Algebra

Serge Lang

August 6, 2021

Contents

1 Groups

1.1 Monoids

1.2 Groups

1.3 Normal Subgroups

Let $f : G \to G'$ be a group homomorphism, and let H be its kernel. If x is an element of G, then $xH = Hx$, because both are equal to $f^{-1}(f(x))$. We can also rewrite this relation as $xHx^{-1} = H$

Conversely, let G be a group and let H be a subgroup. Assume that for all elements $x \in G$, we have $xH \subset Hx$ (or equivalently, $xHx^{-1} \subset H$), which implies $H \subset xHx^{-1}$. Thus our condition is equivalent to the condition $xHx^{-1} = H$ for all $x \in G$. A subgroup H satisfying this condition will be called **normal**

Let G' be the set of cosets of H. (A left coset is equal to a right coset). If xH and yH are cosets, then their product

$$xHyH = xyHH = xyH$$

is also a coset. Hence G' is a group.

Let $f : G \to G'$ be the mapping s.t. $f(x)$ is the coset xH. Then f is clearly a homomorphism and H is equal to the kernel.

The group of cosets of a normal subgroup H is denoted by G/H (which we read G modulo H, or G mod H). The map f of G onto G/H constructed above is called the **canonical map**, and G/H is called the **factor group** of G by H

1.4 Direct Sums and Free Abelian Groups

Let $\{A_i\}_{i \in I}$ be a family of abelian groups. We define their **direct sum**

$$A = \bigoplus_{i \in I} A_i$$

to be the subset of the direct product $\prod A_i$ consisting of all families $(x_i)_{i \in I}$ with $x_i \in A_i$ s.t. $x_i = 0$ for all but a finite number of indices i. For each index $j \in I$, we map

$$\lambda_j : A_j \to A$$

by letting $\lambda_j(x)$ be the element whose j-th component is x, and having all other components equal to 0. Then λ_j is an injective homomorphism

Proposition 1.1. *Let $\{f_i : A_i \to B\}$ be a family of homomorphisms into an abelian group B. Let $A = \bigoplus A_i$. There exists a unique homomorphism*

$$f : A \to B$$

s.t. $f \circ \lambda_j = f_j$ for all j

Proof. Define

$$f((x_i)_{i \in I}) = \sum_{i \in I} f_i(x_i)$$

□

The property in Proposition 1.1 is called the **universal property** of the direct sum.

Let A be an abelian group and B, C subgroups. If $B + C = A$ and $B \cap C = \{0\}$ then the map

$$B \times C \to A$$

given by $(x, y) \mapsto x + y$ is an isomorphism. Instead of writing $A = B \times C$ we shall write $A = B \oplus C$ and say that A is the **direct sum** of B and C. We sue a similar notation for the direct sum of a finite number of subgroups $B_1, \dots, B_n$ s.t.

$$B_1 + \cdots + B_n = A$$

and

$$B_{i+1} \cap (B_1 + \cdots + B_i) = 0$$

In that case, we write

$$A = B_1 \oplus B_2 \oplus \cdots \oplus B_n$$

Let A be an abelian group. Let $\{e_i\}_{i \in I}$ be a family of elements of A. We say that this family is a **basis** of A if the family is not empty, and if every element of A has a unique expression as a linear combination

$$x = \sum x_i e_i$$

with $x_i \in \mathbb{Z}$ and almost all $x_i = 0$. Thus the sum is actually a finite sum. An abelian group is **free** if it has a basis. If that is the case, then if we let $Z_i = \mathbb{Z}$ for all i, then A is isomorphic to the direct sum

$$A \cong \bigoplus_{i \in I} Z_i$$

Now let S be a set. Let $\mathbb{Z}\langle S\rangle$ be the set of all maps $\varphi : S \to \mathbb{Z}$ s.t. $\varphi(x) = 0$ for almost all $x \in S$. Then $\mathbb{Z}\langle S\rangle$ is an abelian group. if k is an integer and $x \in S$, we denote by $k \cdot x$ the map φ s.t. $\varphi(x) = k$ and $\varphi(y) = 0$ if $y \neq x$. Then every element φ of $\mathbb{Z}\langle S\rangle$ can be written in the form

$$\varphi = k_1 \cdot x_1 + \cdots + k_n \cdot x_n$$

for $k_i \in \mathbb{Z}$ and $x_i \in S$, all the x_i being distinct. Furthermore, φ **admits a unique such expression**, because if we have

$$\varphi = \sum_{x \in S} k_x \cdot x = \sum_{x \in S} k'_x \cdot x$$

then

$$0 = \sum_{x \in S} (k_x - k'_x) \cdot x$$

whence $k'_x = k_x$ for all $x \in S$

We map S into $\mathbb{Z}\langle S\rangle$ by the map $f_S = f$ s.t. $f(x) = 1 \cdot x$. $f(S)$ generates $\mathbb{Z}\langle S\rangle$. If $g : S \to B$ is a mapping of S into some abelian group B, then we define a map

$$g_* : \mathbb{Z}\langle S\rangle \to B$$

s.t.

$$g_* \left(\sum_{x \in S} k_x \cdot x \right) = \sum_{x \in S} k_x g(x)$$

It's unique for any such homomorphism g_* must be s.t. $g_*(1 \cdot x) = g(x)$

Proposition 1.2. *if $\lambda : S \to S'$ is a mapping of sets, there is a unique homomorphism $\bar{\lambda}$ making the following diagram commutative*

$$\begin{array}{ccc}
S & \xrightarrow{f_S} & \mathbb{Z}\langle S\rangle \\
\Big\downarrow{\scriptstyle\lambda} & & \Big\downarrow{\scriptstyle\bar{\lambda}} \\
S' & \xrightarrow[f_{S'}]{} & \mathbb{Z}\langle S'\rangle
\end{array}$$

In fact, $\bar{\lambda}$ is none other than $(f_S \circ \lambda)_*$

We shall denote $\mathbb{Z}\langle S\rangle$ also $F_{ab}(S)$ and call $F_{ab}(S)$ the **free abelian group generated by** S. We call elements of S its **free generators**

2 Rings

2.1 Rings and Homomorphisms

A **ring** A is a set

1. w.r.t. addition, A is a commutative group
2. the multiplication is associative, and has a unit element
3. for all $x, y, z \in A$ we have

$$(x+y)z = xz + yz \quad \text{and} \quad z(x+y) = zx + zy$$

(called **distributivity**)

We denote the unit element for addition by 0, and the unit element for multiplication by 1. Observe that $0x = 0$ for all $x \in A$. *Proof:* $0x + x = (0+1)x = x$

For any $x, y \in A$ we have $(-x)y = -(xy)$

Let A be a ring, and let U be the set of elements of A which have both a right and left inverse. Then U is a multiplicative group. Indeed, if a has a right inverse b, so that $ab = 1$, and a left inverse c, so that $ca = 1$, then $cab = b$, whence $c = b$, and we see that c is a two-sided inverse, and that c itself has a two-sided inverse, namely a. Therefore U satisfies all the axioms of a multiplicative group, and is called the group of **units** of A. It is sometimes denoted by A^*, and is also called the group of **invertible** elements of A. A ring A s.t. $1 \neq 0$ and s.t. every non-zero element is invertible is called a **division ring**.

Example 2.1 (The Shift Operator)**.** Let E be the set of all sequences

$$a = (a_1, a_2, a_3, \dots)$$

of integers. One can define addition componentwise. Let R be the set of all mappings $f : E \to E$ of E into itself s.t. $f(a+b) = f(a) + f(b)$. Then R is a ring. Let

$$T(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots)$$

Verify that T is left invertible but not right invertible

A ring A is said to be **commutative** if $xy = yx$ for all $x, y \in A$. A commutative division ring is called a **field**. By definition, a field contains at least two elements, namely 0 and 1.

A subset B of ring A is called a **subring** if it is an additive subgroup, if it contains the multiplicative unit, and if $x, y \in B$ implies $xy \in B$. If that is the case, then B is n itself a ring, the laws of operation in B being the same as the laws of operation in A

For example, the **center** of a ring A is the subset of A consisting of all elements $a \in A$ s.t. $ax = xa$ for all $x \in A$. The center of A is a subring.

