

Chapter 1

Preliminaries

This introductory chapter concentrates on basic notions and properties concerning Noetherian rings, factorization of elements in a domain, field extensions, symmetric polynomials, trace and norm, free abelian groups of finite rank, and Noetherian modules, which might not be familiar to some readers. So we include most of necessary proofs for the reader's convenience.

0. Conventional Review

In this book all rings are *commutative associative* rings with identity 1, and throughout the text,

\mathbb{N} = the set of nonnegative integers,

\mathbb{Z} = the set of integers (ring of integers),

\mathbb{Z}^+ = the set of positive integers,

\mathbb{Q} = the set of rational numbers (field of rational numbers),

\mathbb{R} = the set of real numbers (field of real numbers),

\mathbb{C} = the set of complex numbers (field of complex numbers).

Let R be a ring and A a subring of R . Then we insist that A has identity 1_A and

$$1_R = 1_A.$$

And we write

$$R^\times = R - \{0\}.$$

If $\{U_i\}_{i \in \Lambda}$ and $\{V_1, \dots, V_m\}$ are collections of nonempty subsets of R ,

then the sum of $\{U_i\}_{i \in \Lambda}$ and the product of $\{V_1, \dots, V_m\}$ are defined as

$$\sum_{i \in \Lambda} U_i = \left\{ \sum u_{i_j} \mid u_{i_j} \in U_{i_j} \right\},$$

$$V_1 \cdots V_m = \left\{ \sum v_1 \cdots v_m \mid v_i \in V_i \right\},$$

where the sums involved in both $\sum U_i$ and $V_1 \cdots V_m$ are finite sums. So one understands that

- the sum of given ideals is an ideal;
- the product of finitely many given subrings (ideals) is a subring (an ideal); and
- for subrings (ideals) I, J and $K, I(J + K) = IJ + IK = JI + KI = (J + K)I$.

Let S be a nonempty subset of R and A a subring of R . We set

$$\mathbb{Z}[S] = \text{the subring of } R \text{ generated by } S$$

$$= \left\{ \sum s_{i_1}^{\alpha_1} \cdots s_{i_m}^{\alpha_m} \mid s_{i_j} \in S, m \in \mathbb{Z}^+, \alpha_j \in \mathbb{N} \right\}$$

$$A[S] = \text{the subring of } R \text{ generated by } S \text{ over } A$$

$$= \left\{ \sum a_{(\alpha, j)} s_{i_1}^{\alpha_1} \cdots s_{i_m}^{\alpha_m} \mid a_{(\alpha, j)} \in A, s_{i_j} \in S, m \in \mathbb{Z}^+, \alpha_j \in \mathbb{N} \right\}$$

$\langle S \rangle = \text{the ideal of } R \text{ generated by } S$

$$= \sum_{s \in S} Rs$$

$$= \left\{ \sum r_i s_i \mid r_i \in R, s_i \in S \right\},$$

where the sums involved in $\mathbb{Z}[S]$, $A[S]$ and $\langle S \rangle$ are finite sums. If $S = \{s_1, \dots, s_n\}$ is finite, we write $\mathbb{Z}[S] = \mathbb{Z}[s_1, \dots, s_n]$, $A[S] = A[s_1, \dots, s_n]$, $\langle S \rangle = \langle s_1, \dots, s_n \rangle$, and call them a *finitely generated subring*, a *finitely generated subring over A* , and a *finitely generated ideal* of R , respectively. Clearly we can also write $\langle s_1, \dots, s_n \rangle = \sum_{i=1}^n Rs_i$.

Let $R \xrightarrow{\varphi} R'$ be a ring homomorphism. Then we insist that

$$\varphi \text{ is not the zero-homomorphism and } \varphi(1_R) = 1_{R'},$$

and we write $\text{Ker } \varphi$, $\text{Im } \varphi$ for the kernel and image of φ , respectively. A very useful consequence of the first isomorphism theorem on ring homomorphism states that

- if $R \xrightarrow{\varphi} A$ and $R \xrightarrow{\psi} B$ are ring homomorphisms, φ is surjective, and $\text{Ker}\varphi \subseteq \text{Ker}\psi$, then there is a ring homomorphism $A \xrightarrow{\rho} B$ defined by $\rho(a) = \psi(r)$, where $\varphi(r) = a$, such that the following diagram commutes:

$$\begin{array}{ccc} \text{Ker}\varphi \hookrightarrow R & \xrightarrow{\varphi} & A \\ \psi \downarrow & \swarrow \rho & \\ & & B \end{array} \quad \rho \circ \varphi = \psi$$

if furthermore ψ is surjective, then ρ is surjective as well.

Let R be a ring with identity $1 = 1_R$. If R has no divisors of zero, i.e., $a, b \in R$ and $ab = 0$ implies $a = 0$ or $b = 0$, then R is called an *integral domain*, or simply a *domain*. If R is a domain, then so is the polynomial ring $R[x_1, \dots, x_n]$ in variables x_1, \dots, x_n over R .

If $a, b \in R$ and $ab = 1$, then a (hence b) is called a *unit* of R . If every nonzero $a \in R$ is a unit, then R is called a *field*.

0.1. Proposition Every finite domain is a field.

Proof Exercise. □

Thus, if $p \in \mathbb{Z}$ is a prime number, then the ring $\mathbb{Z}/\langle p \rangle$ of integers modulo p , usually denoted \mathbb{Z}_p , is a field.

Let K be a field. Consider the set of integers

$$o(K) = \left\{ m \in \mathbb{Z}^+ \mid m\lambda = 0 \text{ for some } \lambda \in K^\times \right\}.$$

If $o(K) = \emptyset$, then the *characteristic* of K , denoted $\text{char}K$, is defined to be zero, i.e., $\text{char}K = 0$; if $o(K) \neq \emptyset$, then $\text{char}K$ is defined to be the smallest integer $p \in o(K)$. In the second case p is a prime number (exercise 3).

Every field has a smallest subfield \mathbb{P} (with respect to the inclusion relation on subfields), the *prime subfield*, which is either isomorphic to

$$\mathbb{Q}, \text{ if } \text{char}K = 0,$$

or to

$$\mathbb{Z}_p, \text{ if } \text{char}K = p > 0.$$

Clearly, every finite field F has $\text{char}F > 0$. If a field K has $\text{char}K = p > 0$, then $(a + b)^p = a^p + b^p$ for all $a, b \in K$ (exercise 4).

If R is a domain, then the *field of fractions* of R is constructed via the equivalence relation on $R \times R^\times$:

$$(a, b) \sim (c, d) \text{ if and only if } bc = ad.$$

Write $\frac{a}{b}$ for the equivalence class represented by (a, b) , and write $Q(R)$ for the quotient set $R \times R^\times / \sim$. Then

$$Q(R) = \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\}$$

where the addition and multiplication are defined the same as that for rational numbers. Thus, in $Q(R)$, $\frac{0}{1} = 0$ is the zero of the additive group $(Q(R), +)$, $\frac{1}{1} = 1_{Q(R)}$ is the identity of the multiplicative group $(Q(R), \cdot)$, and if $\alpha = \frac{a}{b} \neq 0$ then $\alpha^{-1} = \frac{b}{a}$.

The ring homomorphism

$$\lambda_R: R \longrightarrow Q(R)$$

$$r \mapsto \frac{r}{1}$$

is injective. In the case where R is a field, λ_R is an isomorphism. So we may view R as a subring of $Q(R)$ and write $R \subseteq Q(R)$. Consequently, if $Q(R)[x]$ is the polynomial ring in variable x over $Q(R)$, then $R[x] \subseteq Q(R)[x]$.

If R' is another domain and $\varphi: R \rightarrow R'$ is an injective ring homomorphism, then φ induces an injective ring homomorphism $\bar{\varphi}: Q(R) \rightarrow Q(R')$, where $\bar{\varphi}\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$. Hence $Q(R)$ may be viewed as a subfield of $Q(R')$, and consequently $Q(R)[x]$ may be viewed as a subring of $Q(R')[x]$. It turns out that if φ is an isomorphism then so is $\bar{\varphi}$. In particular, if $Q(R)$ is the field of fractions of the domain R and $R \subset B \subset Q(R)$, where B is a subring of $Q(R)$, then $Q(B) = Q(R)$.

We assume that the reader is familiar with the basic structural properties of a polynomial ring $R[x_1, \dots, x_n]$ in variables x_1, \dots, x_n over the ring R , for instance, R is a subring of $R[x_1, \dots, x_n]$ consisting of constant polynomials, every $f \in R[x_1, \dots, x_n]$ has a *unique* expression into the linear combination of monomials: $f = \sum r_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_1, \dots, \alpha_n \in \mathbb{N}\}$, and the *degree* of f is defined as

$$\deg f = \max \left\{ \alpha_1 + \cdots + \alpha_n \mid r_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \neq 0 \text{ is a term of } f \right\}.$$

If $f = 0$ then conventionally $\deg f$ is defined as $-\infty$. Thus, for $f = \sum r_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $g = \sum r_\beta x_1^{\beta_1} \cdots x_n^{\beta_n}$, one knows how to determine the

degree of $f + g$ and $f \cdot g$ according to the addition and multiplication of polynomials.

In particular, we recall the following important properties of a polynomial ring.

If $f \in R[x]$ is a nonconstant *monic polynomial*, i.e., $\deg f \geq 1$ and f is of the form

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_i \in R,$$

then a division algorithm on $g \in R[x]$ by f exists:

$$g = qf + r, \quad q, r \in R[x], \quad \deg r < \deg f.$$

Let R be a ring. If $\mathbb{Z}[s_1, \dots, s_n]$ is the subring of R generated by s_1, \dots, s_n , then there is an onto ring homomorphism from the polynomial ring $\mathbb{Z}[x_1, \dots, x_n]$ to $\mathbb{Z}[s_1, \dots, s_n]$:

$$\mathbb{Z}[x_1, \dots, x_n] \longrightarrow \mathbb{Z}[s_1, \dots, s_n]$$

$$f(x_1, \dots, x_n) \mapsto f(s_1, \dots, s_n)$$

Let A be a subring of R . If $A[s_1, \dots, s_n]$ is the subring of R generated by s_1, \dots, s_n over A , then there is an onto ring homomorphism from the polynomial ring $A[x_1, \dots, x_n]$ to $A[s_1, \dots, s_n]$:

$$A[x_1, \dots, x_n] \longrightarrow A[s_1, \dots, s_n]$$

$$f(x_1, \dots, x_n) \mapsto f(s_1, \dots, s_n)$$

Exercises

1. Let A be a subring of the ring R and $S \subseteq R$ a nonempty subset of R . Show that $\mathbb{Z}[S]$ is the smallest subring of R containing S , that $A[S]$ is the smallest subring of R containing A and S , and that $\langle S \rangle$ is the smallest ideal of R containing S . (Here the ordering on subrings and ideals is the usual inclusion ordering on subsets.)
2. Complete the proof of Proposition 0.1. (Hint: If $R = \{a_1, \dots, a_n\}$ is a finite domain and $0 \neq a_i \in R$, then $a_i R = R$.)
3. Let K be a field. Show that if $\text{char} K = p \neq 0$, then p is a prime number.
4. Let K be a field of $\text{char} K = p \neq 0$. Show that $(a + b)^p = a^p + b^p$ for all $a, b \in K$. (Hint: Check the binomial coefficients of the expansion of $(a + b)^p$.)

1. Noetherian Rings

Since Noetherian ring plays a leading role in commutative algebra, we start with this notion.

Let R be a ring. R is said to satisfy the *maximal condition* if every nonempty set of ideals contains a maximal member with respect to the inclusion relation on ideals. R is said to satisfy the *ascending chain condition* if for every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

there is some k such that $I_k = I_j$ for all $j \geq k$.

1.1. Theorem Let R be a ring. The following are equivalent.

- (i) R satisfies the maximal condition.
- (ii) Every ideal of R is finitely generated.
- (iii) R satisfies the ascending chain condition.

Proof (i) \Rightarrow (ii) Let I be a nonzero ideal of R . Set

$$S = \{\text{all finitely generated ideals contained in } I\}.$$

Then $S \neq \emptyset$, and by (i) there is a maximal member in S , say $J = \sum_{i=1}^n Ra_i$ with $a_i \in I$. If $J \neq I$, then there is some $x \in I$, $x \notin J$. Thus, J is properly contained in $J' = J + Rx$ and $J' \in S$, contradicting the choice of J . Therefore $I = J$, a finitely generated ideal.

(ii) \Rightarrow (iii) Let

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

be an ascending chain of ideals in R . Set $I = \cup I_i$. Then I is an ideal of R and hence finitely generated, say $I = \sum_{j=1}^m Ra_j$ with $a_j \in I$. Suppose $a_j \in I_{i_j}$ with $i_1 < i_2 < \cdots < i_m$. Then $a_j \in I_{i_m}$, $j = 1, \dots, m$, and consequently $I = I_{i_m}$. Let $k = i_m$. Then $I_k = I_j$ for all $j \geq k$.

(iii) \Rightarrow (i) Let $S = \{I_i\}$ be a nonempty set of ideals in R . If S did not have a maximal member, there would be a strictly ascending chain of ideals out of S , which does not satisfy the chain condition. \square

1.2. Definition A ring R satisfying one of the equivalent conditions of Theorem 1.1 is called a *Noetherian ring*.

Let R be a ring. If every ideal I of R is a principal ideal, i.e., $I = \langle a \rangle = Ra$ for some $a \in I$, then R is called a *principal ideal ring*. Principal ideal rings are special Noetherian rings. If a principal ideal ring R is also a domain, then we simply call R a PID.

It is a result of the division algorithm in \mathbb{Z} and the division algorithm in the polynomial ring $K[x]$, where K is a field, that both \mathbb{Z} and $k[x]$ are PIDs (exercise 1).

Concerning polynomial rings in finitely many variables over a Noetherian ring, we have the following celebrated result.

1.3. Theorem (Hilbert basis theorem) If R is a Noetherian ring then so is the polynomial ring $R[x]$ in variable x over R . Hence, the polynomial ring $R[x_1, \dots, x_n]$, in any finitely n variables x_1, \dots, x_n , is Noetherian.

Proof We show that if $R[x]$ is not Noetherian then neither is R , by adopting a well-known argumentation (as one may easily find at the site ¹).

Suppose that I is an ideal of $R[x]$ which is not finitely generated. Then a sequence of polynomials from I can be chosen as follows.

$$\begin{aligned} f_1 &\in I \text{ with least degree } n_1, \\ f_2 &\in I - Rf_1 \text{ with least degree } n_2, \\ f_3 &\in I - (Rf_1 + Rf_2) \text{ with least degree } n_3, \\ &\vdots \\ f_{k+1} &\in I - \sum_{i=1}^k Rf_i \text{ with least degree } n_{k+1}, \\ &\vdots \end{aligned}$$

where $n_1 \leq n_2 \leq n_3 \leq \dots \leq n_{k+1} \leq \dots$.

