by permutations and actions can be viewed as two languages for the same mathematical idea. In the next two propositions, two alternative languages for linear representations are given.

Let R be a commutative ring. A representation of an R-algebra A is any homomorphism of R-algebras $F : A \to \operatorname{End}_R M$, where M is an R-module.

Proposition 2.37 *Let G be a group and let R be a commutative ring.*

(a) *If $f : G \to \operatorname{Aut}_R M$ is a representation of G, then*

$$F : R[G] \to \operatorname{End}_R M, \quad \sum_{x \in G} a_x x \mapsto \sum_{x \in G} a_x f(x),$$

is a representation of the R-algebra $R[G]$.

(b) *If $F : R[G] \to \operatorname{End}_R M$ is a representation of $R[G]$, then, for each $x \in G$, $F(x) \in \operatorname{Aut}_R M$ and $F_{|G} : G \to \operatorname{Aut}_R M$ is a representation of G.*

(c) (a) *and* (b) *give a bijective correspondence between representations of the group G and representations of the algebra $R[G]$.*

Proposition 2.38 *Let G be a group and let R be a commutative ring.*

(a) *If $F : R[G] \to \operatorname{End}_R M$ is a representation of $R[G]$, then M is an $R[G]$-module with the scalar multiplication*

$$R[G] \times M \to M, \quad (a, m) \mapsto F(a)(m).$$

(b) *Let M is an $R[G]$-module. By restricting the scalar multiplication to $R \times M$, M becomes an R-module. Then, for each $a \in R[G]$,*

$$F(a) : M \to M, \quad m \mapsto am,$$

is an endomorphism of the R-module M and

$$F : R[G] \to \operatorname{End}_R M, \quad a \mapsto F(a),$$

is a representation of $R[G]$.

(c) (a) *and* (b) *give a bijective correspondence between the representations of $R[G]$ and the $R[G]$-modules.*

Exercises

2.4.1 Let R be a commutative ring and let $h : G \to G'$ be a homomorphism of monoids. Prove that there is a unique homomorphism of R-algebras $\psi : R[G] \to R[G']$ that extends h.

2.4.2 Let G be a monoid and let $\phi : R \to R'$ be a homomorphism of commutative rings. Prove that there is a unique homomorphism of R-algebras $\psi : R[G] \to R'[G]$ that extends ϕ.

2.5 Algebras of polynomials

Let R be a commutative ring. From now on, $X, X_1, \ldots, X_n$ are distinct variables.

Let G be the set of all maps $k : \{X_1, \ldots, X_n\} \to \mathbb{N}_0$, which we call *primitive monomials* in the variables $X_1, \ldots, X_n$. Denote $k \in G$ by $X_1^{k(1)} \cdots X_n^{k(n)}$. In G, define a multiplication as follows: for all $X_1^{k_1} \cdots X_n^{k_n}$, $X_1^{l_1} \cdots X_n^{l_n} \in G$,

$$(X_1^{k_1} \cdots X_n^{k_n})(X_1^{l_1} \cdots X_n^{l_n}) = X_1^{k_1+l_1} \cdots X_n^{k_n+l_n}.$$

It is easy to see that, with this multiplication, G is an Abelian monoid. The identity of G is $X_1^0 \cdots X_n^0$.

We make convention that the symbol X_i also represents

$$X_1^0 \cdots X_{i-1}^0 X_i^1 X_{i+1}^0 \cdots X_n^0 \in G.$$

In this way, $X_1^{k_1} \cdots X_n^{k_n}$ is the product of the elements $X_1^{k_1}, \ldots, X_n^{k_n}$, where each $X_i^{k_i}$ is the k_ith power of $X_i \in G$.

The commutative R-algebra $R[G]$ is called *R-algebra of the polynomials in the variables* $X_1, \ldots, X_n$. This algebra is denoted by $R[X_1, \ldots, X_n]$. The elements of $R[X_1, \ldots, X_n]$ are called *polynomials in the variables* $X_1, \ldots, X_n$ *with coefficients in* R.

As in the previous section, we identify the elements of G and the elements of R with their images in $R[X_1, \ldots, X_n]$ by the monomorphisms i and j (cf. (2.10) and (2.12)). The polynomials of the form $aX_1^{k_1} \cdots X_n^{k_n}$, where $a \in R$, are called *monomials*.

With the previous notation, each polynomial $f \in R[X_1, \ldots, X_n]$ can be written in the form

$$f = \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n},$$

where the elements $a_{k_1,\ldots,k_n}$ belong to R and the set

$$S(f) = \{(k_1, \ldots, k_n) \in \mathbb{N}_0^n : a_{k_1,\ldots,k_n} \neq 0\}$$

is finite. As $S(f)$ is finite, there are $m_1, \ldots, m_n \in \mathbb{N}_0$ such that

$$f = \sum_{k_1=0}^{m_1} \cdots \sum_{k_n=0}^{m_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}.$$

Note that two polynomials

$$f = \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}, \quad g = \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} b_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}, \tag{2.13}$$

are equal if and only if, for all $k_1, \ldots, k_n \in \mathbb{N}_0$, $a_{k_1,\ldots,k_n} = b_{k_1,\ldots,k_n}$.

The operations in $R[X_1, \ldots, X_n]$ can be described as follows: for any polynomials f and g, with the forms (2.13), and any $c \in R$,

$$\begin{aligned} f + g &= \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} (a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n}) X_1^{k_1} \cdots X_n^{k_n}, \qquad (2.14) \\ cf &= \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} c a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}, \\ fg &= \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} \left(\sum_{\substack{r_1, s_1 \in \mathbb{N}_0 \\ r_1 + s_1 = k_1}} \cdots \sum_{\substack{r_n, s_n \in \mathbb{N}_0 \\ r_n + s_n = k_n}} a_{r_1,\ldots,r_n} b_{s_1,\ldots,s_n} \right) X_1^{k_1} \cdots X_n^{k_n}. \end{aligned}$$

Degree

The *degree* of a primitive monomial $X_1^{k_1} \cdots X_n^{k_n}$ is the integer

$$d(X_1^{k_1} \cdots X_n^{k_n}) = k_1 + \cdots + k_n.$$

Let

$$f = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} \in R[X_1, \ldots, X_n].$$

Each $a_{k_1,\ldots,k_n}$ is called the *coefficient* of $X_1^{k_1}\cdots X_n^{k_n}$ in f. It is said that a primitive monomial $X_1^{k_1}\cdots X_n^{k_n}$ *occurs* in f if $a_{k_1,\ldots,k_n}\neq 0$. If $f\neq 0$, the *degree* of f is the largest degree of the primitive monomials that occur in f. If $f=0$, it is said that the *degree* of f is $-\infty$. The degree of f is denoted by $d(f)$.

Addition and order in $\mathbb{N}_0$ are extended to $\{-\infty\}\cup\mathbb{N}_0$ as follows: for all $n\in\{-\infty\}\cup\mathbb{N}_0$,

$$n+(-\infty)=(-\infty)+n=-\infty,\quad -\infty\leq n.$$

Define a total order in the set of the primitive monomials in the variables $X_1,\ldots,X_n$ as follows: it is said that $X_1^{k_1}\cdots X_n^{k_n}>X_1^{l_1}\cdots X_n^{l_n}$ if

- either $d(X_1^{k_1}\cdots X_n^{k_n})>d(X_1^{l_1}\cdots X_n^{l_n})$
- or $d(X_1^{k_1}\cdots X_n^{k_n})=d(X_1^{l_1}\cdots X_n^{l_n})$ and $(k_1,\ldots,k_n)>(l_1,\ldots,l_n)$ for the lexicographic order ([5]).

In variables X_1,X_2, we have

$$1<X_2<X_1<X_2^2<X_1X_2<X_1^2<X_2^3<X_1X_2^2<X_1^2X_2<X_1^3<X_2^4<\cdots.$$

Proposition 2.39 *For all $f,g\in R[X_1,\ldots,X_n]$,*

(a) *$d(f+g)\leq\max\{d(f),d(g)\}$,*

(b) *$d(fg)\leq d(f)+d(g)$,*

(c) *if R is an integral domain, $d(fg)=d(f)+d(g)$,*

(d) *if R is an integral domain, then $R[X_1,\ldots,X_n]$ is also an integral domain.*

Proof Suppose that f and g have the forms (2.13). If any of these polynomials is equal to 0, then (a), (b) and (c) are trivial. Suppose that f and g are different from 0.

It follows from (2.14) that, if a primitive monomial occurs in $f+g$, then it occurs in f or in g. Therefore (a) is satisfied.

On the other hand,

$$fg=\sum_{r_1,\ldots,r_n,s_1,\ldots,s_n\in\mathbb{N}_0}a_{r_1,\ldots,r_n}b_{s_1,\ldots,s_n}X_1^{r_1+s_1}\cdots X_n^{r_n+s_n},$$

which shows that primitive monomials occuring in fg have at most degree $d(f)+d(g)$. Therefore (b) is satisfied.

Suppose now that R is an integral domain. Let $X_1^{p_1}\cdots X_n^{p_n}$ be the largest primitive monomial occuring in f. Let $X_1^{q_1}\cdots X_n^{q_n}$ be the largest primitive monomial occuring in g. Then $d(f)=p_1+\cdots+p_n$ and $d(g)=q_1+\cdots+q_n$. As R is an integral domainl, $a_{p_1,\ldots,p_n}b_{q_1,\ldots,q_n}\neq 0$.

[5] "$(k_1,\ldots,k_n)>(l_1,\ldots,l_n)$ for the lexicographic order" means that $(k_1,\ldots,k_n)\neq(l_1,\ldots,l_n)$ and $k_1=l_1,\ldots,k_{i-1}=l_{i-1},k_i>l_i$ for some $i\in\{1,\ldots,n\}$.

In the following paragraph, we will prove that, if $X_1^{r_1} \cdots X_n^{r_n}$ occurs in f, $X_1^{s_1} \cdots X_n^{s_n}$ occurs in g and $X_1^{p_1+q_1} \cdots X_n^{p_n+q_n} = X_1^{r_1+s_1} \cdots X_n^{r_n+s_n}$, then $X_1^{p_1} \cdots X_n^{p_n} = X_1^{r_1} \cdots X_n^{r_n}$ and $X_1^{q_1} \cdots X_n^{q_n} = X_1^{s_1} \cdots X_n^{s_n}$. From this fact, it follows that $X_1^{p_1+q_1} \cdots X_n^{p_n+q_n}$ occurs in fg with coefficient $a_{p_1,\ldots,p_n} b_{q_1,\ldots,q_n}$. Therefore $R[X_1, \ldots, X_n]$ is an integral domain and $d(fg) \geq d(f) + d(g)$. By (b), $d(fg) = d(f) + d(g)$.

Suppose then that $X_1^{r_1} \cdots X_n^{r_n}$ occurs in f, $X_1^{s_1} \cdots X_n^{s_n}$ occurs in g and

$$X_1^{p_1+q_1} \cdots X_n^{p_n+q_n} = X_1^{r_1+s_1} \cdots X_n^{r_n+s_n}. \tag{2.15}$$

Taking the degrees of both sides of (2.15),

$$(p_1 + \cdots + p_n) + (q_1 + \cdots + q_n) = (r_1 + \cdots + r_n) + (s_1 + \cdots + s_n). \tag{2.16}$$

By the maximality of $X_1^{p_1} \cdots X_n^{p_n}$ and $X_1^{q_1} \cdots X_n^{q_n}$,

$$p_1 + \cdots + p_n \geq r_1 + \cdots + r_n \quad \text{and} \quad q_1 + \cdots + q_n \geq s_1 + \cdots + s_n. \tag{2.17}$$

By (2.16) and (2.17),

$$p_1 + \cdots + p_n = r_1 + \cdots + r_n \quad \text{and} \quad q_1 + \cdots + q_n = s_1 + \cdots + s_n. \tag{2.18}$$

As $X_1^{p_1} \cdots X_n^{p_n} \geq X_1^{r_1} \cdots X_n^{r_n}$ and these monomials have the same degree, $p_1 \geq r_1$. Analogously $q_1 \geq s_1$. By (2.15), $p_1 + q_1 = r_1 + s_1$. Thus $p_1 = r_1$ and $q_1 = s_1$. Again by the maximality of $X_1^{p_1} \cdots X_n^{p_n}$ and $X_1^{q_1} \cdots X_n^{q_n}$, $p_2 \geq r_2$ and $q_2 \geq s_2$. By (2.15), $p_2 + q_2 = r_2 + s_2$. Then $p_2 = r_2$ and $q_2 = s_2$. By repeating this argument, we deduce that $p_i = r_i$ and $q_i = s_i$, for $i \in \{1, \ldots, n\}$. Hence $X_1^{p_1} \cdots X_n^{p_n} = X_1^{r_1} \cdots X_n^{r_n}$ and $X_1^{q_1} \cdots X_n^{q_n} = X_1^{s_1} \cdots X_n^{s_n}$.

■

Evaluation homomorphism

Lemma 2.40 *Let G be the monoid of the primitive monomials in the variables $X_1, \ldots, X_n$. Let H be a monoid and $h_1, \ldots, h_n \in H$. If H is Abelian or $n = 1$, then there is one and only one homomorphism of monoids $\phi : G \to H$ such that, for all $i \in \{1, \ldots, n\}$, $\phi(X_i) = h_i$.*

Proof If such a homomorphism ϕ exists, then, for all $X_1^{k_1} \cdots X_n^{k_n} \in G$,

$$\phi(X_1^{k_1} \cdots X_n^{k_n}) = \phi(X_1)^{k_1} \cdots \phi(X_n)^{k_n} = h_1^{k_1} \cdots h_n^{k_n},$$

which proves unicity.

It is easy to prove that $\phi : G \to H$, $X_1^{k_1} \cdots X_n^{k_n} \mapsto h_1^{k_1} \cdots h_n^{k_n}$, is a homomorphism of monoids such that, for all $i \in \{1, \ldots, n\}$, $\phi(X_i) = h_i$. ■

Proposition 2.41 *Let R be a commutative ring, B an R-algebra and $b = (b_1, \dots, b_n) \in B^n$. If B is commutative or $n = 1$, then there is one and only one homomorphism of R-algebras $\Psi_b : R[X_1, \dots, X_n] \to B$ such that, for all $i \in \{1, \dots, n\}$, $\Psi_b(X_i) = b_i$.*

Proof If such a homomorphism Ψ_b exists, then, for each

$$f = \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} a_{k_1,\dots,k_n} X_1^{k_1} \cdots X_n^{k_n} \in R[X_1, \dots, X_n],$$

$$\begin{aligned}\Psi_b(f) &= \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} a_{k_1,\dots,k_n} \Psi_b(X_1)^{k_1} \cdots \Psi_b(X_n)^{k_n} \\ &= \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} a_{k_1,\dots,k_n} b_1^{k_1} \cdots b_n^{k_n},\end{aligned}$$

which proves unicity.

Let G be the monoid of the primitive monomials in the variables $X_1, \dots, X_n$. By lemma 2.40, there is a homomorphism of monoids $\phi : G \to B$ such that, for each $i \in \{1, \dots, n\}$, $\phi(X_i) = b_i$. By Proposition 2.35, there is a homomorphism of R-algebras $\Psi_b : R[G] = R[X_1, \dots, X_n] \to B$ that extends ϕ. In particular, for each $i \in \{1, \dots, n\}$, $\Psi_b(X_i) = \phi(X_i) = b_i$. ■

With the previous notation, the element $\Psi_b(f)$ is usually denoted by $f(b)$:

$$f(b) = \Psi_b(f) = \sum_{k_1 \in \mathbb{N}_0} \cdots \sum_{k_n \in \mathbb{N}_0} a_{k_1,\dots,k_n} b_1^{k_1} \cdots b_n^{k_n}.$$

The homomorphism Ψ_b is called the *evaluation homomorphism* at b. The image of Ψ_b is denoted by $R[b_1, \dots, b_n]$:

$$R[b_1, \dots, b_n] = \{f(b_1, \dots, b_n) : f \in R[X_1, \dots, X_n]\}.$$

Corollary 2.42 *Let R be a commutative ring, B an R-algebra and $b = (b_1, \dots, b_n) \in B^n$. If B is commutative or $n = 1$, then for all $f, g \in R[X_1, \dots, X_n]$ and $c \in R$,*

$$(f + g)(b) = f(b) + g(b), \quad (fg)(b) = f(b)g(b), \quad (cf)(b) = cf(b).$$

Proof $(f+g)(b) = \Psi_b(f+g) = \Psi_b(f)+\Psi_b(g) = f(b)+g(b)$. The proofs of the other equalities are analogous. ■

Corollary 2.43 *Let R and B be commutative rings, $\phi : R \to B$ a homomorphism of rings and $b = (b_1, \dots, b_n) \in B^n$. There is a unique homomorphism of rings $\Psi_b : R[X_1, \dots, X_n] \to B$ such that, for all $i \in \{1, \dots, n\}$, $\Psi_b(X_i) = b_i$ and, for all $c \in R$, $\Psi_b(c) = \phi(c)$.*

Corollary 2.44 *Let R be a subring of a commutative ring B and $b = (b_1, \dots, b_n) \in B^n$.*

There is a unique homomorphism of rings $\Psi_b : R[X_1, \dots, X_n] \to B$ such that, for all $i \in \{1, \dots, n\}$, $\Psi_b(X_i) = b_i$ and, for all $c \in R$, $\Psi_b(c) = c$.

Subalgebra generated by $\{b_1, \dots, b_n\}$

Proposition 2.45 *Let B be an algebra over a commutative ring R. Let $b_1, \dots, b_n \in B$. Suppose that B is commutative or $n = 1$.*

(a) *$R[b_1, \dots, b_n]$ is the subalgebra of B generated by $\{b_1, \dots, b_n\}$.*

(b) *If R is a subring of B, $R[b_1, \dots, b_n]$ is also the subring of B generated by $R \cup \{b_1, \dots, b_n\}$.*

Proof (a) As $R[b_1, \dots, b_n]$ is the image of the evaluation homomorphism at b, $R[b_1, \dots, b_n]$ is a subalgebra of B. Clearly $\{b_1, \dots, b_n\} \subseteq R[b_1, \dots, b_n]$, and, if S is a subalgebra of B containing $\{b_1, \dots, b_n\}$, then $R[b_1, \dots, b_n] \subseteq S$. Hence $R[b_1, \dots, b_n]$ is the subalgebra of B generated by $\{b_1, \dots, b_n\}$. ■

Proposition 2.46 *Let B be a commutative algebra over a commutative ring R. A homomorphism of R-algebras $\phi : R[X_1, \dots, X_n] \to B$ is surjective if and only if $R[\phi(X_1), \dots, \phi(X_n)] = B$.*

Polynomial functions

Let B be an algebra over a commutative ring R. Let $F(B^n, B)$ be the R-algebra in example 2.26.4., with $X = B^n$. Suppose that B is commutative or $n = 1$. For each polynomial $f \in R[X_1, \dots, X_n]$, the map

$$\Phi_f : B^n \to B, \quad b \mapsto f(b),$$

is called the *polynomial function* associated with f and defined in B^n.

Proposition 2.47 *With the previous notation,*

$$\Phi : R[X_1, \dots, X_n] \to F(B^n, B), \quad f \mapsto \Phi_f,$$

is a homomorphism of R-algebras.

Algebraic independence

Let B be a commutative algebra over a commutative ring R. The elements $b_1, \dots, b_n \in B$ are said to be *algebraically independent* over R fi, for all $f \in R[X_1, \dots, X_n]$,

$$f(b_1, \dots, b_n) = 0 \;\Rightarrow\; f = 0.$$

The elements $X_1, \dots, X_n$ of $R[X_1, \dots, X_n]$ are algebraically independent over R.

Remark 2.48 Let B be a commutative algebra over a commutative ring R. The elements $b_1, \dots, b_n \in B$ are algebraically independent if and only if the elements of the family $(b_1^{k_1} \cdots b_n^{k_n})_{k_1,\dots,k_n \in \mathbb{N}_0}$ are distinct and the set $\{b_1^{k_1} \cdots b_n^{k_n} : k_1, \dots, k_n \in \mathbb{N}_0\}$ is linearly independent.

Proposition 2.49 *Let B be a commutative algebra over a commutative ring R. A homomorphism of R-algebras $\phi : R[X_1, \ldots, X_n] \to B$ is injective if and only if $\phi(X_1), \ldots, \phi(X_n)$ are algebraically independent over R.*

Proof Suppose that ϕ is injective. Let $f \in R[X_1, \ldots, X_n]$ and suppose that $f(\phi(X_1), \ldots, \phi(X_n)) = 0$. As ϕ is a homomorphism of algebras,

$$\phi(f) = f(\phi(X_1), \ldots, \phi(X_n)) = 0.$$

As ϕ is injective, $f = 0$. Hence $\phi(X_1), \ldots, \phi(X_n)$ are algebraically independent.

Conversely, suppose that $\phi(X_1), \ldots, \phi(X_n)$ are algebraically independent. Let $f \in R[X_1, \ldots, X_n]$ and suppose that $\phi(f) = 0$. As ϕ is a homomorphism of algebras,

$$f(\phi(X_1), \ldots, \phi(X_n)) = \phi(f) = 0.$$

As $\phi(X_1), \ldots, \phi(X_n)$ are algebraically independent, $f = 0$. Hence $\ker \phi = 0$ and ϕ is injective. ■

The isomorphism $R[X_1, \ldots, X_n] \cong (R[X_1, \ldots, X_p])[X_{p+1}, \ldots, X_n]$

Let R be a commutative ring.

Recall that $B = (R[X_1, \ldots, X_p])[X_{p+1}, \ldots, X_n]$ is an $R[X_1, \ldots, X_p]$-algebra and $X_{p+1}, \ldots, X_n$ are algebraically independent over $R[X_1, \ldots, X_p]$. As R is a subring of $R[X_1, \ldots, X_p]$, by restricting the scalar multiplication to $R \times B$, B becomes an R-algebra.

Proposition 2.50 *Let R be a commutative ring. There is a unique isomorphism of R-algebras*

$$\phi : R[X_1, \ldots, X_n] \to (R[X_1, \ldots, X_p])[X_{p+1}, \ldots, X_n]$$

such that, for all $i \in \{1, \ldots, n\}$, $\phi(X_i) = X_i$. Moreover, for each

$$f = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} \in R[X_1, \ldots, X_n],$$

$$\phi(f) = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} \in (R[X_1, \ldots, X_p])[X_{p+1}, \ldots, X_n].$$

In particular, for each $c \in R$, $\phi(c) = c$.

Proof Let $B = (R[X_1, \ldots, X_p])[X_{p+1}, \ldots, X_n]$. By Proposition 2.41, there is a unique isomorphism of R-algebras $\phi : R[X_1, \ldots, X_n] \to B$ such that, for all $i \in \{1, \ldots, n\}$, $\phi(X_i) = X_i$.

Let us see that $\phi(X_1), \ldots, \phi(X_n) \in B$ are algebraically independent over R. Let

$$f = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} \in R[X_1, \ldots, X_n]$$

and suppose that

$$0_B = f(\phi(X_1), \ldots, \phi(X_n)) = f(X_1, \ldots, X_n) = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}.$$

Then

$$0_B = \sum_{k_{p+1}} \cdots \sum_{k_n} \left(\sum_{k_1} \cdots \sum_{k_p} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_p^{k_p} \right) X_{p+1}^{k_{p+1}} \cdots X_n^{k_n}.$$

As $X_{p+1}, \ldots, X_n$ are algebraically independent over $R[X_1, \ldots, X_p]$, for all $k_{p+1}, \ldots, k_n \in \mathbb{N}_0$,

$$0_{R[X_1,\ldots,X_p]} = \sum_{k_1} \cdots \sum_{k_p} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_p^{k_p}.$$

As $X_1, \ldots, X_p$ are algebraically independent over R, for all $k_1, \ldots, k_n \in \mathbb{N}_0$, $0_R = a_{k_1,\ldots,k_n}$. Hence $f = 0$ and $\phi(X_1), \ldots, \phi(X_n)$ are algebraically independent over R. By Proposition 2.49, the homomorphism ϕ is injective.

Let

$$b = \sum_{k_{p+1}} \cdots \sum_{k_n} f_{k_{p+1},\ldots,k_n} X_{p+1}^{k_{p+1}} \cdots X_n^{k_n} \in B,$$

where

$$f_{k_{p+1},\ldots,k_n} = \sum_{k_1} \cdots \sum_{k_p} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_p^{k_p} \in R[X_1, \ldots, X_p]$$

and, for all $k_1, \ldots, k_n \in \mathbb{N}_0$, $a_{k_1,\ldots,k_n} \in R$. By replacing and using the properties of the operations in B,

$$b = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} = \sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} \phi(X_1)^{k_1} \cdots \phi(X_n)^{k_n}$$
$$= \phi\left(\sum_{k_1} \cdots \sum_{k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} \right) \in \operatorname{im} \phi,$$

which shows that ϕ é surjective. ■

Corollary 2.51 *If R is a unique factorization domain, then $R[X_1, \ldots, X_n]$ is also a unique factorization domain.*

Proof By induction on n. This result is Proposition 0.71 when $n = 1$. Suppose that $n \geq 2$. By the induction assumption, $R[X_1, \ldots, X_{n-1}]$ is a unique factorization domain. By Proposition 0.71, $R[X_1, \ldots, X_{n-1}][X_n]$ is a unique factorization domain. As $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$, $R[X_1, \ldots, X_n]$ is also a unique factorization domain. ■

Exercises

2.5.1 Let R be a commutative ring and $f = a_nX^n + \cdots + a_0 \in R[X] \setminus 0$. Prove that, if there is $g \in R[X] \setminus 0$ such that $fg = 0$, then there is $b \in R \setminus 0$ such that $a_nb = \cdots = a_0b = 0$.

2.6 Hilbert basis theorem

A module M is said to be *Noetherian* (or M is said to satisfy the *ascending chain condition*) if, for each chain of submodules of M,

$$M_1 \subseteq \cdots \subseteq M_n \subseteq \cdots , \tag{2.19}$$

there is $p \in \mathbb{N}$ such that, for all $n \geq p$, $M_p = M_n$. It is said that a chain (2.19) is *stationary* if there is $p \in \mathbb{N}$ such that, for all $n \geq p$, $M_p = M_n$.

Proposition 2.52 *A module M is Noetherian if and only if all submodules of M are finitely generated.*

Proof. Suppose that all submodules of M are finitely generated. Let

$$M_1 \subseteq \cdots \subseteq M_n \subseteq \cdots ,$$

be a chain of submodules of M. Then $N = \bigcup_{n\geq 1} M_n$ is a submodule of M. Suppose that N is generated by $\{x_1, \ldots , x_r\}$. For each $i \in \{1, \ldots , r\}$, choose $p_i \in \mathbb{N}$ so that $x_i \in M_{p_i}$. Let $p = \max\{p_1, \ldots , p_r\}$. Then $x_1, \ldots , x_r \in M_p$. Thus, for each $n \geq p$, $N \subseteq M_p \subseteq M_n \subseteq N$ and $M_p = M_n$. Therefore M is Noetherian.

Conversely suppose that there is a submodule N of M that is not finitely generated. Recursively define a sequence of elements of N, $x_1, \ldots , x_n, \ldots$, as follows. Choose $x_1 \in N$. Let $n \geq 2$. As N is not finitely generated, $N \neq R\{x_1, \ldots , x_{n-1}\}$. Choose $x_n \in N \setminus R\{x_1, \ldots , x_{n-1}\}$.

For each $n \geq 1$, let $M_n = R\{x_1, \ldots , x_n\}$. Taking into account how the sequence $x_1, \ldots , x_n, \ldots$ has been chosen, $M_1 \subsetneqq \cdots \subsetneqq M_n \subsetneqq \cdots$, which implies that M is not Noetherian. ■

A ring R is said to be *left Noetherian* if the left regular module ${}_RR$ is Noetherian, that is, if, for each chain of left ideals of R,

$$\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots ,$$

there is $p \in \mathbb{N}$ such that, for all $n \geq p$, $\mathfrak{a}_p = \mathfrak{a}_n$. Right Noetherian rings are defined analogously. A ring is said to be *Noetherian* if it is left Noetherian and right Noetherian. For commutative rings, all three concepts coincide.

If D is a division ring, then 0 and D are the unique left ideals and the unique right ideals of D. Therefore D is Noetherian.

By Lemma 0.61, principal ideal domains are Noetherian.