If $x, y_1, \dots, y_n$ are elements of a ring, then by induction one sees that

$$x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n$$

If $x_i (i = 1, \dots, n)$ and $y_j (j = 1, \dots, m)$ are elements of A, then it is also easily proved that

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j$$

Furthermore, distributivity holds for subtraction, e.g.

$$x(y_1 - y_2) = xy_1 - xy_2$$

Example 2.2. Let S be a set and A a ring. Let $\mathrm{Map}(S, A)$ be the set of mappings of S into A. Then $\mathrm{Map}(S, A)$ is a ring if for $f, g \in \mathrm{Map}(S, A)$ we define

$$(fg)(x) = f(x)g(x) \quad \text{and} \quad (f+g)(x) = f(x) + g(x)$$

for all $x \in S$.

Let M be an additive abelian group, and let A be the set $\mathrm{End}(M)$ of group-homomorphisms of M into itself. We define addition in A to be the addition of mappings, and we define multiplication to be **composition** of mappings

Example 2.3 (The convolution product)**.** Let G be a group and let K be a field. Denote by $K[G]$ the set of all formal linear combinations $\alpha = \sum a_x x$ with $x \in G$ and $a_x \in K$, s.t. all but finite number of a_x are equal to 0. If $\beta = \sum b_x x \in K[G]$, then one can define the product

$$\alpha\beta = \sum_{x \in G}\sum_{y \in G} a_x b_y xy = \sum_{z \in G}\left(\sum_{xy=z} a_x b_y\right) z$$

With this product, the **group ring** $K[G]$ is a ring. $K[G]$ is commutative iff G is commutative. The second sum on the right defines what is called a **convolution product**. If f, g are functions on a group G, we define their **convolution** $f * g$ by

$$(f * g)(z) = \sum_{xy=z} f(x)g(y)$$

A **left ideal** $\mathfrak{a}$ in a ring A is a subset of A which is a subgroup of the additive group of A, s.t. $A\mathfrak{a} \subset \mathfrak{a}$ (and hence $A\mathfrak{a} = \mathfrak{a}$ since A contains 1). To define a right ideal, we quire $\mathfrak{a}A = \mathfrak{a}$, and a **two-sided ideal** is a subset which is both a left and right ideal. A two-sided ideal is called an **ideal** in this section.

If A is a ring and $a \in A$, then Aa is a left ideal, called **principal**. We say that a is a generator of $\mathfrak{a}$ (over A). AaA is a principal two-sided ideal if $AaA = \{\sum x_i a y_i \mid x_i, y_i \in A\}$. More generally, let $a_1, \dots, a_n \in A$. We denote by $(a_1, \dots, a_n)$ the set of elements of A which can be written in the form

$$x_1 a_1 + \dots + x_n a_n \quad \text{with} \quad x_i \in A$$

Then this set of elements is immediately verified to be a left ideal, and $a_1, \dots, a_n$ are called **generators** of the left ideal.

If $\{\mathfrak{a}_i\}_{i \in I}$ is a family of ideals, then their intersection

$$\bigcap_{i \in I} \mathfrak{a}_i$$

is also an ideal

A **commutative** ring s.t. every ideal is principal and s.t. $1 \neq 0$ is called a **principal** ring

Example 2.4. The integers $\mathbb{Z}$ form a ring, which is commutative. Let $\mathfrak{a}$ be an ideal $\neq \mathbb{Z}$ and $\neq 0$. If $n \in \mathfrak{a}$ then $-n \in \mathfrak{a}$. Let d be the smallest integer > 0 lying in $\mathfrak{a}$. If $n \in \mathfrak{a}$ then there exists integers q, r with $0 \leq r < d$ s.t.

$$n = dq + r$$

Since $\mathfrak{a}$ is an ideal, it follows that r lies in $\mathfrak{a}$, hence $r = 0$. Hence $\mathfrak{a}$ consists of all multiples qd of d, which $q \in \mathbb{Z}$, and $\mathbb{Z}$ is a principal ring.

Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A. We define $\mathfrak{a}\mathfrak{b}$ to be the set of all sums

$$x_1 y_1 + \dots + x_n y_n$$

with $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$. $\mathfrak{a}\mathfrak{b}$ is an ideal, and that the set of ideals forms a multiplicative monoid, the unit element being the ring itself. This unit element is called the **unit ideal** and is often written (1).

If $\mathfrak{a}, \mathfrak{b}$ are left ideals of A, then $\mathfrak{a} + \mathfrak{b}$ (the sum being taken as additive subgroup of A) is obviously a left ideal. Thus ideals also form a monoid under addition. We also have distributivity: if $\mathfrak{a}_1, \dots, \mathfrak{a}_n, \mathfrak{b}$ are ideals of A, then

$$\mathfrak{b}(\mathfrak{a}_1 + \dots + \mathfrak{a}_n) = \mathfrak{b}\mathfrak{a}_1 + \dots + \mathfrak{b}\mathfrak{a}_n$$

Let $\mathfrak{a}$ be a left ideal. Define $\mathfrak{a}A$ to be the set of all sums $a_1x_1 + \cdots + a_nx_n$ with $a_i \in \mathfrak{a}$ and $x_i \in A$. Then $\mathfrak{a}A$ is an ideal.

Suppose that A is commutative. Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Then trivially

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$$

If $\mathfrak{a} + \mathfrak{b} = A$ then $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$. Suppose $x \in \mathfrak{a} \cap \mathfrak{b}$ and $x = a_x + b_x$, where $a_x \in \mathfrak{a}$ and $b_x \in \mathfrak{b}$. Then $a_x \in \mathfrak{b}$ and $b_x \in \mathfrak{a}$. If $1 = a_1 + b_1$ then $x \cdot 1 = (a_x + b_x)(a_1 + b_1) \in \mathfrak{a}\mathfrak{b}$

By a **ring homomorphism** one means a mapping $f : A \to B$ where A, B are rings, and s.t. f is a monoid-homomorphism for the multiplicative structures on A and B, and also a monoid homomorphism for the additive structure. In other words

$$\begin{array}{ll} f(a + a') = f(a) + f(a') & f(aa') = f(a)f(a') \\ f(1) = 1 & f(0) = 0 \end{array}$$

for all $a, a' \in A$.

The kernel of a ring homomorphism $f : A \to B$ is an ideal of A.

Conversely, let $\mathfrak{a}$ be an ideal of the ring A. We can construct the **factor ring** $A/\mathfrak{a}$ as follows. Viewing A and $\mathfrak{a}$ as additive groups, let $A/\mathfrak{a}$ be the factor group. If $x + \mathfrak{a}$ and $y + \mathfrak{a}$ are two cosets of $\mathfrak{a}$, we define $(x + \mathfrak{a})(y + \mathfrak{a})$ to be the coset $xy + \mathfrak{a}$. This coset is well-defined, for if x_1, y_1 are in the same coset as x, y respectively, then one verifies that x_1y_1 is in the same coset as xy. Unit element is $1 + \mathfrak{a}$.

We therefore defined a ring structure on $A/\mathfrak{a}$ and the caonical map

$$f : A \to A/\mathfrak{a}$$

is then clearly a ring homomorphism

Proposition 2.1. *If $g : A \to A'$ is a ring homomorphism whose kernel contains $\mathfrak{a}$, then there exists a unique ring homomorphism $g_* : A/\mathfrak{a} \to A'$ making the following diagram commutative*

$$\begin{tikzcd} A \arrow[rr, "g"] \arrow[dr, "f"'] & & A' \\ & A/\mathfrak{a} \arrow[ur, "g_*"'] & \end{tikzcd}$$

Indeed, viewing f, g as group homomorphisms, there is a unique group homomorphism g_* making our diagram commutative

Proof. If $x \in A$ then $g(x) = g_* f(x)$. Hence for $x, y \in A$

$$\begin{aligned} g_*(f(x)f(y)) &= g_*(f(xy)) = g(xy) = g(x)g(y) \\ &= g_* f(x) g_* f(y) \end{aligned}$$

Given $\xi, \eta \in A/\mathfrak{a}$, there exists $x, y \in A$ s.t. $f(x) = \xi$ and $f(y) = \eta$. Since $f(1) = 1$, we get $g_* f(1) = g(1) = 1$ and hence the two conditions that g_* be a multiplicative monoid-homomorphism are satisfied $\square$