Claim Let a_i be the leading coefficient of f_i . Then

$$Ra_1 \subset Ra_1 + Ra_2 \subset \dots \subset \sum_{i=1}^n Ra_i \subset \dots$$

is a strictly ascending chain of ideals in R .

If the claim was not true, then $\sum_{i=1}^k Ra_i = \sum_{i=1}^{k+1} Ra_i$ for some k , and this would yield $a_{k+1} = \sum_{i=1}^k r_i a_i$, $r_i \in R$. Note that for $i = 1, \dots, k$, we

¹<http://planetmath.org/encyclopedia/ProofofHilbertBasisTheorem.html>

have

$$\begin{aligned} f_i &= a_i x^{n_i} + \text{strictly lower degree terms,} \\ r_i f_i x^{n_{k+1}-n_i} &= r_i a_i x^{n_{k+1}} + \text{strictly lower degree terms.} \end{aligned}$$

It follows that

$$\begin{aligned} \sum_{i=1}^k r_i f_i x^{n_{k+1}-n_i} &= \left(\sum_{i=1}^k r_i a_i \right) x^{n_{k+1}} + g(x) \\ &= a_{k+1} x^{n_{k+1}} + g(x), \end{aligned}$$

while

$$g(x) = \left(f_{k+1} - \sum_{i=1}^k r_i f_i x^{n_{k+1}-n_i} \right) \notin \sum_{i=1}^k R f_i$$

by the choice of f_{k+1} . But clearly $\deg g(x) < \deg f_{k+1}$, contradicting the choice of f_{k+1} . Therefore the claim holds, i.e., R is not Noetherian. \square

The polynomial ring $K[x_1, \dots, x_n, \dots]$ in infinitely many variables over a field K is non-Noetherian, due to the existence of a strictly ascending chain of ideals:

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, \dots, x_n \rangle \subset \cdots.$$

In Chapter 4 we will see that if \mathcal{A} is the set of all algebraic integers, i.e., the set of complex zeros of monic polynomials in $\mathbb{Z}[x]$, then \mathcal{A} forms a ring and it is not Noetherian; while for a finite dimensional field extension $\mathbb{Q} \subseteq K$ with K a subfield of \mathbb{C} , $\mathcal{A} \cap K$ is always Noetherian.

Noetherian rings stemming from algebraic geometry are given in Chapter 5.

Exercises

1. Show that \mathbb{Z} and $K[x]$ are PIDs, where $K[x]$ is the polynomial ring in x over a field K .
2. Let $R \rightarrow R'$ be an onto ring homomorphism. Show that if R is Noetherian then so is R' .
3. Let A be a Noetherian subring of the ring R , and let $\{r_1, \dots, r_s\}$ be a finite subset of R . Show that the subring $A[r_1, \dots, r_s]$ of R is Noetherian.
4. Let K be a field which, as a subring, is contained in the ring R . Assume that R is finite dimensional over K . Show that R is Noetherian.

5. Let R be a Noetherian ring. The ring of formal power series over R is the associative ring $R[[x]]$ consisting of the formal series

$$f(x) = \sum_{i=0}^{\infty} r_i x^i, \quad r_i \in R,$$

where $f(x) = 0$ if and only if $r_i = 0$ for all $i = 0, 1, \dots$, and the addition and multiplication are defined as for the power series with real coefficients in calculus. Show that $R[[x]]$ is Noetherian. (Hint: Define the degree of a series as the lowest power of x .)

6. By Theorem 1.3, $\mathbb{Z}[x]$ is Noetherian. Show that the ideal $I = \langle 2, x \rangle$ is not a principal ideal.
7. Let $\mathbb{Z}_2[x, y]$ be the polynomial ring over the field \mathbb{Z}_2 . Show that in $\mathbb{Z}_2[x, y]/\langle x^2 + x + y^3 + 1 \rangle$ the ideal $\langle \bar{x}, \overline{y+1} \rangle$ is not a principal ideal.

2. Factorization of Elements in a Domain

Let R be a domain. It is easy to see that the set of units in R , denoted

$$U(R) = \left\{ u \in R \mid u \text{ is a unit in } R \right\},$$

forms a group with respect to the multiplication of R . $U(R)$ is called the *group of units* in R .

2.1. Definition (i) For $r \in R$, $u \in U(R)$, the element $y = ur = ru$ is called an *associate* of r .

(ii) Let $r, s \in R$. r is said to be *divisible* by s , denoted $s|r$, if $r = sz$ for some $z \in R$, where s (hence z) is called a *divisor* (or a *factor*) of r .

For $u \in U(R)$ and $r \in R$, u and ur are called the *trivial divisors* of r (note that $r = (ur)u^{-1} = (u^{-1}r)u$).

(iii) For $r \in R$, if r has only trivial divisors in R , then we say that r is *irreducible* in R ; otherwise, r is *reducible* in R . (So zero is reducible in any domain.)

(iv) For $r \in R$, if r is reducible, then $r = sz$ with nontrivial divisors s, z . In this case we say that r has a *proper factorization*.

Example (i) Let $R = \mathbb{Z}$. Then $U(R) = \{\pm 1\}$.

(ii) Let $R = \mathbb{Z}[i]$ where $i = \sqrt{-1}$. Then $U(R) = \{\pm 1, \pm i\}$ (see Chapter 4

section 3).

(iii) Let $R = K[x]$ be the polynomial ring in x over a field K . Then $U(R) = K^\times$.

Thus, one easily finds elements in each R that have proper factorization.

2.2. Proposition Let R be a domain, $r, s \in R$. The following hold:

- (i) $r \in R$ is a unit if and only if $r|1$.
- (ii) Any two units are associates to each other, and any associate of a unit is a unit.
- (iii) r, s are associates to each other if and only if $r|s$ and $s|r$.
- (iv) r is irreducible if and only if every divisor of r is either an associate of r or a unit.
- (v) Any associate of an irreducible element is irreducible.

Proof Exercise. □

In terms of ideal structure, we may characterize units, divisibility, associates and irreducibility, as follows.

2.3. Proposition Let R be a domain and let r, s be nonzero elements of R .

- (i) $r \in U(R)$ if and only if $\langle r \rangle = R$.
- (ii) $r|s$ if and only if $\langle r \rangle \supseteq \langle s \rangle$.
- (iii) r, s are associates to each other if and only if $\langle r \rangle = \langle s \rangle$.
- (iv) r is irreducible if and only if $\langle r \rangle$ is maximal among the principal ideals of R (with respect to the inclusion ordering on ideals).

Proof Exercise. □

2.4. Definition Let R be a domain. We say that *factorization into irreducible elements is feasible* in R if every nonzero nonunit element may be expressed as a product of finitely many irreducible elements.

2.5. Proposition Factorization into irreducible elements is feasible in a Noetherian domain R .

Proof Let R be a Noetherian domain. Suppose that the assertion was not true. Then the set Ω of nonzero nonunit elements which cannot be factorized into finite products of irreducible elements would be nonempty.

Since R is Noetherian, let $\langle y \rangle$ be a maximal member in

$$S = \left\{ \langle x \rangle \mid x \in \Omega \right\}.$$

Then y is reducible because $y \in \Omega$, and $y = rs$ for $r, s \notin U(R)$. Thus, $\langle y \rangle$ is properly contained in $\langle r \rangle \cap \langle s \rangle$ (otherwise r or s would be a unit by Proposition 2.3). By the choice of $\langle y \rangle$ we have

$$r = p_1 \cdots p_r, \quad s = p_{r+1} \cdots p_n$$

where p_i 's are irreducible elements. But then $y = p_1 \cdots p_r p_{r+1} \cdots p_n$, a product of finitely many irreducible elements. This is a contradiction and hence $\Omega = \emptyset$. \square

2.6. Definition Let R be a domain in which factorization into irreducible elements is feasible. For a nonzero nonunit $x \in R$, if any two factorizations

$$x = p_1 \cdots p_n \text{ and } x = q_1 \cdots q_m$$

satisfy $n = m$ and (up to the arrangement of divisors) $p_i = u_i q_i$, $i = 1, \dots, n$, where $u_i \in U(R)$, then x is said to have a *unique* factorization in R . If every nonzero nonunit element of R has a unique factorization in R , we say that R is a UFD (abbreviation of the phrase “unique factorization domain”).

Remark At this stage, it is better to be aware of two facts.

- (i) There are Noetherian domains which are not UFDs (see exercise 4 of this section and Chapter 4 section 3).
- (ii) There are UFDs which are not Noetherian (exercise 5).

In order to discuss the uniqueness of factorization into irreducible elements, we introduce the notion of a prime in a domain.

2.7. Definition Let R be a domain, $0 \neq x \in R$, and $x \notin U(R)$. x is said to be a *prime* if $x|ab$ implies $x|a$ or $x|b$ for any $a, b \in R$.

2.8. Proposition Let p be a prime in a domain R . The following hold:

- (i) Any associate of p is a prime in R .
- (ii) p is irreducible in R .

Proof Exercise. \square

2.9. Theorem If factorization into irreducible elements is feasible in a domain R , then R is a UFD if and only if every irreducible element is a prime.

Proof Since factorization into irreducible elements is feasible in R , by Proposition 2.2(v), every nonzero nonunit $x \in R$ has a factorization

$$x = p_1 \cdots p_\ell,$$

where p_i may be an associate of some irreducible element.

First suppose that factorization in R is unique. Let p be an irreducible element and $p|ab$ where $a \neq 0$, $b \neq 0$. Then $ab = pc$ for some $0 \neq c \in R$. Consider the unique factorizations: $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, $c = r_1 \cdots r_s$. Then

$$pc = p(r_1, \dots, r_s) = (p_1 \cdots p_n)(q_1 \cdots q_m) = ab.$$

By the uniqueness, p divides some p_i or some q_j . Hence $p|a$ or $p|b$, and this shows that p is a prime.

Conversely, suppose every irreducible element is a prime. Consider the factorization into primes

$$x = p_1 \cdots p_n = q_1 \cdots q_m.$$

Then $p_1|q_1(q_2 \cdots q_m)$. Without loss of generality we may assume $p_1|q_1$. Then, $q_1 = u_1 p_1$ for some $u_1 \in U(R)$ because q_1 has only trivial divisors. Thus, $x = p_1 \cdots p_n = (u_1 p_1)(q_2 \cdots q_m)$ and $p_2 \cdots p_n = (u_1 q_2)(q_3 \cdots q_m)$. After repeating this process n times, up to the arrangements of divisors we derive $q_i = u_i p_i$ with $u_i \in U(R)$, and $m \leq n$. Similarly, $n \leq m$. So $n = m$. This shows that factorization is unique in R . \square

2.10. Theorem Every PID is a UFD.

Proof Let R be a PID. Then factorization into irreducible elements is feasible in R because R is Noetherian.

Let p be an irreducible element in R . Then by Proposition 2.3(iv), $\langle p \rangle$ is maximal among all ideals. Suppose $p|ab$ but $p \nmid a$. Then $\langle p \rangle$ is properly contained in the ideal $\langle p, a \rangle$. By the maximality of $\langle p \rangle$ we have $\langle p, a \rangle = R$. It follows that $1 = ph + aq$ and $b = bph + abq$. This yields $p|b$, showing that p is a prime. By Theorem 2.9, R is a UFD. \square

Remark Recall that before learning a systematic theory on UFDs, in the

arithmetic theory on $R = \mathbb{Z}$ (or in $R = K[x]$ where K is a field) a prime p is defined as the element which has only the divisors ± 1 ($\lambda \in K^\times$), $\pm p$ (λp). If $a, b \in R$, $p|ab$ but $p \nmid a$, then the Euclidean algorithm output the greatest common divisor $\gcd(p, a) = 1$ in the form

$$af + pg = 1, \quad f, g \in R,$$

that yields $p|b$ immediately as in the above proof. That is why we know, without arguing that R is a PID, that R is a UFD. Indeed, there is a class of UFDs that hold a version of Euclidean algorithm, as described below.

2.11. Definition A Euclidean domain is a domain R with a function (called a Euclidean function):

$$\phi : R^\times \longrightarrow \mathbb{N}$$

that satisfies

- (i) if $a, b \in R^\times$ and $a|b$ then $\phi(a) \leq \phi(b)$; and
- (ii) if $a, b \in R^\times$ then there exist $q, r \in R$ such that

$$a = qb + r, \text{ where either } r = 0 \text{ or } \phi(r) < \phi(b).$$

Example (iv) \mathbb{Z} is a Euclidean domain with the Euclidean function given by the absolute value function. $K[x]$ is a Euclidean domain with the Euclidean function given by the degree function. (A consequence of applying the division algorithm to both \mathbb{Z} and $K[x]$.)

2.12. Theorem Every Euclidean domain R is a PID.

Proof Let I be a nonzero ideal of R . If ϕ is the associated Euclidean function on R , let us set

$$\phi(x^*) = \min \left\{ \phi(x) \in \mathbb{N} \mid 0 \neq x \in I \right\}.$$

For any $0 \neq y \in I$, $y = qx^* + r$ with $r = 0$ or $\phi(r) < \phi(x^*)$. But $r = y - qx^* \in I$. By the choice of x^* , $r = 0$. Thus, $y = qx^*$. This shows that $I = \langle x^* \rangle$. \square

2.13. Corollary Every Euclidean domain is a UFD.

Proof This follows from Theorems 2.10–2.12. \square

Except for \mathbb{Z} and $K[x]$, other Euclidean domains will be given in Chapter 4 section 3.

Remark Let $K = \mathbb{Q}(\sqrt{-19})$. By Theorem 3.4 of Chapter 4, the ring \mathcal{A}_K of algebraic integers in K is not a Euclidean domain. However, \mathcal{A}_K is a PID. The reader is referred to <http://www.mathreference.com/id,npid.html> for a beautiful proof on this fact.

We now proceed to show that the polynomial ring $R[x]$ in variable x over a UFD R is a UFD.

2.14. Lemma (Gauss) Let R be a domain. Then any prime of R is a prime in $R[x]$.

Proof Let p be a prime in R and $\bar{R} = R/\langle p \rangle$. Then a direct verification shows that \bar{R} is a domain, and so is the polynomial ring $\bar{R}[x]$. If $f, g \in R[x]$ and $p|fg$, then $fg \in \langle p \rangle$. For $r \in R$, write \bar{r} for the image of r in \bar{R} . Consider the ring homomorphism

$$\begin{aligned} R[x] &\xrightarrow{\varphi} \bar{R}[x] \\ \sum r_i x^i &\mapsto \sum \bar{r}_i x^i \end{aligned}$$

Then $\varphi(fg) = \bar{f} \cdot \bar{g} = 0$. Since $\bar{R}[x]$ is a domain, it follows that $\bar{f} = 0$ or $\bar{g} = 0$, i.e., $p|f$ or $p|g$, as desired. \square

Let R be a UFD. Then for any $r_1, \dots, r_n \in R$, not all zero, the greatest common divisor $\gcd(a_1, \dots, a_n)$ exists in R (exercise 6).