Proposition 2.53 *If R is a Noetherian commutative ring, then the ring $R[X]$ is also Noetherian.*

Proof. Suppose that R is a Noetherian commutative ring. Let B be an ideal of $R[X]$, in order to prove that B is finitely generated. As the case $B = 0$ is trivial, suppose that $B \neq 0$.

Let $n \in \mathbb{N}_0$. Let $\mathfrak{b}_n$ be the subset of R whose elements are 0 and all first coefficients of polynomials of degree n that belong to B. For each $b \in \mathfrak{b}_n \setminus 0$, let $p_{n,b}$ be a polynomial of degree n that belongs to B and whose first coefficient is b.

Let us prove that $\mathfrak{b}_n$ is an ideal of R. By definition of $\mathfrak{b}_n$, $0 \in \mathfrak{b}_n$. Let $b, c \in \mathfrak{b}_n$. If $b = 0$ or $c = 0$ or $b - c = 0$, it is trivial that $b - c \in \mathfrak{b}_n$. Suppose that $b \neq 0$, $c \neq 0$ and $b - c \neq 0$. Then $p_{n,b} - p_{n,c}$ is a polynomial of degree n that belongs to B and whose first coefficient is $b - c$. Thus $b - c \in \mathfrak{b}_n$. Let $a \in R$ and $b \in \mathfrak{b}_n$. If $ab = 0$, then $ab \in \mathfrak{b}_n$. Suppose that $ab \neq 0$. Then $ap_{n,b}$ is a polynomial of degree n that belongs to B and whose first coefficient is ab. Thus $ab \in \mathfrak{b}_n$. Therefore $\mathfrak{b}_n$ is an ideal of R.

Let $b \in \mathfrak{b}_n \setminus 0$. Then $Xp_{n,b}$ is a polynomial of degree $n + 1$ that belongs to B and whose first coefficient is b. Thus $b \in \mathfrak{b}_{n+1}$. Therefore $\mathfrak{b}_n \subseteq \mathfrak{b}_{n+1}$.

As R is Noetherian, there is $k \in \mathbb{N}_0$ such that, for all $n \geq k$, $\mathfrak{b}_k = \mathfrak{b}_n$. As R is Noetherian, for each $n \leq k$, the ideal $\mathfrak{b}_n$ is generated by a finite set C_n. Let

$$Z = \{p_{n,b} : n \leq k \text{ e } b \in C_n \setminus 0\}.$$

The set Z is finite. Let us prove that Z generates the ideal B. Let $B' = R[X]Z$ be the ideal of $R[X]$ generated by Z. As $Z \subseteq B$, $B' \subseteq B$. Let $f \in B \setminus 0$. Let us prove, by induction on $d(f)$, that $f \in B'$.

Suppose that $d(f) = 0$. Then $f \in \mathfrak{b}_0$ and there are $a_1, \ldots, a_r \in R$, $b_1, \ldots, b_r \in C_0 \setminus 0$ such that

$$f = a_1 b_1 + \cdots + a_r b_r = a_1 p_{0,b_1} + \cdots + a_r p_{0,b_r} \in B'.$$

Now suppose that $1 \leq d(f) = n \leq k$. Let c be the first coefficient of f. Then $c \in \mathfrak{b}_n$ and, therefore, there are $a_1, \ldots, a_r \in R$, $b_1, \ldots, b_r \in C_n \setminus 0$ such that $c = a_1 b_1 + \cdots + a_r b_r$. Then $g = f - a_1 p_{n,b_1} - \cdots - a_r p_{n,b_r}$ is a polynomial of degree less than n. As $f, p_{n,b_1}, \ldots, p_{n,b_r} \in B$, $g \in B$. By the induction assumption, $g \in B'$. As $p_{n,b_1}, \ldots, p_{n,b_r} \in Z \subseteq B'$, $f = g + a_1 p_{n,b_1} + \cdots + a_r p_{n,b_r} \in B'$.

Finally suppose that $d(f) = n > k$. Let c be the first coefficient of f. Then $c \in \mathfrak{b}_n = \mathfrak{b}_k$ and, therefore, there are $a_1, \ldots, a_r \in R$, $b_1, \ldots, b_r \in C_k \setminus 0$ suh that $c = a_1 b_1 + \cdots + a_r b_r$. Then $g = f - a_1 X^{n-k} p_{k,b_1} - \cdots - a_r X^{n-k} p_{k,b_r}$ is a polynomial of degree less than n. As $f, p_{k,b_1}, \ldots, p_{k,b_r} \in B$, $g \in B$. By the induction assumption, $g \in B'$. As $p_{k,b_1}, \ldots, p_{k,b_r} \in Z \subseteq B'$, $f = g + a_1 X^{n-k} p_{k,b_1} + \cdots + a_r X^{n-k} p_{k,b_r} \in B'$.

Then $B = B'$ and, therefore, the ideal B is finitely generated. Consequently the ring $R[X]$ is Noetherian. ■

Theorem 2.54 [Hilbert basis theorem] *If R is a Noetherian commutative ring, then the ring $R[X_1, \dots, X_n]$ is also Noetherian.*

Proof. By induction on n. The case $n = 1$ has already been studied in the previous proposition. Suppose that $n \geq 2$. By the induction assumption, the ring $R[X_1, \dots, X_{n-1}]$ is Noetherian. By the previous proposition, the ring $(R[X_1, \dots, X_{n-1}])[X_n]$ is Noetherian. As the rings $R[X_1, \dots, X_n]$ and $(R[X_1, \dots, X_{n-1}])[X_n]$ are isomorphic, $R[X_1, \dots, X_n]$ is Noetherian. ■

Exercises

2.6.1 Prove that a vector space over a field is Noetherian if and only if it is finitely generated.

2.6.2 [Converse of Hilbert basis theorem] Let R be a commutative ring. Prove that, if the ring $R[X_1, \dots, X_n]$ is Noetherian, then the ring R is also Noetherian.

2.7 Algebraic varieties

Throughout this section, K is a field.

A point $b = (b_1, \dots, b_n)$ of the space K^n is said to be a *zero* (or a *root*) of a polynomial $f \in K[X_1, \dots, X_n]$ if $f(b) = f(b_1, \dots, b_n) = 0$.

For each $G \subseteq K[X_1, \dots, X_n]$, let

$$V(G) = \{b \in K^n : \forall f \in G,\ f(b) = 0\},$$

that is, $V(G)$ is the set of zeros common to all polynomials belonging to G. A set of the form $V(G)$ is called the *affine algebraic variety* or, simply, the *variety* in the space K^n defined by G ([6]).

Examples 2.55 Let K be a field.

1. $\emptyset$ is the variety in K^n defined by $\{1\}$ and also by $K[X_1, \dots, X_n]$.
2. If $b = (b_1, \dots, b_n) \in K^n$, then $\{b\}$ is the variety in K^n defined by $\{X_1 - b_1, \dots, X_n - b_n\}$.
3. K^n is the variety in K^n defined by $\{0\}$ and also by $\emptyset$.
4. The set of solutions of a system of linear equations, in n variables, with coefficients in K, is a variety in K^n defined by a set of polynomials of degree ≤ 1. Usually, these varieties are called affine subspaces of K^n.
5. In $\mathbb{R}^2$, the circle with center in $(0, 0)$ and radius 1 is the variety in $\mathbb{R}^2$ defined by the set $\{X_1^2 + X_2^2 - 1\}$.

[6] Algebraic varieties are the central objects of study in Algebraic Geometry. In some publications, the sets $V(G)$ are called *algebraic sets*.

Proposition 2.56 *Let K be a field. For each $S \subseteq K^n$,*

$$I(S) = \{f \in K[X_1, \ldots, X_n] : \forall b \in S,\ f(b) = 0\}.$$

is an ideal of the ring $K[X_1, \ldots, X_n]$.

The ideal $I(S)$ is said to be the ideal of the set S.

Proof. Clearly $0 \in I(S)$. Let $f, g \in I(S)$ and $h \in K[X_1, \ldots, X_n]$. For all $b \in S$, $f(b) = g(b) = 0$. Then $(f - g)(b) = f(b) - g(b) = 0$ and $(hf)(b) = h(b)f(b) = 0$. Then $f - g, hf \in I(S)$. Therefore $I(S)$ is an ideal of $K[X_1, \ldots, X_n]$. ■

Proposition 2.57 *Let K be a field, $G, H \subseteq K[X_1, \ldots, X_n]$, $S, T \subseteq K^n$.*

(a) *$G \subseteq IV(G)$.*

(b) *$S \subseteq VI(S)$.*

(c) *If $G \subseteq H$, then $V(H) \subseteq V(G)$.*

(d) *If $S \subseteq T$, then $I(T) \subseteq I(S)$.*

(e) *$V(G) = VIV(G)$. Thus a variety is always defined by an ideal.*

(f) *$I(S) = IVI(S)$.*

(g) *Let $\mathcal{V}$ be the set of all varieties of K^n. Let $\mathcal{S}$ the set of all ideals of $K[X_1, \ldots, X_n]$ of the form $I(V)$, with $V \in \mathcal{V}$. The maps*

$$V : \mathcal{S} \to \mathcal{V} \quad \text{and} \quad I : \mathcal{V} \to \mathcal{S}$$

are invertible and one is the inverse of the other.

(h) *If $V(H) \subsetneqq V(G)$, then $IV(G) \subsetneqq IV(H)$.*

(i) *If $I(S) \subsetneqq I(T)$, then $VI(T) \subsetneqq VI(S)$.*

Proof. (a) Let $f \in G$. By the definition of $V(G)$, for all $b \in V(G)$, $f(b) = 0$. By the definition of $IV(G)$, $f \in IV(G)$. Hence $G \subseteq IV(G)$.

(c) Suppose that $G \subseteq H$. Let $b \in V(H)$. For all $f \in H$, $f(b) = 0$. As $G \subseteq H$, for all $f \in G$, $f(b) = 0$. Then $b \in V(G)$. Hence $V(H) \subseteq V(G)$.

(e) By (b), $V(G) \subseteq VIV(G)$. By (a), $G \subseteq IV(G)$. By (c), $VIV(G) \subseteq V(G)$. Hence $V(G) = VIV(G)$. ■

Corollary 2.58 *Let K be a field. Let $G \subseteq R = K[X_1, \ldots, X_n]$ and let*

$$RG = \{f_1 g_1 + \cdots + f_p g_p : p \in \mathbb{N}, f_1, \ldots, f_p \in R, g_1, \ldots, g_p \in G\},$$

the ideal of $K[X_1, \ldots, X_n]$ generated by G. Then $V(RG) = V(G)$.

Proof. As $G \subseteq IV(G)$, $G \subseteq RG \subseteq IV(G)$. By Proposition 2.57, $V(G) = V(IV(G)) \subseteq V(RG) \subseteq V(G)$. ■

Proposition 2.59 *Let K be a field. For each variety V in K^n, there is a finite subset F of $K[X_1, \ldots, X_n]$ such that $V = V(F)$.*

Proof. Let V be a variety and let G be a subset of $R = K[X_1, \ldots, X_n]$ such that $V = V(G)$. By the Hilbert basis theorem, there is a finite set $F \subseteq K[X_1, \ldots, X_n]$ that generates the ideal RG. By Corollary 2.58, $V(G) = V(RG) = V(RF) = V(F)$. ■

Proposition 2.60 *Let K be a field. Let $(V_i)_{i \in I}$ be a non-empty family of varieties in K^n. Suppose that, for each $i \in I$, $V_i = V(G_i)$, where $G_i \subseteq K[X_1, \ldots, X_n]$. Then*

$$\bigcap_{i \in I} V_i = V\left(\bigcup_{i \in I} G_i\right).$$

Proof. Let $b \in \bigcap_{i \in I} V_i$. For all $i \in I$, $b \in V_i = V(G_i)$. Then, for all $i \in I$ and $f \in G_i$, $f(b) = 0$. Then, for all $f \in \bigcup_{i \in I} G_i$, $f(b) = 0$. Then $b \in V(\bigcup_{i \in I} G_i)$. Hence $\bigcap_{i \in I} V_i \subseteq V(\bigcup_{i \in I} G_i)$.

Let $j \in I$. As $G_j \subseteq \bigcup_{i \in I} G_i$, $V(\bigcup_{i \in I} G_i) \subseteq V(G_j) = V_j$. Therefore $V(\bigcup_{i \in I} G_i) \subseteq \bigcap_{i \in I} V_i$. ■

Proposition 2.61 *Let $V_1, \ldots, V_p$ be varieties in K^n. Suppose that, for each $i \in \{1, \ldots, p\}$, $V_i = V(G_i)$, where $G_i \subseteq K[X_1, \ldots, X_n]$. Let*

$$G = \{f_1 \cdots f_p : f_1 \in G_1, \ldots, f_p \in G_p\}.$$

Then $V_1 \cup \cdots \cup V_p = V(G)$.

Proof. Let $b \in V_1 \cup \cdots \cup V_p$. There is $i \in \{1, \ldots, p\}$ such that $b \in V_i = V(G_i)$. Then, for all $f_i \in G_i$, $f_i(b) = 0$. Let $f_1 \cdots f_p$ be an element of G, where $f_1 \in G_1, \ldots, f_p \in G_p$. Then $(f_1 \cdots f_p)(b) = f_1(b) \cdots f_p(b) = 0$, which shows that $b \in V(G)$. Therefore $V_1 \cup \cdots \cup V_p \subseteq V(G)$.

Conversely, let $b \in V(G)$. If $b \in V_1 \cup \cdots \cup V_{p-1}$, then $b \in V_1 \cup \cdots \cup V_p$. Now suppose that $b \notin V_1 \cup \cdots \cup V_{p-1}$. Then, for all $i \in \{1, \ldots, p-1\}$, $b \notin V_i = V(G_i)$ and there is $f_i \in G_i$ such that $f_i(b) \neq 0$. Let $f_p \in G_p$. As $b \in V(G)$, $0 = (f_1 \cdots f_{p-1} f_p)(b) = f_1(b) \cdots f_{p-1}(b) f_p(b)$. As $f_1(b), \ldots, f_{p-1}(b)$ are non-zero, $f_p(b) = 0$. Then $b \in V(G_p) = V_p \subseteq V_1 \cup \cdots \cup V_p$. Then $V(G) \subseteq V_1 \cup \cdots \cup V_p$. ■

Zariski topology

Let K be a field. We have seen, in Example 2.55, that $\emptyset$ and K^n are varieties. By Proposition 2.60, the intersection of a non-empty family of varieties is a variety. By Proposition 2.61, the finite union of varieties is a variety. Thus the varieties in K^n are the closed sets in a topology defined in K^n. This topology is called the *Zariski topology* in K^n.

Let τ and τ' topologies in a set X. It is said that τ is weaker that τ' if all closed sets in τ are closed sets in τ'.

Proposition 2.62 *Let K be a field. Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. In $\mathbb{F}^n$, the Zariski topology in weaker than the usual topology.*

Proof. Let V be a variety in $\mathbb{F}^n$, that is, a closed set in the Zariski topology. Suppose that $V = V(G)$, where $G \subseteq \mathbb{F}[X_1, \ldots, X_n]$.

Let $f \in G$. With the usual topologies in $\mathbb{F}^n$ and $\mathbb{F}$, the polynomial function

$$f : \mathbb{F}^n \to \mathbb{F}, \quad b \mapsto f(b), \ (^7)$$

is continuous. As $\{0\}$ is closed in $\mathbb{F}$ with the usual topology, $f^{-1}(\{0\})$ is closed in $\mathbb{F}^n$ with the usual topology. Then

$$V(G) = V\left(\bigcup_{f\in G}\{f\}\right) = \bigcap_{f\in G} V(\{f\}) = \bigcap_{f\in G} f^{-1}(\{0\})$$

is closed in $\mathbb{F}^n$ with the usual topology. ■

Chain conditions in topological spaces

Chain conditions are also used when studying other structures, in addition to modules and rings.

A topological space is said to be *Noetherian* if any ascending chain of open sets is stationary or, equivalently, if any descending chain of closed sets is stationary.

Proposition 2.63 *Let K be a field. The Zariski topology in K^n is Noetherian.*

Proof. Let $V_1 \supseteq V_2 \supseteq \cdots$ be a descending chain of varieties, that is, closed sets in the Zariski topology. For each $n \in \mathbb{N}$, suppose that $V_n = V(G_n)$, where $G_n \subseteq K[X_1, \ldots, X_n]$. Thus $V_n = V(G_n) = VIV(G_n) = VI(V_n)$. By the Hilbert basis theorem, $K[X_1, \ldots, X_n]$ is Noetherian. As $I(V_1) \subseteq I(V_2) \subseteq \cdots$, there is $p \in \mathbb{N}$ such that, for all $n \geq p$, $I(V_p) = I(V_n)$. Thus, for all $n \geq p$, $V_p = VI(V_p) = VI(V_n) = V_n$. ■

Lemma 2.64 *If T is a Noetherian topological space, then T is compact.*

Proof. Let T be a topological space that is not compact. Then there is a non-empty family of closed sets $(F_i)_{i\in I}$ such that $\bigcap_{i\in I} F_i = \emptyset$ and, for each finite subset I_0 of I, $\bigcap_{i\in I_0} F_i \neq \emptyset$.

Let $i_1 \in I$. As $F_{i_1} \neq \emptyset$ and $\bigcap_{i\in I} F_i = \emptyset$, there is $i_2 \in I$ such that $F_{i_1} \not\subseteq F_{i_2}$. Thus $F_{i_1} \supsetneqq F_{i_1} \cap F_{i_2}$. As $F_{i_1} \cap F_{i_2} \neq \emptyset$ and $\bigcap_{i\in I} F_i = \emptyset$, there is $i_3 \in I$ such that $F_{i_1} \cap F_{i_2} \not\subseteq F_{i_3}$ and $F_{i_1} \cap F_{i_2} \supsetneqq F_{i_1} \cap F_{i_2} \cap F_{i_3}$.

By repeating, we recursively define a descending chain of closed sets $F_{i_1} \supsetneqq F_{i_1} \cap F_{i_2} \supsetneqq F_{i_1} \cap F_{i_2} \cap F_{i_3} \supsetneqq \cdots$. Hence T is not Noetherian. ■

Corollary 2.65 *Let K be a field. The Zariski topology in K^n is compact.*

[7] To simplify, we use the same letter f to represent the polynomial and the polynomial function.

Chapter 3

Teoria de Galois

> “A major question in classical algebra was whether or not there were formulas for the solution of higher-degree polynomial equations (analogous to the quadratic formula for second-degree equations). Although formulas for third- and fourth-degree equations were found in the sixteenth century, no further progress was made for almost 300 years. Then Ruffini and Abel provided the surprising answer: There is no formula for the solution of *all* polynomial equations of degree n when $n \geq 5$. This result did not rule out the possibility that the solutions of special types of equations might be obtainable from a formula. Nor did it give any clue as to which equations might be solvable by formula.
>
> It was the amazingly original work of Galois that provided the full explanation, including a criterion for determining which polynomial equations can be solved by a formula. Galois’ ideas had a profound influence on the development of later mathematics, far beyond the scope of the original solvability problem.”
>
> **[Hungerford-2, p. 407]**

Este capítulo segue de perto [Hungerford-2].

3.1 Extensões de corpos

Sejam K um corpo e $F \subseteq K$. Diz-se que F é um *subcorpo* de K se F for um subanel de K e, qualquer que seja $x \in F \setminus 0$, $x^{-1} \in F \setminus 0$. Um subcorpo F de um corpo K é um corpo com as restrições das operações definidas em K a F. Se F for um *subcorpo* de K, também se diz que K é uma *extensão* do corpo F. Se K for uma extensão de um corpo F, chama-se *corpo intermédio* da extensão K de F a qualquer extensão E de F que é subcorpo de K : $F \subseteq E \subseteq K$.

Proposição 3.1 *Se $\sigma : K \to L$ for um homomorfismo de anéis, onde K e L são corpos, então, qualquer que seja $x \in K \setminus 0$, $\sigma(x^{-1}) = \sigma(x)^{-1}$.*

Demonstração. Qualquer que seja $x \in K \setminus 0$, $1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1})$. Logo $\sigma(x)$ é invertível e $\sigma(x^{-1})$ é o seu inverso. ∎

Se $\sigma : K \to L$ for um homomorfismo de anéis, onde K e L são corpos, diz-se que σ é um *homomorfismo de corpos.*

Proposição 3.2 *Se $(F_i)_{i\in I}$ for uma cadeia não vazia de subcorpos de um corpo K, então $\bigcup_{i\in I} F_i$ é um subcorpo de K.*

Proposição 3.3 *Se $(F_i)_{i\in I}$ for uma família não vazia de subcorpos de um corpo K, então $\bigcap_{i\in I} F_i$ é um subcorpo de K.*

Se X for um subconjunto de um corpo K, chama-se *subcorpo de K gerado por X* à intersecção de todos os subcorpos de K que contêm X. Assim, o subcorpo de K gerado por X é o menor subcorpo de K que contém X.

Se K for uma extensão de um corpo F e $u_1, \dots, u_n \in K$, representa-se por $F(u_1, \dots, u_n)$ o subcorpo de K gerado por $F \cup \{u_1, \dots, u_n\}$. Também se diz que $F(u_1, \dots, u_n)$ é a extensão de F gerada por $\{u_1, \dots, u_n\}$. Chama-se *extensão simples* de F a qualquer extensão da forma $F(u)$.

Sejam K e L extensões de um corpo F. Um homomorfismo de corpos $f : K \to L$ chama-se *homomorfismo de extensões* de F ou, mais simplesmente, *F-homomorfismo* se, para cada $a \in F$, $f(a) = a$.

Proposição 3.4 *Sejam K e L extensões de um corpo F. Uma aplicação $f : K \to L$ é um F-homomorfismo se e só se f for um homomorfismo de F-álgebras.*

Demonstração. Suponhamos que f é um F-homomorfismo. Quaisquer que sejam $a \in F$, $b \in K$, $f(ab) = f(a)f(b) = af(b)$. Logo f é um homomorfismo de F-álgebras.

Reciprocamente suponhamos que f é um homomorfismo de F-álgebras. Qualquer que seja $a \in F$, $f(a) = f(a1_K) = af(1_K) = a1_L = a$. Logo f é um F-homomorfismo. ■

Proposição 3.5 *Sejam K, L e M extensões de um corpo F.*

(a) id_K *é um F-automorfismo de K.*

(b) *Se $\sigma : K \to L$ e $\tau : L \to M$ forem F-homomorfismos, então $\tau\sigma : K \to M$ também é um F-homomorfismo.*

(c) *Se $\sigma : K \to L$ for um F-isomorfismo, então $\sigma^{-1} : L \to K$ também é um F-isomorfismo.*

(d) *O conjunto* $\mathrm{Gal}_F K$ *de todos os F-automorfismos de K é um grupo.*

Exercícios

3.1.1 Prove que $\mathbb{Q}(i + 5) = \mathbb{Q}(3 - i/2)$ e $\mathbb{C} = \mathbb{R}(e + \pi i)$.

3.1.2 Sejam K uma extensão de um corpo F e $u_1, \dots, u_p, \dots, u_n \in K$. Prove que $F(u_1, u_2) = F(u_1, u_1 + u_2)$ e $F(u_1, \dots, u_n) = F(u_1, \dots, u_p)(u_{p+1}, \dots, u_n)$.

3.1.3 Prove que $\{1, \sqrt{2}, \sqrt{3}\}$ é linearmente independente sobre $\mathbb{Q}$. (Sugestão: prove que $\{1, \sqrt{2}\}$ é linearmente independente sobre $\mathbb{Q}$ e $\sqrt{3}$ não é combinação linear de $\{1, \sqrt{2}\}$ com coeficientes em $\mathbb{Q}$.)

3.1.4 Sejam K uma extensão de $\mathbb{Q}$ e σ um automorfismo de K. Mostre que σ é um $\mathbb{Q}$-automorfismo de K.

3.2 Extensões algébricas e extensões finitas

Seja K uma extensão de um corpo F e seja $u \in K$. Diz-se que $u \in K$ é *algébrico* sobre F se u for raiz de algum polinómio $f \in F[X] \setminus 0$. Se u não for algébrico sobre F, diz-se que u é *transcendente* sobre F. Diz-se que K é uma *extensão algébrica* de F se todos os elementos de K forem algébricos sobre F.

Proposição 3.6 *Seja K uma extensão de um corpo F e seja E um corpo intermédio: $F \subseteq E \subseteq K$.*

(a) *Se $u \in K$ for algébrico sobre F, então u é algébrico sobre E.*

(b) *Se K for uma extensão algébrica de F, então K é uma extensão algébrica de E e E é uma extensão algébrica de F.*

Exemplos 3.7 1. Na extensão $\mathbb{C}$ de $\mathbb{R}$, i é algébrico sobre $\mathbb{R}$, pois é raiz do polinómio $X^2 + 1$.

2. $\sqrt[3]{2}$ é algébrico sobre $\mathbb{Q}$ pois é raiz do polinómio $X^3 - 2$.

3. Veremos mais adiante que e e π são transcendentes sobre $\mathbb{Q}$.

Se K for uma extensão de um corpo F, então K é um espaço vetorial sobre F com as operações que já estão definidas em K. Se K for finitamente gerado, como espaço vetorial sobre F, diz-se que K é uma *extensão finita* de F e a dimensão de K, como espaço vetorial sobre F, chama-se *grau* da extensão K de F e representa-se por $[K : F]$.

Exemplo 3.8 $\mathbb{C}$ é uma extensão finita do corpo $\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$ uma vez que $\{1, i\}$ é uma base de $\mathbb{C}$ como espaço vetorial real.

Exemplo 3.9 Seja K uma extensão finita de um corpo F, seja n a dimensão de K sobre F e seja $\{u_1, \ldots, u_n\}$ uma base de K sobre F. Claramente $F(u_1, \ldots, u_n) \subseteq K$. Reciprocamente, se $v \in K$, então v é combinação linear de $\{u_1, \ldots, u_n\}$ e, por isso, $v \in F(u_1, \ldots, u_n)$. Assim $K = F(u_1, \ldots, u_n)$.

Proposição 3.10 *Sejam K e L extensões finitas de um corpo F. Se $\sigma : K \to L$ for um F-isomorfismo, então $[K : F] = [L : F]$.*

Demonstração. Pela proposição 3.4, σ é um isomorfismo de espaços vetoriais sobre F. Logo $[K : F] = [L : F]$. ■

Proposição 3.11 *Sejam L uma extensão finita de um corpo K e K uma extensão finita de um corpo F. Então L é uma extensão finita de F e*

$$[L : F] = [L : K][K : F].$$

Demonstração. Sejam $m = [L : K]$ e $n = [K : F]$. Seja $\{u_1, \ldots, u_m\}$ uma base de L sobre K e seja $\{v_1, \ldots, v_n\}$ uma base de K sobre F.

Suponhamos que

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} u_i v_j, \quad \text{onde} \quad a_{i,j} \in F.$$

Então

$$0 = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{i,j} v_j \right) u_i, \quad \text{onde} \quad \sum_{j=1}^{n} a_{i,j} v_j \in K.$$

Como $u_1, \dots, u_m$ são linearmente independentes sobre K,

$$0 = \sum_{j=1}^{n} a_{i,j} v_j, \quad i \in \{1, \dots, m\}.$$

Como $v_1, \dots, v_n$ são linearmente independentes sobre F,

$$0 = a_{i,j}, \quad i \in \{1, \dots, m\},\ j \in \{1, \dots, n\}.$$

Este argumento implica que os elementos $u_i v_j$ são todos distintos e são linearmente independentes. Seja $w \in L$. Como $u_1, \dots, u_m$ geram L sobre K,

$$w = \sum_{i=1}^{m} b_i u_i, \quad \text{para alguns } b_i \in K.$$

Como $v_1, \dots, v_n$ geram K sobre F,

$$b_i = \sum_{j=1}^{n} a_{i,j} v_j, \quad \text{para alguns } a_{i,j} \in F.$$

Assim,

$$w = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{i,j} v_j \right) u_i = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} u_i v_j.$$

Portanto o conjunto

$$\{u_i v_j : i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\} \tag{3.1}$$

gera L sobre F. Logo (3.1) é uma base de L sobre F com cardinal mn, o que completa a demonstração. ■

Proposição 3.12 *Se K for uma extensão finita de um corpo F, então K é uma extensão algébrica de F.*

Demonstração. Seja $n = [K : F]$, a dimensão de K sobre F. Seja $u \in K$. Vejamos que u é algébrico sobre F.