Let A be a ring, and denote its unit element by e for the moment. The map

$$\lambda : \mathbb{Z} \to A$$

s.t. $\lambda(n) = ne$ is a ring homomorphism, and its kernel is an ideal (n), generated by an integer $n \geq 0$. We have a canonical injective homomorphism $\mathbb{Z}/n\mathbb{Z} \to A$ which is a (ring) isomorphism between $\mathbb{Z}/n\mathbb{Z}$ and a subring of A. If $n\mathbb{Z}$ is a prime ideal, then $n = 0$ or $n = p$ for some prime number p. In the first place, A contains as a subring a ring which is isomorphic to $\mathbb{Z}$, and which is often identified with $\mathbb{Z}$. In that case, we say that A has **characteristic** 0. if on the other hand $n = p$ then we say that A has **characteristic** p, and A contains (an isomorphic image of) $\mathbb{Z}/p\mathbb{Z}$ as a subring. We abbreviate $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

If K is a field, then K has characteristic 0 or $p > 0$. (if its characteristic is $a \cdot b$, then $a \cdot b \cdot 1 = 0$ but field is an integral domain). In the first case, K contains as a subfield an isomorphic image of the rational numbers, and in the second case, it contains an isomorphic image of $\mathbb{F}_p$. In either case, this subfield will be called the **prime field** (contained in K). Since this prime field is the smallest subfield of K containing 1 and has no automorphism except the identity, it is customary to identiy it with $\mathbb{Q}$ or $\mathbb{F}_p$ as the case may be. By the **prime ring** (in K) we shall mean either the integers $\mathbb{Z}$ if K has characteristic 0 or $\mathbb{F}_p$ if K has characteristic p.

Let A be a subring of a ring B. Let S be a subset of B commuting with A. We denote by $A[S]$ the set of all elements

$$\sum a_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n}$$

the sum ranging over a finite number of n-tuples $(i_1, \ldots, i_n)$ of integers ≥ 0, and $a_{i_1, \ldots, i_n} \in A$, $s_1, \ldots, s_n \in S$. If $B = A[S]$, we say that S is a set of **generators** (or **ring generators**) for B over A, or that B is **generated** by S over A. If S is finite, B is **finitely generated as a ring over** A. Note that S is not commutative.

Let A be a ring, $\mathfrak{a}$ an ideal, and S a subset of A. We write

$$S \equiv 0 \mod \mathfrak{a}$$

if $S \subset \mathfrak{a}$. If $x, y \in A$ we write

$$x \equiv y \mod \mathfrak{a}$$

if $x - a \in \mathfrak{a}$. If $\mathfrak{a}$ is principal, equal to (a), then we also write

$$x \equiv y \mod a$$

If $f : A \to A/\mathfrak{a}$ is the canonical homomorphism, then $x \equiv y \mod \mathfrak{a}$ means that $f(x) = f(y)$

The factor ring $A/\mathfrak{a}$ is also called a **residue class ring**. Cosets of $\mathfrak{a}$ in A are called **residue classes** modulo $\mathfrak{a}$, and if $x \in A$, then the coset $x + \mathfrak{a}$ is called the **residue class of x modulo $\mathfrak{a}$**

An injective ring homomorphism $f : A \to B$ establishes a ring isomorphism between A and its image. Such a homomorphism will be called an **embedding**

Let $f : A \to A'$ be a ring homomorphism, and let $\mathfrak{a}'$ be an ideal of A'. Then $f^{-1}(a')$ is an ideal $\mathfrak{a}$ in A, and we have an induced injective homomorphism

$$A/\mathfrak{a} \to A'/\mathfrak{a}'$$

Proposition 2.2. *Products exist in the category of rings*

Let A be a ring. Elements $x, y \in A$ are said to be **zero divisors** if $x \neq 0$, $y \neq 0$ and $xy = 0$. A ring A is **entire** if $1 \neq 0$, if A is commutative and if there are no zero divisors in the ring. (Entire rings are also called **integral domains**)

Let m be a positive integer $\neq 1$. The ring $\mathbb{Z}/m\mathbb{Z}$ has zero divisors iff m is not prime.

Proposition 2.3. *Let A be an entire ring, and let a, b be non-zero elements of A. Then a, b generate the same ideal iff there exists a unit u of A s.t. $b = au$.*

Proof. Assume $Aa = Ab$. Then $a = bc$ and $b = ad$ for some $c, d \in A$. Hence $a = adc$ whence $a(1 - dc) = 0$ and therefore $dc = 1$. Hence c is a unit $\square$

2.2 Commutative Rings

Assume A is commutative

A **prime** ideal in A is an ideal $\mathfrak{p} \neq A$ s.t. $A/\mathfrak{p}$ is entire. Equivalently, we could say that it is an ideal $\mathfrak{p} \neq A$ s.t. whenever $x, y \in A$ and $xy \in \mathfrak{p}$ then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. A prime ideal is often called simply a **prime**

Proposition 2.4. *Every maximal ideal is prime*

Proof. Let $\mathfrak{m}$ be maximal and let $x, y \in A$ s.t. $xy \in \mathfrak{m}$. Suppose $x \notin \mathfrak{m}$, then $\mathfrak{m} + Ax$ is an ideal properly containing $\mathfrak{m}$, hence equal to A. Hence we can write

$$1 = u + ax$$

with $u \in \mathfrak{m}$ and $a \in A$. Multiplying by y we find

$$y = yu + axy$$

whence $y \in \mathfrak{m}$. $\square$

Proposition 2.5. *Let $\mathfrak{a}$ be an ideal $\neq A$. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$*

Proposition 2.6. *The ideal $\{0\}$ is a prime ideal of A iff A is entire*

The only ideals of a field are itself and the zero ideal

Proposition 2.7. *If $\mathfrak{m}$ is a maximal ideal of A, then $A/\mathfrak{m}$ is a field*

Proof. If $x \in A$, we denote by $\bar{x}$ its residue class mod $\mathfrak{m}$. Since $\mathfrak{m} \neq A$ we note that $A/\mathfrak{m}$ has a unit element $\neq 0$. Any non-zero element of $A/\mathfrak{m}$ can be written as $\bar{x}$ for some $x \in A$, $x \notin \mathfrak{m}$. To find its inverse, note that $\mathfrak{m} + Ax$ is an ideal of $A \neq \mathfrak{m}$ and hence equal to A. Hence we can write

$$1 = u + yx$$

with $u \in \mathfrak{m}$ and $y \in A$. This means that $\bar{y}\bar{x} = 1 = \bar{1}$ and hence that $\bar{x}$ has an inverse. $\square$

Proposition 2.8. *Let $f : A \to A'$ be a homomorphism of commutative rings. Let $\mathfrak{p}'$ be a prime ideal of A' and let $\mathfrak{p} = f^{-1}\mathfrak{p}'$. Then $\mathfrak{p}$ is prime*

Example 2.5. Let $\mathbb{Z}$ be the ring of integers. Since an ideal is also an additive subgroup of $\mathbb{Z}$, every ideal $\neq \{0\}$ is principal, of the form $n\mathbb{Z}$ for some integer $n > 0$. (proof)

Let $\mathfrak{p}$ be a prime ideal $\neq \{0\}$, $\mathfrak{p} = n\mathbb{Z}$. Then n must be a prime number. Conversely, if p is a prime number, then $p\mathbb{Z}$ is a prime ideal. Furthermore, $p\mathbb{Z}$ is a maximal ideal. Suppose $p\mathbb{Z}$ is contained in some ideal $n\mathbb{Z}$, then $p = nm$ for some integer m, whence $n = p$ or $n = 1$, thereby proving $p\mathbb{Z}$ maximal

if n is an integer, the factor ring $\mathbb{Z}/n\mathbb{Z}$ is called the ring of **integers modulo** n. We also denote