2.15. Definition Let R be a UFD. If a polynomial $r_n x^n + r_{n-1} x^{n-1} + \dots + r_0 = f(x) \in R[x]$ has the property that $\gcd(r_n, r_{n-1}, \dots, r_0) = d \in U(R)$, then $f(x)$ is called a *primitive polynomial*.

2.16. Proposition Let R be a UFD. If $f, g \in R[x]$ are primitive then so is the product fg .

Proof This follows immediately from Gauss lemma. \square

2.17. Theorem Let R be a UFD with the field of fractions $K = Q(R)$.

(i) If $f \in R[x]$ and $f = gh$ for some $g, h \in K[x]$, then there is a unit

$\alpha \in K[x]$ such that $g\alpha, \alpha^{-1}h \in R[x]$.

(ii) Let $f, g \in R[x]$, where g is primitive. If $g|f$ in $K[x]$ then $g|f$ in $R[x]$.

Proof (i) Let $f = gh$ be as assumed. Let $r_0 \in R$ be the common denominator of the coefficients of g . Then $r_0g \in R[x]$. Let d be the greatest common divisor of all coefficients of r_0g . Then $g_1 = \alpha g$ is primitive in $R[x]$, where $\alpha = \frac{r_0}{d} \in K$. Similarly, there exists $\beta \in K$ such that $h_1 = \beta h$ is primitive in $R[x]$. Set $\alpha\beta = \frac{a}{b}$, where a and b have only common divisors which come from $U(R)$. Then

$$\frac{a}{b}f = \alpha\beta gh = g_1h_1 \text{ and } af = bg_1h_1.$$

Now, if $a \in U(R)$, then since $b\alpha\beta = a$, we have $\alpha g = g_1, \alpha^{-1}h = a^{-1}b\beta h = a^{-1}bh_1$ have coefficients in R , as desired. So it remains to show that $a \in U(R)$. If not, there would be some prime p dividing a . Hence $p|bg_1h_1$ but $p \nmid b$ by the choice of a and b , and $p \nmid g_1, p \nmid h_1$ because both g_1 and h_1 are primitive. This contradicts Gauss lemma. Therefore, a must be a unit. (ii) This follows from part (i). \square

Let R be a UFD and $f(x) \in R[x]$ with $\deg f(x) \geq 1$. If d is the greatest common divisor of all coefficients of $f(x)$, then $f(x) = df_1(x)$ where $f_1(x)$ is a primitive polynomial. Bearing this fact in mind, Theorem 2.17 enables us to derive immediately the following.

2.18. Proposition Let R be a UFD with the field of fractions $K = Q(R)$, $p(x) \in R[x]$ with $\deg p(x) \geq 1$. Then $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $K[x]$. \square

2.19. Theorem If R is a UFD then so is $R[x]$.

Proof Since R is a UFD and $R \subset R[x]$, by Gauss lemma we need only to consider polynomials of degree ≥ 1 .

Let $K = Q(R)$ be the field of fractions of R . Then $K[x]$ is a UFD. Thus every $f(x) \in R[x]$ with $\deg f(x) \geq 1$ is factorized into a product of finitely many irreducible elements in $K[x]$. By Theorem 2.17 and Proposition 2.18, factorization of polynomials of degree ≥ 1 into irreducible polynomials is feasible in $R[x]$, and irreducible polynomials in $R[x]$ are primes. Hence $R[x]$ is a UFD. \square

2.20. Corollary For any field K , the polynomial ring $K[x_1, \dots, x_n]$ in finitely many variables x_1, \dots, x_n over K is a UFD. □

We finish this section by Eisenstein's criterion concerning the irreducibility of polynomials in $R[x]$, where R is a domain.

2.21. Theorem Let R be a domain and

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

a polynomial in $R[x]$. Suppose there is a prime $p \in R$ such that

- (a) $p \nmid a_n$,
- (b) $p \mid a_i, i = 0, \dots, n-1$,
- (c) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $R[x]$.

Proof Suppose $f(x) = g(x)h(x)$ for $g(x), h(x) \in R[x]$ where

$$g(x) = c_r x^r + \cdots + c_1 x + c_0$$

$$h(x) = d_s x^s + \cdots + d_1 x + d_0$$

with $c_i, d_j \in R$ and $r, s > 1, r + s = n$. Then by (b) and (c), $p \mid a_0 = c_0 d_0$ and hence p divides c_0 or d_0 but not both. Suppose $p \mid c_0$. By (a), we may let c_m be the first coefficient of $g(x)$ not divisible by p . But note that

$$a_m = c_0 d_m + c_1 d_{m-1} + \cdots + c_{m-1} d_1 + c_m d_0, \text{ where } p \nmid c_m d_0.$$

This implies $p \nmid a_m$, contradicting (b) because $m < n$. Hence $g(x)$ or $h(x)$ must be a unit of R . □

2.22. Corollary If p is a prime number, then the polynomial

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Z}[x]$ and hence irreducible in $\mathbb{Q}[x]$.

Proof Note that $f(x) = \frac{x^p-1}{x-1}$. If we use the translation $x = X + 1$, then

$$\begin{aligned} f(X+1) &= \frac{(X+1)^p - 1}{(X+1) - 1} \\ &= \frac{1}{X} \left(X^p + \binom{p}{1} X^{p-1} + \binom{p}{2} X^{p-2} + \cdots + \binom{p}{p-1} X + 1 - 1 \right) \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \binom{p}{2} X^{p-3} + \cdots + p. \end{aligned}$$

Now, using p as the prime needed in Theorem 2.21, we conclude that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and hence irreducible in $\mathbb{Q}[x]$ by Proposition 2.18.

Exercises

- Complete the proof of Proposition 2.2.
- Complete the proof of Proposition 2.3.
- Complete the proof of Proposition 2.8.
- Let $R = K[t^2, t^3]$ be the subring generated by t^2 and t^3 in the polynomial ring $K[t]$ over a field K . Show that both t^2 and t^3 are irreducible in R but none is a prime. However $t^6 = t^2 t^2 t^2 = t^3 t^3$. (See also Chapter 3 (section 2, exercise 2) and Chapter 3 (section 3, Example (iii)).)
- Show that the polynomial ring $R = K[x_1, x_2, \dots, x_n, \dots]$ in infinitely many variables over a field K is a UFD. (Hint: Any polynomial in R belongs to a polynomial ring in finitely many variables over K .)
- Let R be a domain, $a, b \in R$ not all zero. Up to a unit multiple, define the greatest common divisor of a and b , denoted $\gcd(a, b)$, and the least common multiple of a and b (in case $a \neq 0, b \neq 0$), denoted $\text{lcm}[a, b]$, as in \mathbb{Z} (or as in $K[x]$ with K a field). (In a similar way, for $a_1, \dots, a_n \in R$, $\gcd(a_1, \dots, a_n)$ and $\text{lcm}(a_1, \dots, a_n)$ may be defined.)
Show that the following statements are equivalent for a domain R in which factorization into irreducible elements is feasible.
 - R is a UFD.
 - Every irreducible element of R is a prime.
 - For every $a, b \in R$, not all zero, $\gcd(a, b)$ (or $\text{lcd}[a, b]$ in case $a \neq 0, b \neq 0$) exists.
 - The intersection of two principal ideals of R is another principal ideal.
- Let R be a UFD, $f, g \in R[x]$. Use Theorem 2.17 to show that if f, g

do not have common irreducible divisors in $R[x]$ then f, g do not have common irreducible divisors in $K[x]$ either, where $K = Q(R)$ is the field of fractions of R .

8. Let p be a prime number. Show that $x^n - p$ is irreducible in $\mathbb{Z}[x]$ and hence in $\mathbb{Q}[x]$.
9. Prove that $f = 11yx^8 + 3y^7x^5 + 9x^5 - 7y^7 - 21$ is irreducible in $\mathbb{Z}[x, y]$. (Hint: Consider f in $\mathbb{Z}[y][x]$.)

3. Field Extensions

The study of field extensions stems from the study of zeros of polynomials and the study of irreducibility of polynomials. Let K be a field and $f \in K[x_1, \dots, x_n]$ a polynomial of degree ≥ 2 . Then the property that f has or does not have a zero in K , and the property that f is reducible or irreducible over K , all depends on the ground field K , for instance, first consider the zeros of $x^2 - 1$, $x^2 - 2$ in \mathbb{Q} and the zeros of $x^2 - 3$, $x^2 + 1$ in \mathbb{R} , and then consider the zeros of the given polynomials by extending \mathbb{Q} to \mathbb{R} , \mathbb{R} to \mathbb{C} . A full demonstration of this aspect is given in Chapter 4 and Chapter 5. In this section we focus on several fundamental topics concerning field extensions.

Let K, L be fields. If K is a subfield of L (including the case where $K \xrightarrow{\varphi} L$ is a ring monomorphism), then we call L an *extension field* of K , and from now on $K \subseteq L$ is referred to a *field extension*.

Let $K \subseteq L$ be a field extension and $S \subset L$ a subset of L . Consider the intersection

$$K(S) = \bigcap L_i$$

of all subfields in L containing S . Then it is an easy exercise to verify that

- (a) $K(S)$ is the *smallest* subfield of L containing S , and
- (b) $K(S) = Q(K[S])$, the field of fractions of $K[S]$ (hence $K(S)$ is also the smallest subfield of L containing $K[S]$).

In view of the above (a)–(b), we call $K(S)$ the subfield of L *generated by* S over K . If $S = \{s_1, \dots, s_n\}$ is finite, then we write $K(S) = K(s_1, \dots, s_n)$ and call it a *finitely generated* extension field of K . If S consists of a single element s , then $K(s)$ is called a *simple* extension field of K .

Splitting field

3.1. Definition Let K be a field, and let $f(x)$ be a polynomial in $K[x]$. If $K \subseteq L$ is a field extension such that $f(x)$ factors completely into linear factors over L , i.e., $f(x) = a \prod (x - \alpha_i)$ in $L[x]$, and $f(x)$ does not factor completely into linear factors over any proper subfield of L containing K , then L is called a *splitting field* of $f(x)$.

Let K be a field. To see the existence of a splitting field for an arbitrary $f(x) \in K[x]$, we start with an irreducible polynomial $p(x)$. Note that the quotient ring

$$L = \frac{K[x]}{\langle p(x) \rangle} = \left\{ \overline{\psi(x)} = \sum \lambda_i \bar{x}^i \mid \psi(x) \in K[x] \right\} = K[\bar{x}],$$

where \bar{x} is the image of x in L , is a field, for, if $p(x) \nmid \psi(x)$ then $p(x)h(x) + \psi(x)g(x) = 1$ for some $h(x), g(x) \in K[x]$, and hence $\overline{\psi(x)}$ is invertible in L . Note that via the natural ring homomorphism $K[x] \rightarrow L$ we may write $K \subset L = K[\bar{x}]$. Thus,

$$K[x] \subset L[x] \text{ and consequently } p(\bar{x}) = 0.$$

It follows from the division algorithm that $p(x)$ is factorized in $L[x]$ as

$$p(x) = (x - \bar{x})p_1(x), \quad p_1(x) \in L[x].$$

Now, since $K[x]$ is a UFD, an induction on the degree of polynomials, or a procedure of adding the zeros of each irreducible factor of $f(x)$ successively to the predecessor extension field, yields the following fact.

3.2. Theorem Let K be a field. Every $f(x) \in K[x]$ with $\deg f(x) = n > 0$ has a splitting field. □

Example (i) The field $\mathbb{Q}(\sqrt{-3})$ serves as a splitting field for both $x^2 + 3$ and $x^3 + x^2 + 3x + 3$.

Remark Indeed, any splitting field of $f(x)$ is isomorphic to the one constructed before Theorem 3.2. The reader can refer to any textbook specifying field theory for a detailed proof.

Repeated zeros and separability

Let K be a field and let $f(x) \in K[x]$. In view of Theorem 3.2 we may always talk about the zeros of $f(x)$ in some extension field of K . Furthermore, we explore the following

Question When does $f(x)$ have no repeated zeros?

3.3. Proposition $f(x) \in K[x]$ has no repeated zeros if and only if $f(x)$ and $f'(x) = \frac{df(x)}{dx}$ are coprime, i.e., they do not have nonconstant common divisor.

Proof Over a splitting field E of $f(x)$, we have

$$f(x) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_m)^{n_m}$$

where the α_i 's are distinct. Then it is clear that $f(x)$ and $f'(x)$ have no nonconstant common divisor over E if and only if $n_i = 1$ for $i = 1, \dots, m$. \square

3.4. Proposition Let E be a splitting field of $x^n - 1 = f(x) \in K[x]$, where $n \geq 1$. Suppose that $\text{char}K$ does not divide n . Then the following hold:

- (i) $f(x)$ has exactly n distinct zeros (the n th roots of unity over K) in E .
- (ii) Let

$$U_n = \left\{ \alpha \in E \mid f(\alpha) = 0 \right\}.$$

Then U_n is a cyclic multiplicative subgroup of E^\times .

Proof (i) By the assumption, this follows from Proposition 3.3.

(ii) That U_n forms a subgroup of E^\times is clear. We show that U_n contains an element of order n . To this end, let

$$n = p_1^{e_1} \cdots p_s^{e_s}$$

be the factorization of n into primes, and let $q_i = \frac{n}{p_i}$ for $i = 1, \dots, s$. Then, since the polynomial $x^{q_i} - 1$ has exactly q_i zeros in U_n , for each i , there is $\alpha_i \in U_n$ such that $\alpha_i^{q_i} \neq 1$. Set $\beta_i = \alpha_i^{n/p_i^{e_i}}$. Then $\beta_i^{p_i^{e_i-1}} \neq 1$ but $\beta_i^{p_i^{e_i}} = 1$. It follows that each β_i has order $p_i^{e_i}$. Since $p_1^{e_1}, \dots, p_s^{e_s}$ are pairwise coprime, $\beta = \beta_1 \cdots \beta_s$ is the desired generator for U_n . \square

The last proposition makes the multiplicative structure of a finite field clear.

3.5. Theorem Let K be a finite field. Then the multiplicative group K^\times of K is cyclic.

Proof If $\text{char}K = p > 0$, then $[K : \mathbb{Z}_p] = m$ for some m and hence K^\times has $n = p^m - 1$ elements which are all zeros of $f(x) = x^n - 1 \in \mathbb{Z}_p[x]$. Since $p \nmid n$, Proposition 3.4 can be applied to this case. \square

Since $K[x]$ is a UFD, the general discussion may be further reduced to irreducible elements.

3.6. Theorem Let K be a field and let $q(x) \in K[x]$ be irreducible.

(i) If $\text{char}K = 0$, then $q(x)$ does not have repeated zeros.

(ii) If $\text{char}K = p > 0$, then $q(x)$ has repeated zeros if and only if $q(x) = g(x^p)$ for some $g(x) \in K[x]$.