Caso 1. Suponhamos que existem $i, j \in \mathbb{N}$ tais que $i \neq j$ e $u^i = u^j$. Então u é raiz do polinómio não nulo $X^i - X^j$ e, portanto, u é algébrico sobre F.

Caso 2. Suponhamos que todas as potências u^i, com $i \in \mathbb{N}$, são distintas. Então $u, u^2, \ldots, u^{n+1}$ são $n+1$ elementos distintos do espaço vetorial K, o qual tem dimensão n. Assim $u, u^2, \ldots, u^{n+1}$ são linearmente dependentes e existem escalares $a_1, \ldots, a_{n+1} \in F$, não todos nulos, tais que $a_1u + a_2u^2 + \cdots + a_{n+1}u^{n+1} = 0$. Portanto u é raiz do polinómio não nulo $a_1X + a_2X^2 + \cdots + a_{n+1}X^{n+1}$ e u é algébrico sobre F.

Em qualquer caso, u é algébrico sobre F. Logo K é uma extensão algébrica de F. ■

Polinómios mínimos

Seja F um corpo. Recordemos que o anel de polinómios $F[X]$ é um domínio de ideais principais. Se I for um ideal de $F[X]$ e $g \in F[X]$ gerar I, então $f \in F[X]$ gera I se e só se f e g forem associados em $F[X]$. Assim um ideal não nulo I de $F[X]$ tem um único gerador mónico.

Proposição 3.13 *Seja K uma extensão de um corpo F e seja $u \in K$.*

(a) *O conjunto I de todos os polinómios $f \in F[X]$ tais que $f(u) = 0$ é um ideal de $F[X]$.*

(b) *u é algébrico sobre F se e só se $I \neq 0$.*

(c) *Se u for algébrico sobre F e $g \in I$, então g gera o ideal I se e só se g for irredutível em $F[X]$.*

Demonstração. (a) é um exercício fácil e (b) resulta imediatamente das definições.

(c) Como u é algébrico sobre F, $I \neq 0$. Note-se que $g \notin U(F[X])$ porque as unidades não têm raízes.

($\Rightarrow$) Suponhamos que g gera I. Como $I \neq 0$, $g \neq 0$. Com vista a uma contradição, suponhamos que g é redutível. Então $g = g_1g_2$, onde $g_1, g_2 \notin U(F[X])$. Então $0 = g(u) = g_1(u)g_2(u)$. Como K é um corpo, $g_1(u) = 0$ ou $g_2(u) = 0$. Suponhamos que $g_1(u) = 0$. (O outro caso é análogo.) Então $g_1 \in I$ e $g \mid g_1$. Como $g = g_1g_2$, $g_1 \mid g$. Logo g e g_1 são associados e $g_2 \in U(F[X])$, o que é absurdo. Logo g é irredutível.

($\Leftarrow$) Suponhamos que g é irredutível. Seja h um gerador de I. Então $h \mid g$. Como as unidades não têm raízes, h não é uma unidade. Como g é irredutível, g e h são associados. Como h gera I, g também gera I. ■

Seja K uma extensão de um corpo F e seja $u \in K$ algébrico sobre F. O único gerador mónico do ideal

$$I = \{f \in F[X] : f(u) = 0\}$$

chama-se *polinómio mínimo* de u sobre F. Note-se que o polinómio mínimo de u sobre F também é o único polinómio mónico de grau mínimo que pertence a I. Da proposição anterior também resulta que o polinómio mínimo de u sobre F é o único polinómio mónico e irredutível que pertence a I.

Exemplo 3.14 Seja $u = \sqrt{3} + \sqrt{5} \in \mathbb{R}$. Então $u^2 = 3 + 2\sqrt{3}\sqrt{5} + 5 = 8 + 2\sqrt{15}$. Donde $u^2 - 8 = 2\sqrt{15}$ e $(u^2 - 8)^2 = 60$. Portanto $u = \sqrt{3} + \sqrt{5}$ é raiz do polinómio

$$(X^2 - 8)^2 - 60 = X^4 - 16X^2 + 4 \in \mathbb{Q}[X].$$

Verifique que este polinómio é irredutível sobre $\mathbb{Q}$. Logo este é o polinómio mínimo de u sobre $\mathbb{Q}$.

Exemplo 3.15 Os reais $\sqrt{3}$ e $\sqrt{5}$ não são racionais, mas são algébricos sobre $\mathbb{Q}$. Assim $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ é uma extensão finita de $\mathbb{Q}$. Podemos calcular a dimensão de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$, considerando a cadeia de extensões simples:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3})(\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5}).$$

Como $\sqrt{3}$ é raiz de $X^2 - 3 \in \mathbb{Z}[X]$ e este polinómio é irredutível em $\mathbb{Q}[X]$ pelo critério de Eisenstein, $X^2 - 3$ é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$. Assim $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ e $\{1, \sqrt{3}\}$ é base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$.

Por outro lado, o polinómio $X^2 - 5 \in \mathbb{Q}(\sqrt{3})[X]$ tem duas raízes em $\mathbb{C}$: $\sqrt{5}$ e $-\sqrt{5}$. Seja $u \in \{\sqrt{5}, -\sqrt{5}\}$ e suponhamos, com vista a uma contradição, que $u \in \mathbb{Q}(\sqrt{3})$. Então $u = a + b\sqrt{3}$, onde $a, b \in \mathbb{Q}$. Donde $5 = u^2 = a^2 + 3b^2 + 2ab\sqrt{3}$. Se $ab \neq 0$, $\sqrt{3} = (5 - a^2 - 3b^2)/2ab \in \mathbb{Q}$, o que é absurdo. Também é fácil mostrar que é impossível ter $a = 0$ ou $b = 0$. Assim $X^2 - 5$ não tem raízes em $\mathbb{Q}(\sqrt{3})$ e, portanto, $X^2 - 5$ é irredutível em $\mathbb{Q}(\sqrt{3})[X]$. Logo $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$.

Logo $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$.

Pela proposição 0.55 e pelo corolário 0.53, se F for um corpo e $f \in F[X]$, então f é irredutível se e só se $F[X]f$ for um ideal maximal de $F[X]$ se e só se $F[X]/F[X]f$ for um corpo.

Proposição 3.16 *Seja K uma extensão de um corpo F e $u \in K$ um elemento algébrico sobre F com polinómio mínimo $p \in F[X]$ de grau n.*

(a) *$F(u) = F[u]$.*

(b) *$[F(u) : F] = n$ e $B = \{1, u, \ldots, u^{n-1}\}$ é uma base do espaço vetorial $F(u)$ sobre F.*

(c) *$F[X]/F[X]p$ é um corpo e a aplicação*

$$\psi : \frac{F[X]}{F[X]p} \to F(u), \quad f + F[X]p \mapsto f(u), \tag{3.2}$$

está bem definida e é um isomorfismo de corpos.

Demonstração. Vejamos que

$$F[u] = \{r(u) : r \in F[X] \text{ e } d(r) < n\}. \tag{3.3}$$

Seja $w \in F[u]$. Então $w = f(u)$, com $f \in F[X]$. Dividindo f por p, $f = pq + r$, onde $q, r \in F[X]$ e $d(r) < n = d(p)$. Então $f(u) = p(u)q(u) + r(u) = r(u)$, o que prova uma das inclusões de (3.3). A outra inclusão é trivial.

(a) Como $F \cup \{u\} \subseteq F[u] \subseteq F(u)$ e $F(u)$ é o menor subcorpo de K que contém $F \cup \{u\}$, basta provar que o anel $F[u]$ é um subcorpo de K. Seja $r(u)$ um elemento não nulo de $F[u]$, onde $r \in F[X] \setminus 0$ e $d(r) < n = d(p)$. Como $r \neq 0$ e p é irredutível, deduzimos que r e p são relativamente primos. Assim existem $s, t \in F[X]$ tais que $1 = rs + pt$. Donde $1 = r(u)s(u) + p(u)t(u) = r(u)s(u)$ e, portanto, $r(u)$ é invertível. Logo $F[u]$ é um subcorpo de K.

(b) De (3.3), deduzimos que B gera o espaço vetorial $F[u] = F(u)$ sobre F. Suponhamos agora que

$$0 = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}, \quad \text{onde } a_i \in F.$$

Então

$$0 = r(u), \quad \text{onde} \quad r = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \in F[X].$$

Como u é raiz de r e r tem grau inferior ao grau de p que é o polinómio mínimo de u, deduzimos que $r = 0$. Portanto $0 = a_0 = \cdots = a_{n-1}$. Logo os elementos $1, u, \ldots, u^{n-1}$ são todos distintos e B é linearmente independente, o que conclui a demonstração de (b).

(c) Como p é irredutível, $F[X]/F[X]p$ é um corpo. A aplicação $\phi : F[X] \to F[u] = F(u)$, $f \mapsto f(u)$, é um epimorfismo de anéis e

$$\ker \phi = \{f \in F[X] : f(u) = 0\} = F[X]p.$$

Pelo primeiro teorema de isomorfismo, proposição 0.40, (3.2) é um isomorfismo de anéis e, portanto, de corpos. ■

Exemplo 3.17 Vimos no exemplo 3.14 que $X^4 - 16X^2 + 4$ é o polinómio mínimo de $\sqrt{3} + \sqrt{5}$ sobre $\mathbb{Q}$. Assim

$$\{1, \sqrt{3} + \sqrt{5}, (\sqrt{3} + \sqrt{5})^2, (\sqrt{3} + \sqrt{5})^3\}$$

é uma base do espaço $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ sobre $\mathbb{Q}$ e $[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}] = 4$.

Proposição 3.18 *Seja K uma extensão de um corpo F. Se $u_1, \ldots, u_n \in K$ forem elementos algébricos sobre F, então $K = F(u_1, \ldots, u_n)$ é uma extensão finita e algébrica de F.*

Demonstração. Consideremos a cadeia de corpos

$$F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n = K,$$

onde, para cada $i \in \{1, \ldots, n\}$, $E_i = F(u_1, \ldots, u_i) = E_{i-1}(u_i)$. Como u_i é algébrico sobre F, u_i também é algébrico sobre E_{i-1}. Pela proposição 3.16, $[E_i : E_{i-1}] = [E_{i-1}(u_i) : E_{i-1}]$ é finito. Aplicando repetidamente a proposição 3.11, deduzimos que K é uma extensão finita de F e

$$[K : F] = [E_n : E_{n-1}][E_{n-1} : E_{n-2}] \cdots [E_1 : E_0].$$

Pela proposição 3.12, K é uma extensão algébrica de F. ■

Proposição 3.19 *Se L for uma extensão algébrica de um corpo K e K for uma extensão algébrica de um corpo F, então L é uma extensão algébrica de F.*

Demonstração. Seja $u \in L$. Como u é algébrico sobre K, existe um polinómio $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X] \setminus 0$ tal que $f(u) = 0$. Pela proposição 3.18, $E = F(a_0, a_1, \ldots, a_n)$ é uma extensão finita de F. Por outro lado, como $f(u) = 0$, u é algébrico sobre E. Pela proposição 3.18, $E(u)$ é uma extensão finita de E. Pela proposição 3.11, $E(u)$ é uma extensão finita, e, portanto, algébrica, de F. Donde u é algébrico sobre F. Como u é um elemento arbitrário de L, L é uma extensão algébrica de F. ■

Proposição 3.20 *Seja K uma extensão de um corpo F. Seja E o conjunto de todos os elementos de K que são algébricos sobre F. Então E é um corpo intermédio da extensão K de F e é uma extensão algébrica de F.*

Demonstração. Claramente $F \subseteq E \subseteq K$. Sejam $u, v \in E$. Pela proposição 3.18, $F(u, v)$ é uma extensão algébrica de F. Portanto $u - v$ e uv são algébricos sobre F e, se $u \neq 0$, então u^{-1} também é algébrico sobre F. Logo E é um subcorpo de K. Como todos os elementos de E são algébricos sobre F, E é uma extensão algébrica de F. ■

Proposição 3.21 *Seja $\sigma : K \to L$ um F-homomorfismo, onde K e L são extensões de um corpo F. Seja $f \in F[X]$. Se $u \in K$ for uma raiz de f, então $\sigma(u)$ também é uma raiz de f.*

Demonstração. Suponhamos que $f = a_n X^n + \cdots + a_1 X + a_0$. Suponhamos que $f(u) = 0$. Então

$$\begin{aligned} f(\sigma(u)) &= a_n \sigma(u)^n + \cdots + a_1 \sigma(u) + a_0 \\ &= \sigma(a_n)\sigma(u)^n + \cdots + \sigma(a_1)\sigma(u) + \sigma(a_0) \\ &= \sigma(a_n u^n + \cdots + a_1 u + a_0) = \sigma(f(u)) = \sigma(0) = 0. \end{aligned}$$ ■

Proposição 3.22 *Seja $\sigma : K \to L$ um homomorfismo de anéis. Para cada $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$, seja*

$$\sigma f = \sigma(a_n) X^n + \cdots + \sigma(a_1) X + \sigma(a_0) \in L[X].$$

Então

$$\phi : K[X] \to L[X], \quad f \mapsto \sigma f,$$

é um homomorfismo de anéis que estende σ *(i. e.,* $\forall a \in K, \phi(a) = \sigma(a)$*). Se* σ *for um isomorfismo,* ϕ *também é um isomorfismo.*

Demonstração. Claramente ϕ estende σ. Assim $\phi(1) = \sigma(1) = 1$. Quaisquer que sejam,

$$f = \sum_{n\in\mathbb{N}_0} a_n X^n,\ g = \sum_{n\in\mathbb{N}_0} b_n X^n \in K[X],$$

$$\begin{aligned}
\phi(f+g) &= \sigma(f+g) = \sigma \sum_{n\in\mathbb{N}_0} (a_n + b_n)X^n = \sum_{n\in\mathbb{N}_0} \sigma(a_n+b_n)X^n \\
&= \sum_{n\in\mathbb{N}_0} (\sigma(a_n) + \sigma(b_n))X^n = \sum_{n\in\mathbb{N}_0} \sigma(a_n)X^n + \sum_{n\in\mathbb{N}_0} \sigma(b_n)X^n \\
&= \sigma f + \sigma g = \phi(f) + \phi(g), \\
\phi(fg) &= \sigma(fg) = \sigma \sum_{n\in\mathbb{N}_0} \left(\sum_{k,l\in\mathbb{N}_0, kl=n} a_k b_l \right) X^n = \sum_{n\in\mathbb{N}_0} \sigma \left(\sum_{k,l\in\mathbb{N}_0, kl=n} a_k b_l \right) X^n \\
&= \sum_{n\in\mathbb{N}_0} \left(\sum_{k,l\in\mathbb{N}_0, kl=n} \sigma(a_k)\sigma(b_l) \right) X^n = \left(\sum_{n\in\mathbb{N}_0} \sigma(a_n)X^n \right) \left(\sum_{n\in\mathbb{N}_0} \sigma(b_n)X^n \right) \\
&= (\sigma f)(\sigma g) = \phi(f)\phi(g).
\end{aligned}$$

Portanto ϕ é um homomorfismo de anéis. Fica ao cuidado do leitor provar a última afirmação da proposição. ■

Proposição 3.23 *Seja* $\sigma : F \to E$ *um isomorfismo de corpos. Suponhamos que* u *é um elemento algébrico sobre* F*, pertencente a alguma extensão de* F*, com polinómio mínimo* $f \in F[X]$ *sobre* F*. Suponhamos que* v *é um elemento algébrico sobre* E*, pertencente a alguma extensão de* E*, com polinómio mínimo* $\sigma f \in E[X]$ *sobre* E*. Então existe um isomorfismo de corpos* $\tau : F(u) \to E(v)$ *que estende* σ *e aplica* u *em* v*.*

Em particular, se $F = E$ *e* $\sigma = \mathrm{id}_F$*, então existe um* F*-isomorfismo* $\tau : F(u) \to F(v)$ *tal que* $\tau(u) = v$*.*

Demonstração. Pela proposição 3.22, $\phi : F[X] \to E[X]$, $g \mapsto \sigma g$, é um isomorfismo que estende σ. Seja

$$p : E[X] \to \frac{E[X]}{E[X](\sigma f)}, \quad h \mapsto h + E[X](\sigma f),$$

o epimorfismo canónico. Então

$$\psi = p\phi : F[X] \to \frac{E[X]}{E[X](\sigma f)}, \quad g \mapsto \sigma g + E[X](\sigma f),$$

é um epimorfismo de anéis. Qualquer que seja $g \in F[X]$,

$$\begin{aligned} g \in \ker \psi &\Leftrightarrow \sigma g + E[X](\sigma f) = E[X](\sigma f) \Leftrightarrow \sigma g \in E[X](\sigma f) \Leftrightarrow \sigma f \mid \sigma g \\ &\Leftrightarrow \phi(f) \mid \phi(g) \Leftrightarrow f \mid g \Leftrightarrow g \in F[X]f. \end{aligned}$$

Donde $\ker \psi = F[X]f$. Pelo primeiro teorema de isomorfismo, proposição 0.40,

$$\kappa : \frac{F[X]}{F[X]f} = \frac{F[X]}{\ker \psi} \to \frac{E[X]}{E[X](\sigma f)}, \quad g + F[X]f \mapsto \sigma g + E[X](\sigma f),$$

é um isomorfismo de anéis. Pela proposição 3.16, $F[X]/F[X]f$ e $E[X]/E[X](\sigma f)$ são corpos e, portanto, κ é um isomorfismo de corpos. Pela proposição 3.16, existem isomorfismos de corpos

$$\lambda : \frac{F[X]}{F[X]f} \to F(u), \quad g + F[X]f \mapsto g(u),$$

$$\text{e} \qquad \mu : \frac{E[X]}{E[X](\sigma f)} \to E(v), \quad h + E[X](\sigma f) \mapsto h(v).$$

Assim

$$\tau = \mu\kappa\lambda^{-1} : F(u) \to E(v), \quad g(u) \mapsto (\sigma g)(v),$$

é um isomorfismo de corpos que estende σ e $\tau(u) = v$. ■

Exemplo 3.24 O polinómio $X^3 - 2$ é irredutível em $\mathbb{Q}[X]$ pelo critério de Eisenstein e tem uma raiz $\sqrt[3]{2} \in \mathbb{R}$. Verifique que $\sqrt[3]{2}\omega$ e $\sqrt[3]{2}\overline{\omega}$, onde $\omega = (-1 + \sqrt{3}\,i)/2 \in \mathbb{C}$ é uma raiz cúbica de 1, também são raízes de $X^3 - 2$. Assim $X^3 - 2$ é o polinómio mínimo de qualquer uma destas três raízes.

Pela proposição anterior, existe um $\mathbb{Q}$-isomorfismo $\tau : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\omega)$ tal que $\tau(\sqrt[3]{2}) = \sqrt[3]{2}\omega$.

Exercícios

3.2.1 Prove que os elementos $3 + 5i$, $\sqrt{i - \sqrt{2}}$, e $1 + \sqrt[3]{2}$ são algébricos sobre $\mathbb{Q}$.

3.2.2 Prove que $\sqrt{\pi}$ é algébrico sobre $\mathbb{Q}(\pi)$.

3.2.3 Prove que os números complexos são algébricos sobre $\mathbb{R}$.

3.2.4 Sejam K uma extensão de um corpo F e $u \in K$. Prove que, se u^2 for algébrico sobre F, então u é algébrico sobre F.

3.2.5 Seja K uma extensão de um corpo F. Seja E o corpo dos elementos de K algébricos sobre F (cf. proposição 3.20). Prove que os elementos de $K \setminus E$ são transcendentes sobre E.

3.2.6 Seja K uma extensão de um corpo F. Seja $u \in K$ um elemento algébrico sobre F cujo polinómio mínimo tem grau primo. Prove que, se E for um corpo intermédio $F \subseteq E \subseteq F(u)$, então $E = F$ ou $E = F(u)$.

3.2.7 Calcule os polinómios mínimos de $\sqrt{1 + \sqrt{5}}$ e $\sqrt{3}\,i + \sqrt{2}$ sobre $\mathbb{Q}$.

3.2.8 Calcule uma base para cada uma das seguintes extensões de $\mathbb{Q}$: $\mathbb{Q}(\sqrt{5}, i)$, $\mathbb{Q}(\sqrt{5}, \sqrt{7})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$.

3.2.9 Verifique que $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$ e $[\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{10}) : \mathbb{Q}] = 4$.

3.3 Corpos de decomposição

Seja K uma extensão de um corpo F. Seja $f \in F[X] \setminus F$. Diz-se que f *se decompõe* no corpo K se

$$f = c(X - u_1) \cdots (X - u_n), \quad \text{para alguns} \quad c \in F \text{ e } u_1, \ldots, u_n \in K.$$

Se, além disso, $K = F(u_1, \ldots, u_n)$, diz-se que K é um *corpo de decomposição* de f sobre F.

Se $f = cX + d \in F[X]$ tiver grau 1, então $f = c(X - (-d/c))$ decompõe-se em F e F é o único corpo de decomposição de f sobre F.

Exemplo 3.25 O polinómio $f = X^4 - X^2 - 2 = (X^2 - 2)(X^2 + 1) \in \mathbb{Q}[X]$ tem quatro raízes complexas $\pm\sqrt{2}$ e $\pm i$. Assim $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i)$ é um corpo de decomposição de f sobre $\mathbb{Q}$.

Exemplo 3.26 O corpo $\mathbb{C}$ dos números complexos é um corpo de decomposição do polinómio $X^2 + 1 = (X - i)(X + i)$ sobre $\mathbb{R}$, uma vez que

$$\mathbb{R}(i, -i) = \mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}.$$

Contudo $\mathbb{C}$ não é um corpo de decomposição de $X^2 + 1$ sobre $\mathbb{Q}$.

Proposição 3.27 *Sejam K uma extensão de um corpo F e E um corpo intermédio: $F \subseteq E \subseteq K$. Se K for um corpo de decomposição de algum polinómio f sobre F, então K é um corpo de decomposição de f sobre E.*

Sejam F um corpo e $f \in F[X]$ um polinómio que não é invertível. Então $F[X]f \neq F[X]$ e o anel $F[X]/F[X]f$ não é trivial. Consideremos o homomorfismo de anéis

$$j : F \to \frac{F[X]}{F[X]f}, \quad a \mapsto a + F[X]f.$$

Como $j(1) = 1 + F[X]f \neq 0 + F[X]f$, $\ker j \neq F$. Como F é um corpo, $\ker j = 0$ e j é um monomorfismo. Se identificarmos os elementos de F com as respetivas imagens por j, então $F = j(F)$ é um subanel de $F[X]/F[X]f$.

Proposição 3.28 *Sejam F um corpo, $f \in F[X]$ um polinómio mónico e $K = F[X]/F[X]f$. Para cada $g \in F[X]$, seja $\overline{g} = g + F[X]f$.*

Se f for irredutível, então, considerando K como extensão de F, $\overline{X} \in K$ é uma raiz de f no corpo K, $\overline{X}$ é algébrico sobre F e f é o polinómio mínimo de $\overline{X}$ sobre F.

Demonstração. Suponhamos que $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, com $a_i \in F$. Então

$$\begin{aligned} f(\overline{X}) &= \overline{X}^n + a_{n-1}\overline{X}^{n-1} + \cdots + a_0 = \overline{X^n} + \overline{a_{n-1}}\overline{X}^{n-1} + \cdots + \overline{a_0} \\ &= \overline{f} = f + F[X]f = F[X]f = 0_K. \end{aligned}$$

Logo $\overline{X}$ é raiz de f. Como $f \neq 0$, $\overline{X}$ é algébrico sobre F. Como f é irredutível e mónico, f é o polinómio mínimo de $\overline{X}$ sobre F. ■

Proposição 3.29 *Sejam F um corpo e $f \in F[X]$ um polinómio de grau $n \geq 1$. Existe um corpo de decomposição K do polinómio f sobre F tal que $[K : F] \leq n!$.*

Demonstração. Por indução em n. Se $n = 1$, então F é um corpo de decomposição de f sobre F e $[F : F] = 1 \leq 1!$.

Suponhamos que $n \geq 2$. Sabemos que f se fatoriza como produto de polinómios irredutíveis em $F[X]$. Seja $p \in F[X]$ um polinómio mónico e irredutível que divide f. Pela proposição 3.28, existe uma extensão E de F tal que p tem uma raiz $u \in E$ e p é o polinómio mínimo de u sobre F. Pela proposição 3.16, $[F(u) : F] = d(p) \leq d(f) = n$. Como $X - u \mid f$, $f = (X - u)g$, onde $g \in F(u)[X]$. Como $d(g) = n - 1$, a hipótese de indução garante que existe um corpo de decomposição K do polinómio g sobre o corpo $F(u)$ tal que $[K : F(u)] \leq (n - 1)!$. Assim

$$g = c(X - u_1) \cdots (X - u_{n-1}),$$

onde $c, u_1, \ldots, u_{n-1} \in K$, e, portanto,

$$f = c(X - u)(X - u_1) \cdots (X - u_{n-1}).$$

Como

$$K = F(u)(u_1, \ldots, u_{n-1}) = F(u, u_1, \ldots, u_{n-1}),$$

concluímos que K é um corpo de decomposição de f sobre F. Além disso,

$$[K : F] = [K : F(u)][F(u) : F] \leq (n - 1)!n = n!.$$ ■

Proposição 3.30 *Sejam $\sigma : F \to E$ um isomorfismo de corpos e $f \in F[X] \backslash F$. Se K for um corpo de decomposição de f sobre F e L for um corpo de decomposição de σf sobre E, então existe um isomorfismo $\overline{\sigma} : K \to L$ que estende σ. Em particular, se $F = E$ e $\sigma = \mathrm{id}_F$, então existe um F-isomorfismo $K \to L$.*

Demonstração. Por indução em $n = d(f)$. Note-se que $d(f) = d(\sigma f)$. Se $n = 1$, então $K = F$, $L = E$ e o resultado é trivial. Suponhamos que $n \geq 2$. Pela proposição 3.22, σ estende-se a um isomorfismo de anéis

$$\phi : F[X] \to E[X], \quad h \mapsto \sigma h.$$

Como K é um corpo de decomposição de f sobre F,

$$f = c(X - u_1) \cdots (X - u_n) \quad \text{e} \quad K = F(u_1, \ldots, u_n),$$

para alguns $c \in F, u_1, \ldots, u_n \in K$. Como L é um corpo de decomposição de σf sobre E,

$$\sigma f = \sigma(c)(X - v_1) \cdots (X - v_n) \quad \text{e} \quad L = E(v_1, \ldots, v_n),$$

para alguns $v_1, \ldots, v_n \in L$.

Seja $p \in F[X]$ o polinómio mínimo de u_1 sobre F. Claramente σp é mónico. Como $f(u_1) = 0$, $p \mid f$. Como ϕ é um isomorfismo, deduzimos que $\sigma p = \phi(p)$ é irredutível em $E[X]$ e $\sigma p \mid \sigma f$. Como $\sigma p \mid \sigma f$, σp é produto de alguns dos polinómios $X - v_i$. Sem perda de generalidade, suponhamos que v_1 é raiz de σp. Assim σp é o polinómio mínimo de v_1 sobre E.

Pela proposição 3.23, existe um isomorfismo de corpos $\tau : F(u_1) \to E(v_1)$ que estende σ e aplica u_1 em v_1. Pela proposição 3.22, τ estende-se a um isomorfismo de anéis

$$\psi : F(u_1)[X] \to E(v_1)[X], \quad h \mapsto \tau h.$$

Como $f = (X - u_1)g$, onde $g = c(X - u_2) \cdots (X - u_n) \in F(u_1)[X]$,

$$\sigma f = \tau f = \psi(f) = \psi(X - u_1)\psi(g) = (\tau(X - u_1))(\tau g) = (X - v_1)(\tau g).$$

Assim $\tau g = \sigma(c)(X - v_2) \cdots (X - v_n)$.

Como $K = F(u_1, \ldots, u_n) = F(u_1)(u_2, \ldots, u_n)$, K é um corpo de decomposição de g sobre $F(u_1)$. Como $L = E(v_1, \ldots, v_n) = E(v_1)(v_2, \ldots, v_n)$, L é um corpo de decomposição de τg sobre $E(v_1)$. Pela hipótese de indução, existe um isomorfismo de corpos $\overline{\sigma} : K \to L$ que estende τ e, portanto, também estende σ. ■

Exercícios

3.3.1 Prove que $X^2 - 3$ e $X^2 - 2X - 2$ são irredutíveis em $\mathbb{Q}[X]$ e têm o mesmo corpo de decomposição $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$.