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}(n)$$

If n is a prime number p, then the ring of integers modulo p is in fact a field, denoted by $\mathbb{F}_p$. In particular, the multiplicative group of $\mathbb{F}_p$ is called the group of non-zero integers modulo p. From the elementary properties of groups, we get a standard fact of elementary number theory: if x is an integer $\neq 0 \mod p$, then $x^{p-1} \equiv 1 \mod p$ (Fermat's Theorem). Similarly given an integer $n > 1$, the units in the ring $\mathbb{Z}/n\mathbb{Z}$ consist of those residue class mod $n\mathbb{Z}$ which are represented by integers $m \neq 0$ and prime to n. The order of the group of units in $\mathbb{Z}/n\mathbb{Z}$ is called by definition $\varphi(n)$ (where φ is known as the **Euler phi-function**). Consequently, if x is an integer prime to n, then $x^{\varphi(n)} \equiv 1 \mod n$

Theorem 2.9 (Chinese Remainder Theorem)**.** *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A s.t. $\mathfrak{a}_i + \mathfrak{a}_j = A$ for all $i \neq j$. Given elements $x_1, \dots, x_n \in A$,there exists $x \in A$ s.t. $x \equiv x_i \mod \mathfrak{a}_i$ for all i*

Proof. For $n = 2$ we have an expression

$$1 = a_1 + a_2$$

for some $a_i \in \mathfrak{a}_i$, and we let $x = x_2a_1 + x_1a_2$

For each $i \geq 2$ we can find elements $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ s.t.

$$a_i + b_i = 1, \quad i \geq 2$$

The products $\prod_{i=2}^{n}(a_i + b_i)$ is equal to 1, and lies in

$$\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i$$

Hence

$$\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i = A$$

By theorem for $n = 2$, we can find an element $y_1 \in A$ s.t.

$$y_1 \equiv 1 \mod \mathfrak{a}_1$$
$$y_1 \equiv 0 \mod \prod_{i=2}^{n} \mathfrak{a}_i$$

We find similarly elements $y_2, \dots, y_n$ s.t.

$$y_j \equiv 1 \mod \mathfrak{a}_j \quad \text{and} \quad y_j \equiv 0 \mod \mathfrak{a}_i \text{ for } i \neq j$$

Then $x = x_1y_1 + \cdots + x_ny_n$ satisfies our requirements □

In the same vein as above, we observe that if $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ are ideals of a ring A s.t.

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = A$$

and if $v_1, \dots, v_n$ are positive integers, then

$$\mathfrak{a}_1^{v_1} + \cdots + \mathfrak{a}_n^{v_n} = A$$

Corollary 2.10. *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A. Assume that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for $i \neq j$. Let*

$$f : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i = (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$$

be the map of A into the product induced by the canonical map of A onto $A/\mathfrak{a}_i$ for each factor. Then the kernel of f is $\bigcap_{i=1}^{n} \mathfrak{a}_i$ and f is surjective, thus giving an isomorphism

$$A/\bigcap \mathfrak{a}_i \cong \prod A/\mathfrak{a}_i$$

Proof. Surjectivity follows from the theorem □

Let m be an integer > 1, and let

$$m = \prod_i p_i^{r_i}$$

be a factorization of m into primes, with exponents $r_i \geq 1$. Then we have a ring isomorphism

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

If A is a ring, we denote as usual by A^* the multiplicative group of invertible elements of A

Proposition 2.11. *The preceding ring isomorphism of $\mathbb{Z}/m\mathbb{Z}$ onto the product induces a group isomorphism*

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \prod_i (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$$

In view of our isomorphism, we have

$$\varphi(m) = \prod_i \varphi(p_i^{r_i})$$

If p is a prime number and r an integer ≥ 1, then

$$\varphi(p^r) = (p-1)p^{r-1}$$

If $r = 1$, then $\mathbb{Z}/p\mathbb{Z}$ is a field, and the multiplicative group of that field has order $p-1$. Let r be ≥ 1, and consider the canonical ring homomorphism

$$\mathbb{Z}/p^{r+1}\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$$

arising from the inclusion of ideals $(p^{r+1}) \subset (p^r)$. We get an induced group homomorphism

$$\lambda : (Z/p^{r+1}\mathbb{Z})^* \to (\mathbb{Z}/p^r\mathbb{Z})^*$$

which is surjective because any integer a which represents an element of $\mathbb{Z}/p^r\mathbb{Z}$ and is prime to p will represent an element of $(\mathbb{Z}/p^{r+1}\mathbb{Z})^*$. Let a be an integer representing an element of $(\mathbb{Z}/p^{r+1}\mathbb{Z})^*$ s.t. $\lambda(a) = 1$. Then

$$a \equiv 1 \mod p^r\mathbb{Z}$$

P96

Application: The ring of endomorphisms of a cyclic group.

Theorem 2.12. *Let A be a cyclic group of order n. For each $k \in \mathbb{Z}$ let $f_k : A \to A$ be the endomorphism $x \mapsto kx$ (writing A additively). Then $k \mapsto f_k$ induces a ring homomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{End}(A)$, and a group isomorphism $(\mathbb{Z}/n\mathbb{Z})^* \cong \boldsymbol{Aut}(A)$*

Proof. The fact that $k \mapsto f_k$ is ring homomorphism is a restatement of the formulas

$$1a = a, \quad (k+k')a = ka + k'a, \quad (kk')a = k(k'a)$$

□

2.3 Polynomials and Group Rings

Consider an infinite cyclic group generated by an element X. We let S be the subset consisting of powers X^r with $r \geq 0$. Then S is a monoid. We define the set of **polynomials** $A[X]$ to be the set of functions $S \to A$ which are equal to 0 except for a finite number of elements of S. For each element $a \in A$ we denote by aX^n the function which has the value a on X^n and the value 0 for all other elements of S. Then it is immediate that a polynomial can be written uniquely as a finite sum

$$a_0X^0 + \cdots + a_nX^n$$

for some integer $n \in \mathbb{N}$ and $a_i \in A$. Such a polynomial is denoted by $f(X)$. The elements $a_i \in A$ are called the **coefficients** of f. We define the product according to the convolution rule. Thus, given polynomials

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad \text{and} \quad g(X) = \sum_{j=0}^{m} b_j X^j$$

we define the product to be

$$f(X)g(X) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^k$$

This product is associative and distributive. $1X^0$ is the unit element. There is also an embedding

$$\begin{aligned} A &\to A[X] \\ a &\mapsto aX^0 \end{aligned}$$

Let A be a subring of a commutative ring B. Let $x \in B$. If $f \in A[X]$ is a polynomial, we define the associated **polynomial function**

$$f_B : B \to B$$

by letting

$$f_B(x) = f(x) = a_0 + a_1x + \cdots + a_nx^n$$

Given an element $b \in B$, directly from the definition of multiplication of polynomials, we find

Proposition 2.13. *The association*

$$ev_b : f \mapsto f(b)$$

is a ring homomorphism of $A[X]$ into B

This homomorphism is called the **evaluation homomorphism**, and is also said to be obtained by **substituting** b for X in the polynomial

Let $x \in B$. We see that the subring $A[x]$ of B generated by x over A is a ring of all polynomial values $f(x)$ for $f \in A[X]$. If the evaluation map $f \mapsto f(x)$ gives an isomorphism of $A[X]$ with $A[x]$, then we say that x is **transcendental** over A, or that x is a **variable** over A. In particular, X is a variable over A

Example 2.6. Let $\alpha = \sqrt{2}$. Then the set of all real numbers of the form $a + b\alpha$, with $a, b \in \mathbb{Z}$ is a subring of the real numbers, generated by $\sqrt{2}$. α is not transcendental over $\mathbb{Z}$, because the polynomial $X^2 - 2$ lies in the kernel of the evaluation map $f \mapsto f(\sqrt{2})$. On the other hand, it can be shown that e and π are transcendental over $\mathbb{Q}$

Example 2.7. Let p be a prime number and let $K = \mathbb{Z}/p\mathbb{Z}$. Then K is a field. Let $f(X) = X^p - X \in K[X]$. Then f is not the zero polynomials. But f_K is the zero function. Indeed, $f_K(0) = 0$. If $x \in K$, $x \neq 0$, then since the multiplicative group of K has order $p - 1$. it follows that $x^{p-1} = 1$, whence $x^p = x$, so $f(x)$. Thus a non-zero polynomial gives rise to the zero function on K

Let

$$\varphi : A \to B$$

be a homomorphism of commutative rings. Then there is an associated homomorphism of the polynomial rings $A[X] \to B[X]$ s.t.

$$f(X) = \sum a_i X^i \mapsto \sum \varphi(a_i) X^i = (\varphi f)(X)$$

We call $f \mapsto \varphi f$ the **reduction map**

Let $\mathfrak{p}$ be a prime ideal of A. Let $\varphi : A \to A'$ be the canonical homomorphism of A onto $A/\mathfrak{p}$. If $f(X)$ is a polynomial in $A[X]$, then φf will sometimes be called the **reduction of f modulo $\mathfrak{p}$**.