Proof We apply Proposition 3.3 to both cases.

(i) If $\text{char}K = 0$, then since $q(x)$ is irreducible, we have $q'(x) \neq 0$ (otherwise $q(x)$ would be a constant), $\deg q'(x) < \deg q(x)$, and hence $q(x)$ and $q'(x)$ are coprime.

(ii) Suppose $\text{char}K = p > 0$. Let $q(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $a_n \neq 0$. Then $q'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$ with $\deg q'(x) = n-1 < \deg q(x) = n$. Thus,

$$\begin{aligned} q(x) \text{ and } q'(x) \text{ have a nonconstant common divisor} &\Leftrightarrow r a_r = 0 \\ &\Leftrightarrow p|r, \text{ say } r = s_r p. \end{aligned}$$

Consequently, $q(x)$ has repeated zeros if and only if $q(x) = a_{tp} x^{tp} + \cdots + a_{2p} x^{2p} + a_p x^p + a_0$. Therefore, $q(x) = g(x^p)$ where $g(y) = a_0 + a_p y + a_{2p} y^2 + \cdots + a_{tp} y^t$, as claimed. \square

3.7. Corollary Let K be a finite field and let $q(x) \in K[x]$ be irreducible. Then $q(x)$ has no repeated zeros.

Proof Since K is finite, we know that $\text{char}K = p > 0$ for some prime number p . Then \mathbb{Z}_p is the prime field of K and K is a finite dimensional \mathbb{Z}_p -vector space, say $\dim_{\mathbb{Z}_p} K = n$. Hence K has p^n elements. Thus, the multiplicative group of K , which is K^\times , has order $p^n - 1$ and $\lambda^{p^n} = \lambda$ for all $\lambda \in K$. (We assumed that the reader is familiar with elementary group theory.) It follows that if $g(x^p) \in K[x]$, say $g(x^p) = a_0 + a_1 x^p + \cdots + a_n x^{np}$,

then, after setting $a_i^{p^{n-1}} = b_i$, $i = 0, 1, \dots, n$,

$$\begin{aligned} g(x^p) &= a_0 + a_1x^p + \cdots + a_nx^{np} \\ &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} \\ &= (b_0 + b_1x + \cdots + b_nx^n)^p, \end{aligned}$$

which can never be irreducible. This shows that the irreducible $q(x)$ cannot have repeated zeros by Theorem 3.6. \square

3.8. Definition If a polynomial $f(x) \in K[x]$ has no repeated zeros, then $f(x)$ is called a *separable polynomial* over K , and otherwise an *inseparable polynomial* over K . (See also Definition 3.11 below.)

Algebraic extension and primitive elements

We now start with a field extension $K \subseteq L$ and consider $\alpha \in L$. If there is some $f(x) \in K[x]$ such that $f(\alpha) = 0$, then we say that α is an *algebraic element* over K ; otherwise, we say that α is a *transcendental element* over K . If every element of L is algebraic over K , then L is called an *algebraic extension field* of K , and we refer $K \subseteq L$ to an *algebraic field extension*. If L contains a transcendental element over K , then $K \subseteq L$ is referred to a *transcendental field extension*.

Let $K \subseteq L$ be a field extension. Then L is naturally viewed as a K -vector space. In the literature, the dimension $\dim_K L$ is also called the *degree* of L over K , denoted $[L : K]$.

Clearly, if a field extension $K \subseteq L$ has finite $[L : K]$, then L is algebraic over K . For instance, $[\mathbb{C} : \mathbb{R}] = 2$. If L contains a transcendental element over K , then $[L : K] = \infty$. It is known that e and π are transcendental over \mathbb{Q} . So $[\mathbb{R} : \mathbb{Q}] = \infty$. Another familiar transcendental extension is $K \subset K(x)$, where $K(x)$ is the field of fractions of the polynomial ring $K[x]$. Also, not every algebraic field extension is finite dimensional (exercise 4).

To understand the structure of a field extension $K \subseteq L$, simple extension plays a key role. Let $\alpha \in L$. Consider the subring $K[\alpha] \subseteq L$ and the ring

homomorphism

$$\varphi: K[x] \longrightarrow K[\alpha]$$

$$g(x) \mapsto g(\alpha).$$

If α is a transcendental element over K , then

$$\text{Ker}\varphi = \{0\} \text{ and } K[x] \cong K[\alpha].$$

If α is algebraic over K , then $\text{ker}\varphi \neq \{0\}$ and hence $\text{Ker}\varphi = \langle p(x) \rangle$ for some nonconstant $p(x) \in K[x]$ because $K[x]$ is a PID. We may assume that $p(x)$ is *monic*. It is a consequence of the division algorithm in $K[x]$ that $p(x)$ has the *smallest* positive degree among all polynomials in $\text{Ker}\varphi$. This leads to the following

3.9. Definition For an algebraic element α over K , the monic polynomial $p(x)$, which is the generator of $\text{ker}\varphi$, is called the *minimal polynomial* of α over K .

3.10. Theorem Let $K \subseteq L$ be a field extension and $\alpha \in L$. If α is algebraic over K and $p(x)$ is its minimal polynomial, the following hold:

- (i) $p(x)$ is irreducible and unique in $K[x]$.
- (ii) $K[x]/\langle p(x) \rangle \cong K[\alpha]$ is a field containing K . Thus, $k[\alpha] = K(\alpha)$.
- (iii) If $\deg p(x) = n$, then every element $\beta \in k(\alpha)$ has a unique expression

$$\beta = \lambda_{n-1}\alpha^{n-1} + \lambda_{n-2}\alpha^{n-2} + \cdots + \lambda_1\alpha + \lambda_0, \lambda_i \in K.$$

Thus, $\{\alpha^{n-1}, \dots, \alpha, 1\}$ forms a K -basis for $K(\alpha)$, $[K(\alpha) : K] = n$. Consequently, $K(\alpha)$ is a simple algebraic extension field of K .

Proof Using division algorithm by $p(x)$ in $K[x]$, all conclusions are easy exercises. \square

Later in exercise 2 the reader will be asked to show that if $\alpha_1, \dots, \alpha_m \in L$ are finitely many algebraic elements over K , then $K \subseteq K(\alpha_1, \dots, \alpha_m)$ is an algebraic field extension and $[F : K] < \infty$. When K plays the role as in the case of Theorem 3.6(i) and Corollary 3.7, our next goal is to show that the finitely generated algebraic field extension $K(\alpha_1, \dots, \alpha_m)$ is actually a simple extension. But first, we need the notion of a separable extension.

3.11. Definition (i) Let $K \subseteq L$ be a field extension and let $\alpha \in L$ be an

algebraic element over K . If the minimal polynomial $p(x)$ of α over K is separable in the sense of Definition 3.8, then α is said to be *separable* over K ; otherwise α is *inseparable* over K .

(ii) Let $K \subseteq L$ be an algebraic field extension. If every element of L is separable over K , then L is said to be *separable* over K ; otherwise L is *inseparable* over K .

By Theorem 3.6 and Corollary 3.7, inseparable field extension is, indeed, quite rare.

3.12. Theorem Let $K \subseteq F = K(\alpha_1, \alpha_2, \dots, \alpha_m)$ be a finitely generated algebraic field extension. Suppose that $\alpha_2, \dots, \alpha_m$ are separable over K . Then $F = K(\vartheta)$ for some $\vartheta \in F$.

Proof If K is finite then so is F (by Exercise 2), and the conclusion follows from Theorem 3.5.

Suppose that K is infinite. We consider only the case where $F = K(\alpha, \beta)$ with β separable over K since the general conclusion may be obtained by an induction.

Let L be a field over which the minimal polynomial $p(x)$ of α and the minimal polynomial $q(x)$ of β are factorized as

$$p(x) = \prod_{i=1}^n (x - \alpha_i), \quad q(x) = \prod_{j=1}^m (x - \beta_j),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \dots, \beta_m \in L$, and $\alpha_1 = \alpha$, $\beta_1 = \beta$. (The existence of L is guaranteed by Theorem 3.2.) By the assumption, β_1, \dots, β_m are distinct. Thus, the equations

$$\alpha_i - \alpha_1 = \lambda_{ik}(\beta_1 - \beta_k), \quad k \neq 1,$$

have only finitely many solutions $\lambda_{ik} \in K$. Hence, there exists $c \in K$ such that

$$\alpha_i - \alpha_1 \neq c(\beta_1 - \beta_k), \quad 1 \leq i \leq n, \quad 2 \leq k \leq m.$$

Set $\vartheta = \alpha + c\beta$. Then clearly $K(\vartheta) \subseteq F$. Below we show that $\beta \in K(\vartheta)$ and then it follows that $F = K(\vartheta)$.

Note that $\alpha = \vartheta - c\beta$. We have $p(\vartheta - c\beta) = p(\alpha) = 0$. Consider the polynomial $r(x) = p(\vartheta - cx) \in K(\vartheta)[x]$. Then, by the choice of c , β is the only common zero of $q(x)$ and $r(x)$ in F . This shows that the

minimal polynomial of β in $K(\vartheta)[x]$ is of the form $t - \mu$ for some $\mu \in K(\vartheta)$. Therefore, $\beta = \mu \in K(\vartheta)$ as expected. \square

3.13. Definition The element ϑ that appears in Theorem 3.12 is called a *primitive element* of F .

Example (ii) $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Let F be a field. If every nonconstant polynomial $f(x) \in F[x]$ splits in F , i.e., $f(x) = \prod_{i=1}^n \lambda(x - \lambda_i)$, $\lambda, \lambda_i \in F$, then F is said to be *algebraically closed*. Clearly, if F is algebraically closed, then there is no proper algebraic extension of F . For instance, the field \mathbb{C} of complex numbers is algebraically closed (this is also known as the content of the fundamental theorem of algebra). Without proof we mention the following theorem (the reader is referred to any textbook specializing field theory for the classical proof given by Emil Artin).

Theorem Let K be a field. Then there is an extension field L of K that is algebraically closed.

Lüroth's theorem

Within the context of Theorem 3.6(i), Corollary 3.7 and Theorem 3.12, it is easy to see that if $K \subseteq L = K(\vartheta)$ is a simple field extension, then any intermediate field extension F of K with $K \subsetneq F \subseteq L$ is a simple extension. The final part of this section deals with a similar situation on simple transcendental field extension.

Let K be a field and x a transcendental element over K . Given coprime polynomials $u(x), v(x) \in K[x]$, consider $h = \frac{u(x)}{v(x)} \in K(x)$ and the simple extension $K \subset K(h)$. Set

$$hv(t) - u(t) = q(t) \in K(h)[t],$$

where $K(h)[t]$ is the polynomial ring in t over $K(h)$.

3.14. Lemma With notation as above, the following hold:

- (i) h is transcendental over K .
- (ii) $q(t)$ is irreducible in $K(h)[t]$.
- (iii) $[K(x) : K(h)] = \deg q(t) = \max\{\deg u(x), \deg v(x)\}$.

Proof (i) Exercise.

(ii) Note that $q(t)$ is linear with respect to h in the polynomial ring $K[h, t]$ which is a UFD. Hence $q(t)$ is irreducible in $K[h, t]$, for $u(x)$ and $v(x)$ are coprime by the assumption. It follows from Proposition 2.18 that $q(t)$ is irreducible in $K(h)[t]$.

(iii) By the construction of $q(t)$, $q(x) = 0$. It follows from part (ii) that $q(t)$ (assuming monic) is the minimal polynomial of x over $K(h)$. Thus, $[K(x) : K(h)] = \deg q(t) = \max\{\deg u(x), \deg v(x)\}$, as desired. \square

3.15. Corollary (i) Let E be any intermediate extension field of K with $K \subsetneq E \subseteq K(x)$. Then $[K(x) : E] < \infty$.

(ii) Every automorphism of the ring $K(x)$ which is K -linear is given by

$$x \mapsto \frac{ax + b}{cx + d}, \quad a, b, c, d \in K, \quad ad - bc \neq 0.$$

Proof Exercise. \square

3.16. Theorem (Lüroth) Let K be a field and x a transcendental element over K . Let E be an intermediate extension field of K with $K \subsetneq E \subseteq K(x)$. Then $E = K(y)$ for some $y \in K(x)$ (hence $E \cong K(x)$) and $[K(x) : E] < \infty$.

Proof By Corollary 3.15, $[K(x) : E] < \infty$. Let $p(t) \in E[t]$ be the minimal polynomial of x over E , say

$$p(t) = t^n + r_{n-1}t^{n-1} + \cdots + r_0, \quad r_i \in E.$$

If we multiply $p(t)$ by the least common multiple, say s , of the denominators of r_i 's, the obtained polynomial

$$(1) \quad f(x, t) = sp(t) = s_n t^n + s_{n-1} t^{n-1} + \cdots + s_0, \quad s_i \in K[x],$$

is primitive in $K[x][t]$ with respect to t (check it!). Write $\deg_t f(x, t)$ for the degree of $f(x, t)$ in t . Then

$$n = \deg_t f(x, t) = \deg p(t) = [K(x) : E].$$

Note that $s_n = s$ and all $\frac{s_i}{s_n} \in E$. As x is transcendental over K , there is at least one $\frac{s_i}{s_n} \in E - K$. Set $h = \frac{u(x)}{v(x)} = \frac{s_i}{s_n}$ for convenience, where $u(x)$ and $v(x)$ are coprime in $K[x]$. Then

$$q(t) = hv(t) - u(t)$$

is irreducible in $K(h)[t]$ and

$$(2) \quad [K(x) : K(h)] = \deg q(t) = \max\{\deg u(x), \deg v(x)\}$$

by Lemma 3.14. Since $K \subsetneq K(h) \subseteq E \subseteq K(x)$, we complete the proof by having the equality

$$[K(x) : E] = [K(x) : K(h)].$$

To this end, note that $q(x) = 0$ and $q(t) \in E[t]$. Hence $q(t) = p(t)p_1(t)$ with $p_1(t) \in E[t]$, for $p(t)$ is the minimal polynomial of x over E . Thus, by formula (1),

$$\begin{aligned} u(x)v(t) - v(x)u(t) &= v(x)p(t)p_1(t) \\ &= \left(\frac{v(x)}{s} p_1(t) \right) f(x, t). \end{aligned}$$

But $f(x, t)$ is primitive in $K[x][t]$ with respect to t . It follows from Theorem 2.17(ii) that

$$(3) \quad u(x)v(t) - v(x)u(t) = df(x, t), \quad d \in K[x][t].$$

Suppose $\deg_x f(x, t) = m$. Then $\max\{\deg u(x), \deg v(x)\} \leq m$ by formula (1). So the above formula (3) implies that

$$(4) \quad \deg_x (u(x)v(t) - v(x)u(t)) = m$$

and d is a constant. Note that $u(x)v(t) - v(x)u(t)$ is antisymmetric in x and t . Therefore, (2) + (4) yields

$$\begin{aligned} [K(x) : K(h)] &= \max\{\deg u(x), \deg v(x)\} = m \\ &= \deg_x (u(x)v(t) - v(x)u(t)) \\ &= \deg_t (u(x)v(t) - v(x)u(t)) \\ &= \deg_t f(x, t) \\ &= n = [K(x) : E], \end{aligned}$$

as desired. □

More results concerning field extensions are given in section 5 and (Chapter 3 Theorems 1.8 and 2.4).