3.3.2 Calcule um corpo de decomposição de $X^4 - 4X^2 - 5$ sobre $\mathbb{Q}$ e mostre que tem dimensão 4 sobre $\mathbb{Q}$.

3.3.3 Calcule corpos de decomposição dos seguintes polinómios sobre $\mathbb{Q}$: $X^4 + 1$, $X^4 - 2$, e $X^6 + X^3 + 1$.

3.3.4 Prove que $\mathbb{Q}(\sqrt{2}, i)$ é um corpo de decomposição de $X^2 - 2\sqrt{2}x + 3$ sobre $\mathbb{Q}(\sqrt{2})$.

3.3.5 Calcule um corpo de decomposição de $X^3 + X + 1$ sobre $\mathbb{Z}_2$.

3.4 Corpos algebricamente fechados

Recorde-se que um corpo K diz-se *algebricamente fechado* se todo o polinómio $f \in K[X] \setminus K$ tiver uma raiz em K.

Uma extensão K de um corpo F chama-se *fecho algébrico* de F se K for algebricamente fechado e for uma extensão algébrica de F.

Proposição 3.31 *Seja K um corpo. São equivalentes:*

(a) *K é algebricamente fechado.*

(b) *Todo o polinómio $f \in K[X] \setminus K$ se decompõe em K.*

(c) *Qualquer que seja u pertencente a alguma extensão de K, se u for algébrico sobre K, então $u \in K$.*

(d) *K é a única extensão algébrica de K.*

Proposição 3.32 *Seja K um fecho algébrico de um corpo F. Qualquer que seja o corpo intermédio $F \subseteq E \subseteq K$, se E for algebricamente fechado, então $E = K$.*

Demonstração. Seja $u \in K$. Como u é algébrico sobre F, u é raiz de um polinómio $f \in F[X] \setminus F$. Como E é algebricamente fechado, $u \in E$. Logo $K \subseteq E$ e $K = E$. ■

Proposição 3.33 *Seja K uma extensão de um corpo F. Seja A o corpo intermédio formado pelos elementos de K que são algébricos sobre F. (Cf. proposição* 3.20.*)*

Se K for algebricamente fechado, então A é o único fecho algébrico de F contido em K.

Demonstração. Para provar que A é um fecho algébrico de F, só falta ver que A é algebricamente fechado. Seja $g \in A[X] \setminus A$. Como K é algebricamente fechado, g tem uma raiz $u \in K$. Então u é algébrico sobre A e $A(u)$ é uma extensão algébrica de A. Como A é uma extensão algébrica de F, $A(u)$ também é uma extensão algébrica de F. Portanto u é algébrico sobre F e $u \in A$. Logo A é algebricamente fechado.

Suponhamos agora que E também é um fecho algébrico de F contido em K. Como os elementos de E são algébricos sobre F, $E \subseteq A$. Pela proposição 3.32, $E = A$. ■

Lema 3.34 *Se K for uma extensão algébrica de um corpo F, então $|K| \leq \aleph_0 |F|$.*

Demonstração. Para cada $n \in \mathbb{N}$, seja P_n o conjunto dos polinómios $f \in F[X]$ com grau n. Então $|P_n| = |(F \setminus 0) \times F^n| \leq \aleph_0 |F|$.

Como $F[X] \setminus F = \bigcup_{n \in \mathbb{N}} P_n$, $|F[X] \setminus F| \leq \aleph_0(\aleph_0 |F|) = \aleph_0 |F|$.

Como cada elemento de K é raiz de algum polinómio $f \in F[X] \setminus F$ e todos os polinómios pertencentes a $F[X] \setminus F$ têm um número finito de raízes, $|K| \leq \aleph_0 |F[X] \setminus F| \leq \aleph_0(\aleph_0 |F|) = \aleph_0 |F|$. ■

Teorema 3.35 *Todo o corpo F tem um fecho algébrico.*

Demonstração. Seja S um conjunto tal que $F \subseteq S$ e $\aleph_0|F| < |S|$ ([1]). Seja $\mathcal{S}$ o conjunto de todas as extensões algébricas de F contidas em S. (Duas extensões algébricas de F contidas em S com o mesmo conjunto suporte

[1] Por exemplo, $S = \mathcal{P}(\mathbb{N} \times F) \cup F$, a união do conjunto das partes de $\mathbb{N} \times F$ com F.

contam como elementos distintos de $\mathcal{S}$ se as operações forem distintas.) Como $F \in \mathcal{S}$, $\mathcal{S} \neq \emptyset$. Definimos uma ordem parcial em $\mathcal{S}$ do seguinte modo: $E_1 \leq E_2$ se e só se E_2 for uma extensão de E_1. Seja $(E_i)_{i\in I}$ uma cadeia não vazia de elementos de $\mathcal{S}$. Seja $E = \bigcup_{i\in I} E_i$. Sejam $x, y \in E$. Como $(E_i)_{i\in I}$ é uma cadeia, existe $j \in I$ tal que $x, y \in E_j$. Representamos por $x + y$ e xy a soma e o produto, respetivamente, de x e y em E_j. Verifique que $x + y$ e xy não dependem de E_j, isto é, se E_j e E_k forem elementos de $\mathcal{S}$ tais que $x, y \in E_j \cap E_k$, então as somas de x e y em E_j e em E_k coincidem e os produtos de x e y em E_j e em E_k também coincidem. Deste modo, ficam definidos, sem ambiguidade uma adição e uma multiplicação em E. Verifique que, com estas operações, E é um corpo que pertence a $\mathcal{S}$ e é um majorante da família $(E_i)_{i\in I}$. Pelo lema de Zorn, $\mathcal{S}$ tem um elemento maximal K.

Vejamos que K é algebricamente fechado. Com vista a uma contradição, suponhamos que não é. Pela proposição 3.31, existe um elemento u algébrico sobre K pertencente a alguma extensão de K e que não pertence a K. Então $K(u)$ é uma extensão algébrica de K diferente de K. Como K é uma extensão algébrica de F, $K(u)$ também é uma extensão algébrica de F. Pelo lema 3.34, $|K(u)| \leq \aleph_0|F| < |S|$. Donde $|K(u) \setminus K| < |S \setminus K|$. Seja $\epsilon : K(u) \setminus K \to S \setminus K$ uma aplicação injetiva. Então

$$\zeta : K(u) \to S, \quad a \mapsto a \text{ se } a \in K, \quad a \mapsto \epsilon(a) \text{ se } a \notin K,$$

é uma aplicação injetiva. Em $L = \zeta(K(u))$, definimos uma adição e uma multiplicação do seguinte modo: quaisquer que sejam $a, b \in K(u)$,

$$\zeta(a) + \zeta(b) := \zeta(a + b), \quad \zeta(a)\zeta(b) := \zeta(ab).$$

Claramente $K \subsetneqq L \subseteq S$, L é um corpo K-isomorfo a $K(u)$ e, portanto, também F-isomorfo a $K(u)$. Donde L é uma extensão algébrica de F e $L \in \mathcal{S}$, o que contradiz a maximalidade de K. Logo K é algebricamente fechado. Logo K é um fecho algébrico de F. ■

Teorema 3.36 *Sejam K e L fechos algébricos de um corpo F. Então K e L são F-isomorfos.*

Demonstração. Seja $\mathcal{S}$ o conjunto dos ternos (E, N, τ) tais que E é um corpo intermédio da extensão K de F, N é um corpo intermédio da extensão L de F e $\tau : E \to N$ é um F-isomorfismo.

Como $(F, F, \mathrm{id}_F) \in \mathcal{S}$, $\mathcal{S} \neq \emptyset$. Definimos em $\mathcal{S}$ uma ordem parcial do seguinte modo: $(E, N, \tau) \leq (E', N', \tau')$ se e só se E for subcorpo de E', N for subcorpo de N' e $\tau = \tau'_{|E}$.

Seja $(E_i, N_i, \tau_i)_{i\in I}$ uma cadeia não vazia de elementos de $\mathcal{S}$. Então $E = \bigcup_{i\in I} E_i$ é um corpo intermédio da extensão K de F e $N = \bigcup_{i\in I} N_i$ é um corpo intermédio da extensão L de F. Definimos uma aplicação $\tau : E \to N$

do seguinte modo: se $x \in E$, então $\tau(x) = \tau_j(x)$, onde j é um índice tal que $x \in E_j$. Verifique que τ está bem definido, isto é, $\tau(x)$ não depende do índice j escolhido. Mostre que τ é um F-isomorfismo. Assim $(E, N, \tau) \in \mathcal{S}$ e é um majorante da família $(E_i, N_i, \tau_i)_{i \in I}$. Pelo lema de Zorn, $\mathcal{S}$ tem um elemento maximal (D, M, σ).

Suponhamos que $D \neq K$. Seja $u \in K \setminus D$. Seja $f \in F[X] \setminus F$ tal que $f(u) = 0$. Como f se decompõe em K, K contém um corpo de decomposição C de f sobre D. Analogamente L contém um corpo de decomposição P de $\sigma f = f$ sobre M. Pela proposição 3.30, existe um isomorfismo $\overline{\sigma} : C \to P$ que estende σ. Note-se que $D \subsetneqq C$ porque $u \in C \setminus D$. Logo $(D, M, \sigma) < (C, P, \overline{\sigma})$, o que contradiz a maximalidade de (D, M, σ). Logo $D = K$.

Analogamente, se supusermos que $M \neq L$, podemos encontrar um F-isomorfismo $\overline{\nu} : P \to C$, onde $M \subsetneqq P \subseteq L$, $D \subseteq C \subseteq K$ e $\overline{\nu}$ estende $\nu = \sigma^{-1} : M \to D$. Assim $(D, M, \sigma) < (C, P, \overline{\nu}^{-1})$, uma contradição.

Logo $\sigma : K \to L$ é um F-isomorfismo. ■

Exercícios

3.4.1 Prove que não existe um corpo algebricamente fechado finito. (Sugestão: se $F = \{a_1, \ldots, a_n\}$ for um corpo algebricamente fechado finito com $a_1 \neq 0$, considere o polinómio $a_1 + (X - a_1) \cdots (X - a_n) \in F[X]$.

3.4.2 Seja K uma extensão algébrica de um corpo F tal que todo o polinómio $f \in F[X] \setminus F$ se decompõe em K. Prove que K é um fecho algébrico de F.

3.5 Extensões normais

Diz-se que um corpo K é uma extensão *normal* de um corpo F se K for uma extensão algébrica de F e, para qualquer polinómio irredutível $p \in F[X]$, se p tiver uma raiz em K, então p decompõe-se em K.

Um corpo F é uma extensão normal de F, uma vez que, se um polinómio irredutível $p \in F[X]$ tiver uma raiz em F, então $d(p) = 1$ e p decompõe-se em F.

Exemplo 3.37 Considere-se o exemplo 3.24. O polinómio irredutível $X^3 - 2 \in \mathbb{Q}[X]$ tem uma raiz real $\sqrt[3]{2}$. Assim $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ e $\mathbb{Q}(\sqrt[3]{2})$ não contém a raiz complexa não real $\sqrt[3]{2}\omega$ de $X^3 - 2$. Logo $\mathbb{Q}(\sqrt[3]{2})$ não é uma extensão normal de $\mathbb{Q}$.

Proposição 3.38 *Seja K uma extensão normal de um corpo F e seja E um corpo intermédio ($F \subseteq E \subseteq K$). Então K é uma extensão normal de E.*

Demonstração. Como K é uma extensão normal de F, K é uma extensão algébrica de F e, portanto, K é uma extensão algébrica de E. Seja $g \in E[X]$ um polinómio irredutível que tem uma raiz $u \in K$. Seja $f \in F[X]$ o polinómio mínimo de u sobre F. Sejam $q, r \in E[X]$ tais que $f = gq + r$ e $d(r) < d(g)$. Como g é irredutível, g é o polinómio mínimo de u sobre E, a menos do produto por uma unidade. Como $0 = f(u) = g(u)q(u) + r(u) = r(u)$ e $d(r) < d(g)$, deduzimos que $r = 0$. Assim $f = gq$ e $g \mid f$. Como f se decompõe em K, g também se decompõe em K. Logo K é uma extensão normal de E. ■

Proposição 3.39 *Seja F um corpo. Uma extensão K de F é um corpo de decomposição de algum polinómio f sobre F se e só se K for uma extensão finita e normal de F.*

Demonstração. Suponhamos que K é um corpo de decomposição de um polinómio $f \in F[X]$. Então f decompõe-se em K e $K = F(u_1, \ldots, u_n)$, onde $u_1, \ldots, u_n$ são as raízes de f em K. Pela proposição 3.18, K é uma extensão finita e algébrica de F. Seja $p \in F[X]$ um polinómio irredutível que tem uma raiz $v \in K$. Seja L um corpo de decomposição de p sobre K. Assim $F \subseteq K \subseteq L$. Para provar que p se decompõe em K basta mostrar que as raízes de p em L pertencem a K.

Seja $w \in L$ uma raiz de p. Pela proposição 3.23, existe um F-isomorfismo $\tau : F(v) \to F(w)$ tal que $\tau(v) = w$. Como

$$K(w) = F(u_1, \ldots, u_n)(w) = F(w)(u_1, \ldots, u_n),$$

$K(w)$ é um corpo de decomposição de f sobre $F(w)$. Como $v \in K$,

$$K = K(v) = F(u_1, \ldots, u_n)(v) = F(v)(u_1, \ldots, u_n)$$

e, portanto, K é um corpo de decomposição de f sobre $F(v)$. Pela proposição 3.30, o F-isomorfismo τ estende-se a um F-isomorfismo $\overline{\tau} : K \to K(w)$. Pelas proposições 3.10 e 3.11, $[K : F] = [K(w) : F] = [K(w) : K][K : F]$. Assim $[K(w) : K] = 1$. Donde $K(w) = K$ e $w \in K$. Provámos que todas as raízes de p em L pertencem a K. Logo K é uma extensão normal de F.

Reciprocamente, suponhamos que K é uma extensão finita e normal de F. Seja $\{u_1, \ldots, u_n\}$ uma base de K sobre F. Então $K = F(u_1, \ldots, u_n)$. Como K é uma extensão algébrica de F, cada u_i é algébrico sobre F. Seja $p_i \in F[X]$ o polinómio mínimo de u_i sobre F. Como K é uma extensão normal de F, cada p_i decompõe-se em K. Portanto $f = p_1 \cdots p_n$ decompõe-se em K. Como o conjunto das raízes de f em K contém $\{u_1, \ldots, u_n\}$, deduzimos que K é um corpo de decomposição de f sobre F. ■

Exercícios

3.5.1 Seja $\omega = e^{2\pi i/3}$. Quais das seguintes extensões de corpos são normais e quais não são?

(a) A extensão $\mathbb{Q}(\sqrt{-3})$ de $\mathbb{Q}$.

(b) A extensão $\mathbb{Q}(i, \sqrt{3})$ de $\mathbb{Q}$.
(c) A extensão $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$.
(d) A extensão $\mathbb{Q}(\omega, \sqrt[3]{2})$ de $\mathbb{Q}(\omega)$.
(e) A extensão $\mathbb{Q}(\omega)$ de $\mathbb{Q}$.
(f) A extensão $\mathbb{Q}(\omega\sqrt[3]{2})$ de $\mathbb{Q}$.
(g) A extensão $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ de $\mathbb{Q}$.
(h) A extensão $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ de $\mathbb{Q}$.

3.5.2 Seja K uma extensão de um corpo F tal que $[K : F] = 2$. Prove que K é normal.

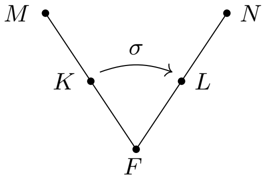
3.6 Extensões separáveis

Seja F um corpo. Um polinómio $f \in F[X] \setminus F$ de grau n diz-se *separável* se tiver n raízes distintas em alguma extensão de F onde f se decompõe.

Seja K uma extensão de um corpo F. Um elemento $u \in K$ diz-se *separável* sobre F se u for algébrico sobre F e o polinómio mínimo de u sobre F for separável. O corpo K diz-se uma extensão *separável* de F se todos os elementos de K forem separáveis sobre F. Assim, as extensões separáveis são algébricas.

Proposição 3.40 *Seja F um corpo. Um polinómio $f \in F[X] \setminus F$ de grau n é separável se e só se f tiver n raízes distintas em **qualquer** extensão de F onde f se decompõe.*

Demonstração. Seja $f \in F[X] \setminus F$ um polinómio de grau n. Suponhamos que f é separável sobre F. Então f tem n raízes distintas nalguma extensão M de F onde f se decompõe. O subcorpo K de M gerado por F e pelas raízes de f em M é um corpo de decomposição de f sobre F.



Seja N uma extensão de F onde f se decompõe. O subcorpo L de N gerado por F e pelas raízes de f em N também é um corpo de decomposição de f sobre F. Pela proposição 3.30, existe um F-isomorfismo $\sigma : K \to L$. Pela proposição 3.21, σ aplica raízes de f em raízes de f. Como σ é bijetivo, f tem n raízes distintas em L e, portanto, f tem n raízes distintas em N.

Reciprocamente, suponhamos que f tem n raízes distintas em qualquer extensão de F onde f se decompõe. Pela proposição 3.29, existe um corpo de decomposição de f sobre F. Logo f é separável sobre F. ■

Proposição 3.41 *Sejam K uma extensão de um corpo F e E um corpo intermédio ($F \subseteq E \subseteq K$).*

(a) *Se $u \in K$ for separável sobre F, então u é separável sobre E.*

(b) *Se K for uma extensão separável de F, então K é uma extensão separável de E e E é uma extensão separável de F.*

Demonstração. (a) Sejam $u \in K$ um elemento separável sobre F, f o polinómio mínimo de u sobre F e $n = d(f)$. Seja L um corpo de decomposição de f sobre K. Sejam $u_1, \ldots, u_n$ as raízes de f em L. Como f é separável, $u_1, \ldots, u_n$ são distintas. Seja q o polinómio mínimo de u sobre E. Como $f \in E[X]$ e $f(u) = 0$, $q \mid f$ em $E[X]$. Assim q decompõe-se em L e as raízes de q em L são todas distintas e são $u_{i_1}, \ldots, u_{i_m}$, onde $m = d(q)$ e $1 \leq i_1 < \cdots < i_m \leq n$. Logo q é separável e u é separável sobre E.

(b) É uma consequência de (a) e da definição de extensão separável. ■

Sejam F um corpo e $f = a_nX^n + \cdots + a_2X^2 + a_1X + a_0 \in F[X]$. O polinómio

$$f' = na_nX^{n-1} + \cdots + 2a_2X + a_1 \in F[X].$$

chama-se *derivada* de f.

Proposição 3.42 *Seja F um corpo. Quaisquer que sejam $a \in F$, $f, g \in F[X]$, $n \geq 2$,*

$$(af)' = af', \quad (f+g)' = f' + g', \quad (fg)' = fg' + f'g, \quad (f^n)' = nf^{n-1}f'.$$

Proposição 3.43 *Sejam F um corpo e $f \in F[X]$. Se f e f' forem relativamente primos em $F[X]$, então f é separável.*

Demonstração. Suponhamos que f não é separável. Seja K um corpo de decomposição de f sobre F. Então f tem uma raiz múltipla $u \in K$, isto é, $f = (X-u)^2g$, para algum $g \in K[X]$. Derivando

$$f' = (X-u)^2g' + 2(X-u)g.$$

Assim $u \in K$ é uma raiz comum a f e f'. Se $p \in F[X]$ for o polinómio mínimo de u sobre F, então $p \mid f$ e $p \mid f'$, o que mostra que f e f' não são relativamente primos em $F[X]$. ■

Proposição 3.44 *Seja K uma extensão de um corpo F de característica 0.*

(a) *Todo o polinómio irredutível $f \in F[X]$ é separável.*

(b) *K é uma extensão algébrica de F se e só se K for uma extensão separável de F.*

Demonstração. (a) Seja $f \in F[X]$ um polinómio irredutível. Suponhamos que $f = cX^n + g$, onde $c \in F \setminus 0$, $n \geq 1$ e $g \in F[X]$ tem grau inferior a n. Então $f' = ncX^{n-1} + g'$, onde g' tem grau inferior a $n-1$. Como F tem característica 0, $nc \neq 0$. Assim f' é um polinómio não nulo com grau inferior a n. Como f é irredutível, f e f' são relativamente primos. Pela proposição anterior, f é separável.

(b) Suponhamos que K é uma extensão algébrica de F. Por (a), para cada $u \in K$, o polinómio mínimo de u sobre F é separável. Logo K é uma extensão separável de F.

A afirmação recíproca resulta da definição de extensão separável. ■

Teorema 3.45 [Teorema do elemento primitivo] *Seja F um corpo infinito* ([2])*. Seja K uma extensão finita e separável de F. Então $K = F(u)$, para algum $u \in K$* ([3])*.*

Demonstração. Como K é uma extensão finita de F, existem $u_1, \ldots, u_n \in K$ tais que $K = F(u_1, \ldots, u_n)$. A demonstração é por indução em n. Se $n = 1$, o resultado é trivial.

Suponhamos que $n = 2$. Suponhamos que $K = F(v, w)$. (Estamos a substituir u_1, u_2 por v, w para simplificar a escrita.) Sejam p o polinómio mínimo de v sobre F e q o polinómio mínimo de de w sobre F. Como K é uma extensão separável de F, os polinómios p, q são separáveis. Seja L um corpo de decomposição do polinómio $pq \in F[X] \subseteq K[X]$ sobre K. Sejam $v_1 = v, v_2, \ldots, v_m$ as raízes de p em L e $w_1 = w, w_2, \ldots, w_k$ as raízes de q em L. Como

$$\begin{aligned} L &= K(v_1, \ldots, v_m, w_1, \ldots, w_k) = F(v_1, w_1)(v_1, \ldots, v_m, w_1, \ldots, w_k) \\ &= F(v_1, \ldots, v_m, w_1, \ldots, w_k), \end{aligned}$$

L também é um corpo de decomposição de pq sobre F.

Como F é infinito, existe $c \in F$ tal que

$$c \neq \frac{v_i - v}{w - w_j}, \quad \text{quaisquer que sejam } i \in \{1, \ldots, m\}, j \in \{2, \ldots, k\}.$$

Seja $u = v + cw$. Vamos provar que $K = F(u)$.

Seja $h = p(u - cX) \in F(u)[X]$. Então $h(w) = p(u - cw) = p(v) = 0$. Suponhamos que existe $j \in \{2, \ldots, k\}$ tal que $h(w_j) = 0$. Então $0 = h(w_j) = p(u - cw_j) = p(v + cw - cw_j)$. Assim $v - cw - cw_j = v_i$, para algum $i \in \{1, \ldots, m\}$. Donde $c = (v_i - v)/(w - w_j)$, o que é uma contradição. Portanto w é a única raiz comum de q e h.

Seja r o polinómio mínimo de w sobre $F(u)$. Então $r \mid q$ e $r \mid h$. Como q se decompõe em L, r também se decompõe em L. Como q e h têm uma única raiz comum, $d(r) = 1$ e w é a única raiz de r em L. Assim, como $r \in F(u)[X]$, $w \in F(u)$. Donde $v = u - cw \in F(u)$. Donde $K = F(v, w) \subseteq F(u)$. Como $u = v + cw \in F(v, w) = K$, $F(u) \subseteq K$. Logo $K = F(u)$.

Suponhamos que $n > 2$. Seja $E = F(u_1, \ldots, u_{n-1})$. Como $F \subseteq E \subseteq K$, E também é uma extensão finita e separável de F. Pela hipótese de indução, $E = F(v)$, para algum $v \in E$. Assim $K = E(u_n) = F(v)(u_n) = F(v, u_n)$. Pelo caso anterior, $K = F(u)$, para algum $u \in K$. ■

[2] Este teorema é verdadeiro se F for finito, mas não demonstraremos isso nesta disciplina. Mais adiante, a proposição 3.54 e o teorema 3.59 também são válidos em corpos finitos mas estão enunciados para corpos infinitos porque dependem deste teorema.

[3] Um tal elemento u chama-se elemento *primitivo* de K sobre F.

Exercícios

3.6.1 Demonstre a proposição 3.42. Sugestão para demonstrar $(fg)' = fg' + f'g$: suponha que $g = b_m X^m + \cdots + b_0$; para cada k, tome $g_k = b_k X^k$ e prove que $(fg_k)' = fg_k' + f'g_k$; utilize a fórmula para a derivada da soma.

Sugestão para demonstrar $(f^n)' = nf^{n-1}f'$: demonstre por indução em n e utilize a fórmula para a derivada do produto.

3.6.2 Seja F um corpo. Sejam $f, g \in F[X]$ tais que $0 \neq g \mid f$. A fração f/g representa o único polinómio $h \in F[X]$ tal que $f = gh$. Prove que

$$g^2 \mid f'g - fg' \quad \text{e} \quad \left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}.$$

Sugestão: tomando $h = f/g$, derive ambos os lados da igualdade $f = gh$.

3.6.3 Sejam F um corpo e $p \in F[X]$ um polinómio irredutível. Prove que p é separável se e só se $p' \neq 0$.

3.6.4 Utilize a demonstração do teorema do elemento primitivo para provar as seguintes igualdades.

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(b) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + r\sqrt{3})$, para qualquer $r \in \mathbb{Q} \setminus \{0\}$.

(c) $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

(d) $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{3})$.

(e) $\mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$.

(f) $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\omega + \sqrt[3]{2})$, onde $\omega = e^{2\pi i/3}$.

3.6.5 Prove que, se $p, q \in \mathbb{N}$ forem números primos distintos, então $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p+q})$.

3.6.6 Seja K uma extensão de um corpo infinito F. Sejam $v, w \in K$ algébricos sobre F e suponhamos que w é uma raiz de um polinómio separável com coeficientes em F. Prove que $F(v, w) = F(u)$, para algum $u \in F$. Sugestão: adapte a demonstração do teorema do elemento primitivo.

3.7 Grupos de Galois

Seja K uma extensão de um corpo F. Seja $\operatorname{Gal}_F K$ o conjunto de todos os F-automorfismos de K. Vimos, na proposição 3.5, que $\operatorname{Gal}_F K$ é um grupo, que se chama *grupo de Galois* de K sobre F.

Proposição 3.46 *Sejam K uma extensão de um corpo F, $f \in F[X]$ e $\sigma \in \operatorname{Gal}_F K$. Para cada $u \in K$, u é raiz de f se e só se $\sigma(u)$ for raiz de f.*

Demonstração. Resulta da proposição 3.21. ■

Proposição 3.47 *Seja F um corpo. Seja K um corpo de decomposição de algum polinómio sobre F. Sejam $u, v \in K$. Existe $\sigma \in \operatorname{Gal}_F K$ tal que $\sigma(u) = v$ se e só se u e v tiverem o mesmo polinómio mínimo sobre F.*

Demonstração. Suponhamos que existe $\sigma \in \operatorname{Gal}_F K$ tal que $\sigma(u) = v$. Para qualquer polinómio $f \in F[X]$, $f(u) = 0 \Leftrightarrow f(\sigma(u)) \Leftrightarrow f(v) = 0$. Como u e v são raízes dos mesmos polinómios $f \in F[X]$, u e v têm o mesmo polinómio mínimo.

Reciprocamente, suponhamos que u e v têm o mesmo polinómio mínimo sobre F. Pela proposição 3.23, existe um F-isomorfismo $\tau : F(u) \to F(v)$ tal que $\tau(u) = v$. Como K é um corpo de decomposição de algum polinómio g sobre F, K também é um corpo de decomposição de g sobre $F(u)$ e sobre $F(v)$. Pela proposição 3.30, existe um automorfismo σ de K que estende τ. Assim $\sigma \in \operatorname{Gal}_F K$ e $\sigma(u) = v$. ■

Exemplo 3.48 É fácil verificar que a aplicação conjugação

$$\sigma : \mathbb{C} \to \mathbb{C}, \quad a + bi \mapsto a - bi,$$

é um $\mathbb{R}$-automorfismo de $\mathbb{C}$. Note-se que i e $-i$ são as raízes de $X^2 + 1 \in \mathbb{R}[X]$, $\sigma(i) = -i$, $\sigma(-i) = i$.