For example, taking $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$ for some prime number p, we can speak of the polynomial $3X^4 - X + 2$ as a polynomial mod 5, viewing the coefficients as elements of $\mathbb{Z}/5\mathbb{Z}$

Proposition 2.14. *Let $\varphi : A \to B$ be a homomorphism of commutative rings. Let $x \in B$. There is a unique homomorphism extending φ*

$$A[X] \to B \quad s.t. \quad X \mapsto x$$

and for this homomorphism $\sum a_i X^i \mapsto \sum \varphi(a_i) x^i$

The homomorphism of the above statement may be views as the composite

$$A[X] \longrightarrow B[X] \xrightarrow{\mathrm{ev}_x} B$$

When writing a polynomial $f(X) = \sum_{i=1}^{n} a_i X^i$, if $a_n \neq 0$ then we define n to be the **degree** of f. Thus the degree of f is the smallest integer n s.t. $a_r = 0$ for $r > n$. If $f = 0$ (i.e. f is the zero polynomial), then by convention, we define the degree of f to be $-\infty$. We agree to the convention that

$$-\infty + -\infty = -\infty, \quad -\infty + n = -\infty, \quad -\infty < n$$

for all $n \in \mathbb{Z}$, and no other operation with $-\infty$ is defined. A polynomial of degree 1 is also called a **linear** polynomial. If $f \neq 0$ and $\deg f = n$ then we call a_n the **leading coefficient** of f. We call a_0 its **constant term**

Let

$$g(X) = b_0 + \cdots + b_m X^m$$

be a polynomial in $A[X]$, of degree m, and assume $g \neq 0$. Then

$$f(X)g(X) = a_0 b_0 + \cdots + a_n b_m X^{m+n}$$

Therefore

Proposition 2.15. *If we assume that at least one of the leading coefficients a_n or b_m is not a divisor of 0 in A, then*

$$\deg(fg) = \deg f + \deg g$$

and the leading coefficient of fg is $a_n b_m$. This holds in particular when a_n or b_m is a unit in A, or when A is entire. Consequently, when A is entire, $A[X]$ is also entire

If $f = 0$ or $g = 0$ we still have

$$\deg(fg) = \deg f + \deg g$$

if we agree that $-\infty + m = -\infty$ for any integer m

Let A be a subring of a commutative ring B. Let $x_1, \dots, x_n \in B$. For each n-tuple of integers $(v_1, \dots, v_n) = \mathbf{v} \in \mathbb{N}^n$, let $\mathbf{x} = (x_1, \dots, x_n)$, and

$$M_{\mathbf{v}}(\mathbf{x}) = x_1^{v_1} \dots x_n^{v_n}$$

The set of such elements forms a monoid under multiplication. Let $A[x] = A[x_1, \dots, x_n]$ be the subring of B generated by $x_1, \dots, x_n$ over A. Then every element of $A[x]$ can be written as a finite sum

$$\sum a_{\mathbf{v}} M_{\mathbf{v}}(\mathbf{x}) \quad \text{and} \quad a_{\mathbf{v}} \in A$$

Using the construction of polynomials in one variable repeatedly, we may form the ring

$$A[X_1, \dots, X_n] = A[X_1][X_2] \dots [X_n]$$

selecting X_n to be variable over $A[X_1, \dots, X_{n-1}]$. Then every element f of $A[X_1, \dots, X_n] = A[X]$ has a *unique* expression as a finite sum

$$f = \sum_{j=0}^{d_n} f_j(X_1, \dots, X_{n-1}) X_n^j \quad \text{with} \quad f_j \in A[X_1, \dots, X_{n-1}]$$

Therefore by induction we can write f uniquely as a sum

$$\begin{aligned} f &= \sum_{v_n=0}^{d_n} \left(\sum_{v_1, \dots, v_{n-1}} a_{v_1 \dots v_n} X_1^{v_1} \dots X_{n-1}^{v_{n-1}} \right) X_n^{v_n} \\ &= \sum a_{\mathbf{v}} M_{\mathbf{v}}(X) = \sum a_{\mathbf{v}} X_1^{v_1} \dots X_n^{v_n} \end{aligned}$$

with elements $a_{\mathbf{v} \in A}$, which are called the **coefficients** of f. The products

$$M_{\mathbf{v}}(X) = X_1^{v_1} \dots X_n^{v_n}$$

will be called **primitive monomials**. Elements of $A[X]$ are called **polynomials** (in n variables). We call $a_{\mathbf{v}}$ its **coefficients**

GIven $\mathbf{x} = (x_1, \dots, x_n)$ and f, we define

$$f(x) = \sum a_{\mathbf{v}} M_{\mathbf{v}}(\mathbf{x}) = \sum a_{\mathbf{v}} x_1^{v_1} \dots x_n^{v_n}$$

Then the **evaluation map**

$$\mathrm{ev}_{\mathbf{x}} : A[X] \to B \quad \text{with} \quad f \mapsto f(x)$$

is a ring homomorphism

Elements $x_1, \dots, x_n \in B$ are called **algebraically independent** over A if the evaluation map

$$f \mapsto f(x)$$

is injective. Equivalently, we could say that if $f \in A[X]$ is a polynomial and $f(x) = 0$ then $f = 0$.; in other words, there are no non-trivial polynomial relations among $x_1, \dots, x_n$ over A.

By the **degree** of a primitive monomial

$$M_{\mathbf{v}}(X) = X_1^{v_1} \dots X_n^{v_n}$$

we shall mean the integer $|v| = v_1 + \cdots + v_n$

A polynomial

$$aX_1^{v_1} \dots X_n^{v_n} \quad (a \in A)$$

will be called a **monomial**

If $f(X)$ is a polynomial in $A[X]$ written as

$$f(X) = \sum a_{\mathbf{v}} X_1^{v_1} \dots X_n^{v_n}$$

we define the **degree** of f to be the maximum of the degrees of the monomials $M_{\mathbf{v}}(X)$ s.t. $a_{\mathbf{v}} \neq 0$. (Such monomials are said to **occur** in the polynomial)

For each integer $d \geq 0$, given a polynomial f, let $f^{(d)}$ be the sum of all monomials occuring in f and having degree d. Then

$$f = \sum_d f^{(d)}$$

Suppose $f \neq 0$, we say that f is **homogeneous** of degree d if $f = f^{(d)}$

Algebraically independent elements will also be called **variables**

2.4 Localization

A a commutative ring

By a **multiplicative subset** of A we shall mean a submonoid of A

We shall now construct the **quotient ring of A by S**, also known as the **ring of fractions of A by S**

We consider pairs (a, s) with $a \in A$ and $s \in S$. We define a relation

$$(a, s) \sim (a', s')$$

if there exists $s_1 \in S$ s.t.

$$s_1(s'a - sa') = 0$$

The equivalence class containing a pair (a, s) is denoted by a/s. The set of equivalence classes is denoted by $S^{-1}A$

if $0 \in S$, then $S^{-1}A$ has precisely one element $0/1$

$$(a/s)(a'/s') = aa'/ss'$$
$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'}$$

Let $\varphi_S : A \to S^{-1}A$ be the s.t. $\varphi_S(a) = a/1$. Every element of $\varphi_S(S)$ is invertible in $S^{-1}(A)$ (the inverse of $s/1$ is $1/s$)

Let $\mathcal{C}$ be the category whose objects are ring homomorphism

$$f : A \to B$$

s.t. for every $s \in S$ the elements $f(s)$ is invertible in B. If $f : A \to B$ and

Proposition 2.16. *Let A be an entire ring, and let S be a multiplicative subset which does not contain 0. Then*

$$\varphi_S : A \to S^{-1}A$$

is injective

Let A be an entire ring, and let S be the set of non-zero elements of A. Then S is a multiplicative set, and $S^{-1}A$ is then a field, called the **quotient field** or the *field of fractions of A.