Exercises

1. Let $K \subseteq L$ be a field extension and $\alpha_1, \dots, \alpha_m \in L$. Show that if $\alpha_1, \dots, \alpha_m$ are algebraic over K , then $K \subseteq F = K(\alpha_1, \dots, \alpha_m)$ is an algebraic field extension and $[F : K]$ is finite. (Hint: Note that $F = K(\alpha_1)(\alpha_2) \cdots (\alpha_m)$ and use Theorem 3.10(iii).)
2. Let $K \subseteq L \subseteq E$ be a tower of algebraic field extension, i.e., L is algebraic over K and E is algebraic over L . Use exercise 1 to show that E is also algebraic over K . Moreover, show that if $[L : K] < \infty$ and $[E : L] < \infty$, then $[E : K] = [L : K][E : L]$. (Hint: If $\alpha \in E$ and $\lambda_n \alpha^n + \cdots + \lambda_1 \alpha + \lambda_0 = 0$ for $\lambda_i \in L$, then consider $K \subseteq K(\lambda_n, \dots, \lambda_0) \subseteq K(\lambda_n, \dots, \lambda_0)(\alpha)$.)
3. Use Theorem 3.10(iii) to show that if $K \subseteq L$ is a field extension, then all elements of L which are algebraic over K form a subfield \widehat{K} of L containing K . \widehat{K} is called the *algebraic closure* of K in L . (Hint: For $\alpha, \beta \in L$, algebraic over K , consider $K \subseteq K[\alpha] \subseteq k[\alpha][\beta]$.)
4. Let F be the subfield of \mathbb{C} consisting of all algebraic elements over \mathbb{Q} . Use (section 2, exercise 8) to show that $[F : \mathbb{Q}] = \infty$.
5. Show that if K is an algebraically closed field, then K is infinite (or equivalently, that a finite field cannot be algebraically closed). (Hint: If $F = \{a_1, \dots, a_n\}$ is a finite field, consider the polynomial $p(x) = \prod_{i=1}^n (x - a_i) + 1$ in $F[x]$.)
6. Let $d \in \mathbb{Z}$ be square-free. Then every element $\alpha \in \mathbb{Q}(\sqrt{d})$ is of the form $\alpha = r + s\sqrt{d}$, where $r, s \in \mathbb{Q}$. Show that α has the minimal polynomial

$$p_\alpha(x) = x^2 - 2rx + (r^2 - s^2d).$$

7. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Find a primitive element for F .
8. Prove Lemma 3.14(i).
9. Complete the proof of Corollary 3.15.

4. Symmetric Polynomials

Let R be a ring and $R[x_1, \dots, x_n]$ the polynomial ring in variables x_1, \dots, x_n over R . Put

$$\mathbb{N}^n = \left\{ \alpha = (\alpha_1, \dots, \alpha_n) \mid \alpha_i \in \mathbb{N} \right\}.$$

Then every element $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ has a *unique* expression

$$(*) \quad f(x_1, \dots, x_n) = \sum_{\alpha} c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n, \quad c_{\alpha} \in R.$$

Let S_n denote the permutation group of $\{1, 2, \dots, n\}$. A polynomial $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ is said to be *symmetric* if

$$f(x_1, \dots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}), \quad \text{for all } \pi \in S_n.$$

For example, $x_1^2 + x_2^2 + x_3^2$, $(x_1 + x_2 + x_3 + x_4)(x_1 x_2 x_3 x_4)^3$.

Important symmetric polynomials are those *elementary symmetric polynomials*:

$$\begin{aligned} s_1(x_1, \dots, x_n) &= x_1 + x_2 + \cdots + x_n \\ s_2(x_1, \dots, x_n) &= x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n \\ &\quad + x_2 x_3 + x_2 x_4 + \cdots + x_2 x_n \\ &\quad \vdots \\ &\quad + x_{n-2} x_{n-1} + x_{n-2} x_n \\ &\quad + x_{n-1} x_n \\ &\quad \vdots \\ s_k(x_1, \dots, x_n) &= \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} \\ &\quad \vdots \\ s_n(x_1, \dots, x_n) &= x_1 x_2 \cdots x_n. \end{aligned}$$

Let $R[s_1, \dots, s_n]$ be the subring of $R[x_1, \dots, x_n]$ generated by R and $\{s_1, s_2, \dots, s_n\}$. Then it is clear that every $g(s_1, s_2, \dots, s_n) \in R[s_1, \dots, s_n]$ is a symmetric polynomial. The next theorem, due to Newton, shows that the converse is also true.

4.1. Theorem If $f = f(x_1, \dots, x_n)$ is a symmetric polynomial in $R[x_1, \dots, x_n]$, then $f(x_1, \dots, x_n) \in R[s_1, \dots, s_n]$.

Proof To reduce $f = f(x_1, \dots, x_n) = \sum_{\alpha} c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ into a polynomial in elementary symmetric polynomials, in view of previous (*) we order the set of monomials

$$\left\{ x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n \right\}$$

by the lexicographic ordering:

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \prec_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n}$$

if and only if

$$\alpha_1 = \beta_1, \alpha_2 = \beta_2, \dots, \alpha_{s-1} = \beta_{s-1} \text{ while } \alpha_s < \beta_s \text{ for some } s \leq n.$$

Thus, the terms of f are ordered lexicographically (note that \prec_{lex} is a total ordering), and we may assume that the leading monomial of f is $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.

Since f is symmetric, $x_{\pi(1)}^{\alpha_1} x_{\pi(2)}^{\alpha_2} \cdots x_{\pi(n)}^{\alpha_n}$ occurs in f for every $\pi \in S_n$. It follows that the leading monomial of f has the property that $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. For example, the leading monomial of

$$s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} = (x_1 + \cdots + x_n)^{k_1} \cdots (x_1 \cdots x_n)^{k_n}$$

is

$$x_1^{k_1 + \cdots + k_n} x_2^{k_2 + \cdots + k_n} \cdots x_n^{k_n}.$$

By choosing $k_1 = \alpha_1 - \alpha_2, \dots, k_{n-1} = \alpha_{n-1} - \alpha_n, k_n = \alpha_n$, we can make this the same as the leading monomial of f . Suppose that the leading coefficient of f is c , then $f - cs_1^{k_1} s_2^{k_2} \cdots s_n^{k_n}$ has a lexicographic leading term

$$dx_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}, \quad \beta_1 \geq \beta_2 \geq \cdots \geq \beta_n$$

which comes after $cx_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ in the ordering. Since only a finite number of monomials $x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_n^{\gamma_n}$ in f satisfying $\gamma_1 \geq \gamma_2 \geq \cdots \geq \gamma_n$ follow $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ lexicographically, a finite number of repetitions of the above process reduce f to a polynomial in s_1, \dots, s_n . \square

Example (i) The symmetric polynomial

$$f = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2$$

is written lexicographically. And by the method given in the proof we may derive that $f = s_1s_2 + 3s_3$. Similarly, $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3) = s_1s_2 - s_3$.

An application of symmetric polynomials to field extension is given as follows.

If $K \subseteq L$ is a field extension, $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = f(x) \in K[x]$ with $\deg f(x) = n$, and $f(r_i) = 0$ with $r_1, \dots, r_n \in L$, then, $f(x)$ factors in $L[x]$ as

$$\begin{aligned} f(x) &= a_n(x - r_1)(x - r_2) \cdots (x - r_n) \\ &= a_n(x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n) \end{aligned}$$

where $c_i = (-1)^i s_i(r_1, r_2, \dots, r_n)$, $i = 1, \dots, n$. After comparing coefficients of both sides, we have

$$(-1)^i a_n s_i(r_1, r_2, \dots, r_n) = a_{n-i} \in K, \quad i = 1, \dots, n.$$

4.2. Corollary Let $K \subseteq L$ be a field extension, $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = f \in K[x]$ with $\deg f = n$, and $f(r_i) = 0$ with $r_1, \dots, r_n \in L$. If $h(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ is a symmetric polynomial, then $h(r_1, r_2, \dots, r_n) \in K$, i.e., $\{r_1, \dots, r_n\}$ defines a function

$$\begin{aligned} K[s_1, \dots, s_n] &\longrightarrow K \\ h &\longmapsto h(r_1, \dots, r_n) \end{aligned}$$

□

Example (ii) Suppose that r_1, r_2, r_3 are the zeros of $f(x) = x^3 + x^2 - x + 1$ in \mathbb{C} . Find $r_1^2 + r_2^2 + r_3^2$ and $r_1^3 + r_2^3 + r_3^3$.

Solution Since $f(x) = (x - r_1)(x - r_2)(x - r_3)$, it follows that

$$r_1 + r_2 + r_3 = -1,$$

$$r_1r_2 + r_1r_3 + r_2r_3 = -1,$$

$$r_1r_2r_3 = -1.$$

From $(r_1 + r_2 + r_3)^2 = r_1^2 + r_2^2 + r_3^2 + 2(r_1r_2 + r_1r_3 + r_2r_3)$ we derive that $r_1^2 + r_2^2 + r_3^2 = 1 + 2 = 3$; and from $f(x_i) = 0$, $i = 1, 2, 3$, we derive that $r_1^3 + r_2^3 + r_3^3 = -(r_1^2 + r_2^2 + r_3^2) + (r_1 + r_2 + r_3) - 3 = -7$.

More generally, the following recurrence relations, called *Newton's formulas*, can be used to establish formulas for $p_i = (-1)^i(x_1^i + x_2^i + \cdots + x_n^i)$, $i \geq 1$, in terms of s_1, s_2, \dots, s_n .

$$p_1 + s_1 = 0,$$

$$p_2 + s_1 p_1 + 2s_2 = 0,$$

$$p_3 + s_1 p_2 + s_2 p_1 + 3s_3 = 0,$$

...

$$p_n + s_1 p_{n-1} + s_2 p_{n-2} + \cdots + s_{n-1} p_1 + n s_n = 0.$$

We close with an application to polynomial building.

Example (iii) Let r_1, r_2, r_3 be the zeros of $f(x) = x^3 - x + 2$ in \mathbb{C} . Find the polynomial $g(x)$ that has zeros r_1^2, r_2^2, r_3^2 .

Solution Suppose the desired polynomial is of the form $g(x) = x^3 + Ax^2 + Bx + C$. Then

$$\begin{aligned} A &= -(r_1^2 + r_2^2 + r_3^2) = -p_2(r_1, r_2, r_3) \\ &= -s_1(r_1, r_2, r_3)^2 + 2s_2(r_1, r_2, r_3) \\ &= 0 + 2(-1) = -2, \end{aligned}$$

$$\begin{aligned} B &= r_1^2 r_2^2 + r_1^2 r_3^2 + r_2^2 r_3^2 = s_2(r_1, r_2, r_3)^2 - 2s_1(r_1, r_2, r_3)s_3(r_1, r_2, r_3) \\ &= (-1)^2 - 2(0)(-2) = 1, \end{aligned}$$

$$C = -r_1^2 r_2^2 r_3^2 = -s_3(r_1, r_2, r_3)^2 = -4.$$

Hence $g(x) = x^3 - 2x^2 + x - 4$.

Exercises

- Express the product $(x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2)$ in terms of s_1, s_2, s_3 .
- Let r_1, r_2, r_3 be the zeros of $f(x) = x^3 - 6x + 11 - 6$ in \mathbb{C} . Determine the polynomial $g(x)$ that has zeros $r_1^2 + r_2^2, r_1^2 + r_3^2, r_2^2 + r_3^2$.
- Let r_1, r_2, r_3, r_4 be the zeros of $f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$ in

- \mathbb{C} , where $a_i \in \mathbb{Q}$. Suppose $a_4 = -5$ and the elementary polynomials in r_1, r_2, r_3, r_4 are $s_1 = \frac{3}{5}$, $s_2 = 16$, $s_3 = -8$, $s_4 = -\frac{1}{10}$. Find a_3, a_2, a_1, a_0 .
4. Let R be a ring. A polynomial belonging to $R[x_1, \dots, x_n]$ is said to be *antisymmetric* if it is invariant under even permutations of the variables, but changes sign under odd permutations. Let

$$\Delta = \prod_{i < j} (x_i - x_j).$$

Show that

- (a) Δ is antisymmetric, and
 (b) if $2r = 0$ implies $r = 0$ for $r \in R$, then any antisymmetric polynomial f is expressible as a polynomial in the elementary symmetric polynomials, together with Δ . (Hint: Note that $f(x_1, x_2, x_3, \dots, x_n) = -f(x_2, x_1, x_3, \dots, x_n)$, $2f(x_1, x_1, x_3, \dots, x_n) = 0$. Thus, f vanishes when $x_1 = x_2$. So a division on f by $x_1 - x_2$ in $R[x_2, \dots, x_n][x_1]$ yields $(x_1 - x_2) \mid f$. Similarly, $(x_1 - x_i) \mid f$, $i = 3, \dots, n$. Writing $f = \prod_{i \neq 1} (x_1 - x_i) f_1$, where $f_1 \in R[x_2, \dots, x_n]$ and is antisymmetric. Now an induction on n finishes the proof.)

5. Trace and Norm

Throughout this section we let $K \subsetneq L$ be a *simple algebraic field extension*, that is, $L = K(\vartheta)$, $\vartheta \in L$. If $p(x) \in K[x]$ is the minimal polynomial of ϑ over K , we may set a tower of field extensions

$$K \subset L \subset E$$

such that E contains *all distinct zeros* of $p(x)$, say $\vartheta_1 = \vartheta, \vartheta_2, \dots, \vartheta_m$, where $m \leq n = [L : K] = \deg p(x)$, that is, E contains the splitting field of $p(x)$.

5.1. Proposition With notation as above, there are exactly m distinct ring monomorphisms $L \rightarrow E$ that are K -linear. Moreover each K -linear monomorphism $L \rightarrow E$ is given by $\vartheta \rightarrow \vartheta_i$, $1 \leq i \leq m$.

Proof If $\sigma: L \rightarrow E$ is a monomorphism as described, then $0 = \sigma(p(\vartheta)) = p(\sigma(\vartheta))$, i.e., $\sigma(\vartheta)$ is a zero of $p(x)$. Note that the elements of L are of the form $\sum \lambda_j \vartheta^j$. It follows that if $L \xrightarrow{\sigma_1} E$ and $L \xrightarrow{\sigma_2} E$ are two K -linear ring

monomorphisms such that $\sigma_1(\vartheta) = \sigma_2(\vartheta)$, then $\sigma_1 = \sigma_2$.