Seja $\tau \in \operatorname{Gal}_{\mathbb{R}}(\mathbb{C})$. Como i é uma raiz de $X^2 + 1$, $\tau(i)$ também é uma raiz de $X^2 + 1$.

Suponhamos que $\tau(i) = i$. Qualquer que seja $a + bi \in \mathbb{C}$, $\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a + bi$. Assim $\tau = \mathrm{id}_{\mathbb{C}}$.

Suponhamos que $\tau(i) = -i$. Qualquer que seja $a + bi \in \mathbb{C}$, $\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a - bi$. Assim $\tau = \sigma$.

Logo $\operatorname{Gal}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$.

Note-se que qualquer $\mathbb{R}$-automorfismo de $\mathbb{C}$ fica completamente determinado pela imagem de i. A proposição seguinte generaliza este facto.

Proposição 3.49 *Seja $K = F(u_1, \ldots, u_n)$ uma extensão algébrica de um corpo F. Sejam $\sigma, \tau \in \operatorname{Gal}_F K$.*

Se, para cada $i \in \{1, \ldots, n\}$, $\sigma(u_i) = \tau(u_i)$, então $\sigma = \tau$.

Demonstração. Seja $\beta = \tau^{-1}\sigma$. Para cada $i \in \{1, \ldots, n\}$,

$$\beta(u_i) = \tau^{-1}\sigma(u_i) = \tau^{-1}\tau(u_i) = u_i. \tag{3.4}$$

Seja $u_0 = 1$. Vamos provar, por indução em $i \in \{0, \ldots, n\}$, que, qualquer que seja $v \in F(u_0, \ldots, u_i)$, $\beta(v) = v$. Esta afirmação é verdadeira quando $i = 0$ porque $F(u_0) = F$ e β é um F-automorfismo. Seja $i \in \{1, \ldots, n\}$. Seja $v \in F(u_0, \ldots, u_i)$. Como u_i é algébrico sobre F, u_i também é algébrico sobre $F(u_0, \ldots, u_{i-1})$. Assim $v \in F(u_0, \ldots, u_{i-1})(u_i) = F(u_0, \ldots, u_{i-1})[u_i]$ e

$$v = c_0 + c_1 u_i + \cdots + c_k u_i^k, \quad \text{para alguns } c_0, c_1, \ldots, c_k \in F(u_0, \ldots, u_{i-1}).$$

Pela hipótese de indução, $\beta(c_i) = c_i$, para cada $i \in \{0, \ldots, k\}$. Por (3.4),

$$\beta(v) = \beta(c_0) + \beta(c_1)\beta(u_i) + \cdots + \beta(c_k)\beta(u_i)^k = c_0 + c_1 u_i + \cdots + c_k u_i^k = v.$$

Logo, para cada $v \in K = F(u_1, \dots, u_n)$, $\beta(v) = v$. Logo $\beta = \mathrm{id}_K$ e $\sigma = \tau$. ■

Exemplo 3.50 Seja $\sigma \in G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}, \sqrt{5}))$. Como $\sqrt{3}$ é raiz do polinómio $X^2 - 3 \in \mathbb{Q}[X]$, $\sigma(\sqrt{3})$ também é raiz de $X^2 - 3$, pela proposição 3.46. Assim $\sigma(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$. Analogamente $\sigma(\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$.

Pela proposição 3.49, σ fica completamente determinada pelos valores $\sigma(\sqrt{3})$ e $\sigma(\sqrt{5})$. Assim existem quando muito quatro elementos em G:

$$\begin{aligned}
\sigma_1 : &\quad \sqrt{3} \mapsto \sqrt{3}, &\quad \sqrt{5} \mapsto \sqrt{5},\\
\sigma_2 : &\quad \sqrt{3} \mapsto -\sqrt{3}, &\quad \sqrt{5} \mapsto \sqrt{5},\\
\sigma_3 : &\quad \sqrt{3} \mapsto \sqrt{3}, &\quad \sqrt{5} \mapsto -\sqrt{5},\\
\sigma_4 : &\quad \sqrt{3} \mapsto -\sqrt{3}, &\quad \sqrt{5} \mapsto -\sqrt{5}.
\end{aligned}$$

Vejamos agora que, para cada $j \in \{1, \dots, 4\}$, existe de facto $\sigma_j \in G$ cujas imagens de $\sqrt{3}$ e $\sqrt{5}$ são as indicadas acima.

Suponhamos que $j = 4$. Os argumentos nos outros casos são análogos. Pelo critério de Eisenstein, $X^2 - 3$ é irredutível em $\mathbb{Q}[X]$ e, portanto, é o polinómio mínimo de $\sqrt{3}$ e de $-\sqrt{3}$ sobre $\mathbb{Q}$. Pela proposição 3.23, existe um $\mathbb{Q}$-isomorfismo $\tau_4 : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(-\sqrt{3}) = \mathbb{Q}(\sqrt{3})$ tal que $\tau_4(\sqrt{3}) = -\sqrt{3}$.

De acordo com o exemplo 3.15, o polinómio $g = X^2 - 5$ é irredutível em $\mathbb{Q}(\sqrt{3})[X]$. Assim g é o polinómio mínimo de $\sqrt{5}$ e de $-\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$. Pela proposição 3.23, existe um isomorfismo $\sigma_4 : \mathbb{Q}(\sqrt{3})(\sqrt{5}) \to \mathbb{Q}(\sqrt{3})(-\sqrt{5})$ que estende τ_4 e tal que $\sigma_4(\sqrt{5}) = -\sqrt{5}$.

Claramente $\sigma_4 \in G$, $\sigma_4(\sqrt{3}) = -\sqrt{3}$ e $\sigma_4(\sqrt{5}) = -\sqrt{5}$.

Proposição 3.51 *Seja F um corpo. Se K for um corpo de decomposição de um polinómio separável $f \in F[X]$ de grau n, então $\mathrm{Gal}_F K$ é isomorfo a um subgrupo de S_n.*

Demonstração. Como f é separável, f tem n raízes distintas $u_1, \dots, u_n \in K$. Seja $R = \{u_1, \dots, u_n\}$. Seja $\sigma \in \mathrm{Gal}_F K$. Pela proposição 3.46, $\sigma(R) = R$ e, portanto, $\sigma_{|R} : R \to R$ é uma permutação de R. É fácil verificar que

$$\theta : \mathrm{Gal}_F K \to \mathrm{Sym}\, R, \quad \sigma \mapsto \sigma_{|R},$$

é um homomorfismo de grupos.

Pela definição de corpo de decomposição, $K = F(u_1, \dots, u_n)$. Sejam $\sigma, \tau \in \mathrm{Gal}_F K$ e suponhamos que $\theta(\sigma) = \theta(\tau)$. Assim, para cada $i \in \{1, \dots, n\}$, $\sigma(u_i) = \tau(u_i)$. Pela proposição 3.49, $\sigma = \tau$. Logo θ é injetivo e $\mathrm{Gal}_F K \cong \mathrm{im}\, \theta \leq \mathrm{Sym}\, R \cong S_n$. ■

Exercícios

3.7.1 Calcule os seguintes grupos de Galois.

(a) $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2})$, $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[3]{2})$, e $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[4]{2})$.

(b) $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Q}$ e $\sqrt{d} \notin \mathbb{Q}$.

(c) $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{\omega})$, onde $\omega = (-1 + \sqrt{3}\,i)/2$ é uma raiz cúbica de 1.

(d) $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(e) $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{p}, \sqrt{q})$, onde p e q são números primos positivos distintos.

(f) $\mathrm{Gal}_{\mathbb{Q}}\,K$, onde K é um corpo de decomposição de $X^4 - X^2 - 2$ sobre $\mathbb{Q}$.

3.7.2 Seja σ um automorfismo do corpo $\mathbb{R}$. Pelo exercício 3.1.4, $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\,\mathbb{R}$.

(a) Prove que, $\forall r, s \in \mathbb{R}, r > s \Rightarrow \sigma(r) > \sigma(s)$. Sugestão: recorde que os números reais positivos são os quadrados dos números reais não nulos e prove primeiro que $r > 0 \Rightarrow \sigma(r) > 0$.

(b) Prove que $\sigma = \mathrm{id}_{\mathbb{R}}$. Portanto $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{R} = \{\mathrm{id}_{\mathbb{R}}\}$.

3.8 Correspondências de Galois

Seja K uma extensão finita de um corpo F. Seja $\mathcal{E}$ o conjunto dos corpos intermédios desta extensão. Seja $\mathcal{S}$ o conjunto dos subgrupos de $\mathrm{Gal}_F\,K$.

Proposição 3.52 *Para cada* $E \in \mathcal{E}$, $\mathrm{Gal}_E\,K \in \mathcal{S}$. *Para cada* $H \in \mathcal{S}$,

$$E_H = \{c \in K : \forall \sigma \in H, \sigma(c) = c\} \in \mathcal{E}.$$

Diz-se que E_H é o *corpo fixo* de H.

A *correspondência de Galois* consiste nas duas aplicações seguintes:

$$\begin{aligned} \Phi &: \mathcal{E} \to \mathcal{S}, \quad E \mapsto \mathrm{Gal}_E\,K, \quad \text{e} \\ \Psi &: \mathcal{S} \to \mathcal{E}, \quad H \mapsto E_H. \end{aligned}$$

Proposição 3.53 *Com a notação anterior,*

(a) $\Phi(K) = \{\mathrm{id}_K\}$.

(b) $\Phi(F) = \mathrm{Gal}_F\,K$.

(c) $\Psi(\{\mathrm{id}_K\}) = K$.

(d) *Para quaisquer* $E, E' \in \mathcal{E}$, $E \subseteq E' \Rightarrow \Phi(E') \subseteq \Phi(E)$ *e* $E \subseteq \Psi\Phi(E)$.

(e) *Para quaisquer* $H, H' \in \mathcal{S}$, $H \subseteq H' \Rightarrow \Psi(H') \subseteq \Psi(H)$ *e* $H \subseteq \Phi\Psi(H)$.

Proposição 3.54 *Seja* K *uma extensão finita de um corpo infinito* ([4]) F. *Seja* H *um subgrupo de* $\mathrm{Gal}_F\,K$.

[4] Esta proposição também é verdadeira quando F for finito. Contudo a demonstração neste texto de apoio depende do teorema do elemento primitivo que só demonstrámos para corpos infinitos.

(a) *K é uma extensão simples, normal e separável de E_H.*

(b) *$H = \operatorname{Gal}_{E_H} K$ e $|H| = [K : E_H]$.*

(c) *Com a notação introduzida acima, $\Phi\Psi = \mathrm{id}_{\mathcal{S}}$.*

Demonstração. Seja $u \in K$. Como K é uma extensão finita e, portanto, algébrica de F, u é algébrico sobre F. Assim u também é algébrico sobre o corpo intermédio E_H. Seja p_u o polinómio mínimo de u sobre E_H. Seja

$$H_u = \{\tau(u) : \tau \in H\} \ (\subseteq K).$$

Pela definição de E_H,

$$H \subseteq \operatorname{Gal}_{E_H} K. \tag{3.5}$$

Pela proposição 3.46, todos os elementos de H_u são raízes de p_u. Assim H_u é finito. Sejam $t = |H_u|$ e $u = u_1, u_2, \ldots, u_t$ os elementos de H_u.

Seja $\sigma \in H$. Qualquer que seja $\tau \in H$, $\sigma\tau \in H$ e $\sigma(\tau(u)) = (\sigma\tau)(u) \in H_u$. Assim $\sigma(H_u) \subseteq H_u$. Como σ é injetivo e H_u é finito, $\sigma(H_u) = H_u$ e $\sigma_{|H_u}$ é uma permutação de H_u. Seja

$$f_u = (X - u_1) \cdots (X - u_t) \in K[X]. \tag{3.6}$$

Como $u_1, \ldots, u_t$ são distintos, f_u é separável.

Vejamos que $f_u \in E_H[X]$. Seja $\sigma \in H$. Pela proposição 3.22, $\phi : K[X] \to K[X]$, $g \mapsto \sigma g$, é um isomorfismo de anéis que estende σ. Como $\sigma_{|H_u}$ é uma permutação de H_u,

$$\begin{aligned}\sigma f_u &= \phi(f_u) = \phi(X - u_1) \cdots \phi(X - u_t)\\ &= (X - \sigma(u_1)) \cdots (X - \sigma(u_t)) = (X - u_1) \cdots (X - u_t) = f_u.\end{aligned}$$

Assim σ aplica cada coeficiente de f_u nele próprio. Como σ é um elemento arbitrário de H, os coeficientes de f_u pertencem a E_H e $f_u \in E_H[X]$. Como u é raiz de $f_u \in E_H[X]$, $p_u \mid f_u$.

(a) Como f_u é separável, p_u também é separável. Logo u é separável sobre E_H. Como u é um elemento arbitrário de K, K é uma extensão separável de E_H.

Como K é uma extensão finita de F, K também é uma extensão finita do corpo intermédio E_H. Pelo teorema do elemento primitivo (teorema 3.45), $K = E_H(u)$, para algum $u \in K$.

A este elemento primitivo u, associemos o polinómio f_u definido acima. Então $K = E_H(u) \subseteq E_H(u_1, \ldots, u_t) \subseteq K$. Donde $K = E_H(u_1, \ldots, u_t)$. Assim K é um corpo de decomposição de f_u sobre E_H. Pela proposição 3.39, K é uma extensão normal de E_H.

(b) Por (3.5), $|H| \leq |\operatorname{Gal}_{E_H} K|$. Vimos acima que $K = E_H(u)$, para algum $u \in K$ algébrico sobre E_H. Seja p_u o polinómio mínimo de u sobre E_H. Pela proposição 3.16, $d(p_u) = [K : E_H]$.

Seja $\sigma \in \operatorname{Gal}_{E_H} K$. Pela proposição 3.46, $\sigma(u)$ é uma raiz de p_u. Pela proposição 3.49, σ fica completamente determinado pela imagem $\sigma(u)$. Logo $|\operatorname{Gal}_{E_H} K| \leq d(p_u) = [K : E_H]$.

Definamos f_u como em (3.6). Como $f_u(u) = 0$, $p_u \mid f_u$. Assim $[K : E_H] = d(p_u) \leq d(f_u) = |H_u| \leq |H|$.

Das desigualdades anteriores, $|H| = |\operatorname{Gal}_{E_H} K| = [K : E_H]$. Como $H \subseteq \operatorname{Gal}_{E_H} K$, $H = \operatorname{Gal}_{E_H} K$.

(c) Qualquer que seja $H \in \mathcal{S}$, $H = \operatorname{Gal}_{E_H} K = \Phi\Psi(H)$. ■

Exemplo 3.55 No exemplo 3.50, vimos que

$$\operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$$

Calcule a tabela da multiplicação deste grupo. Verifique que os subgrupos de $\operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ são

$$H_1 = \{\sigma_1\},\ H_2 = \{\sigma_1, \sigma_2\},\ H_3 = \{\sigma_1, \sigma_3\},\ H_4 = \{\sigma_1, \sigma_4\},\ H_5 = \operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5}).$$

Como $f = X^2 - 3$ é irredutível em $\mathbb{Q}[X]$, f é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$. Pela proposição 3.16, $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$. Analogamente, como $g = X^2 - 5$ é irredutível em $\mathbb{Q}(\sqrt{3})[X]$, g é o polinómio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$ e $\{1, \sqrt{5}\}$ é uma base de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}(\sqrt{3})$. Na demonstração da proposição 3.11, vimos que $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5}\}$ é uma base de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$. Prove que

$$E_{H_1} = \mathbb{Q}(\sqrt{3}, \sqrt{5}),\ E_{H_2} = \mathbb{Q}(\sqrt{5}),\ E_{H_3} = \mathbb{Q}(\sqrt{3}),\ E_{H_4} = \mathbb{Q}(\sqrt{15}),\ E_{H_5} = \mathbb{Q},$$

e confira que, para cada $i \in \{1, \ldots, 5\}$, $\operatorname{Gal}_{E_{H_i}} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = H_i$.

3.9 Extensões de Galois

Se K for uma extensão finita, normal e separável de um corpo F, diz-se que K é uma *extensão de Galois* de F.

Proposição 3.56 *Seja K uma extensão de um corpo F com característica* 0. *Então K é uma extensão de Galois de F se e só se K for um corpo de decomposição de algum polinómio sobre F.*

Demonstração. Resulta das proposições 3.39 e 3.44. ■

Proposição 3.57 *Sejam K uma extensão de Galois de um corpo F e E um corpo intermédio.*

(a) *K é uma extensão de Galois de E.*

(b) *E é o corpo fixo do subgrupo* $\operatorname{Gal}_E K$ *de* $\operatorname{Gal}_F K$.

(c) *Com a notação introduzida na secção anterior,* $\Psi\Phi = \mathrm{id}_{\mathcal{E}}$.

Demonstração. (a) Pela proposição 3.39, K é um corpo de decomposição de algum polinómio f sobre F. Como $F \subseteq E \subseteq K$, K também é um corpo de decomposição de f sobre E. De novo pela proposição 3.39, K é uma extensão finita e normal de E.

Por outro lado, pela proposição 3.41 ((b)), K é uma extensão separável de E. Logo K é uma extensão de Galois de E.

(b) Seja E_0 o corpo fixo de $\operatorname{Gal}_E K$. Pela proposição 3.53, $E \subseteq \Psi\Phi(E) = \Psi(\operatorname{Gal}_E K) = E_0$.

Seja $u \in K \setminus E$. Como K é uma extensão finita de F, K também é uma extensão finita de E. Portanto K é uma extensão algébrica de E e u é algébrico sobre E. Seja p o polinómio mínimo de u sobre E. Como $u \notin E$, $d(p) \geq 2$. Como K é uma extensão normal e separável de E, p decompõe-se em K e todas as raízes de p em K são distintas. Seja $v \in K$ uma raiz de p diferente de u. Como u e v têm o mesmo polinómio mínimo p sobre E, existe, pela proposição 3.47, $\sigma \in \operatorname{Gal}_E K$ tal que $\sigma(u) = v$. Portanto $u \notin E_0$. Logo $E_0 \subseteq E$. Logo $E_0 = E$.

(c) Qualquer que seja $E \in \mathcal{E}$, $E = E_0 = E_{\operatorname{Gal}_E K} = \Psi\Phi(E)$. ■

Proposição 3.58 *Sejam K uma extensão de um corpo F e E um corpo intermédio que é extensão normal de F.*

(a) *Se $\sigma \in \operatorname{Gal}_F K$, então $\sigma(E) = E$ e $\sigma_{|E} \in \operatorname{Gal}_F E$.*

(b) *Se K for uma extensão finita e normal de F, então*

$$\theta : \operatorname{Gal}_F K \to \operatorname{Gal}_F E, \quad \sigma \mapsto \sigma_{|E},$$

é um epimorfismo de grupos e $\ker\theta = \operatorname{Gal}_E K$.

Demonstração. (a) Seja $\sigma \in \operatorname{Gal}_F K$. Seja $u \in E$. Como E é uma extensão normal de F, u é algébrico sobre F e o polinómio mínimo p de u sobre F decompõe-se em E. Pela proposição 3.46, $\sigma(u) \in K$ é uma raiz de p. Como p se decompõe em E, $\sigma(u) \in E$. Assim $\sigma(E) \subseteq E$. Analogamente $\sigma^{-1}(E) \subseteq E$. Donde $\sigma(E) = E$ e $\sigma_{|E} \in \operatorname{Gal}_F E$.

(b) É fácil verificar que θ é um homomorfismo de grupos. Além disso, $\sigma \in \ker\theta \Leftrightarrow \sigma_{|E} = \operatorname{id}_E \Leftrightarrow \sigma \in \operatorname{Gal}_E K$.

Pela proposição 3.39, K é um corpo de decomposição de algum polinómio g sobre F. Como $F \subseteq E \subseteq K$, K também é um corpo de decomposição de g sobre E.

Seja $\tau \in \operatorname{Gal}_F E$. Note-se que $\tau g = g$. Pela proposição 3.30, existe um automorfismo $\sigma : K \to K$ que estende τ. Assim $\sigma \in \operatorname{Gal}_F K$ e $\theta(\sigma) = \sigma_{|E} = \tau$. Logo θ é sobrejetivo. ■

Teorema 3.59 [Teorema fundamental da teoria de Galois] *Seja K uma extensão de Galois de um corpo infinito F.* ([5])

[5] Este teorema também é verdadeiro quando F for finito. Contudo a demonstração neste texto de apoio depende da proposição 3.54 que só demonstrámos para corpos infinitos.

(a) *As aplicações Φ e Ψ da correspondência de Galois são invertíveis e uma é a inversa da outra.*

(b) *Para cada corpo intermédio E,*

$$[K : E] = |\operatorname{Gal}_E K| \quad e \quad [E : F] = [\operatorname{Gal}_F K : \operatorname{Gal}_E K].$$

(c) *Um corpo intermédio E é uma extensão normal de F se e só se $\operatorname{Gal}_E K \trianglelefteq \operatorname{Gal}_F K$. Neste caso,*

$$\operatorname{Gal}_F E \cong \frac{\operatorname{Gal}_F K}{\operatorname{Gal}_E K}.$$

Demonstração. (a) Pela proposição 3.54, $\Phi\Psi = \mathrm{id}_{\mathcal{S}}$. Pela proposição 3.57, $\Psi\Phi = \mathrm{id}_{\mathcal{E}}$. Logo Φ e Ψ são invertíveis e uma é a inversa da outra.

(b) Seja E um corpo intermédio. Pela sobrejetividade de Ψ, $E = \Psi(H) = E_H$, para algum $H \leq \operatorname{Gal}_F K$. Por (a), $H = \Phi\Psi(H) = \operatorname{Gal}_E K$. Pela proposição 3.54 (b),

$$|\operatorname{Gal}_E K| = [K : E].$$

Assim $|\operatorname{Gal}_F K| = [K : F] = [K : E][E : F] = |\operatorname{Gal}_E K|[E : F]$. Donde

$$[E : F] = [\operatorname{Gal}_F K : \operatorname{Gal}_E K].$$

(c) Suponhamos que $\operatorname{Gal}_E K \trianglelefteq \operatorname{Gal}_F K$. Seja p um polinómio irredutível em $F[X]$ que tem uma raiz $u \in E$, com vista a mostrar que p se decompõe em E. Como K é uma extensão normal de F, p decompõe-se em K. Assim basta mostrar que qualquer raiz v de p em K pertence a E. Seja $v \in K$ uma raiz de p. O polinómio mínimo de u e de v sobre F é p, a menos do produto por uma unidade. Pela proposição 3.39, K é um corpo de decomposição de algum polinómio sobre F. Pela proposição 3.47, existe $\sigma \in \operatorname{Gal}_F K$ tal que $\sigma(u) = v$.

Seja $\tau \in \operatorname{Gal}_E K$. Como $\operatorname{Gal}_E K \trianglelefteq \operatorname{Gal}_F K$, $(\operatorname{Gal}_E K)\sigma = \sigma(\operatorname{Gal}_E K)$ e $\tau\sigma = \sigma\tau'$, para algum $\tau' \in \operatorname{Gal}_E K$. Como $u \in E$, $\tau(v) = \tau(\sigma(u)) = \sigma(\tau'(u)) = \sigma(u) = v$. Logo v pertence ao corpo fixo de $\operatorname{Gal}_E K$ que é igual a E por (a). Logo E é uma extensão normal de F.

Reciprocamente, suponhamos que E é uma extensão normal de F. Pela proposição 3.58, existe um epimorfismo de grupos $\theta : \operatorname{Gal}_F K \to \operatorname{Gal}_F E$ tal que $\ker\theta = \operatorname{Gal}_E K$. Portanto $\operatorname{Gal}_E K = \ker\theta \trianglelefteq \operatorname{Gal}_F K$ e, pelo primeiro teorema de isomorfismo para grupos, $\operatorname{Gal}_F E \cong \operatorname{Gal}_F K/\operatorname{Gal}_E K$. ∎

Exercícios

3.9.1 Justifique que, no exemplo 3.55, $E_{H_1}, \ldots, E_{H_5}$ são os únicos corpos intermédios da extensão $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ de $\mathbb{Q}$. Portanto, o exemplo 3.55 descreve completamente a correspondência de Galois desta extensão.

3.9.2 Descreva a correspondência de Galois da extensão $\mathbb{Q}(i, \sqrt{2})$ de $\mathbb{Q}$.

3.9.3 Descreva a correspondência de Galois do corpo de decomposição do polinómio $(X^3 - 2)(X^2 - 3)$ sobre $\mathbb{Q}$.

3.10 Raízes primitivas da unidade

Seja F um corpo com característica 0. Uma raiz ζ do polinómio $X^n - 1$, pertencente a alguma extensão de F, chama-se *raiz n-ésima da unidade*.

Como a característica de F é 0, a derivada nX^{n-1} do polinómio $X^n - 1 \in F[X]$ não é nula. Os polinómios nX^{n-1} e $X^n - 1$ são relativamente primos, porque X é o único (a menos do produto por unidades) polinómio irredutível que divide nX^{n-1} e X não divide $X^n - 1$. Pela proposição 3.43, $X^n - 1$ é separável. Seja L uma extensão de F onde o polinómio $X^n - 1$ se decompõe. O conjunto U_n das raizes da unidade que pertencem a L é um subgrupo multiplicativo de $L \setminus 0$. De facto, é trivial que $1 \in U_n \subseteq L \setminus 0$ e, se $\zeta, \tau \in U_n$, então

$$1 = \zeta^n \tau^n = (\zeta\tau)^n \quad \text{e} \quad 1 = (\zeta\zeta^{-1})^n = \zeta^n(\zeta^{-1})^n = (\zeta^{-1})^n,$$

o que mostra que $\zeta\tau, \zeta^{-1} \in U_n$. Como $X^n - 1$ é separável, $|U_n| = n$. Pela proposição 1.13, U_n é cíclico. Chama-se *raiz n-ésima primitiva da unidade* a qualquer gerador do grupo U_n.

Proposição 3.60 *Seja F um corpo com característica 0 que contém uma raiz n-ésima primitiva da unidade. Para cada divisor positivo d de n, F contém uma raiz d-ésima primitiva da unidade.*

Demonstração. Seja $x \in F$ uma raiz n-ésima primitiva da unidade. Suponhamos que $n = dc$, onde $d, c \in \mathbb{N}$. Pela proposição 0.29, $|x^c| = d$. Donde $(x^c)^d = 1$ e $x^c \in U_d$. Como $|x^c| = d = |U_d|$, x^c gera U_d e x^c é uma raiz d-ésima primitiva da unidade. ■

Proposição 3.61 *Seja F um corpo de característica 0. Seja ζ uma raiz n-ésima primitiva da unidade que pertence a alguma extensão L de F. Então $K = F(\zeta)$ é uma extensão normal de F e o grupo $\operatorname{Gal}_F K$ é Abeliano.*

Demonstração. O corpo K contém as potências de ζ e, portanto, contém todas as raízes de $X^n - 1$ que são $\zeta, \zeta^2, \ldots, \zeta^n = 1$. Assim $K = F(\zeta) = F(\zeta, \zeta^2, \ldots, \zeta^n)$ é um corpo de decomposição de $X^n - 1$ sobre F. Pela proposição 3.39, K é uma extensão normal de F.

Sejam $\sigma, \tau \in \operatorname{Gal}_F K$. Pela proposição 3.46, $\sigma(\zeta) = \zeta^k$ e $\tau(\zeta) = \zeta^l$, para alguns $k, l \in \{1, \ldots, n\}$. Assim $\sigma\tau(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = (\zeta^k)^l = \zeta^{kl}$. Analogamente $\tau\sigma(\zeta) = \zeta^{kl}$. Pela proposição 3.49, $\sigma\tau = \tau\sigma$. Logo $\operatorname{Gal}_F K$ é Abeliano. ■

Proposição 3.62 *Seja F um corpo de característica 0 que contém uma raiz n-ésima primitiva da unidade. Seja u uma raiz de um polinómio $X^n - c \in F[X]$ pertencente a alguma extensão de F. Então $K = F(u)$ é uma extensão normal de F e $\operatorname{Gal}_F K$ é Abeliano.*

Demonstração. Seja $\zeta \in F$ uma raiz n-ésima primitiva da unidade. Qualquer que seja $k \in \mathbb{N}$, $(\zeta^k u)^n = (\zeta^k)^n u^n = (\zeta^n)^k c = c$. Como $\zeta, \zeta^2, \ldots, \zeta^n = 1$ são elementos distintos de F, $\zeta u, \zeta^2 u, \ldots, \zeta^n u = u$ são n raízes distintas de $X^n - c$ pertencentes a K. Assim $X^n - c$ decompõe-se em K e $K = F(u) =$

$F(\zeta u, \zeta^2 u, \ldots, \zeta^n u)$ é um corpo de decomposição de $X^n - c$ sobre F. Pela proposição 3.39, K é uma extensão normal de F.