2.5 Principal and Factorial Rings

Let A be an entire ring. An element $a \neq 0$ is called **irreducible** if it is not a unit, and if whenever one can write $a = bc$ with $b \in A$ and $c \in A$, then b or c is a unit

Let $a \neq 0$ be an element of A and assume that the principal ideal (a) is prime. Then (a) is irreducible. If we write $a = bc.$, then b or c lies in (a), say b. Then we can write $b = ad$ with some $d \in A$ and hence $a = acd$. Since A is entire, it follows that $cd = 1$, in other words, c is a unit.

The converse of the preceding assertion is not always true. We shall discuss under which conditions it is true. An element $a \in A$, $a \neq 0$ is said to have a **unique factorization into irreducible elements** if there exists a unit u and there exist irreducible elements p_i in A s.t.

$$a = u \prod_{i=1}^{r} p_i$$

and if given two factorization into irreducible elements

$$a = u \prod_{i=1}^{r} p_i = u' \prod_{j=1}^{s} q_j$$

we have $r = s$ and after a permutation of the indices i, we have $p_i = u_i q_i$ for some unit $u_i \in A$

A ring is called **factorial** (or **unique factorization ring**) if it is entire and if every element $\neq 0$ has a unique factorization into irreducible elements.

Let A be an entire ring and $a, b \in A$, $ab \neq 0$. We say that a **divides** b and write $a \mid b$ if there exists $c \in A$ s.t. $ac = b$. We say that $d \in A$, $d \neq 0$ is a **greatest common divisor** (**g.c.d.**) of a and b if $d \mid a$ and $d \mid b$ and if any element e of A $e \neq 0$ which divides both a and b also divides d

Proposition 2.17. *Let A be a principal entire ring and $a, b \in A$, $a, b \neq 0$. Let $(a, b) = (c)$. Then c is a greatest common divisor of a and b*

Theorem 2.18. *Let A be a principal entire ring. Then A is factorial*

Proof. We first prove that every non-zero element of A has a factorization into irreducible elements. Let S be the set of principal ideals $\neq 0$ whose generators do not have a factorization into irreducible elements, and suppose S is not empty. Let $(a_1) \in S$ be in S. Consider an ascending chain

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \ldots$$

of ideals in S. We contend that such a chain cannot be infinite. Indeed, the union of such a chain is an ideal of A, which is principal, say equal to (a). The generator a must already lie in some element of the chain, say (a_n), and then we see that $(a_n) \subset (a) \subset (a_n)$, whence the chain stops at (a_n). Hence S is inductively ordered, and has a maximal element (a). Therefore any ideal of A containing (a) and $\neq (a)$ has a generator admitting a factorization.

We note that a_n cannot be irreducible and hence we can write $a = bc$ with neither b nor c equal to a unit. But then $(b) \neq (a)$ and $(c) \neq (a)$ and hence both b and c admit factorizations into irreducible elements. The product of these factorizations is a factorization for a, contradicting the assumption that S is not empty

To prove uniqueness, we first remark that if p is an irreducible element of A and $a, b \in A$, $p \mid ab$, then $p \mid a$ or $p \mid b$. *Proof*: if $p \nmid a$, then the g.c.d. of p, a is 1 and hence we can write

$$1 = xp + ya$$

for some $x, y \in A$. Then $b = bxp + yab$ and since $p \mid ab$ we conclude that $p \mid b$

Suppose that a has two factorizations

$$a = p_1 \dots p_r = q_1 \dots q_s$$

into irreducible elements. Since p_1 divides $q_1 \dots q_s$, p_1 divides one of the factors, which we may assume to be q_1 after renumbering these factors. Then there exists a unit u_1 s.t. $q_1 = u_1 p_1$. We can now cancel p_1 from both factorizations and get

$$p_2 \dots p_r = u_1 q_2 \dots q_s$$

□

We could call two elements $a, b \in A$ equivalent if there exists a unit u s.t. $a = bu$. let us select irreducible element p out of each equivalence class belonging to such an irreducible element, and let us denote by P the set of such representatives. Let $a \in A, a \neq 0$. Then there exists a unit u and integers $v(p) \geq 0$, equal to 0 for almost all $p \in P$ s.t.

$$a = u \prod_{p \in P} p^{v(p)}$$

Furthermore, the unit u and the integers $v(p)$ are uniquely determined by a. We call $v(p)$ the **order** of a at p, also written as $\operatorname{ord}_p a$

If A is a factorial ring, then an irreducible element p generates a prime ideal (p). Thus in a factorial ring, an irreducible element will also be called a **prime element**, or simply **prime**

3 Modules

3.1 Basic Definitions

Let A be a ring. A **left module** over A, or a left A-module M is an abelian group, together with an operation of A on M, s.t. for all $a, b \in A$ and $x, y \in M$

$$(a + b)x = ax + bx \quad \text{and} \quad a(x + y) = ax + ay$$

Let A be an entire ring and let M be an A-module. We define the **torsion submodule** M_{tor} to be the subset of elements $x \in M$ s.t. there exist$a \in A$s , $a \neq 0$ s.t. $ax = 0$.

By a **module homomorphism** we means a map

$$f : M \to M'$$

which is an additive group homomorphism and s.t.

$$f(ax) = af(x)$$

for all $a \in A$ and $x \in M$. If we wish to refer to the ring A, we also say that f is an A**-homomorphism**, or also that it is an A**-linear map**

For any module M and M', the map $\zeta : M \to M'$ s.t. $\zeta(x) = 0$ for all $x \in M$ is a homomorphism, called **zero**

Let $f : M \to M'$ be a homomorphism. By the **cokernel** of f we mean the factor module $M'/\operatorname{im} f = M'/f(M)$.

Like groups

Proposition 3.1. *Let N, N' be two submodules of a module of M. Then $N + N'$ is also a submodule, and we have an isomorphism*

$$N/(N \cap N') \cong (N + N')/N'$$

If $M \supset M' \supset M''$ are modules, then

$$(M/M'')/(M'/M'') \cong M/M'$$

If $f : M \to M'$ is a module homomorphism, and N' is a submodule of M', then $f^{-1}(N')$ is a submodule of M and we have a canonical injective homomorphism

$$\bar{f} : M/f^{-1}(N') \to M'/N'$$

If f is surjective, then $\bar{f}$ is a module isomorphism

A sequence of module homomorphisms

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is **exact** if $\operatorname{im} f = \ker g$. If N is a submodule of M, then

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

If a homomorphism $u : N \to M$ is s.t.

$$0 \longrightarrow N \xrightarrow{u} M$$

is exact, then we also say that u is a **monomorphism** or an **embedding**. Dually if

$$N \xrightarrow{u} M \longrightarrow 0$$

is exact, we say that u is an **epimorphism**

Let A be a commutative ring. Let E, F be modules. By a **bilinear map**

$$g : E \times E \to F$$

we mean a map s.t. given $x \in E$ the map $y \mapsto g(x, y)$ is A-linear and given $y \in E$, the map $x \mapsto g(x, y)$ is A-linear. By an A**-algebra** we mean a module together with a bilinear map $g : E \times E \to E$. We view such a map as a law of composition on E.

3.2 The Group of Homomorphisms

Let A be a ring, and let X, X' be A-modules. We denote by $\mathrm{Hom}_A(X', X)$ the set of A-homomorphisms of X' into X. Then $\mathrm{Hom}_A(X', X)$ is an abelian group, the law of addition being that of addition for mappings into an abelian group.