Conversely, each ϑ_i defines a desired monomorphism

$$\begin{aligned} \sigma_i : \quad L &\longrightarrow E \\ \sum \lambda_j \vartheta^j &\mapsto \sum \lambda_j \vartheta_i^j \end{aligned}$$

because all ϑ_i 's have the same minimal polynomial $p(x)$. □

With the help of Proposition 5.1 we may determine, for every $\alpha \in L$, the minimal polynomial $p_\alpha(x)$ of α over K and the splitting field of $p_\alpha(x)$. To see this, let $\sigma_1, \dots, \sigma_m$ be all distinct monomorphisms $L \rightarrow E$ defined by $\sigma_i(\vartheta) = \vartheta_i$, $i = 1, \dots, m$. Suppose that each ϑ_i has multiplicity $e_i \geq 1$, that is, $p(x) = \prod_{i=1}^m (x - \vartheta_i)^{e_i}$ in $E[x]$. Then

$$e_1 + e_2 + \dots + e_m = n = \deg p(x),$$

and each $\alpha \in L = K(\vartheta)$ is associated to a monic polynomial in $E[x]$, that is,

$$f_\alpha(x) = \prod_{i=1}^m (x - \sigma_i(\alpha))^{e_i}.$$

For convenience, we call $f_\alpha(x)$ the *total polynomial* of α .

5.2. Proposition Let $K \subseteq L = K(\vartheta) \subset E$ be as above. For any $\alpha \in L = K(\vartheta)$, the following hold:

- (i) $f_\alpha(x) \in K[x]$.
- (ii) Let $p_\alpha(x) \in K[x]$ be the minimal polynomial of α over K . Then $f_\alpha(x) = p_\alpha(x)^s$ for some $s \geq 1$.
- (iii) E contains the splitting field of the minimal polynomial $p_\alpha(x)$ of α over K .

Proof (i) Since $\alpha = r(\vartheta) = \sum_{i=1}^{n-1} \lambda_i \vartheta^i$, where $r(x) = \sum_{i=1}^{n-1} \lambda_i x^i \in K[x]$, we have

$$\begin{aligned} f_\alpha(x) &= \prod_{i=1}^m (x - \sigma_i(r(\vartheta)))^{e_i} \\ &= \prod_{i=1}^m (x - r(\vartheta_i))^{e_i}. \end{aligned}$$

Note that all $\lambda_i \in K$. After expanding the latter product we see that the coefficients of $f_\alpha(x)$ are given by symmetric polynomials in the n zeros of $p(x)$. By Corollary 4.2, $f_\alpha(x) \in K[x]$.

(ii) By part (i), $f_\alpha(x) \in K[x]$ and $f_\alpha(\alpha) = 0$. It follows that $f_\alpha(x) = p_\alpha(x)^s h(x)$, where $h(x) \in K[x]$ and $p_\alpha(x)$, $h(x)$ are coprime and both are monic. If $h(x)$ is not a constant, then some $\sigma_i(\alpha)$ is a zero of $h(x)$. Let $\alpha = r(\vartheta) = \sum_{i=1}^{n-1} \lambda_i \vartheta^i$ with $r(x) = \sum_{i=1}^{n-1} \lambda_i x^i \in K[x]$. Then $\sigma_i(\alpha) = r(\vartheta_i)$ and $h(\sigma_i(\alpha)) = h(r(\vartheta_i)) = 0$. Set $g(x) = h(r(x)) \in K[x]$. Then $g(\vartheta_i) = h(r(\vartheta_i)) = 0$ implies $p(x)|g(x)$, for $p(x)$ is the minimal polynomial of ϑ and hence the minimal polynomial of each ϑ_i . It follows that $0 = g(\vartheta) = h(r(\vartheta)) = h(\alpha)$ and $p_\alpha(x)|h(x)$, a contradiction. This shows that $h(x)$ is a constant and $h(x) = 1$ because it is monic. Thus, $f_\alpha(x) = p_\alpha(x)^s$.

(iii) By parts (i) and (ii), $f_\alpha(x) \in K[x]$ and $f_\alpha(x) = \prod_{i=1}^m (x - \sigma_i(\alpha))^{e_i} = p_\alpha(x)^s$ for some $s \geq 1$. So $p_\alpha(x)$ factors into linear divisors over E . \square

We now introduce two functions on L that will play important roles in Chapter 3 section 3 and throughout Chapter 4.

Let $\alpha \in L = K(\vartheta)$. By Proposition 5.2(i), the total polynomial $f_\alpha(x)$ of α belongs to $K[x]$. By the definition, $f_\alpha(x) = \prod_{i=1}^m (x - \sigma_i(\alpha))^{e_i}$, where $e_1 + \dots + e_m = n = [L : K] = \deg p(x)$. If we check the expanded expression of $f_\alpha(x)$, then $f_\alpha(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$ with $c_{n-1} = -\sum_{i=1}^m e_i \sigma_i(\alpha)$ and $c_0 = (-1)^n \prod_{i=1}^m \sigma_i(\alpha)^{e_i}$. Thus, we have obtained two well-defined functions:

$$T_{L/K} : L \longrightarrow K$$

$$\alpha \mapsto \sum_{i=1}^m e_i \sigma_i(\alpha)$$

$$N_{L/K} : L \longrightarrow K$$

$$\alpha \mapsto \prod_{i=1}^m \sigma_i(\alpha)^{e_i}$$

5.3. Definition For $\alpha \in L$, $T_{L/K}(\alpha)$ is called the *trace* of α in K and $N_{L/K}(\alpha)$ is called the *norm* of α in K .

5.4. Proposition For $\alpha, \beta \in L$, $\lambda, \mu \in K$, the following hold:

(i) $T_{L/K}(\lambda\alpha + \mu\beta) = \lambda T_{L/K}(\alpha) + \mu T_{L/K}(\beta)$.

- (ii) $T_{L/K}(\alpha\beta) = T_{K/L}(\beta\alpha)$.
 (iii) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.

Proof Exercise. □

Knowledge on bilinear forms needed by the next theorem and Chapter 3 Theorem 3.2 is given as an appendix at the end of this section.

Viewing L as an n -dimensional K -vector space, Proposition 5.4 enables us to define a symmetric bilinear form on L :

$$\begin{aligned} L \times L &\longrightarrow K \\ (\alpha, \beta) &\mapsto T_{L/K}(\alpha\beta) \end{aligned}$$

5.5. Theorem For $K \subseteq L = K(\vartheta)$ with $[L : K] = n$, if the minimal polynomial $p(x)$ of ϑ over K has n distinct zeros $\vartheta_1 = \vartheta, \vartheta_2, \dots, \vartheta_n$, then the bilinear form defined above is nondegenerate.

Proof Set $r(k) = (\vartheta_1^k, \dots, \vartheta_n^k)$, $k = 0, \dots, n-1$, and write V for the Vandermonde matrix

$$V = \begin{pmatrix} r(0) \\ r(1) \\ r(2) \\ \vdots \\ r(n-1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vartheta_1 & \vartheta_2 & \cdots & \vartheta_n \\ \vartheta_1^2 & \vartheta_2^2 & \cdots & \vartheta_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \vartheta_1^{n-1} & \vartheta_2^{n-1} & \cdots & \vartheta_n^{n-1} \end{pmatrix}.$$

Let $\sigma_1, \dots, \sigma_n$ be all the n distinct K -linear monomorphisms from L to E as described in Proposition 5.1 such that $\sigma_i(\vartheta) = \vartheta_i$, $i = 1, \dots, n$. If we consider the standard K -basis $\{1, \vartheta, \dots, \vartheta^{n-1}\}$ of L , then since

$$T_{L/K}(\vartheta^k \vartheta^j) = \sum_{i=1}^n \sigma_i(\vartheta^k \vartheta^j) = \sum_{i=1}^n \vartheta_i^k \vartheta_i^j = \vartheta(k)(\vartheta(j))^t,$$

the matrix of the bilinear form is given by

$$(T_{L/K}(\vartheta^k \vartheta^j)) = VV^t$$

and hence

$$\det(T_{L/K}(\vartheta^k \vartheta^j)) = (\det(V))^2.$$

Since all the ϑ_i are distinct, $\det(V) = \prod_{i < j} (\vartheta_i - \vartheta_j) \neq 0$. This shows that the bilinear form is nondegenerate. □

5.6. Corollary If $K \subseteq L$ is a finite dimensional separable field extension, then Theorem 5.5 hold. □

Appendix. Bilinear forms

Let U and V be two vector spaces over a field K , $U \times V = \{(u, v) \mid u \in U, v \in V\}$ the Cartesian product of U and V . A *bilinear form* on $U \times V$ is a mapping

$$\begin{aligned} \langle \ , \ \rangle: U \times V &\longrightarrow K \\ (u, v) &\mapsto \langle u, v \rangle \end{aligned}$$

satisfying

$$\begin{aligned} \langle \lambda u_1 + \mu u_2, v \rangle &= \lambda \langle u_1, v \rangle + \mu \langle u_2, v \rangle \\ \langle u, \lambda v_1 + \mu v_2 \rangle &= \lambda \langle u, v_1 \rangle + \mu \langle u, v_2 \rangle \end{aligned}$$

for all $u_1, u_2 \in U, v_1, v_2 \in V$ and $\lambda, \mu \in K$.

A bilinear form $\langle \ , \ \rangle$ on $V \times V$ is called a *bilinear form on V* . A bilinear form $\langle \ , \ \rangle$ on V is said to be *symmetric* if $\langle x, y \rangle = \langle y, x \rangle$ for all $x, y \in V$.

If $\langle \ , \ \rangle$ is a bilinear form on $U \times V$ which satisfies

$$\begin{aligned} \langle u, v' \rangle = 0 \text{ for all } u \in U &\text{ implies } v' = 0, \text{ and} \\ \langle u', v \rangle = 0 \text{ for all } v \in V &\text{ implies } u' = 0, \end{aligned}$$

then $\langle \ , \ \rangle$ is called a *nondegenerate* bilinear form.

Let U and V be finite dimensional K -spaces. Given a basis $\{u_1, \dots, u_m\}$ of U and a basis $\{v_1, \dots, v_n\}$ of V , if $\langle \ , \ \rangle$ is any bilinear form on $U \times V$, then there is an associated $m \times n$ matrix $A = (a_{ij})$ with

$$a_{ij} = \langle u_i, v_j \rangle, \quad i = 1, \dots, m, \quad j = 1, \dots, n,$$

and $\langle \ , \ \rangle$ is completely determined by A , that is, given

$$(1) \quad u = \sum_{i=1}^m \lambda_i u_i, \quad v = \sum_{j=1}^n \mu_j v_j,$$

it follows from the bilinear property of $\langle \ , \ \rangle$ that

$$\begin{aligned} \langle u, v \rangle &= \langle \sum \lambda_i u_i, \sum \mu_j v_j \rangle \\ &= \sum \lambda_i \mu_j \langle u_i, v_j \rangle \\ &= \sum \lambda_i a_{ij} \mu_j \\ &= (\lambda_1, \dots, \lambda_m) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}. \end{aligned}$$

Conversely, any $m \times n$ matrix over K yields a bilinear form on $U \times V$ in this way.

Now, suppose that $\{u'_1, \dots, u'_m\}$ and $\{v'_1, \dots, v'_n\}$ are new bases for U and V respectively, and that

$$(2) \quad u = \sum_{i=1}^m \lambda'_i u'_i, \quad v = \sum_{j=1}^n \mu'_j v'_j.$$

Then it follows from a change of bases and (1) that

$$(\lambda_1, \dots, \lambda_m) = (\lambda'_1, \dots, \lambda'_m)P,$$

$$(\mu_1, \dots, \mu_n) = (\mu'_1, \dots, \mu'_n)Q$$

for some invertible matrices $P = P_{m \times m}$, $Q = Q_{n \times n}$. Thus,

$$\langle u, v \rangle = (\lambda'_1, \dots, \lambda'_m)PAQ^t \begin{pmatrix} \mu'_1 \\ \vdots \\ \mu'_n \end{pmatrix},$$

and consequently, the matrix referred to the new bases is PAQ^t .

5.7. Theorem (i) Let U and V be finite dimensional vector spaces over a field K , where $\dim_K U = m$ and $\dim_K V = n$. If $\langle \ , \ \rangle$ is any nondegenerate bilinear form on $U \times V$, then $m = n$, and for any basis $\{u_1, \dots, u_n\}$ of U there exists a unique basis $\{v_1, \dots, v_n\}$ of V such that

$$\langle u_i, v_j \rangle = \delta_{ij} = \begin{cases} 0, & \text{if } i \neq j, \\ 1, & \text{if } i = j. \end{cases}$$

(ii) A bilinear form $\langle \cdot, \cdot \rangle$ on a finite n -dimensional K -space V is nondegenerate if and only if the associated matrix $A = (a_{ij})$, where $a_{ij} = \langle v_i, v_j \rangle$, is invertible for any basis $\{v_1, \dots, v_n\}$ of V .

Proof (i) Let $\{u_1, \dots, u_m\}$ be any basis of U . Consider the linear mapping induced by $\langle \cdot, \cdot \rangle$

$$\begin{aligned} \sigma : V &\longrightarrow K^m = \{(\lambda_1, \dots, \lambda_m) \mid \lambda_i \in K\} \\ v &\mapsto (\langle u_1, v \rangle, \dots, \langle u_m, v \rangle) \end{aligned}$$

Then σ is injective because $\langle \cdot, \cdot \rangle$ is nondegenerate. Thus, $n = \dim_K V \leq \dim_K U = m$. Similarly we also have $m \leq n$. Hence $m = n$.

Note that σ is now an isomorphism. If we use the standard basis $\{e_1, \dots, e_m\}$ of K^m , where

$$e_j = (\underbrace{0, \dots, 0}_{j-1}, 1, 0, \dots, 0), \quad j = 1, \dots, m,$$

and write v_j for the inverse image of e_j under σ , then it is clear that $\{v_1, \dots, v_m\}$ is a basis for V and $\langle u_i, v_j \rangle = \delta_{ij}$, $i, j = 1, \dots, m$. If $\{v'_1, \dots, v'_m\}$ is another basis of V with this property, then $\sigma(v_i - v'_i) = 0$ implies $v_i = v'_i$, $i = 1, \dots, m$, because σ is injective.

(ii) This follows from part (i) and previous discussion on the associated matrices of $\langle \cdot, \cdot \rangle$ with respect to given bases.