Sejam $\sigma, \tau \in \operatorname{Gal}_F K$. Pela proposição 3.46, $\sigma(u) = \zeta^k u$ e $\tau(u) = \zeta^l u$, para alguns $k, l \in \{1, \ldots, n\}$. Como $\zeta \in F$, $\sigma(\zeta) = \zeta$ e, portanto,

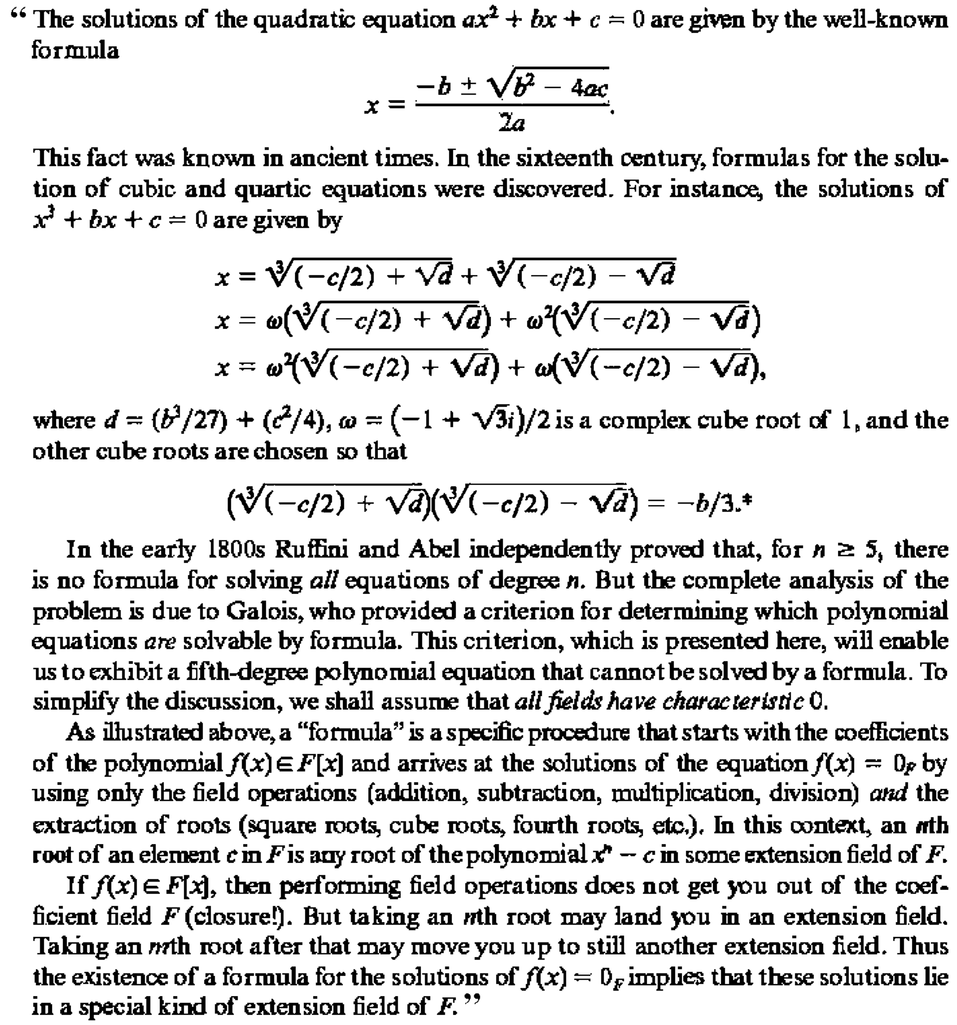
$$(\sigma\tau)(u) = \sigma(\tau(u)) = \sigma(\zeta^l u) = \sigma(\zeta^l)\sigma(u) = \zeta^l \zeta^k u = \zeta^{k+l} u.$$

Analogamente $(\tau\sigma)(u) = \zeta^{k+l} u$. Pela proposição 3.49, $\sigma\tau = \tau\sigma$. Logo $\operatorname{Gal}_F K$ é Abeliano. ■

Exercícios

3.10.1 Seja $\zeta \in \mathbb{C}$ uma raiz décima primitiva da unidade. Descreva $\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$.

3.11 Critério de Galois



“ The solutions of the quadratic equation $ax^2 + bx + c = 0$ are given by the well-known formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This fact was known in ancient times. In the sixteenth century, formulas for the solution of cubic and quartic equations were discovered. For instance, the solutions of $x^3 + bx + c = 0$ are given by

$$x = \sqrt[3]{(-c/2) + \sqrt{d}} + \sqrt[3]{(-c/2) - \sqrt{d}}$$
$$x = \omega\left(\sqrt[3]{(-c/2) + \sqrt{d}}\right) + \omega^2\left(\sqrt[3]{(-c/2) - \sqrt{d}}\right)$$
$$x = \omega^2\left(\sqrt[3]{(-c/2) + \sqrt{d}}\right) + \omega\left(\sqrt[3]{(-c/2) - \sqrt{d}}\right),$$

where $d = (b^3/27) + (c^2/4)$, $\omega = (-1 + \sqrt{3}i)/2$ is a complex cube root of 1, and the other cube roots are chosen so that

$$\left(\sqrt[3]{(-c/2) + \sqrt{d}}\right)\left(\sqrt[3]{(-c/2) - \sqrt{d}}\right) = -b/3.*$$

In the early 1800s Ruffini and Abel independently proved that, for $n \geq 5$, there is no formula for solving *all* equations of degree n. But the complete analysis of the problem is due to Galois, who provided a criterion for determining which polynomial equations *are* solvable by formula. This criterion, which is presented here, will enable us to exhibit a fifth-degree polynomial equation that cannot be solved by a formula. To simplify the discussion, we shall assume that *all fields have characteristic* 0.

As illustrated above, a “formula” is a specific procedure that starts with the coefficients of the polynomial $f(x) \in F[x]$ and arrives at the solutions of the equation $f(x) = 0_F$ by using only the field operations (addition, subtraction, multiplication, division) *and* the extraction of roots (square roots, cube roots, fourth roots, etc.). In this context, an *n*th root of an element c in F is any root of the polynomial $x^n - c$ in some extension field of F.

If $f(x) \in F[x]$, then performing field operations does not get you out of the coefficient field F (closure!). But taking an *n*th root may land you in an extension field. Taking an *m*th root after that may move you up to still another extension field. Thus the existence of a formula for the solutions of $f(x) = 0_F$ implies that these solutions lie in a special kind of extension field of F. ”

[Hungerford-2, p. 423]

Nesta secção, apenas estudamos corpos de característica 0.

Um corpo K chama-se *extensão radical* de um subcorpo F de característica 0 se existir uma cadeia finita de corpos intermédios

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K$$

tal que, qualquer que seja $i \in \{1, \ldots, t\}$, $F_i = F_{i-1}(u_i)$, onde $u_i^{n_i} \in F_{i-1}$, para algum $n_i \in \mathbb{N}$. Note-se que as extensões radicais são finitas.

Sejam F um corpo de característica 0 e $f \in F[X] \setminus F$. Diz-se que o polinómio f é *resolúvel por radicais* sobre F (ou que a equação polinomial $f(X) = 0$ é *resolúvel por radicais* sobre F) se existir uma extensão radical de F que contém um corpo de decomposição de f sobre F. Note-se que, com esta definição, a resolubilidade por radicais de f não implica que se conheça um algoritmo para calcular as raízes de f partindo dos coeficientes de f e utilizando as quatro operações definidas nos corpos e a extração de raízes. Por outro lado, a existência de um tal algoritmo implica a resolubilidade por radicais de f. Se K for um corpo de decomposição de f sobre F, então K é um corpo de decomposição de f sobre K e, trivialmente, f é resolúvel por radicais sobre K.

Exemplo 3.63 Pela citação de [Hungerford-2] reproduzida acima, as raízes do polinómio $X^3 + 3X + 2$ em $\mathbb{C}$ são

$$\sqrt[3]{-1+\sqrt{2}} + \sqrt[3]{-1-\sqrt{2}}, \ \ \omega\sqrt[3]{-1+\sqrt{2}} + \omega^2\sqrt[3]{-1-\sqrt{2}}, \ \ \omega^2\sqrt[3]{-1+\sqrt{2}} + \omega\sqrt[3]{-1-\sqrt{2}}.$$

Todas estas soluções pertencem ao último termo da seguinte cadeia de extensões de corpos

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}\left(\omega, \sqrt{2}\right) \subseteq \mathbb{Q}\left(\omega, \sqrt{2}, \sqrt[3]{-1+\sqrt{2}}\right) \subseteq \mathbb{Q}\left(\omega, \sqrt{2}, \sqrt[3]{-1+\sqrt{2}}, \sqrt[3]{-1-\sqrt{2}}\right).$$

Claramente o último termo é uma extensão radical de $\mathbb{Q}$ e o polinómio $X^3 + 3X + 2$ é resolúvel por radicais sobre $\mathbb{Q}$.

Proposição 3.64 *Sejam K e L corpos de decomposição de um polinómio f sobre um corpo F. Então* $\operatorname{Gal}_F K \cong \operatorname{Gal}_F L$.

Demonstração. Pela proposição 3.30, existe um F-isomorfismo $\tau : K \to L$. Mostre que $\operatorname{Gal}_F K \to \operatorname{Gal}_F L$, $\sigma \mapsto \tau\sigma\tau^{-1}$, é um isomorfismo de grupos. ■

Sejam F um corpo e $f \in F[X] \setminus F$. Chama-se *grupo de Galois* de f sobre F a qualquer grupo $\operatorname{Gal}_F K$, onde K é um corpo de decomposição de f sobre F. Como estes grupos são todos isomorfos, é usual chamar qualquer um deles ***o** grupo de Galois* de f.

Teorema 3.65 [Critério de Galois] *Sejam F um corpo de característica 0 e $f \in F[X] \setminus F$. O polinómio f é resolúvel por radicais sobre F se e só se o grupo de Galois de f sobre F for resolúvel.*

Neste curso demonstraremos apenas que, *se f for resolúvel por radicais sobre F, então o grupo de Galois de f é resolúvel sobre F.* A demonstração está mais adiante. Esta afirmação será utilizada para encontrar um polinómio que não é resolúvel por radicais. Em [Hungerford, Chapter V, Section 9], está uma demonstração da afirmação recíproca.

Antes da demonstração, vejamos alguns resultados auxiliares e exemplos.

Proposição 3.66 *Sejam F um corpo de característica 0 e $g, h \in F[X]\backslash F$ polinómios resolúveis por radicais sobre F. Então o polinómio $f = gh$ é resolúvel por radicais sobre F.*

Demonstração. Existem cadeias finitas de subcorpos

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K \quad \text{e} \quad F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_s = L,$$

$$\text{onde} \quad F_i = F_{i-1}(u_i), \quad u_i^{n_i} \in F_{i-1}, \quad E_j = E_{j-1}(v_j), \quad v_j^{m_j} \in E_{j-1},$$

K contém um corpo de decomposição de g sobre F, e L contém um corpo de decomposição de h sobre F. Seja $K_0 = K$ e, para cada $j \in \{0, \ldots, s\}$, seja $K_j = K_{j-1}(v_j)$. É fácil provar por indução em $j \in \{1, \ldots, s\}$ que $E_j \subseteq K_j$. Em particular, $L = E_s \subseteq K_s$. Assim, para cada $j \in \{1, \ldots, s\}$, $v_j^{m_j} \in E_{j-1} \subseteq K_{j-1}$. Donde

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s$$

e K_s é uma extensão radical de F. Como g se decompõe em $K \subseteq K_s$ e h se decompõe em $L \subseteq K_s$, $f = gh$ também se decompõe em K_s. Portanto K_s contém um corpo de decomposição de f sobre F. Logo f é resolúvel por radicais sobre F. ■

Proposição 3.67 *Sejam F um corpo de característica 0 e $f \in F[X] \backslash F$ um polinómio de grau n. Então o grupo de Galois de f sobre F é isomorfo a um subgrupo de S_n.*

Demonstração. Seja K um corpo de decomposição de f sobre F. Suponhamos que $f = af_1^{r_1} \cdots f_t^{r_t}$, onde $a \in F\backslash 0$, $f_1, \ldots, f_t \in F[X]$ são polinómios irredutíveis mónicos distintos, e $r_1, \ldots, r_t \in \mathbb{N}$. Pela proposição 3.44, $f_1, \ldots, f_t$ são separáveis. Sejam $i, j \in \{1, \ldots, t\}$ com $i \neq j$. Se f_i e f_j tivessem uma raiz comum $u \in K$, então f_i e f_j seriam ambos o polinómio mínimo de u sobre F, o que é absurdo pois $f_i \neq f_j$. Logo $g = f_1 \cdots f_t$ é separável e K é um corpo de decomposição de g sobre F. Pela proposição 3.51, $\operatorname{Gal}_F K$ é isomorfo a um subgrupo e S_m, onde $m = d(g) \leq n = d(f)$. Para cada $\sigma \in S_m$,

$$\overline{\sigma} : \{1, \ldots, n\} \to \{1, \ldots, n\}, \quad i \mapsto \sigma(i) \text{ se } i \leq m, \quad \text{e} \quad i \mapsto i \text{ se } i > m,$$

é uma permutação de $\{1, \ldots, n\}$. É fácil ver que $S_m \to S_n$, $\sigma \mapsto \overline{\sigma}$, é um monomorfismo de grupos. É fácil concluir que $\operatorname{Gal}_F K$, o grupo de Galois de f sobre F, também é isomorfo a um subgrupo de S_n. ■

Exemplo 3.68 Sejam F um corpo de característica 0 e $f \in F[X \setminus F$ um polinómio de grau $n \leq 4$. Pela proposição anterior, o grupo G de Galois de f sobre F é isomorfo a um subgrupo de S_n. Como $n \leq 4$, S_n é resolúvel e, portanto, G também é resolúvel. Pelo critério de Galois, f é resolúvel por radicais sobre F.

Exemplo de um polinómio que não é resolúvel por radicais

Lema 3.69 *Seja G um subgrupo de S_5 que contém uma transposição $\sigma = (r, s)$ e um ciclo τ de comprimento 5. Então $G = S_5$.*

Demonstração. Mostre que, para algum $k \in \mathbb{N}$, τ^k é da forma (r, s, x, y, z). Para simplificar a escrita, suponhamos que $\sigma = (1, 2)$ e $\tau^k = (1, 2, 3, 4, 5)$.

Mostre que $(1, 2), (2, 3), (3, 4), (1, 5) \in G$. (Sugestão: considere $\tau^k \sigma \tau^{-k}$, para $k \geq 1$.)

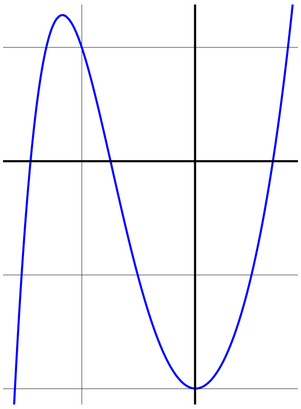
Mostre que $(1, 3), (1, 4), (4, 5) \in G$. (Sugestão: $(1, 2)(2, 3)(1, 2) = ?$)

Mostre que todas as transposições pertencem a G.

Logo $G = S_n$. ■

Exemplo 3.70 Vamos provar que o polinómio $f = X^5 + 4X^2 - 2$ não é resolúvel por radicais sobre $\mathbb{Q}$.

Com argumentos elementares de Cálculo, deduz-se que a função polinomial $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^5 + 4x^2 - 2$, tem apenas 3 raízes reais, as quais são distintas. Assim $f = gh$, onde $g, h \in \mathbb{R}[X]$, g tem grau 3 e decompõe-se em $\mathbb{R}$, e h tem grau 2 e duas raízes complexas não reais conjugadas que se podem calcular pela fórmula resolvente para as equações polinomiais do segundo grau. Portanto f é separável, decompõe-se em $\mathbb{C}$ e $\mathbb{C}$ contém um corpo de decomposição K de f sobre $\mathbb{Q}$. Pela proposição 3.56, K é uma extensão de Galois de $\mathbb{Q}$.



Seja R o conjunto das raízes de f pertencentes a K. Pela demonstração da proposição 3.51,

$$\theta : \operatorname{Gal}_{\mathbb{Q}} K \to \operatorname{Sym} R, \quad \sigma \mapsto \sigma_{|R},$$

é um monomorfismo de grupos. A aplicação conjugação $\gamma : \mathbb{C} \to \mathbb{C}$, $x \mapsto \overline{x}$, é um $\mathbb{Q}$-automorfismo de $\mathbb{C}$ que deixa invariantes as 3 raízes reais de f e aplica cada uma das 2 raízes não reais na outra. Como K é um corpo de decomposição de f sobre $\mathbb{Q}$, deduz-se que $\gamma(K) = K$, $\gamma_{|K} : K \to K$ pertence a $\operatorname{Gal}_{\mathbb{Q}} K$, e $\theta(\gamma_{|K}) \in \theta(\operatorname{Gal}_{\mathbb{Q}} K) \leq \operatorname{Sym} R$ é uma transposição.

Pelo critério de Eisenstein, f é irredutível em $\mathbb{Q}[X]$. Se u for uma raiz de f em K, então f é o polinómio mínimo de u sobre $\mathbb{Q}$ e $[\mathbb{Q}(u) : \mathbb{Q}] = 5$. Donde $5 \mid [K : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = [K : \mathbb{Q}]$. Pelo teorema fundamental da teoria de Galois (teorema 3.59), $[K : \mathbb{Q}] = |\operatorname{Gal}_{\mathbb{Q}} K|$. Pelo teorema de Cauchy (teorema 1.10), $\operatorname{Gal}_{\mathbb{Q}} K$ tem um elemento τ de ordem 5. Assim $\theta(\tau) \in \theta(\operatorname{Gal}_{\mathbb{Q}} K) \leq \operatorname{Sym} R$ é um ciclo de comprimento 5.

Pelo lema 3.69, $\theta(\operatorname{Gal}_{\mathbb{Q}} K) = \operatorname{Sym} R$. Como

$$\operatorname{Gal}_{\mathbb{Q}} K \cong \theta(\operatorname{Gal}_{\mathbb{Q}} K) = \operatorname{Sym} R \cong S_5$$

e S_5 não é resolúvel, $\operatorname{Gal}_{\mathbb{Q}} K$ também não é resolúvel. Pelo critério de Galois, f não é resolúvel por radicais sobre $\mathbb{Q}$.

Demonstração parcial do critério de Galois

Lema 3.71 *Seja*

$$F \subseteq E \subseteq E(v) \subseteq C$$

uma cadeia de corpos de característica 0, *onde C é algebricamente fechado, $E(v)$ é uma extensão finita de F, E é uma extensão normal de F e $v^k \in E$, para algum $k \in \mathbb{N}$.*

Então existe um subcorpo M de C que contém $E(v)$, é uma extensão radical de E e é uma extensão normal de F.

Demonstração. Pela proposição 3.39, E é um corpo de decomposição de algum polinómio g sobre F. Sejam $u_1, \ldots, u_r$ as raízes de g em E. Seja $p \in F[X]$ o polinómio mínimo de v sobre F. Como p se decompõe em C, C contém um corpo de decomposição M de p sobre $E(v)$. Sejam $v = v_1, v_2, \ldots, v_s$ as raízes de p em M. Então

$$\begin{aligned} M &= E(v)(v, v_2, \ldots, v_s) = E(v)(v, v_2, \ldots, v_s) = E(v, v_2, \ldots, v_s) \\ &= F(u_1, \ldots, u_r)(v, v_2, \ldots, v_s) = F(u_1, \ldots, u_r, v, v_2, \ldots, v_s), \end{aligned}$$

o que mostra que M é um corpo de decomposição de gp sobre F. Pela proposição 3.39, M é uma extensão normal de F. Como p é mónico e irredutível em $F[X]$, p é o polinómio mínimo de todas as suas raízes sobre F. Seja $i \in \{1, \ldots, s\}$. Pela proposição 3.47, existe $\sigma_i \in \operatorname{Gal}_F M$ tal que $\sigma_i(v) = v_i$. Pela proposição 3.58, $\sigma_i(E) = E$. Então

$$v_i^k = (\sigma_i(v))^k = \sigma_i(v^k) \in E \subseteq E(v_1, \ldots, v_{i-1}).$$

Como

$$E \subseteq E(v) = E(v_1) \subseteq E(v_1, v_2) \subseteq \cdots \subseteq E(v_1, v_2, \cdots, v_s) = M,$$

M é uma extensão radical de E. ■

Lema 3.72 *Seja*

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t \subseteq C$$

uma cadeia de corpos de característica 0 *tal que* C *é algebricamente fechado e, qualquer que seja* $i \in \{1, \dots, t\}$, $F_i = F_{i-1}(u_i)$, *onde* $u_i^{n_i} \in F_{i-1}$ *e* $n_i \in \mathbb{N}$.

Então existe um subcorpo M *de* C *que contém* F_t *e é uma extensão radical e normal de* F *.*

Demonstração. Por indução em t. Se $t = 0$, basta tomar $M = F$.

Suponhamos que $t \geq 1$. Pela hipótese de indução, existe um subcorpo E de C que contém F_{t-1} e é uma extensão radical e normal de F. Como u_t é raiz do polinómio $X^{n_t} - u_t^{n_t} \in F_{t-1}[X] \subseteq E[X]$, u_t é algébrico sobre E e $E(u_t)$ é uma extensão finita de E. Como E é uma extensão radical de F, E é uma extensão finita de F. Portanto $E(u_t)$ é uma extensão finita de F.

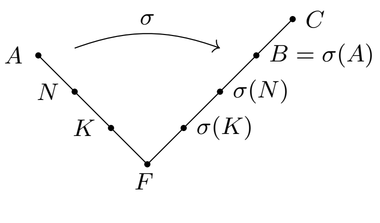
Pelo lema anterior, existe um subcorpo M de C que contém $E(u_t)$, é uma extensão radical de E e é uma extensão normal de F. Como E é uma extensão radical de F, M também é uma extensão radical de F.

Claramente $F_t = F_{t-1}(u_t) \subseteq E(u_t) \subseteq M$. ■

Proposição 3.73 *Sejam* F *um corpo de característica* 0, C *uma extensão algebricamente fechada de* F *e* $f \in F[X] \setminus F$.

Se f *for resolúvel por radicais sobre* F, *então existe um subcorpo* M *de* C *que é extensão radical e normal de* F *e contém um corpo de decomposição de* f *sobre* F.

Demonstração. Suponhamos que f é resolúvel por radicais sobre F. Pela definição, existe uma extensão radical N de F que contém um corpo de decomposição K de f sobre F. Seja A um fecho algébrico de N. Como N é uma extensão algébrica de F, A também é um fecho algébrico de F. Como C é algebricamente fechado, C contém um fecho algébrico B de F. Pelo teorema 3.36, existe um F-isomorfismo $\sigma : A \to B$. Então $\sigma(N)$ é uma extensão radical de F e contém $\sigma(K)$ que é um corpo de decomposição de f sobre F. Suponhamos que



$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = \sigma(N),$$

onde, qualquer que seja $i \in \{1, \dots, t\}$,
$F_i = F_{i-1}(u_i)$ e $u_i^{n_i} \in F_{i-1}$, para algum $n_i \in \mathbb{N}$. Pelo lema anterior, existe um subcorpo M de C que contém F_t e é uma extensão radical e normal de F. Assim M também contém $\sigma(K)$. ■

Proposição 3.74 *Sejam* F *um corpo de característica* 0, K *uma extensão normal e radical de* F *e* E *um corpo intermédio. Se* E *for uma extensão normal de* F, *então o grupo* $\operatorname{Gal}_F E$ *é resolúvel.*

Demonstração. Como K é uma extensão radical de F, existe uma cadeia de subcorpos de K

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K,$$

onde, qualquer que seja $i \in \{1, \ldots, t\}$, $F_i = F_{i-1}(u_i)$ e $u_i^{n_i} \in F_{i-1}$, para algum $n_i \in \mathbb{N}$. Seja $n = \text{mmc}\{n_1, \ldots, n_t\}$. Seja ζ uma raiz n-ésima primitiva da unidade pertencente a algum corpo de decomposição de $X^n - 1$ sobre K. Para cada $i \in \{0, \ldots, t\}$, seja $E_i = F_i(\zeta)$. Então $E_0 = F(\zeta)$, $\zeta^n = 1 \in F$ e, para $i > 0$,

$$E_i = F_i(\zeta) = F_{i-1}(u_i)(\zeta) = F_{i-1}(\zeta)(u_i) = E_{i-1}(u_i)$$

e $u_i^{n_i} \in F_{i-1} \subseteq E_{i-1}$. Assim $F \subseteq E_0 \subseteq E_1 \subseteq \cdots \subseteq E_t$ e E_t é uma extensão radical de F que contém $K = F_t$. Como K é uma extensão radical de F, K é uma extensão finita de F. Pela hipótese, K também é uma extensão normal de F. Pela proposição 3.39, K é um corpo de decomposição de algum polinómio f sobre F. Assim

$$E_t = F_t(\zeta) = K(\zeta) = K(\zeta, \zeta^2, \ldots, \zeta^n)$$

é um corpo de decomposição do polinómio $(X^n - 1)f$ sobre F. Pela proposição 3.39, E_t é uma extensão finita e normal de F. Pela proposição 3.44, E_t é uma extensão separável de F. Logo $L = E_t$ é uma extensão de Galois de F. A seguir, vamos provar que o grupo $\text{Gal}_F L$ é resolúvel, mostrado que, na cadeia de subgrupos

$$\{\text{id}_L\} = \text{Gal}_{E_t} L \subseteq \text{Gal}_{E_{t-1}} L \subseteq \cdots \subseteq \text{Gal}_{E_1} L \subseteq \text{Gal}_{E_0} L \subseteq \text{Gal}_F L,$$

cada subgrupo é normal no seguinte e o quociente de cada subgrupo pelo anterior é Abeliano.

Pela proposição 3.61, E_0 é uma extensão normal de F e $\text{Gal}_F E_0$ é Abeliano. Pelo teorema fundamental (teorema 3.59), $\text{Gal}_{E_0} L \trianglelefteq \text{Gal}_F L$ e o grupo quociente $\text{Gal}_F L / \text{Gal}_{E_0} L$ é isomorfo ao grupo Abeliano $\text{Gal}_F E_0$. Seja agora $i \in \{1, \ldots, t\}$. Note-se que $\zeta \in E_{i-1}$ e u_i é uma raiz do polinómio $X^n - u_i^n \in E_{i-1}[X]$. Pela proposição 3.62, $E_i = E_{i-1}(u_i)$ é uma extensão normal de E_{i-1} e $\text{Gal}_{E_{i-1}} E_i$ é Abeliano. Como L é uma extensão de Galois de F, L é uma extensão finita e normal de F. Como E_{i-1} é um corpo intermédio, L é uma extensão finita de E_{i-1}. Pela proposição 3.38, L é uma extensão normal de E_{i-1}. Como estamos a trabalhar com corpos de característica 0, L também é uma extensão separável de E_{i-1}. Logo L é uma extensão de Galois de E_{i-1}. Note-se que $E_{i-1} \subseteq E_i \subseteq L$ e L também é uma extensão normal de E_i. Pelo teorema fundamental (teorema 3.59), $\text{Gal}_{E_i} L \trianglelefteq \text{Gal}_{E_{i-1}} L$ e o grupo quociente $\text{Gal}_{E_{i-1}} L / \text{Gal}_{E_i} L$ é isomorfo ao grupo Abeliano $\text{Gal}_{E_{i-1}} E_i$. Logo $\text{Gal}_F L$ é resolúvel.