If A is *commutative* then we can make $\mathrm{Hom}_A(X', X)$ into an A-module by defining af for $a \in A$ and $f \in \mathrm{Hom}_A(X', X)$ to be the map s.t.

$$(af)(x) = af(x)$$

Let Y be an A-module, and let

$$X' \xrightarrow{f} X$$

be an A-homomorphism. Then we get an induced homomorphism

$$\mathrm{Hom}_A(f, Y) : \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X', Y)$$

given by $g \mapsto g \circ f$. The fact that $\mathrm{Hom}_A(f, Y)$ is a homomorphism is a rephrasing of the $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$

If we have a sequence of A-homomorphisms

$$X' \longrightarrow X \longrightarrow X''$$

then we get an induced sequence

$$\mathrm{Hom}_A(X', Y) \longleftarrow \mathrm{Hom}_A(X, Y) \longleftarrow \mathrm{Hom}_A(X'', Y)$$

Proposition 3.2. *A sequence*

$$X' \xrightarrow{\lambda} X \longrightarrow X'' \longrightarrow 0$$

is exact iff the sequence

$$\mathrm{Hom}_A(X', Y) \longleftarrow \mathrm{Hom}_A(X, Y) \longleftarrow \mathrm{Hom}_A(X'', Y) \longleftarrow 0$$

is exact for all Y

Proof. Suppose the first sequence is exact. If $g : X'' \to Y$ is an A-homomorphism, its image in $\mathrm{Hom}_A(X, Y)$ is obtained by composing g with the surjective map of X on X''. If this composition is 0, it follows that $g = 0$. Consider a homomorphism $g : X \to Y$ s.t. the composition

$$X' \xrightarrow{\lambda} X \xrightarrow{g} Y$$

is 0. Then g vanishes on the image of λ. Hence we can factor g through the factor module

$$\begin{tikzcd} & X/\operatorname{im}\lambda \arrow[dr] & \\ X \arrow[ur] \arrow[rr, "g"'] & & Y \end{tikzcd}$$

Since $X \to X''$ is surjective, we have an isomorphism

$$X/\operatorname{im}\lambda \cong X''$$

Hence we can factor g through X'', thereby showing that the kernel of

$$\mathrm{Hom}_A(X', Y) \longleftarrow \mathrm{Hom}_A(X, Y)$$

is contained in the image of

$$\mathrm{Hom}_A(X, Y) \longleftarrow \mathrm{Hom}_A(X'', Y)$$

□

similarly, we have

Proposition 3.3. *A sequence*

$$0 \longrightarrow Y' \longrightarrow Y \longrightarrow Y''$$

is exact iff

$$0 \longrightarrow \mathrm{Hom}_A(X, Y') \longrightarrow \mathrm{Hom}_A(X, Y) \longrightarrow \mathrm{Hom}_A(X, Y'')$$

is exact for all X

Let $\text{Mod}(A)$ and $\text{Mod}(B)$ be the categories of modules over rings A and B, and let $F : \text{Mod}(A) \to \text{Mod}(B)$ be a functor. One says that F is **exact** if F transforms exact sequences into exact sequences.

let M be an A-module. From the relations

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$$
$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$$

and the fact that there is an identity for composition, namely id_M, we conclude that $\text{Hom}_A(M, M)$ is a ring. We call $\text{End}_A(M) = \text{Hom}_A(M, M)$ the ring of **endomorphisms**

3.3 Direct Products and Sums of Modules

Proposition 3.4. *Let M be an A-module and n an integer ≥ 1. For each $i = 1, \dots, n$ let $\varphi_i : M \to M$ be an A-homomorphism s.t.*

$$\sum_{i=1}^{n} \varphi_i = \text{id} \quad \textit{and} \quad \varphi_i \circ \varphi_j = 0 \quad \textit{if } i \neq j$$

Then $\varphi_i^2 = \varphi_i$ for all i. Let $M_i = \varphi_i(M)$, and let $\varphi : M \to \prod M_i$ be s.t.

$$\varphi(x) = (\varphi_1(x), \dots, \varphi_n(x))$$

Then φ is an A-isomorphism of M onto the direct product $\prod M_i$

Proof. for each j, we have

$$\varphi_j = \varphi_j \circ \text{id} = \varphi_j \circ \sum_{i=1}^{n} \varphi_i = \varphi_j \circ \varphi_j = \varphi_j^2$$

thereby proving the first assertion. It is clear that φ is an A-homomorphism. Let $x \in \ker \varphi$. Since

$$x = \text{id}(x) = \sum_{i=1}^{n} \varphi_i(x)$$

we conclude that $x = 0$, so φ is injective. $\square$

Let M be a module over a ring A and let S be a subset of M. By a **linear combination** of elements of S (with coefficients in A) one means a sum

$$\sum_{x \in S} a_x x$$

where $\{a_x\}$ is a set of elements of A, almost all of which are equal to 0. Let N be the set of all linear combinations of elements of S. Then N is a submodule of M, for if

$$\sum_{x \in S} a_x x \quad \text{and} \quad \sum_{x \in S} b_x x$$

are two linear combinations, then their sum is equal to

$$\sum_{x \in S} (a_x + b_x) x$$

and if $c \in A$, then

$$c \left(\sum_{x \in S} a_x x \right) = \sum_{x \in S} c a_x x$$

We shall call N the submodule **generated** by S, and we call S a set of **generators** for N. We sometimes write $N = A\langle S \rangle$. If S consists of one element x, the module generated by x is also written Ax, or simply (x), and sometimes we say that (x) is a **principal module**

A module M is said to be **finitely generated**, or of **finite type** or **finite** over A, if it has a finite number of generators

A subset S of a module M is said to be **linearly independent** (over A) if whenever we have a linear combination

$$\sum_{x \in S} a_x x$$

which is equal to 0, then $a_x = 0$ for all $x \in S$. If S is linearly independent and if two linear combinations

$$\sum a_x x \quad \text{and} \quad \sum b_x x$$

are equal, then $a_x = b_x$ for all $x \in S$.

Let M be an A-module, and let $\{M_i\}_{i \in I}$ be a family of submodules. Since we have inclusion-homomorphism

$$\lambda_i : M_i \to M$$

we have an induced homomorphism

$$\lambda_* : \bigoplus M_i \to M$$

which is s.t. for any family of elements $(x_i)_{i \in I}$ all but a finite number of which are 0, we have

$$\lambda_*((x_i)) = \sum_{i \in I} x_i$$

if λ_* is an isomorphism, then we say that $\{M_i\}_{i\in I}$ is a **direct sum decomposition** of M. This is equivalent to saying that every element of M has a unique expression as a sum

$$\sum x_i$$

with $x_i \in M$ and almost all $x_i = 0$. By abuse of notation, we also write

$$M = \bigoplus M_i$$

in this case

If M is a module and N, N' are two submodules s.t. $N + N' = M$ and $N \cap N' = 0$, then we have a module isomorphism

$$M \cong N \oplus N'$$

Proposition 3.5. *Let M, M', N be modules. Then we have an isomorphism of abelian groups*

$$\mathrm{Hom}_A(M \oplus M', N) \cong \mathrm{Hom}_A(M, N) \times \mathrm{Hom}_A(M', N)$$

and

$$\mathrm{Hom}_A(N, M \times M') \cong \mathrm{Hom}_A(N, M) \times \mathrm{Hom}_A(N, M')$$

Proof. if $f : M \oplus M' \to N$ is a homomorphism, then f induces a homomorphism $f_1 : M \to N$ and a homomorphism $f_2 : M' \to N$ by composing injections

$$M \to M \oplus \{0\} \subset M \oplus M' \xrightarrow{f} N$$

$$M' \to \{0\} \oplus M' \subset M \oplus M' \xrightarrow{f} N$$

Then

$$f \mapsto (f_1, f_2)$$

is an isomorphism □

Proposition 3.6. *Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence of modules. The following are equivalent*

1. *there exists a homomorphism $\varphi : M'' \to M$ s.t. $g \circ \varphi = \mathrm{id}$*

2. *there exists a homomorphism $\psi : M \to M'$ s.t. $\psi \circ f = \mathrm{id}$*

if these conditions are satisfied, then we have isomorphisms

$$M = \operatorname{im} f \oplus \ker \psi, \qquad M = \ker g \oplus \operatorname{im} \varphi$$
$$M \cong M' \oplus M''$$

Proof. Let $x \in M$, then $x - \varphi(g(x)) \in \ker g$, and hence $M = \ker g + \operatorname{im} \varphi$. If $x \in \ker g \cap \operatorname{im} \varphi$, then $x = \varphi(w)$ and $g(x) = g(\varphi(w)) = w = 0$, thus $\ker g \cap \operatorname{im} \varphi = \{0\}$

□

when these conditions are satisfied, the exact sequence is said to **split**. ψ **splits** f and φ **splits** g