Exercises

1. Complete the proof of Proposition 5.4.
2. Let $d \in \mathbb{Z}$ be square-free, $K = \mathbb{Q}(\sqrt{d})$. Find all \mathbb{Q} -linear ring monomorphisms $K \rightarrow \mathbb{C}$.
3. Let $K = \mathbb{Q}(\sqrt{d})$ be as in exercise 2 above, $\alpha = r + s\sqrt{d}$. Show that $T_{K/\mathbb{Q}}(\alpha) = 2r$ and $N_{K/\mathbb{Q}}(\alpha) = r^2 - s^2d$. (Compare with section 3, exercise 6.)
4. Let $\vartheta = \sqrt{2} + \sqrt{3}$, $K = \mathbb{Q}(\vartheta)$. Find the minimal polynomial $p(x)$ of ϑ . (Hint: Note that $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}) \subset K$. Any \mathbb{Q} -linear ring monomorphism $\sigma: K \rightarrow \mathbb{C}$ induces a \mathbb{Q} -linear ring monomorphism $\sigma_1: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{C}$ and a \mathbb{Q} -linear ring monomorphism $\sigma_2: \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{C}$, such that $\sigma(\vartheta) = \sigma_1(\sqrt{2}) + \sigma_2(\sqrt{3})$. The answer is $p(x) = x^4 - 10x^2 + 1$.)

Can you generalize this result to $\vartheta = \sqrt{p} + \sqrt{q}$ for arbitrary square-free $p \neq q$?

6. Free Abelian Groups of Finite Rank

Let G be an abelian group with the binary additive operation $+$ and the identity element 0 . For $g \in G$, we write $\mathbb{Z}g$ for the cyclic subgroup of G generated by g , and consequently, we write $\sum_{g \in \Omega} \mathbb{Z}g$ for the subgroup of G generated by a nonempty subset $\Omega \subseteq G$.

A subset $\Omega = \{g_i\}_{i \in J}$ of G is said to be \mathbb{Z} -linearly independent if for any finitely many $g_{i_1}, g_{i_2}, \dots, g_{i_n} \in \Omega$, there do not exist $s_1, \dots, s_n \in \mathbb{Z}$, not all zero, such that $s_1g_{i_1} + s_2g_{i_2} + \dots + s_n g_{i_n} = 0$. If Ω is not \mathbb{Z} -linearly independent, then it is \mathbb{Z} -linearly dependent.

6.1. Definition Let $\Omega = \{g_i\}_{i \in J} \subset G$. If $G = \sum_{g_i \in \Omega} \mathbb{Z}g_i$ and Ω is \mathbb{Z} -linearly independent, then G is called a *free abelian group* and Ω is called a \mathbb{Z} -basis of G , or just a *basis* of G .

Below we focus on free abelian groups with finite \mathbb{Z} -basis.

6.2. Proposition If a free abelian group G has two bases $\{g_1, \dots, g_n\}$ and $\{h_1, \dots, h_m\}$, then $m = n$.

Proof Suppose $m < n$. Then, as dealing with vector bases over a field in linear algebra, after expressing each g_i as a \mathbb{Z} -linear combination of h_i 's, we may derive, by passing to \mathbb{Q} , that $\{g_1, \dots, g_n\}$ is \mathbb{Z} -linearly dependent, a contradiction. Hence, $m \geq n$. By symmetry, $n \geq m$. Thus, $m = n$ as desired. \square

6.3. Definition An abelian group G with a basis of n elements is called a *free abelian group of \mathbb{Z} -rank n* , or just a *free abelian group of rank n* .

\mathbb{Z} is a free abelian group of rank 1 and $\{1\}$ is a basis for \mathbb{Z} . The direct sum

$$\mathbb{Z}^n = \mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z} = \left\{ (k_1, \dots, k_n) \mid k_i \in \mathbb{Z} \right\}$$

of n copies of \mathbb{Z} , where

$$(k_1, \dots, k_n) + (\ell_1, \dots, \ell_n) = (k_1 + \ell_1, \dots, k_n + \ell_n),$$

$$m(k_1, \dots, k_n) = (mk_1, \dots, mk_n), \quad m \in \mathbb{Z},$$

is a free abelian group of rank n with the standard basis

$$\left\{ e_i = \underbrace{(0, \dots, 0)}_{i-1}, 1, 0, \dots, 0 \mid i = 1, \dots, n \right\}.$$

6.4. Proposition Any finitely generated abelian group $G = \sum_{i=1}^n \mathbb{Z}g_i$ is a homomorphic image of some free abelian group of rank n . If G is free and $\{g_1, \dots, g_n\}$ is a basis of G , then $G \cong \mathbb{Z}^n$.

Proof Exercise. □

In view of Proposition 6.4, from now on we write

$$G = \bigoplus_{i=1}^n \mathbb{Z}g_i$$

for the free abelian group G with basis $\{g_1, \dots, g_n\}$.

Let $M_n(\mathbb{Z})$ be the set of all $n \times n$ matrices over \mathbb{Z} . If $A \in M_n(\mathbb{Z})$ and $\det(A) = \pm 1$, then we say that A is *unimodular*.

If $A \in M_n(\mathbb{Z})$ is unimodular, then A is invertible and

$$A^{-1} = \frac{1}{\det(A)} A^* = \pm A^*$$

where A^* is the adjoint matrix of A . Clearly, the construction of A^* implies $A^* \in M_n(\mathbb{Z})$. It follows that $A^{-1} \in M_n(\mathbb{Z})$.

6.5. Lemma If $\{u_1, \dots, u_n\}$ is a basis for the free abelian group G , then $\{v_1, \dots, v_n\}$, where

$$v_i = \sum_j^n a_{ij} u_j, \quad a_{ij} \in \mathbb{Z}, \quad i = 1, \dots, n,$$

is a basis for G if and only if $A = (a_{ij})$ is unimodular.

Proof With the help of the above remark, this is an easy exercise. □

6.6. Theorem Let G be a free abelian group of rank n and H a nonzero subgroup of G . Then the following hold:

(i) H is free of rank $s \leq n$.

(ii) There exist a basis $\{g_1, \dots, g_n\}$ for G and integers $\ell_1, \dots, \ell_s \in \mathbb{Z}^+$ such that $\{\ell_1 g_1, \dots, \ell_s g_s\}$ is a basis for H .

Proof We prove the theorem by induction on the rank of G . If $\text{rank} G = 1$, then $G \cong \mathbb{Z}$ and the conclusions (i) and (ii) are clear.

Suppose the assertions (i) and (ii) are true for any free abelian group of rank $< n$.

Let G be a free abelian group of rank n and let H be a nonzero subgroup of G . Then, with respect to a fixed basis $\{e_1, \dots, e_n\}$ of G , H contains elements

$$(1) \quad h = k_1 e_1 + \dots + k_n e_n, \text{ some } k_i \text{'s are positive.}$$

Choose a basis $\{x_1, \dots, x_n\}$ of G such that ℓ_1 is the smallest positive coefficient with respect to (1), and rearrange the members of this basis (if necessary) so that H contains an element of the form

$$f_1 = \ell_1 x_1 + m_2 x_2 + \dots + m_n x_n.$$

On division by ℓ_1 , write

$$(2) \quad m_i = \ell_1 q_i + r_i, \quad q_i, r_i \in \mathbb{Z}, \quad 0 \leq r_i < \ell_1, \quad 2 \leq i \leq n.$$

If we define

$$g_1 = x_1 + q_2 x_2 + \dots + q_n x_n$$

$$g_2 = x_2$$

$$\vdots$$

$$g_n = x_n,$$

then

$$\begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{pmatrix} = \begin{pmatrix} 1 & q_2 & \cdots & q_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

where the square matrix is clearly unimodular. By Lemma 6.5, $\{g_1, x_2, \dots, x_n\}$

is a basis of G . With respect to this new basis and previous formula (2),

$$\begin{aligned}
 f_1 &= \ell_1 x_1 + m_2 x_2 + \cdots + m_n x_n \\
 &= \ell_1 (g_1 - q_2 x_2 - \cdots - q_n x_n) + m_2 x_2 + \cdots + m_n x_n \\
 &= \ell_1 g_1 + (m_2 - \ell_1 q_2) x_2 + \cdots + (m_n - \ell_1 q_n) x_n \\
 &= \ell_1 g_1 + r_2 x_2 + \cdots + r_n x_n.
 \end{aligned}$$

By the choice of ℓ_1 , we must have $r_2 = \cdots = r_n = 0$. It follows that

$$(3) \quad f_1 = \ell_1 g_1.$$

Now, with respect to the new basis $\{g_1, x_2, \dots, x_n\}$, each $h \in H$ has the expression

$$h = c_1 g_1 + c_2 x_2 + \cdots + c_n x_n, \quad c_i \in \mathbb{Z}.$$

Write $c_1 = \ell_1 q + r$ with $q, r \in \mathbb{Z}$, $0 \leq r < \ell_1$. Then by the above (3), H contains

$$\begin{aligned}
 h - qf_1 &= \ell_1 q g_1 + r g_1 - \ell_1 q g_1 + c_2 x_2 + \cdots + c_n x_n \\
 &= r g_1 + c_2 x_2 + \cdots + c_n x_n.
 \end{aligned}$$

Again by the choice of ℓ_1 we have $r = 0$. This yields

$$qf_1 + c_2 x_2 + \cdots + c_n x_n = h \in \mathbb{Z}f_1 + G^* \text{ with } G^* = \bigoplus_{j=2}^n \mathbb{Z}x_j.$$

Thus

$$\varphi: H \longrightarrow G^*$$

$$h \mapsto c_2 x_2 + \cdots + c_n x_n$$

defines a group homomorphism and $H \cong \mathbb{Z}f_1 + \varphi(H)$. Note that $\varphi(H)$ is a subgroup of G^* that is free of rank $n - 1$. By the induction hypothesis, there exist basis $\{g_2, \dots, g_n\}$ of G^* and integers $\ell_2, \dots, \ell_s \in \mathbb{Z}^+$, where $s \leq n - 1$, such that $\{\ell_2 g_2, \dots, \ell_s g_s\}$ forms a basis for $\varphi(H)$. Thus, $\{\ell_1 g_1 = f_1, \ell_2 g_2, \dots, \ell_s g_s\}$ forms a basis for H , as desired. \square

6.7. Theorem Let G be a free abelian group of rank n and H a subgroup of G . The following statements hold:

(i) G/H is finite if and only if $\text{rank}G = \text{rank}H$.

(ii) If $\text{rank}G = \text{rank}H = n$, $\{x_1, \dots, x_n\}$ is a basis for G , $\{y_1, \dots, y_n\}$ is a basis for H , and

$$y_i = \sum_{j=1}^n a_{ij}x_j, \quad a_{ij} \in \mathbb{Z}, \quad i = 1, \dots, n,$$

then the number of elements of G/H is equal to $|\det(A)|$, where $A = (a_{ij})$.

Proof (i) By Theorem 6.6, choose a basis $\{g_1, \dots, g_n\}$ of G and a basis $\{f_1, \dots, f_s\}$ of H with $f_i = \ell_i g_i$ and $\ell_i \in \mathbb{Z}^+$, $i = 1, \dots, s \leq n$. Thus

$$G = \mathbb{Z}g_1 \oplus \mathbb{Z}g_2 \oplus \cdots \oplus \mathbb{Z}g_n$$

$$H = \mathbb{Z}\ell_1 g_1 \oplus \mathbb{Z}\ell_2 g_2 \oplus \cdots \oplus \mathbb{Z}\ell_s g_s$$

and we have the group isomorphism

$$G/H \xrightarrow{\cong} \mathbb{Z}_{\ell_1} \oplus \mathbb{Z}_{\ell_2} \oplus \cdots \oplus \mathbb{Z}_{\ell_s} \oplus (\mathbb{Z}g_{s+1} \oplus \cdots \oplus \mathbb{Z}g_n)$$

$$\overline{\sum_{i=1}^s k_i g_i + \sum_{j=s+1}^n k_j g_j} \mapsto \sum_{i=1}^s \overline{k_i} + \sum_{j=s+1}^n k_j g_j$$

It follows that G/H is finite if and only if $n = s$.

(ii) By the proof of part (i), if G/H is finite then it has exactly $\ell_1 \ell_2 \cdots \ell_n$ elements. Employing the chosen bases in part (i), we have

$$g_i = \sum_{j=1}^n b_{ij}x_j$$

$$f_i = \sum_{j=1}^n c_{ij}g_j = \ell_i g_i$$

$$y_i = \sum_{j=1}^n d_{ij}f_j$$

Then $(b_{ij}) = B$ and $(d_{ij}) = D$ are unimodular, and

$$C = (c_{ij}) = \begin{pmatrix} \ell_1 & 0 & \cdots & 0 \\ 0 & \ell_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \ell_n \end{pmatrix}.$$

Taking the matrix $A = (a_{ij})$ from the assumption of part (ii) into account, we get $A = BCD$ and $\det(A) = \det(B)\det(C)\det(D)$. Therefore, $|\det(A)| = \ell_1\ell_2\cdots\ell_n$.

Exercises

1. Let $i = \sqrt{-1}$. Show that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z} \oplus \mathbb{Z}$.
2. Complete the proof of Proposition 6.4.
3. Complete the proof of Lemma 6.5.
4. An abelian group G is said to be *torsion-free* if G does not have finite order nonzero element. Show that a finitely generated torsion-free abelian group is free of finite rank. (Hint: Use Proposition 6.4 and refer to the proof of Theorem 6.7.)
5. Show that a finitely generated abelian group G is either finite or isomorphic to the direct sum of a free abelian group of finite rank and a finite abelian group.

7. Noetherian Modules

Let R be a ring.

7.1. Definition Let M be an abelian group with the binary additive operation $+$ and the identity element 0 . We say that M is an R -module if there is a mapping

$$\begin{aligned} \alpha: R \times M &\longrightarrow M \\ (r, m) &\mapsto \alpha(r, m) = rm \end{aligned}$$

(called the R -action on M) satisfying

- (M1) $(r + s)m = rm + sm$,
- (M2) $r(m + m') = rm + rm'$,
- (M3) $r(sm) = (rs)m$,

$$(M4) \quad 1m = m$$

for all $r, s \in R$ and $m, m' \in M$.

By definition, a \mathbb{Z} -module is nothing but an abelian group M (binary operation is written additively). Conversely, given an (additive) abelian group M , M can be made into a \mathbb{Z} -module by defining

$$0m = 0 \text{ and } 1m = m \text{ for } m \in M,$$

then inductively

$$(n + 1)m = nm + m \text{ for } n \in \mathbb{Z}^+, m \in M,$$

and

$$(-n)m = -nm \text{ for } n \in \mathbb{Z}^+, m \in M.$$

If $R = K$ is a field, then an R -module is nothing but a K -vector space. In this sense we may view an R -module as the generalization of a vector space. However, since not every nonzero element in an arbitrary ring R is a unit, many of the techniques developed in vector space theory cannot be performed directly to deal with R -modules.

From the definition it is clear that if M is an R -module then every $r \in R$ defines an endomorphism of the abelian group M , that is, $\rho_r: M \rightarrow M$ with $\rho_r(m) = rm$. One easily checks that this yields a ring homomorphism $\sigma: R \rightarrow \text{End}_{\mathbb{Z}}M$ with $\sigma(r) = \rho_r$, where $\text{End}_{\mathbb{Z}}M$ is the ring of endomorphisms of M . Conversely, if M is an abelian group then any ring homomorphism $\varphi: R \rightarrow \text{End}_{\mathbb{Z}}M$ induces an R -module structure: $rm = \varphi(r)(m)$. This is the idea of modern representation theory of rings and algebras.