Seja agora E um corpo intermédio ($F \subseteq E \subseteq K$) que é uma extensão normal de F. Pelo teorema 3.59, $\text{Gal}_E L \trianglelefteq \text{Gal}_F L$ e $\text{Gal}_F E \cong \text{Gal}_F L / \text{Gal}_E L$. Pela proposição 1.28, $\text{Gal}_F E$ é resolúvel. ■

Proposição 3.75 *Sejam F um corpo de característica 0 e $f \in F[X]\backslash F$. Se f for resolúvel por radicais sobre F, então o grupo de Galois de f sobre F é resolúvel.*

Demonstração. Suponhamos que f é resolúvel por radicais sobre F. Seja C uma extensão algebricamente fechada de F. Pela proposição 3.73, existe um subcorpo K de C que é extensão radical e normal de F e contém um corpo de decomposição E de f sobre F. Pela proposição 3.39, E é uma extensão normal de F. Pela proposição 3.74, $\mathrm{Gal}_F E$, o grupo de Galois de f sobre F, é resolúvel. ■

Exercícios

3.11.1 Para cada um dos números seguintes, encontre uma extensão radical de $\mathbb{Q}$ que o contém: $\sqrt[4]{1+\sqrt{7}} - \sqrt[5]{2+\sqrt{5}}$, $(\sqrt[5]{\sqrt{2}+i})/\sqrt[3]{5}$, $(\sqrt[3]{3-\sqrt{2}})/(4+\sqrt{2})$.

3.11.2 Para cada um dos polinómios seguintes, calcule o respetivo grupo de Galois sobre $\mathbb{Q}$: X^6-4X^3+4, X^4-5X^2+6, X^5+6X^3+9X, X^4+3X^3-2X-6.

3.11.3 Determine se os polinómios seguintes são resolúveis por radicais sobre $\mathbb{Q}$: $X^6+2X^3+1=0$, $3X^5-15X+5=0$, $2X^5-5X^4+5=0$, $X^5-X^4-16X+16=0$.

3.11.4 Demonstre que, se $f \in \mathbb{Q}[X]$ for irredutível de grau 5 e tiver três raízes reais e duas raízes complexas não reais, então f não é resolúvel por radicais sobre $\mathbb{Q}$.

Chapter 4

Teorema fundamental da Álgebra

O teorema fundamental da Álgebra afirma que todo o polinómio $f \in \mathbb{C}[X] \setminus \mathbb{C}$ tem uma raiz em $\mathbb{C}$. Não existem demonstrações apenas algébricas deste teorema, pois todas elas utilizam, de alguma forma, a completude dos números reais. O seu nome foi atribuído num tempo em que a Álgebra se dedicava principalmente ao estudo das equações polinomiais.

Conhecem-se muitas demonstrações do teorema fundamental da Álgebra, algumas das quais podem encontrar-se em [Fine&al]. A demonstração seguinte, uma das mais curtas, resulta do teorema de Liouville da Análise Complexa e, provavelmente, já será conhecida pelos estudantes.

O teorema de Liouville afirma que toda a função holomorfa limitada $\phi : \mathbb{C} \to \mathbb{C}$ é constante. Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Suponhamos que f não tem uma raiz em $\mathbb{C}$. É fácil verificar que $|f(z)| \to +\infty$ quando $z \to \infty$. Assim existe $r \in \mathbb{R}^+$ tal que $|f(z)| \geq 1$ sempre que $|z| \geq r$. Como $S = \{z \in \mathbb{C} : |z| \leq r\}$ é compacto e a função

$$\alpha : \mathbb{C} \to \mathbb{R}, \quad z \mapsto |f(z)|,$$

é contínua, $\alpha(S)$ é compacto e, portanto, tem um mínimo $\mu \in \mathbb{R}^+$. Seja $\epsilon = \min\{1, \mu\}$. Então, qualquer que seja $z \in \mathbb{C}$, $|f(z)| \geq \epsilon$. A função

$$\phi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto f(z)^{-1},$$

é holomorfa e, qualquer que seja $z \in \mathbb{C}$, $|\phi(z)| \leq \epsilon^{-1}$. Pelo teorema de Liouville, ϕ deveria ser constante, o que é falso.

4.1 Polinómios simétricos

Seja R um anel comutativo. Um polinómio $f \in R[X_1, \ldots, X_n]$ diz-se *simétrico* nas variáveis $X_1, \ldots, X_n$ se, para qualquer $\sigma \in S_n$,

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Os polinómios

$$X_1^2X_2^2, \quad 2X_1+2X_2 \quad \text{e} \quad X_1^2X_2^2+2X_1+2X_2-1$$

são simétricos nas variáveis X_1, X_2. Os polinómios da forma

$$p_k(X_1,\ldots,X_n)=\sum_{j_1+\cdots+j_n=k} X_1^{j_1}\cdots X_n^{j_n}, \quad \text{onde} \quad k\in\mathbb{N}_0,$$

são simétricos nas variáveis $X_1,\ldots,X_n$ e chamam-se *polinómios simétricos homogéneos completos* nas variáveis $X_1,\ldots,X_n$.

Na álgebra de polinómios $R[X_1,\ldots,X_n][X]$,

$$\begin{aligned}(X-X_1)\cdots(X-X_n)&=X^n-(X_1+\cdots+X_n)X^{n-1}+\cdots+(-1)^nX_1\cdots X_n\\ &=X^n+\sum_{k=1}^n(-1)^k\left(\sum_{j_1<\cdots<j_k}X_{j_1}\cdots X_{j_k}\right)X^{n-k}.\end{aligned}$$

Os polinómios

$$s_k=\sum_{j_1<\cdots<j_k}X_{j_1}\cdots X_{j_k}, \quad \text{onde} \quad k\in\{1,\ldots,n\},$$

são simétricos nas variáveis $X_1,\ldots,X_n$ e chamam-se *polinómios simétricos elementares* nas variáveis $X_1,\ldots,X_n$. Com esta notação,

$$(X-X_1)\cdots(X-X_n)=X^n+\sum_{k=1}^n(-1)^ks_kX^{n-k}. \tag{4.1}$$

Consideremos os monómios primitivos nas variáveis $X_1,\ldots,X_n$ totalmente ordenados como está descrito na página 71. Para cada $k\in\mathbb{N}_0$, existe um número finito de monómios primitivos nas variáveis $X_1,\ldots,X_n$ com grau k. Assim cada monómio primitivo $X_1^{k_1}\cdots X_n^{k_n}$ tem um número finito de monómios primitivos inferiores. Seja $o(X_1^{k_1}\cdots X_n^{k_n})$ o número de monómios primitivos inferiores a $X_1^{k_1}\cdots X_n^{k_n}$. A aplicação o, do conjunto G dos monómios primitivos em $X_1,\ldots,X_n$ para $\mathbb{N}_0$, é bijetiva e respeita a ordem. Diz-se que $o(X_1^{k_1}\cdots X_n^{k_n})$ é a ordem do monómio primitivo $X_1^{k_1}\cdots X_n^{k_n}$. Chama-se ordem de um polinómio $f\in R[X_1,\ldots,X_n]\setminus 0$ à ordem do maior monómio primitivo que ocorre em f. A ordem de um polinómio f representa-se por $o(f)$.

Teorema 4.1 [Teorema fundamental dos polinómios simétricos] *Seja R um anel comutativo e $f\in R[X_1,\ldots,X_n]$ um polinómio simétrico nas variáveis $X_1,\ldots,X_n$. Então existe um polinómio $g\in R[X_1,\ldots,X_n]$ tal que $f=g(s_1,\ldots,s_n)$.* ([1])

[1] Um tal polinómio g é único mas não demonstraremos a unicidade nesta disciplina.

Demonstração. Por indução em $o(f)$. Se $f = 0$ ou $o(f) = 0$, então $f \in F$ e basta tomar $g = f$. Suponhamos que $o(f) \geq 1$. Seja $X_1^{k_1} \cdots X_n^{k_n}$ o maior monómio primitivo que ocorre em f. O maior monómio primitivo que ocorre no polinómio simétrico

$$s = s_1^{k_1-k_2} s_2^{k_2-k_3} \cdots s_{n-1}^{k_{n-1}-k_n} s_n^{k_n} \qquad \text{é}$$

$$X_1^{k_1-k_2}(X_1X_2)^{k_2-k_3} \cdots (X_1 \cdots X_{n-1})^{k_{n-1}-k_n}(X_1 \cdots X_n)^{k_n} = X_1^{k_1} \cdots X_n^{k_n}.$$

Este monómio primitivo ocorre em s com coeficiente igual a 1. Seja $a_{k_1,\ldots,k_n}$ o coeficiente de $X_1^{k_1} \cdots X_n^{k_n}$ em f. Então o polinómio simétrico $e = f - a_{k_1,\ldots,k_n} s$ tem ordem inferior à ordem de f. Pela hipótese de indução, existe um polinómio $h \in R[X_1, \ldots, X_n]$ tal que $e = h(s_1, \ldots, s_n)$. Donde $f = a_{k_1,\ldots,k_n} s + h(s_1, \ldots, s_n)$. ■

4.2 Teorema fundamental da Álgebra

O teorema de Bolzano, conhecido das disciplinas de Análise Matemática da licenciatura, afirma que, se $[a, b]$ for um intervalo real, $f : [a, b] \to \mathbb{R}$ for uma função contínua e $f(a)f(b) < 0$, então existe $c \in [a, b]$ tal que $f(c) = 0$.

Lema 4.2 *Se f for um polinómio real de grau ímpar, então f tem uma raiz real.*

Demonstração. Suponhamos que $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$, onde $a_n \neq 0$ e n é ímpar. Suponhamos que $a_n > 0$. (O caso $a_n < 0$ é análogo.) A função polinomial $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$, é contínua. Claramente

$$\lim_{x \to -\infty} f(x) = -\infty \quad \text{e} \quad \lim_{x \to +\infty} f(x) = +\infty.$$

Assim existem $a, b \in \mathbb{R}$, com $a < b$, tais que $f(a) < 0$ e $f(b) > 0$. Pelo teorema de Bolzano, existe $c \in [a, b]$ tal que $f(c) = 0$, isto é, c é uma raiz real do polinómio f. ■

Corolário 4.3 *Se f for um polinómio real irredutível com grau maior do que* 1, *então $d(f)$ é par.*

Lema 4.4 *Todo o polinómio complexo de grau* 2 *se decompõe em* $\mathbb{C}$.

Demonstração. Seja $f = aX^2 + bX + c \in \mathbb{C}[X]$, onde $a \neq 0$. Sabemos que todo o número complexo tem uma raiz quadrada em $\mathbb{C}$. Seja $\sqrt{b^2 - 4ac}$ uma raiz quadrada de $b^2 - 4ac$ em $\mathbb{C}$. É fácil verificar que

$$f = a\left(X - \frac{-b + \sqrt{b^2 - 4ac}}{2a}\right)\left(X - \frac{-b - \sqrt{b^2 - 4ac}}{2a}\right),$$

o que mostra que f se decompõe em $\mathbb{C}$. ■

Chamamos *conjugado* de $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$ ao polinómio $\overline{f} = \overline{a_n}X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_0} \in \mathbb{C}[X]$.

Lema 4.5 *Sejam $f, g \in \mathbb{C}[X]$.*

(a) $\overline{f(z)} = \overline{f}(\overline{z})$, *qualquer que seja $z \in \mathbb{C}$.*

(b) *f é um polinómio real se e só se $f = \overline{f}$.*

(c) $\overline{fg} = \overline{f}\overline{g}$.

(d) $f\overline{f} \in \mathbb{R}[X]$.

(e) *Se f for um polinómio real e $c \in \mathbb{C}$ for uma raiz de f, então $\overline{c}$ também é uma raiz de f.*

Lema 4.6 *Se todo o polinómio real não constante tiver uma raiz complexa, então todo o polinómio complexo não constante tem uma raiz complexa.*

Demonstração. Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Pelo lema anterior, $g = f\overline{f} \in \mathbb{R}[X]$. Claramente g não é constante. Pela hipótese, g tem uma raiz $c \in \mathbb{C}$. Assim $0 = g(c) = f(c)\overline{f}(c)$. Donde $0 = f(c)$ ou $0 = \overline{f}(c) = \overline{f(\overline{c})}$. Donde $0 = f(c)$ ou $0 = f(\overline{c})$. ■

Lema 4.7 *Todo o polinómio real não constante tem uma raiz complexa.*

Demonstração. Seja $f = a_nX^n + \cdots + a_0 \in \mathbb{R}[X]$, onde $n \geq 2$ e $a_n \neq 0$. Suponhamos que $n = 2^mq$, onde q é ímpar. A demonstração é por indução em m. Se $m = 0$, então n é ímpar e, pelo lema 4.4, f tem uma raiz real. Suponhamos agora que $m > 0$.

Seja K um corpo de decomposição de f sobre $\mathbb{C}$ e suponhamos que $f = a_n(X - u_1) \cdots (X - u_n)$, onde $u_1, \ldots, u_n \in K$. Substituindo em (4.1) cada X_i por u_i e multiplicando ambos os membros por a_n, vem

$$f = a_n(X - u_1) \cdots (X - u_n) = a_nX^n + a_n \sum_{k=1}^{n} (-1)^k s_k(u_1, \ldots, u_n)X^{n-k}.$$

Como f é um polinómio real, $s_k(u_1, \ldots, u_n) \in \mathbb{R}$, qualquer que seja $k \in \{1, \ldots, n\}$. Para cada $r \in \mathbb{R}$, seja

$$h_r = \prod_{1 \leq i < j \leq n} X - X_i - X_j - rX_iX_j \in \mathbb{R}[X][X_1, \ldots, X_n].$$

É fácil verificar que h_r é simétrico nas variáveis $X_1, \ldots, X_n$. Pelo teorema fundamental dos polinómios simétricos, existe $g_r \in \mathbb{R}[X][X_1, \ldots, X_n]$ tal que $h_r = g_r(s_1, \ldots, s_n)$. Assim

$$h_r(u_1, \ldots, u_n) = g_r(s_1(u_1, \ldots, u_n), \ldots, s_n(u_1, \ldots, u_n)) \in \mathbb{R}[X].$$

Além disso

$$d(h_r(u_1, \ldots, u_n)) = \binom{n}{2} = \frac{n!}{(n-2)!\,2!} = \frac{n(n-1)}{2} = 2^{m-1}q(2^m q - 1)$$

Como $q(2^m q - 1)$ é ímpar, resulta da hipótese de indução que

$$h_r(u_1, \ldots, u_n) = \prod_{1 \leq i < j \leq n} X - u_i - u_j - ru_iu_j \in \mathbb{R}[X]$$

tem uma raiz em $\mathbb{C}$. Assim, para cada $r \in \mathbb{R}$, existe um par (i, j) tal que $u_i + u_j + ru_iu_j \in \mathbb{C}$. Como o número de pares (i, j) é finito, existem $r, t \in \mathbb{R}$ e existe um par (i, j) tais que $r \neq t$ e $u_i + u_j + ru_iu_j, u_i + u_j + tu_iu_j \in \mathbb{C}$. Donde deduzimos que $u_i + u_j, u_iu_j \in \mathbb{C}$. Assim $(X - u_i)(X - u_j) = X^2 - (u_i + u_j)X + u_iu_j \in \mathbb{C}[X]$. Como os polinómios complexos de grau 2 se decompõem em $\mathbb{C}$, $u_i, u_j \in \mathbb{C}$. ■

Teorema 4.8 [Teorema fundamental da Álgebra] *Todo o polinómio complexo não constante tem uma raiz complexa.*

Demonstração. Resulta imediatamente dos lemas 4.6 e 4.7. ■

4.3 Números algébricos e números inteiros algébricos

Diz-se que $u \in \mathbb{C}$ é um *número algébrico* se u for algébrico sobre $\mathbb{Q}$. Pela proposição 3.33, o conjunto $\mathbb{A}$ dos números algébricos é o único fecho algébrico de $\mathbb{Q}$ contido em $\mathbb{C}$.

Exemplo 4.9 Seja $n \in \mathbb{N}$. Pelo critério de Eisenstein, o polinómio $f_n = X^n - 2$ é irredutível em $\mathbb{Q}[X]$. Como $\mathbb{A}$ é algebricamente fechado, f_n tem uma raiz $u_n \in \mathbb{A}$. Portanto f_n é o polinómio mínimo de u_n sobre $\mathbb{Q}$ e, pela proposição 3.16, $[\mathbb{Q}(u_n) : \mathbb{Q}] = n$. Assim o espaço vetorial $\mathbb{A}$ sobre $\mathbb{Q}$ contém subespaços com dimensão finita arbitrariamente grande e, portanto, não é finitamente gerado e não é uma extensão finita de $\mathbb{Q}$.

Se $u \in \mathbb{A}$, chamamos *conjugados* de u às raízes, pertencentes a $\mathbb{A}$, do polinómio mínimo de u sobre $\mathbb{Q}$.

Lema 4.10 *Se $u \in \mathbb{A}$, existe um único polinómio primitivo e irredutível $q \in \mathbb{Z}[X]$ com primeiro coeficiente positivo tal que $q(u) = 0$. As raízes de q em $\mathbb{A}$ são os conjugados de u.*

O polinómio q referido no lema anterior chama-se *polinómio mínimo inteiro* de u.

Demonstração. Existência. Seja f o polinómio mínimo de u sobre $\mathbb{Q}$. Pelo lema 0.68 (a), existem $a/b \in \mathbb{Q} \setminus 0$ e um polinómio primitivo $p \in \mathbb{Z}[X]$

tais que $f = (a/b)p$. Como $f(u) = 0$, $p(u) = 0$. Como f e p são associados em $\mathbb{Q}[X]$ e f é irredutível em $\mathbb{Q}[X]$, p também é irredutível em $\mathbb{Q}[X]$. Como p é primitivo, p é irredutível em $\mathbb{Z}[X]$. Se o primeiro coeficiente de p for positivo, então $q = p$ é o polinómio pretendido. No caso contrário, $q = -p$ é o polinómio pretendido. As raízes de q em $\mathbb{A}$ são os conjugados de u porque f e q são associados em $\mathbb{Q}[X]$.

Unicidade. Sejam $p, q \in \mathbb{Z}[X]$ polinómios primitivos e irredutíveis com primeiro coeficiente positivo tais que $p(u) = q(u) = 0$. Então p e q também são irredutíveis em $\mathbb{Q}[X]$ e são ambos associados ao polinómio mínimo de u sobre $\mathbb{Q}$. Assim existe $a/b \in \mathbb{Q} \setminus 0$ tal que $p = (a/b)q$. Donde $bp = aq$. Pelo lema 0.64 (c), existe $v \in U(\mathbb{Z}) = \{1, -1\}$ tal que $b = av$ e, portanto, $vp = q$. Como p e q têm primeiro coeficiente positivo, $v = 1$ e $p = q$. ■

Diz-se que $u \in \mathbb{C}$ é um *número inteiro algébrico* se u for raiz de um polinómio mónico $f \in \mathbb{Z}[X]$. Representamos por $\mathbb{I}$ o conjunto dos números inteiros algébricos.

Proposição 4.11 *$\mathbb{I}$ é um subanel de $\mathbb{A}$.*

Demonstração. Claramente $\mathbb{I} \subseteq \mathbb{A}$.

Como 1 é raiz do polinómio mónico $X - 1$, $1 \in \mathbb{I}$.

Sejam $a, b \in \mathbb{I}$. Sejam $p, q \in \mathbb{Z}[X]$ polinómios mónicos tais que $p(a) = q(b) = 0$. Como $\mathbb{A}$ é algebricamente fechado,

$$p = (X - a_1) \cdots (X - a_n) \quad \text{e} \quad q = (X - b_1) \cdots (X - b_m),$$

para alguns $a_1 = a, a_2, \ldots, a_n, b_1 = b, b_2, \ldots, b_m \in \mathbb{A}$. Recorde-se que

$$p = X^n - s_1(a_1, \ldots, a_n)X^{n-1} + \cdots + (-1)^n s_n(a_1, \ldots, a_n),$$

onde $s_1, \ldots, s_n$ são os polinómios simétricos elementares em n variáveis e, portanto, para cada i, $s_i(a_1, \ldots, a_n) \in \mathbb{Z}$. Analogamente

$$q = X^m - \sigma_1(b_1, \ldots, b_m)X^{m-1} + \cdots + (-1)^n \sigma_m(b_1, \ldots, b_m),$$

onde $\sigma_1, \ldots, \sigma_m$ são os polinómios simétricos elementares em m variáveis e, portanto, para cada j, $\sigma_j(b_1, \ldots, b_m) \in \mathbb{Z}$.

Sejam $X, X_1, \ldots, X_n, Y_1, \ldots, Y_m$ variáveis distintas. O polinómio

$$F = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - (X_i - Y_j)) \in \mathbb{Z}[X][X_1, \ldots, X_n][Y_1, \ldots, Y_m]$$

é simétrico nas variáveis $Y_1, \ldots, Y_m$. Pelo teorema fundamental, existe $G \in \mathbb{Z}[X][X_1, \ldots, X_n][Y_1, \ldots, Y_m]$ tal que $F = G(\sigma_1, \ldots, \sigma_m)$. Como $\sigma_j(b_1, \ldots, b_m) \in \mathbb{Z}$,

$$\begin{aligned} F' = F(b_1, \ldots, b_m) &= G(\sigma_1(b_1, \ldots, b_m), \ldots, \sigma_m(b_1, \ldots, b_m)) \\ &\in \mathbb{Z}[X][X_1, \ldots, X_n]. \end{aligned}$$

O polinómio

$$F' = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - (X_i - b_j)) \in \mathbb{Z}[X][X_1, \ldots, X_n]$$

é simétrico nas variáveis $X_1, \ldots, X_n$. Pelo teorema fundamental, existe $G' \in \mathbb{Z}[X][X_1, \ldots, X_n]$ tal que $F' = G'(s_1, \ldots, s_n)$. Como $s_i(a_1, \ldots, a_n) \in \mathbb{Z}$,

$$f = F'(a_1, \ldots, a_n) = G'(s_1(a_1, \ldots, a_n), \ldots, s_n(a_1, \ldots, a_n)) \in \mathbb{Z}[X].$$

Além disso,

$$f = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - (a_i - b_j))$$

é mónico e $a - b = a_1 - b_1$ é uma das suas raízes. Logo $a - b \in \mathbb{I}$.

Com um argumento análogo, prove que $ab \in \mathbb{I}$. Logo $\mathbb{I}$ é subanel de $\mathbb{A}$.

■

Proposição 4.12 *Sejam $a \in \mathbb{A}$ e q o polinómio mínimo inteiro de a.*

(a) *Se $a \in \mathbb{I}$, então os conjugados de a também são inteiros algébricos.*

(b) *$a \in \mathbb{I}$ se e só se q for mónico.*

(c) *Se b for o primeiro coeficiente de q, então $ba \in \mathbb{I}$.*

Demonstração. Sejam $a = a_1, \ldots, a_n$ os conjugados de a.

(a) Seja $f \in \mathbb{Z}[X]$ um polinómio mónico tal que $f(a) = 0$. Seja $p \in \mathbb{Q}[X]$ o polinómio mínimo de a sobre $\mathbb{Q}$. Então $p \mid f$. Como $a_1, \ldots, a_n$ são as raízes de p em $\mathbb{A}$, $a_1, \ldots, a_n$ também são raízes de f e, portanto, $a_1, \ldots, a_n \in \mathbb{I}$.

(b) Suponhamos que $a \in \mathbb{I}$. Como $a_1, \ldots, a_n$ são as raízes de q e $q \in \mathbb{Z}[X]$ tem primeiro coeficiente positivo, $q = b(X - a_1) \cdots (X - a_n)$, onde $b \in \mathbb{N}$. Utilizando a notação introduzida em (a), como $q \sim p \mid f$, existe $h \in \mathbb{Q}[X]$ tal que $f = qh$. Pelo lema 0.68 (a), existem $c/d \in \mathbb{Q} \setminus 0$ e um polinómio primitivo $h' \in \mathbb{Z}[X]$ tais que $h = (c/d)h'$. Donde $df = cqh'$. Como f, q, h' são primitivos, $d \sim C(df) = C(cqh') \sim c$. Assim $d = \pm c$ e $f = \pm qh'$. Como f é mónico e o primeiro coeficiente de q é positivo, deduzimos que q é mónico. A implicação recíproca de (b) é trivial.

(c) Suponhamos que $q = bX^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0$. Então

$$\begin{aligned} b^{n-1}q &= (bX)^n + c_{n-1}(bX)^{n-1} + c_{n-2}b(bX)^{n-2} + \cdots + c_1 b^{n-2}(bX) + c_0 b^{n-1} \\ &= g(bX), \end{aligned}$$

onde

$$g = Y^n + c_{n-1}Y^{n-1} + \cdots + c_1 b^{n-2} Y + c_0 b^{n-1} \in \mathbb{Z}[Y]$$

é mónico. Como $g(ba) = b^{n-1}q(a) = 0$, $ba \in \mathbb{I}$. ■

Proposição 4.13 $\mathbb{Q} \cap \mathbb{I} = \mathbb{Z}$.

Demonstração. Seja $a \in (\mathbb{Q} \cap \mathbb{I}) \setminus 0$. Seja

$$f = X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 \in \mathbb{Z}[X] \setminus \mathbb{Z}$$

tal que $f(a) = 0$. Suponhamos que $a = c/d$, onde $c, d \in \mathbb{Z} \setminus 0$ são relativamente primos. Então

$$c^n + b_{n-1}c^{n-1}d + \cdots + b_1 cd^{n-1} + b_0 d^n = 0.$$

Donde

$$d \mid b_{n-1}c^{n-1}d + \cdots + b_1 cd^{n-1} + b_0 d^n = -c^n.$$

Como c e d são relativamente primos, $d \in U(\mathbb{Z})$. Donde $a \in \mathbb{Z}$. Logo $\mathbb{Q} \cap \mathbb{I} \subseteq \mathbb{Z}$. A outra inclusão é trivial. ■

4.4 Números transcendentes

Recorde-se que $\mathbb{A}$ representa o conjunto dos números algébricos, isto é, dos números complexos que são algébricos sobre $\mathbb{Q}$. Se $u \in \mathbb{C}$ não for um número algébrico, diz-se que u é um *número transcendente.* Pelo lema 3.34, $|\mathbb{A}| = |\mathbb{Q}| = \aleph_0$. Como $|\mathbb{C}| > \aleph_0$, existe uma infinidade não numerável de números transcendentes. Contudo, provar que um número complexo particular é transcendente é usualmente difícil. Nesta secção, provaremos que e e π são transcendentes.

A existência de números transcendentes foi pela primeira vez provada por Liouville, em 1844, ao mostrar que o número $\sum_{j=1}^{\infty} 10^{-j!}$ é transcendente. Em 1873, Hermite provou que e é transcendente. Em 1882, Lindemann provou que π é transcendente.

Lema 4.14 *Seja $a \in \mathbb{R}$. Suponhamos que a é algébrico e é raiz de um polinómio $f \in \mathbb{Z}[X]$ de grau n. Então existe $k \in \mathbb{R}^+$ tal que, quaisquer que sejam $r \in \mathbb{Z}$ e $s \in \mathbb{N}$, se $a \neq r/s$, então*

$$\frac{k}{s^n} < \left| \frac{r}{s} - a \right|. \tag{4.2}$$

Demonstração. Como

$$f'(a) = \lim_{x \to a} \frac{f(x) - f(a)}{x - a} = \lim_{x \to a} \frac{f(x)}{x - a},$$

existe $\delta \in \mathbb{R}^+$ tal que, para cada $x \in \mathbb{R} \setminus \{a\}$, se $|x - a| < \delta$, então

$$\left| \frac{f(x)}{x - a} - f'(a) \right| < 1. \tag{4.3}$$

Como f tem um número finito de raízes, existe $\epsilon \in \mathbb{R}^+$ tal que a é a única raiz de f no intervalo real $[a-\epsilon, a+\epsilon]$. Seja

$$k = \min\left\{\delta, \epsilon, \frac{1}{1+|f'(a)|}\right\}.$$

Sejam $r \in \mathbb{Z}$ e $s \in \mathbb{N}$. Seja $x = r/s \in \mathbb{Q}$ e suponhamos que $a \neq x$. Se $k \leq |x-a|$, então (4.2) é trivial. Suponhamos agora que $|x-a| < k$. De (4.3), vem, sucessivamente,

$$\begin{aligned} |f(x) - f'(a)(x-a)| &< |x-a|, \\ |f(x)| - |f'(a)||(x-a)| &< |x-a|, \\ |f(x)| &< (1+|f'(a)|)|x-a|, \\ k|f(x)| &< |x-a|. \end{aligned} \tag{4.4}$$

Como f é um polinómio com coeficientes inteiros de grau n,

$$f(x) = f(r/s) = t/s^n, \quad \text{para algum } t \in \mathbb{Z}.$$

Como $x \neq a$ e $|x-a| < k \leq \epsilon$, $f(x) \neq 0$. Portanto $1/s^n \leq |f(x)|$. De (4.4), resulta (4.2). ■

Proposição 4.15 $a = \sum_{j=1}^{\infty} 10^{-j!}$ *é transcendente.*

Demonstração. É fácil verificar a série acima é convergente. Com vista a uma contradição, suponhamos que a é algébrico e é raiz de um polinómio $f \in \mathbb{Z}[X]$ de grau n. Pelo lema anterior, existe $k \in \mathbb{R}^+$ tal que, quaisquer que sejam $r \in \mathbb{Z}$ e $s \in \mathbb{N}$, se $a \neq r/s$, então (4.2) é satisfeita.