Two special kinds of module will be used frequently in the follow-up chapters:

- If R is a subring of a ring S (note that $1_R = 1_S$ by our convention made on rings), then S is an R -module with the action given by the ring multiplication.
- If I is an ideal of the ring R . Then I is an R -module with the action given by the ring multiplication.

Let M be an R -module and N an (additive) subgroup of M . If $rx \in N$ for all $r \in R$ and $x \in N$, then N is called an R -submodule of M .

Given a family $\{N_i\}_{i \in I}$ of R -submodules of M , the sum $\sum_{i \in I} N_i$ of subgroups forms an R -submodule in a natural way; and the intersection

$\bigcap_{i \in I} N_i$ is an R -submodule.

Given an R -submodule of a module M , an R -action on the quotient group M/N is defined as

$$r\bar{m} = \overline{rm}, \quad r \in R, \quad \bar{m} \in M/N.$$

With the R -action defined above, M/N is called the *quotient R -module* determined by N .

Let M and N be R -modules. An R -module homomorphism from M to N is a homomorphism of abelian groups $\psi: M \rightarrow N$ satisfying $\psi(rm) = r\psi(m)$ for all $r \in R$ and $m \in M$. It can be verified directly that $\text{Ker}\psi$ is an R -submodule of M , that $\text{Im}\psi$ is a submodule of N , and furthermore, that the following R -module isomorphism theorems hold:

- (a) $M/\text{Ker}\psi \cong \text{Im}\psi$.
- (b) Let A, B be submodules of the R -module M . Then, $(A + B)/B \cong A/(A \cap B)$.
- (c) Let A, B be submodules of the R -module M . If $A \subseteq B$ then $(M/A)/(B/A) \cong M/B$.
- (d) Let N be a submodule of the R -module M . Then there is a bijection between the submodules of M which contain N and the submodules of M/N :

$$\alpha: A \longleftrightarrow (A + N)/N$$

such that $\alpha(A + B) = \alpha(A) + \alpha(B)$ and $\alpha(A \cap B) = \alpha(A) \cap \alpha(B)$ for all submodules A, B of M containing N .

Let $S \subseteq M$, where M is an R -module, and $T \subseteq R$. Put

$$TS = \left\{ \text{finite sums } \sum r_i m_i \mid r_i \in T, m_i \in S \right\}.$$

With notation as above, the reader is also asked to check the following statements.

- (e) If $T = R$, then RS forms an R -submodule of M ; moreover, $RS = \sum_{m_i \in S} Rm_i$ and it is the smallest R -submodule of M containing S .
- (f) If T is an ideal of R , then TM forms an R -submodule.

The R -submodule $N = RS$ obtained in part (e) above is called an R -submodule of M *generated by S* , where S is called a *set of generators* of N . If $M = RS$ with a finite set of generators $S = \{m_1, \dots, m_s\}$, then $M = \sum_{i=1}^s Rm_i$ and is called a *finitely generated R -module*.

Given a family of R -modules $\{M_i\}_{i \in J}$, the direct sum of abelian groups

$$\bigoplus_{i \in J} M_i = \left\{ (m_i)_{i \in J} \mid 0 \neq m_i \in M_i \text{ for only finitely many } m_i \right\}$$

is an R -module, where

$$(m_i)_{i \in J} + (m'_i)_{i \in J} = (m_i + m'_i)_{i \in J},$$

$$r(m_i)_{i \in J} = (rm_i)_{i \in J}, \quad r \in R,$$

and is called the *direct sum* of $\{M_i\}_{i \in J}$.

For the direct sum $\bigoplus_{i \in J} M_i$ of given R -modules defined above, it is not hard to see that there is an injective R -module homomorphism $M_i \rightarrow \bigoplus_{i \in J} M_i$ with $m_i \mapsto (x_i)_{i \in J}$, where $x_i = m_i$ and $x_j = 0$ for $j \neq i$. Hence M_i is isomorphic to a submodule of $\bigoplus_{i \in J} M_i$. Conversely, let $\{N_i\}_{i \in J}$ be a family of submodules of some R -module M , and let $N = \sum_{i \in J} N_i$. Then

$$\phi : \bigoplus_{i \in J} N_i \longrightarrow N = \sum_{i \in J} N_i$$

$$(x_i)_{i \in J} \mapsto \sum x_i$$

defines an R -module homomorphism. If ϕ is an isomorphism then N is said to be the *direct sum of its submodules* N_i , $i \in J$, and we also write $N = \bigoplus_{i \in J} N_i$.

Let M be an R -module and suppose that $M = \bigoplus_{i \in J} M_i$ for some submodules $M_i \subset M$, $i \in J$. Then it is clear that every element $m \in M$ has a *unique* expression $m = \sum m_i$, i.e., $\sum m_i = 0$ if and only if $m_i = 0$.

7.2. Definition An R -module M is said to be *free* if there are $\xi_i \in M$, $i \in J$, such that $M = \bigoplus_{i \in J} R\xi_i$, where $\{\xi_i\}_{i \in J}$ is called an *R -basis* of M .

Example (i) Any vector space V over a field K is a free K -module. Any free abelian group (as defined in section 6) is a free \mathbb{Z} -module.

(ii) For any set J of indices, $F = \bigoplus_{i \in J} R_i$ with $R_i \cong R$ (as R -modules) is a free R -module.

7.3. Proposition Any R -module M is the homomorphic image of some free R -module.

Proof The R -module homomorphism $\oplus_{m \in M} Rm \rightarrow M = \sum_{m \in M} Rm$ defined by $\sum r_m \mapsto \sum r_m m$ does the job. \square

An R -module M is said to be *Noetherian* if every R -submodule of M is finitely generated.

7.4. Theorem For an R -module M , the following statements are equivalent.

- (i) M is Noetherian.
- (ii) For any ascending chain

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

of R -submodules in M , there is some k such that $M_k = M_j$ for all $j \geq k$.

- (iii) Every nonempty set of R -submodules has a maximal element with respect to \subseteq .

Proof Exercise (see the proof of Theorem 1.1). \square

7.5. Theorem (i) Let $\varphi: M \rightarrow H$ be an onto R -module homomorphism. If R is Noetherian then so are $\text{Ker}\varphi$ and H .

(ii) Let N be an R -submodule of the R -module M . Then M is Noetherian if and only if N and M/N are Noetherian.

Proof To better understand the argumentation, the reader is reminded to bear the foregoing R -isomorphism theorems (a)–(d) in mind.

(i) This follows from the fact that ascending chains of R -submodules in $\text{Ker}\varphi$ and H correspond to some ascending chains of submodules in M .

(ii) If M is Noetherian then so are N and M/N by part (i). Now let

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$

be an ascending chain of R -submodules of M . Then

$$N \cap M_1 \subset N \cap M_2 \subset \cdots \subset N \cap M_n \subset \cdots$$

is a chain of R -submodules in N and for some $\ell \geq 1$

$$(1) \quad N \cap M_\ell = N \cap M_{\ell+i}, \quad i = 1, 2, \dots$$

On the other hand, we also have a chain of R -submodules in M/N

$$\frac{M_1 + N}{N} \subset \frac{M_2 + N}{N} \subset \cdots \subset \frac{M_n + N}{N} \subset \cdots$$

and (without loss of generality) for $\ell \geq 1$

$$(2) \quad \frac{M_\ell + N}{N} = \frac{M_{\ell+i} + N}{N}, \quad i = 1, 2, \dots$$

Thus, for $m \in M_{\ell+i}$, formula (2) implies $m = m' + x$ for some $m' \in M_\ell$ and $x \in N$. But then

$$x = m - m' \subset M_{\ell+i} \cap N = M_\ell \cap N$$

by (1) above. It follows that $m - m' = m''$ with $m'' \in M_\ell \cap N$, and consequently $m = m' + m'' \in M_\ell$. This shows that $M_j = M_\ell$ for $j \geq \ell$, that is, M is Noetherian. \square

7.6. Theorem (i) Given finitely many Noetherian R -modules M_1, \dots, M_s , the direct sum $\bigoplus_{i=1}^s M_i$ is a Noetherian R -module.

(ii) If R is a Noetherian ring and M is a finitely generated R -module, then every submodule of M is Noetherian, in particular, M is Noetherian.

Proof (i) Set $M = M_1 \oplus M_2$. Then M_1 and $M/M_1 \cong M_2$ are Noetherian by the assumption. It follows from Proposition 7.5(ii) that M is Noetherian. Now an induction on s shows that $\bigoplus_{i=1}^s M_i$ is Noetherian.

(ii) Suppose $M = \sum_{i=1}^s R\xi_i$, $\xi_i \in M$. Then there is an onto R -module homomorphism

$$\underbrace{R \oplus R \oplus \dots \oplus R}_s \longrightarrow M = \sum_{i=1}^s R\xi_i$$

$$\sum_{i=1}^s r_i \quad \mapsto \quad \sum_{i=1}^s r_i \xi_i$$

So the conclusion now follows from part (i) and Theorem 7.5. \square

We complete this chapter with the celebrated Krull's intersection theorem.

7.7. Theorem (Krull) Let R be a Noetherian ring and I an ideal of R . Given a finitely generated R -module M , let

$$U = \bigcap_{n=1}^{\infty} I^n M.$$

Then $IU = U$.

Proof First note that every $I^n M$, hence U and IU are R -submodules. So it is clear that we need only to show $U \subseteq IU$. For this purpose, noticing $U \cap IU = IU$, let us consider

$$\Omega = \left\{ S \mid S \text{ a submodule of } M, S \cap U = IU \right\}.$$

Then Ω has a maximal member, say S , with respect to \subseteq on submodules, for M is Noetherian by Theorem 7.6.

Claim For the maximal S obtained above, there is some n such that $I^n M \subseteq S$, and consequently, $U = I^n M \cap U \subseteq S \cap U = IU$.

To find the above claimed n , let $I = \sum_{i=1}^s R\xi_i$, $\xi_i \in I$. If we can find, for each ξ_i , some n_i such that

$$(*) \quad \xi_i^{n_i} M \subseteq S,$$

then there will be some n , large enough, such that $I^n M \subseteq S$. As a matter of fact, we may reach the above mentioned property $(*)$ for any $a \in I$. To see this, define, for each $k \geq 1$, the R -submodule

$$M_k = \left\{ m \in M \mid a^k m \in S \right\}.$$

Then we obtain an ascending chain

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_q \subseteq \cdots$$

and there is some z such that $M_z = M_j$ for all $j \geq z$. For this fixed z , obviously $IU \subseteq (a^z M + S) \cap U$. On the other hand, if $u \in (a^z M + S) \cap U$, then $u = a^z m + v$ with $m \in M$ and $v \in S$. Hence $au \in aU \subseteq IU \subseteq S$, and $a^{z+1} m \in S$. This shows that $m \in M_{z+1} = M_z$, and it follows that $a^z m \in S$. But this yields $u \in S \cap U = IU$, and consequently $IU = (a^z M + S) \cap U$. If $a^z M + S = M$, then $U = IU$; otherwise, by the maximality of S in Ω , $a^z M \subseteq S$, as desired. \square

7.8. Corollary Let R be a Noetherian domain, and let M be a finitely generated torsion-free R -module, i.e., for $r \in R$ and $m \in M$, $rm = 0$ implies $r = 0$ or $m = 0$. Then

$$\bigcap_{n=1}^{\infty} I^n M = \{0\}.$$

Proof This follows from Theorem 7.7 and later exercise 6.

Exercises

- Find all \mathbb{Z} -submodules of \mathbb{Z} and all \mathbb{Z} -module homomorphisms $\mathbb{Z} \rightarrow \mathbb{Z}$.
- Complete the proof of Proposition 7.4.
- Let R be a domain with the field of fractions K . Let $\lambda \in R$ be nonzero and nonunit. Show that $R[\frac{1}{\lambda}]$, the subring of K generated by $\frac{1}{\lambda}$ over R , is not a finitely generated R -module. (Hint: If there was a finite set of generators, then $1, \frac{1}{\lambda}, \frac{1}{\lambda^2}, \dots, \frac{1}{\lambda^s}$ would be a set of generators for some $s > 0$. After expressing $\frac{1}{\lambda^{s+1}}$ as an R -linear combination of the foregoing generators, see what happens.)
- Show that there is no nonzero \mathbb{Z} -module homomorphism $\mathbb{Q} \rightarrow \mathbb{Z}$.
- Let R be a ring and let I_1, \dots, I_s be finitely many ideals of R . Suppose that R/I_j is Noetherian, $j = 1, \dots, s$, and that $\bigcap_{j=1}^s I_j = \{0\}$. Show that R is Noetherian. (Hint: Consider the R -module homomorphism $R \rightarrow \bigoplus_{j=1}^s (R/I_j)$ with $r \mapsto \sum x_j$, where $x_j = \bar{r} \in R/I_j$, $j = 1, \dots, s$.)
- For any ring R , one may also define matrices $(r_{ij})_{m \times n}$ of finite order with entries $r_{ij} \in R$, define addition and multiplication of matrices, and define the determinant, adjoint and inverse of a square matrix, as in classical linear algebra.

Let $M = \sum_{i=1}^s R\xi_i$ be a finitely generated R -module, where $\xi_i \in M$, $i = 1, \dots, s$, and let I be an ideal of R . Show that if $IM = M$ then there is some $r \in R$ such that $rM = \{0\}$ and $1 - r \in I$. (Hint: Note that $IM = M$ implies $\xi_i = \sum_{j=1}^s a_{ij}\xi_j$, $i = 1, \dots, s$, $a_{ij} \in I$. Thus

$$\begin{pmatrix} a_{11} - 1 & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} - 1 & \cdots & a_{2s} \\ \vdots & & \ddots & \\ a_{s1} & a_{s2} & \cdots & a_{ss} - 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiplying by the adjoint $(a_{ij})^*$ of (a_{ij}) , it follows that $\det(a_{ij})M = \{0\}$, where $\det(a_{ij}) = 1 - a$ for some $a \in I$.)

- Let R and K be as in exercise 3 above. Use problem 6 to show that K is not a finitely generated R -module. (Hint: Take a nonzero nonunit $\lambda \in R$ and note that $\lambda K = K$.)
- Let $R = A[x_1, \dots, x_n]$ be the polynomial ring in x_1, \dots, x_n over a ring A . Let $R_i = \sum_{\alpha_1 + \dots + \alpha_n = i} Ax_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $i \in \mathbb{N}$, which is called the *ith homogeneous part* of R . Show that, as A -modules, $R = \bigoplus_{i \in \mathbb{N}} R_i$, and that, as subsets, $R_i R_j = R_{i+j}$, $i, j \in \mathbb{N}$.