Seja $q \in \mathbb{N}$ tal que $1/2^q < k$. Seja $p \in \mathbb{N}$ tal que $q + n < p$. A soma parcial $a_p = \sum_{j=1}^{p} 10^{-j!}$ é racional, diferente de a e $a_p = r/s$, onde $r \in \mathbb{N}$ e $s = 10^{p!} > 2$. Então

$$\begin{aligned} \left|\frac{r}{s} - a\right| &= \sum_{j=p+1}^{\infty} \frac{1}{10^{j!}} = \frac{1}{10^{(p+1)!}}\left(1 + \frac{1}{10^{(p+2)!-(p+1)!}} + \frac{1}{10^{(p+3)!-(p+1)!}} + \cdots\right) \\ &< \frac{1}{10^{(p+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots\right) = \frac{1}{10^{(p+1)!}} \frac{1}{1-(1/10)} \\ &= \frac{1}{10^{(p+1)!}}\frac{10}{9} = \frac{1}{10^{p!p}}\frac{1}{10^{p!}}\frac{10}{9} < \frac{1}{(10^{p!})^p} = \frac{1}{s^p} < \frac{1}{s^q}\frac{1}{s^n} < \frac{1}{2^q}\frac{1}{s^n} < \frac{k}{s^n}, \end{aligned}$$

o que contradiz (4.2). Logo a é transcendente. ■

As derivadas do produto

Sejam $f_1, \ldots, f_n : \mathbb{F} \to \mathbb{F}$, onde $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, funções que têm derivadas de todas as ordens. É bem conhecida a regra da derivada do produto:

$$(f_1 f_2)' = f_1' f_2 + f_1 f_2'.$$

Por indução em n,

$$(f_1 \cdots f_n)' = f_1' f_2 \cdots f_n + f_1 f_2' f_3 \cdots f_n + \cdots + f_1 \cdots f_{n-1} f_n'.$$

Por indução em j, obtemos a seguinte regra para derivadas de ordem j:

$$(f_1 \cdots f_n)^{(j)} = \sum_{\substack{j_1, \dots, j_n \in \mathbb{N}_0 \\ j_1 + \cdots + j_n = j}} f_1^{(j_1)} \cdots f_n^{(j_n)},$$

onde a derivada de ordem 0 de uma função f é igual a f. As igualdades anteriores também são verdadeiras se $f_1, \dots, f_n$ forem polinómios numa variável e as derivadas forem formais.

Módulo de um polinómio

Para cada $f = a_n X^n + \cdots + a_0 \in \mathbb{C}[X]$, seja

$$|f| = |a_n| X^n + \cdots + |a_0| \in \mathbb{R}[X].$$

Lema 4.16 *Quaisquer que sejam $f, g \in \mathbb{C}[X]$, $z \in \mathbb{C}$,*

$$|f(z)| \leq |f|(|z|) \qquad e \qquad |fg|(|z|) \leq (|f|(|z|))(|g|(|z|)).$$

A função auxiliar $I(z)$

Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$ e consideremos a função

$$I : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \int_0^1 z e^{z - zt} f(zt) dt, \tag{4.5}$$

onde t é uma variável real. No argumento seguinte, as derivadas são sempre em relação a t. Assim

$$(-e^{z-zt} f(zt))' = z e^{z-zt} f(zt) - z e^{z-zt} f'(zt).$$

Donde

$$I(z) = \int_0^1 z e^{z-zt} f(zt) dt = \int_0^1 (-e^{z-zt} f(zt))' dt + \int_0^1 z e^{z-zt} f'(zt) dt.$$

Esta operação chama-se integração por partes nas disciplinas de Análise Matemática. Donde

$$I(z) = e^z f(0) - f(z) + \int_0^1 z e^{z-zt} f'(zt) dt. \tag{4.6}$$

Integrando de novo por partes,

$$\int_0^1 z e^{z-zt} f'(zt) dt = e^z f'(0) - f'(z) + \int_0^1 z e^{z-zt} f^{(2)}(zt) dt.$$

Substituindo em (4.6),

$$I(z) = e^z(f(0) + f'(0)) - (f(z) + f'(z)) + \int_0^1 ze^{z-zt} f^{(2)}(zt)dt.$$

Repetindo sucessivamente o argumento e tendo em conta que $f^{(n+1)} = 0$, obtemos

$$I(z) = e^z(f(0) + \cdots + f^{(n)}(0)) - (f(z) + \cdots + f^{(n)}(z)). \tag{4.7}$$

Por outro lado,

$$\begin{aligned} |I(z)| &\leq \int_0^1 |ze^{z-zt} f(zt)|dt \leq \int_0^1 |z|\, e^{|z-zt|}\, |f|(|zt|)dt \quad (^2) \\ &\leq |z| \left(\max_{t\in[0,1]} e^{|z-zt|} \right) \left(\max_{t\in[0,1]} |f|(|zt|) \right). \end{aligned}$$

Donde

$$|I(z)| \leq |z|e^{|z|}|f|(|z|). \tag{4.8}$$

Transcendência de e

Teorema 4.17 *O número e é transcendente.*

Demonstração. Com vista a uma contradição, suponhamos que e é algébrico. Então e é raiz de um polinómio $g = b_rX^r + \cdots + b_0 \in \mathbb{Z}[X] \setminus 0$, onde $b_0 \neq 0$. Seja p um número primo maior do que $\max\{r, |b_0|\}$. Seja

$$f = X^{p-1}(X-1)^p \cdots (X-r)^p \in \mathbb{Z}[X].$$

Seja $n = d(f) = (r+1)p - 1$. Se $j \in \mathbb{N}_0$, derivando f, obtemos

$$f^{(j)} = \sum_{\substack{j_0,\dots,j_r\in\mathbb{N}_0 \\ j_0+\cdots+j_r=j}} (X^{p-1})^{(j_0)}((X-1)^p)^{(j_1)} \cdots ((X-r)^p)^{(j_r)}, \tag{4.9}$$

onde

$$(X^{p-1})^{(j_0)} = \begin{cases} \dfrac{(p-1)!}{(p-1-j_0)!} X^{p-1-j_0} & \text{se } j_0 \leq p-1, \\ 0 & \text{se } j_0 > p-1, \end{cases}$$

e, para $k \in \{1, \dots, r\}$,

$$((X-k)^p)^{(j_k)} = \begin{cases} \dfrac{p!}{(p-j_k)!} (X-k)^{p-j_k} & \text{se } j_k \leq p, \\ 0 & \text{se } j_k > p. \end{cases}$$

[2] Recorde-se que, se $w \in \mathbb{C}$, então $|e^w| = |\sum_{n=0}^{\infty} w^n/n!| \leq \sum_{n=0}^{\infty} |w|^n/n! = e^{|w|}$.

Assim, quaisquer que sejam $j \in \mathbb{N}_0$, $k \in \{0, 1, \ldots, r\}$,

$$f^{(j)}(k) = \sum_{\substack{j_0,\ldots,j_r \in \mathbb{N}_0 \\ j_0+\cdots+j_r=j}} \Big((X^{p-1})^{(j_0)}(k)\Big) \Big(((X-1)^p)^{(j_1)}(k)\Big) \cdots \Big(((X-r)^p)^{(j_r)}(k)\Big) \tag{4.10}$$

é um número inteiro. Vamos estudar as parcelas do lado direito de (4.10).

Suponhamos que $k = 0$. Se a parcela

$$\Big((X^{p-1})^{(j_0)}(0)\Big) \Big(((X-1)^p)^{(j_1)}(0)\Big) \cdots \Big(((X-r)^p)^{(j_r)}(0)\Big) \in \mathbb{Z} \tag{4.11}$$

for diferente de 0, então $j_0 = p-1$ e $j_i \leq p$ para $i \in \{1, \ldots, r\}$. Se $j_0 = p-1$ e $j_1 = \cdots = j_r = 0$, (4.11) é igual a

$$(p-1)!(-1)^p \cdots (-r)^p = (p-1)!(-1)^{rp} r!;$$

como p é primo e $p > r$, p não divide esta parcela. Se $(j_0, j_1, \ldots, j_r) \neq (p-1, 0, \ldots, 0)$, então $j_0 \neq p-1$ ou $j_i > 0$ para algum $i \in \{1, \ldots, r\}$; se $j_0 \neq p-1$, então (4.11) é igual a 0; se $j_0 = p-1$ e $j_i > 0$ para algum $i \in \{1, \ldots, r\}$, então (4.11) é um número inteiro,

$$(p-1)! = (X^{p-1})^{(j_0)}(0) \quad \text{e} \quad p \mid ((X-i)^p)^{(j_i)};$$

portanto, $p!$ divide (4.11). Das observações anteriores, resulta que

$$\begin{aligned} &f^{(j)}(0) = 0 && \text{se } j < p-1, \\ &p \nmid f^{(p-1)}(0) = (p-1)!(-1)^{rp} r!, \\ &p! \mid f^{(j)}(0) && \text{se } j > p-1. \end{aligned}$$

Suponhamos agora que $k \in \{1, \ldots, r\}$. Se a parcela

$$\Big((X^{p-1})^{(j_0)}(k)\Big) \Big(((X-1)^p)^{(j_1)}(k)\Big) \cdots \Big(((X-r)^p)^{(j_r)}(k)\Big) \in \mathbb{Z} \tag{4.12}$$

for diferente de 0, então $j_k = p$, $j_0 \leq p-1$ e $j_i \leq p$ para $i \notin \{0, k\}$. Neste caso, $p!$ divide sempre (4.12). Das observações anteriores, resulta que, se $k \in \{1, \ldots, r\}$, então

$$\begin{aligned} &f^{(j)}(k) = 0 && \text{se } j < p, \\ &p! \mid f^{(j)}(k) && \text{se } j \geq p. \end{aligned}$$

Consideremos a função $I(z)$, que foi definida em (4.5), associada ao polinómio f. Seja

$$J = b_0 I(0) + \cdots + b_r I(r).$$

Por (4.7),

$$\begin{aligned} J &= \sum_{k=0}^{r} b_k I(k) = \sum_{k=0}^{r} b_k \sum_{j=0}^{n} (e^k f^{(j)}(0) - f^{(j)}(k)) \\ &= \sum_{j=0}^{n} \left(\sum_{k=0}^{r} b_k e^k f^{(j)}(0) - \sum_{k=0}^{r} b_k f^{(j)}(k) \right) \\ &= \sum_{j=0}^{n} \left(g(e) f^{(j)}(0) - \sum_{k=0}^{r} b_k f^{(j)}(k) \right). \end{aligned}$$

Como $g(e) = 0$,

$$J = -\sum_{j=0}^{n} \sum_{k=0}^{r} b_k f^{(j)}(k).$$

As parcelas do lado direito são divisíveis por $p!$, exceto a parcela

$$b_0 f^{(p-1)}(0) = b_0 (p-1)! (-1)^{rp} (r!)^p,$$

a qual é divisível por $(p-1)!$ mas não é divisível por $p!$. Assim J é divisível por $(p-1)!$ mas não é divisível por $p!$. Donde $J \neq 0$ e $|J| \geq (p-1)!$. Por outro lado, para cada $k \in \{0, \dots, r\}$,

$$\begin{aligned} |f|(k) &\leq (|X|^{p-1}(k))(|X-1|^p(k)) \cdots (|X-r|^p(k)) \\ &= k^{p-1}(k+1)^p \cdots (k+r)^p \leq ((2r)^{r+1})^p. \end{aligned}$$

Utilizando esta desigualdade e (4.8),

$$|J| \leq \sum_{k=0}^{r} |b_k||I(k)| \leq \sum_{k=0}^{r} |b_k| k e^k |f|(k) \leq \sum_{k=0}^{r} |b_k| k e^k ((2r)^{r+1})^p = cd^p,$$

onde c e d são constantes positivas que não dependem de p. Assim

$$1 \leq \frac{|J|}{(p-1)!} \leq \frac{cd^p}{(p-1)!},$$

o que é absurdo, pois

$$\lim_{m \to \infty} \frac{cd^m}{(m-1)!} = 0$$

e p pode ser escolhido arbitrariamente grande. Logo e é transcendente. ■

Transcendência de π

Teorema 4.18 *O número π é transcendente.*

Demonstração. Com vista a uma contradição, suponhamos que π é algébrico. Então $i\pi$ também é algébrico. Seja g o polinómio mínimo inteiro de $i\pi$. Sejam $i\pi = \theta_1, \theta_2, \ldots, \theta_r$ os conjugados de $i\pi$. Seja b o primeiro coeficiente de g. Pela proposição 4.12 (c), para cada $k \in \{1, \ldots, r\}$, $b\theta_k$ é inteiro algébrico. Como $1 + e^{i\pi} = 0$ e $\theta_1 = i\pi$,

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \cdots (1 + e^{\theta_r}) = 0.$$

O lado esquerdo desta igualdade é uma soma de 2^r parcelas da forma e^{ϕ}, onde

$$\phi = \epsilon_1\theta_1 + \epsilon_2\theta_2 + \cdots + \epsilon_r\theta_r \tag{4.13}$$

e cada ϵ_j pertence a $\{0, 1\}$. Como os números $b\theta_k$ são inteiros algébricos, deduzimos que $b\phi$ também é inteiro algébrico, para qualquer número ϕ da forma (4.13). Sejam $\phi_1, \ldots, \phi_{2^r}$ os 2^r elementos da forma (4.13). Sem perda de generalidade, suponhamos que $\phi_1, \ldots, \phi_n$ são diferentes de 0 e $\phi_{n+1}, \ldots, \phi_{2^r}$ são iguais a 0. Então

$$q + e^{\phi_1} + \cdots + e^{\phi_n} = 0, \quad \text{onde } q = 2^r - n > 0.$$

Sejam $s_1, \ldots, s_r \in \mathbb{Z}[X][X_1, \ldots, X_r]$ os polinómios simétricos elementares nas variáveis $X_1, \ldots, X_r$. Como

$$g = b(X - \theta_1) \cdots (X - \theta_r) = bX^r + \sum_{k=1}^{r} (-1)^k b s_k(\theta_1, \ldots, \theta_r) X^{r-k} \in \mathbb{Z}[X],$$

$s_k(\theta_1, \ldots, \theta_r) \in \mathbb{Q}$ para $k \in \{1, \ldots, r\}$. Para cada $k \in \{1, \ldots, r\}$, o polinómio

$$F_k = \prod_{1 \le j_1 < \cdots < j_k \le r} (X - (X_{j_1} + \cdots + X_{j_k})) \in \mathbb{Z}[X][X_1, \ldots, X_r]$$

é simétrico nas variáveis $X_1, \ldots, X_r$. Portanto

$$F = X \prod_{k=1}^{r} F_k \in \mathbb{Z}[X][X_1, \ldots, X_r]$$

também é simétrico nas variáveis $X_1, \ldots, X_r$. Pelo teorema fundamental dos polinómios simétricos, existe $G \in \mathbb{Z}[X][X_1, \ldots, X_r]$ tal que $F = G(s_1, \ldots, s_r)$. Assim

$$\begin{aligned} X^q \prod_{j=1}^{n} (X - \phi_j) = \prod_{j=1}^{2^r} (X - \phi_j) = X \prod_{k=1}^{r} \prod_{1 \le j_1 < \cdots < j_k \le r} (X - (\theta_{j_1} + \cdots + \theta_{j_k})) \\ = F(\theta_1, \ldots, \theta_r) = G(s_1(\theta_1, \ldots, \theta_r), \ldots, s_r(\theta_1, \ldots, \theta_r)) \in \mathbb{Q}[X]. \end{aligned} \tag{4.14}$$

Sejam $\sigma_1, \ldots, \sigma_n \in \mathbb{Z}[X][X_1, \ldots, X_n]$ os polinómios simétricos elementares nas variáveis $X_1, \ldots, X_n$. De (4.14),

$$\mathbb{Q}[X] \ni \prod_{j=1}^{n} (X - \phi_j) = X^n + \sum_{k=1}^{n} (-1)^k \sigma_k(\phi_1, \ldots, \phi_n) X^{n-k}. \tag{4.15}$$

Donde, qualquer que seja $k \in \{1, \dots, n\}$, $\sigma_k(\phi_1, \dots, \phi_n) \in \mathbb{Q}$ e

$$b^k \sigma_k(\phi_1, \dots, \phi_n) = \sum_{1 \leq j_1 < \cdots < j_k \leq n} (b\phi_{j_1}) \cdots (b\phi_{j_k}) \in \mathbb{Q} \cap \mathbb{I} = \mathbb{Z}. \tag{4.16}$$

Em particular

$$b^n \phi_1 \cdots \phi_n \in \mathbb{Z}. \tag{4.17}$$

Seja p um número primo maior do que $\max\{q, |b^n \phi_1 \cdots \phi_n|\}$. Seja

$$f = b^{np} X^{p-1} (X - \phi_1)^p \cdots (X - \phi_n)^p.$$

Por (4.15),

$$f = X^{p-1} \left(b^n X^n + \sum_{k=1}^{n} (-1)^k b^n \sigma_k(\phi_1, \dots, \phi_n) X^{n-k} \right)^p.$$

Por (4.16), $f \in \mathbb{Z}[X]$. Seja $m = d(f) = (n+1)p - 1$.

Consideremos a função $I(z)$, que foi definida em (4.5), associada ao polinómio f. Seja

$$J = I(\phi_1) + \cdots + I(\phi_n).$$

Por (4.7),

$$J = \sum_{k=1}^{n} \sum_{j=0}^{m} (e^{\phi_k} f^{(j)}(0) - f^{(j)}(\phi_k)) = \sum_{k=1}^{n} e^{\phi_k} \sum_{j=0}^{m} f^{(j)}(0) - \sum_{k=1}^{n} \sum_{j=0}^{m} f^{(j)}(\phi_k).$$

Donde

$$J = -\sum_{j=0}^{m} q f^{(j)}(0) - \sum_{j=0}^{m} \sum_{k=1}^{n} f^{(j)}(\phi_k). \tag{4.18}$$

Vamos calcular limites, inferior e superior, para $|J|$.

O argumento seguinte sobre as derivadas de f é análogo a um argumento paralelo na demonstração da transcendência de e. Se $j \in \mathbb{N}_0$, derivando f, obtemos

$$f^{(j)} = b^{np} \sum_{\substack{j_0, \dots, j_n \in \mathbb{N}_0 \\ j_0 + \cdots + j_n = j}} (X^{p-1})^{(j_0)} \prod_{i=1}^{n} ((X - \phi_i)^p)^{(j_i)} \in \mathbb{Z}[X], \tag{4.19}$$

onde

$$(X^{p-1})^{(j_0)} = \begin{cases} \dfrac{(p-1)!}{(p-1-j_0)!} X^{p-1-j_0} & \text{se } j_0 \leq p-1, \\ 0 & \text{se } j_0 > p-1, \end{cases}$$

e, para $k \in \{1, \dots, n\}$,

$$((X - \phi_k)^p)^{(j_k)} = \begin{cases} \dfrac{p!}{(p-j_k)!} (X - \phi_k)^{p-j_k} & \text{se } j_k \leq p, \\ 0 & \text{se } j_k > p. \end{cases}$$

Resulta de (4.19) que, quaisquer que sejam $j \in \mathbb{N}_0$, $l \in \{0, \phi_1 \ldots, \phi_n\}$,

$$f^{(j)}(l) = \sum_{\substack{j_0,\ldots,j_n \in \mathbb{N}_0 \\ j_0+\cdots+j_n=j}} b^{np}(X^{p-1})^{(j_0)}(l) \prod_{i=1}^{n}((X-\phi_i)^p)^{(j_i)}(l). \tag{4.20}$$

Calculemos agora $\sum_{j=0}^{m} qf^{(j)}(0)$. De (4.20),

$$\sum_{j=0}^{m} qf^{(j)}(0) = \sum_{j=0}^{m} \sum_{j_0,\ldots,j_n} qb^{np} \frac{(p-1)!}{(p-1-j_0)!} 0^{p-1-j_0} \prod_{i=1}^{n} \frac{p!}{(p-j_i)!}(-\phi_i)^{p-j_i}, \tag{4.21}$$

onde $0^0 = 1$ e os índices j_i variam dentro dos seguintes limites: $0 \leq j_0 \leq p-1$, $0 \leq j_i \leq p$ para $i \in \{1, \ldots, n\}$ e $j_0 + j_1 + \cdots + j_n = j$. Note-se que todas as parcelas do lado direito de (4.21) em que $j_0 \neq p-1$ são nulas. Assim só se obtêm parcelas não nulas do lado direito de (4.21) com $j \geq p-1$. Com $j = p-1$, só se obtém uma parcela não nula (com $j_0 = p-1$ e $j_1 = \cdots = j_n = 0$); esta parcela é igual a

$$qb^{np}(p-1)!(-\phi_1)^p \cdots (-\phi_n)^p = (p-1)!s, \tag{4.22}$$

onde $s = q(-1)^{np}b^{np}(\phi_1 \cdots \phi_n)^p \in \mathbb{Z}$ por (4.17); assim esta parcela é um número inteiro divisível por $(p-1)!$; como p é primo e $p > \max\{q, |b^n\phi_1 \cdots \phi_n|\}$, p não divide (4.22).

Assim

$$\sum_{j=0}^{m} qf^{(j)}(0) = (p-1)!s + h, \tag{4.23}$$

onde

$$h = \sum_{j=p}^{m} \sum_{j_1,\ldots,j_n} qb^{np}(p-1)! \prod_{i=1}^{n} \frac{p!}{(p-j_i)!}(-\phi_i)^{p-j_i}, \tag{4.24}$$

e os índices j_i variam dentro dos seguintes limites: $0 \leq j_i \leq p$ para $i \in \{1, \ldots, n\}$ e $j_1 + \cdots + j_n = j - p + 1$. Note-se que, para qualquer parcela do lado direito de (4.24), existe $k \in \{1, \ldots, n\}$ tal que $j_k > 0$ e, portanto, $p \mid (p!/(p-j_k)!)$. Assim

$$h = p! \sum_{j=p}^{m} \sum_{j_1,\ldots,j_n} r_{j_1,\ldots,j_n} \prod_{i=1}^{n} (b\phi_i)^{p-j_i}, \tag{4.25}$$

onde

$$r_{j_1,\ldots,j_n} = qb^{j_1+\cdots+j_n}(-1)^{np-j_1-\cdots-j_n} \frac{1}{p} \prod_{i=1}^{n} \frac{p!}{(p-j_i)!} \in \mathbb{Z}.$$

Como os números $b\phi_i$ são inteiros algébricos, h é inteiro algébrico. O polinómio

$$H = \sum_{j=p}^{m} \sum_{j_1,\ldots,j_n} r_{j_1,\ldots,j_n} \prod_{i=1}^{n} X_i^{p-j_i} \in \mathbb{Z}[X_1, \ldots, X_n]$$

é simétrico nas variáveis $X_1, \ldots, X_n$. Pelo teorema fundamental dos polinómios simétricos, existe $K \in \mathbb{Z}[X_1, \ldots, X_n]$ tal que $H = K(\sigma_1, \ldots, \sigma_n)$, onde $\sigma_1, \ldots, \sigma_n \in \mathbb{Z}[X_1, \ldots, X_n]$ são os polinómios simétricos elementares nas variáveis $X_1, \ldots, X_n$. Donde

$$t := H(b\phi_1, \ldots, b\phi_n) = K(\sigma_1(b\phi_1, \ldots, b\phi_n), \ldots, \sigma_n(b\phi_1, \ldots, b\phi_n)) \in \mathbb{Z}.$$

Donde $p! \mid p!t = h$. Como $p \nmid (p-1)!s$, deduzimos de (4.23) que

$$(p-1)! \mid \sum_{j=0}^{m} qf^{(j)}(0) \quad \text{e} \quad p \nmid \sum_{j=0}^{m} qf^{(j)}(0) \tag{4.26}$$

Calculemos agora $\sum_{k=1}^{n} f^{(j)}(\phi_k)$. De (4.20),

$$\sum_{k=1}^{n} f^{(j)}(\phi_k) = \sum_{k=1}^{n} \sum_{j_0, \ldots, j_n} b^{np} \frac{(p-1)!}{(p-1-j_0)!} \phi_k^{p-1-j_0} \prod_{i=1}^{n} \frac{p!}{(p-j_i)!} (\phi_k - \phi_i)^{p-j_i}, \tag{4.27}$$

onde os índices j_i variam dentro dos seguintes limites: $0 \leq j_0 \leq p-1$, $0 \leq j_i \leq p$ para $i \in \{1, \ldots, n\}$ e $j_0 + j_1 + \cdots + j_n = j$. Note-se que, se $j_k \neq p$, então as parcelas correspondentes do lado direito de (4.27) são nulas. Assim, se (4.27) for diferente de 0, então $j \geq p$ e

$$\sum_{k=1}^{n} f^{(j)}(\phi_k) = p! b^N \sum_{k=1}^{n} \sum_{j_0, \ldots, j_{k-1}, j_{k+1}, \ldots, j_n} r_* (b\phi_k)^{p-1-j_0} \prod_{\substack{i=1 \\ i \neq k}}^{n} (b\phi_k - b\phi_i)^{p-j_i}, \tag{4.28}$$

onde $N = j - p + 1 \in \mathbb{N}$, r_* representa números naturais que dependem dos índices j_i, os índices j_i variam dentro dos seguintes limites: $0 \leq j_0 \leq p-1$, $0 \leq j_i \leq p$ para $i \in \{1, \ldots, n\} \backslash \{k\}$ e $j_0 + j_1 + \cdots + j_{k-1} + j_{k+1} + \cdots + j_n = j - p$. O polinómio

$$P_j = \sum_{k=1}^{n} \sum_{j_0, \ldots, j_{k-1}, j_{k+1}, \ldots, j_n} r_* X_k^{p-1-j_0} \prod_{\substack{i=1 \\ i \neq k}}^{n} (bX_k - bX_i)^{p-j_i} \in \mathbb{Z}[X_1, \ldots, X_n]$$

é simétrico nas variáveis $X_1, \ldots, X_n$. Pelo teorema fundamental dos polinómios simétricos, existe $Q_j \in \mathbb{Z}[X_1, \ldots, X_n]$ tal que $P_j = Q_j(\sigma_1, \ldots, \sigma_n)$. Assim

$$P_j(b\phi_1, \ldots, b\phi_n) = Q_j(\sigma_1(b\phi_1, \ldots, b\phi_n), \ldots, \sigma_n(b\phi_1, \ldots, b\phi_n)) \in \mathbb{Z}$$

e

$$p! \mid \sum_{k=1}^{n} f^{(j)}(\phi_k) = p! b^N P_j(b\phi_1, \ldots, b\phi_n). \tag{4.29}$$

De (4.26) e de (4.29) deduzimos que J é divisível por $(p-1)!$ mas não é divisível por p. Donde $|J| \geq (p-1)!$. Tal como na demonstração da transcendência de e, é fácil mostrar que existe uma constante positiva d tal que $|f|(|\phi_k|) \leq d^p$, $k \in \{1, \ldots, n\}$. Utilizando (4.8),

$$|J| \leq \sum_{k=1}^{n} |I(\phi_k)| \leq \sum_{k=1}^{n} |\phi_k| e^{|\phi_k|} |f|(|\phi_k|) \leq cd^p,$$

onde c e d são reais positivos que não dependem de p. Assim

$$1 \leq \frac{|J|}{(p-1)!} \leq \frac{cd^p}{(p-1)!},$$

o que é absurdo, pois

$$\lim_{m \to \infty} \frac{cd^m}{(m-1)!} = 0$$

e p pode ser escolhido arbitrariamente grande. Logo π é transcendente. ■