Consider first a category $\mathfrak{C}$ s.t. $\operatorname{Mor}(E, F)$ is an abelian group for each pair of objects E, F of $\mathfrak{C}$, satisfying the following two conditions

- AB 1 The law of composition of morphisms is bilinear, and there exists a zero object 0, i.e., s.t. $\operatorname{Mor}(0, E)$ and $\operatorname{Mor}(E, 0)$ have precisely one element for each object E
- AB 2 Finite products and finite coproducts exists in the category

Then we say that $\mathfrak{C}$ is an **additive category**

Given a morphism $E \xrightarrow{f} F$ in $\mathfrak{C}$, we define a **kernel** of f to be a morphism $E' \to E$ s.t. for all objects X in the category, the following sequence is exact

$$0 \longrightarrow \operatorname{Mor}(X, E') \longrightarrow \operatorname{Mor}(X, E) \longrightarrow \operatorname{Mor}(X, F)$$

we define a **cokernel** for f to be a morphism $F \to F''$ s.t. for all objects X in the category, the following sequence is exact

$$0 \longrightarrow \operatorname{Mor}(F'', X) \longrightarrow \operatorname{Mor}(F, X) \longrightarrow \operatorname{Mor}(E, X)$$

- AB 3 Kernels and cokernels exist
- AB 4 If $f : E \to F$ is a morphism whose kernel is 0, then f is the kernel of its cokernel. If $f : E \to F$ is a morphism whose cokernel is 0, then f is the cokernel of its kernel. A morphism whose kernel and cokernel are 0 is an isomorphism

A category $\mathfrak{C}$ satisfying the above four axioms is called an **abelian category**

In an abelian category, the group of morphisms is usually denote by Hom, so

$$\mathrm{Mor}(E, F) = \mathrm{Hom}(E, F)$$

The morphisms are usually called **homomorphisms**. Given an exact sequence

$$0 \longrightarrow M' \longrightarrow M$$

we say that M' is a **subobject** of M, or that the homomorphism of M' into M is a **monomorphism**. Dually, in an exact sequence

$$M \longrightarrow M'' \longrightarrow 0$$

we say that M'' is a **quotient object** of M, or that the homomorphism of M to M'' is an **epimorphism**

3.4 Free Modules

Let M be a module over a ring A and let S be a subset of M. S is a **basis** of M if S is not empty, if S generates M, and if S is linearly independent. If S is a basis of M, then in particular $M \neq \{0\}$ if $A \neq \{0\}$ and every element of M has a unique expression as a linear combination of elements of S

If A is a ring, then as a module over itself, A admits a basis, consisting of the unit element 1.

Let I be a non-empty set, and for each $i \in I$, let $A_i = A$, viewed as an A-module. Let

$$F = \bigoplus_{i \in I} A_i$$

then F admits a basis, which consists of the elements e_i of F whose i-th component is the unit element of A_i, and having all other components equal to 0

By a **free** module we mean a module which admits a basis, or the zero module

Theorem 3.7. *Let A be a ring and M a module over A. Let I be a non-empty set, and let $\{x_i\}_{i \in I}$ be a basis of M. Let N be an A-module, and let $\{y_i\}_{i \in I}$ be a family of elements of N. Then there exists a unique homomorphism $f : M \to N$ s.t. $f(x_i) = y_i$ for all i.*

Corollary 3.8. *Let the notation be as in the theorem, and assume that $\{y_i\}_{i \in I}$ is a basis of N. Then the homomorphism f is an isomorphism*

Corollary 3.9. *Two modules having bases whose cadinalities are equal are isomorphic*

Let M be a free module over A, with basis $\{x_i\}_{i \in I}$, so that

$$M = \bigoplus_{i \in I} Ax_i$$

Let $\mathfrak{a}$ be a two sided ideal of A. Then $\mathfrak{a}M$ is a submodule of M. Each $\mathfrak{a}x_i$ is a submodule of Ax_i. We *have an isomorphism*

$$M/\mathfrak{a}M \cong \bigoplus_{i \in I} Ax_i/\mathfrak{a}x_i$$

A module M is called **principal** if there exists an element $x \in M$ s.t. $M = Ax$. The map

$$a \mapsto ax$$

is an A-module homomorphism of A onto M, whose kernel is a left ideal $\mathfrak{a}$.

3.5 Vector Spaces

A module over a field is called a **vector space**

Theorem 3.10. *Let V be a vector space over a field K, and assume that $V \neq \{0\}$. Let Γ be a set of generators of V over K and let S be a subset of Γ which is linearly independent. Then there exists a basis $\mathfrak{B}$ of V s.t. $S \subset \mathfrak{B} \subset \Gamma$.*

Proof. Zorn's lemma □

Theorem 3.11. *Let V be a vector space over a field K. Then two bases of V over K have the same cardinality*

Proof. First assume that there exists a basis of V with a finite number of elements, say $\{v_1, \dots, v_m\}$, $m \geq 1$. It is suffice to prove: if $w_1, \dots, w_n$ are elements of V which are linearly independent over K, then $n \leq m$ (for then we can use symmetry). We proceed by induction. There exist elements $c_1, \dots, c_m$ of K s.t.

$$w_1 = c_1 v_1 + \cdots + c_m v_m$$

and some c_i, say c_1 is not equal to 0. Then v_1 lies in the space generated by $w_1, v_2, \dots, v_m$ over K, and this space must therefore be equal to V itself. Furthermore, $w_1, v_2, \dots, v_m$ are linearly independent, for suppose $b_1, \dots, b_m$ are elements of K s.t.

$$b_1 w_1 + \cdots + b_m v_m = 0$$

if $b_1 \neq 0$, divide by b_1 and express w_1 as a linear combination of $v_2, \dots, v_m$, would yield a relation of linear dependence among the v_i. Hence $b_1 = 0$, and again we must have all $b_i = 0$

Suppose inductively that after a suitable renumbering of the v_i, we have found $w_1, \dots, w_r$ $(r < n)$ s.t.

$$\{w_1, \dots, w_r, v_{r+1}, \dots, v_m\}$$

is a basis of V.

$$w_{r+1} = c_1 w_1 + \cdots + c_r w_r + c_{r+1} w_{r+1} + \cdots + c_m v_m$$

with $c_i \in K$. Similarly we still can replace v_{r+1} by w_{r+1}. □

Theorem 3.12. *Let V be a vector space over a field K, and let W be a subspace. Then*

$$\dim_K V = \dim_K W + \dim_K V/W$$

If $f : V \to U$ is a homomorphism of vector spaces over K, then

$$\dim V = \dim \ker f + \dim \operatorname{im} f$$

Proof. The first statement is a special case of the second, taking for f the canonical map. Let $\{u_i\}_{i\in I}$ be a basis of $\operatorname{im} f$ and $\{w_i\}_{i\in J}$ a basis of $\ker f$. Let $\{v_i\}_{i\in I}$ be a family of V s.t. $f(v_i) = u_i$ for each $i \in I$. We contend that

$$\{v_i, w_j\}_{i\in I, j\in J}$$

is a basis for V

Let $x \in V$. Then there exist elements $\{a_i\}_{i\in I}$ of K almost all of which are 0 s.t.

$$f(x) = \sum_{i\in I} a_i u_i$$

Hence $f(x - \sum a_i v_i) = 0$. Thus

$$x - \sum a_i v_i \in \ker f$$

thus there exists elements $\{b_j\}_{j\in J}$ of K almost all of which are 0 s.t.

$$x - \sum a_i v_i = \sum b_j w_j$$

From this we see that $x = \sum a_i v_i + \sum b_j w_j$, and that $\{v_i, w_j\}$ generated V. It remains to show that the family is linearly independent. Suppose that there exists elements c_i, d_j s.t.

$$0 = \sum c_i v_i + \sum d_j w_j$$

applying f yields

$$0 = \sum c_i f(v_i) = \sum c_i u_i$$

whence all $c_i = 0$.From this we conclude that all $d_j = 0$ $\square$

Corollary 3.13. *Let V be a vector space and W a subspace. Then*

$$\dim W \leq \dim V$$

If V is finite dimensional and $\dim W = \dim V$ *then $W = V$*

4 Polynomials

4.1 Basic Properties for Polynomials in One Variable

Theorem 4.1. *Let A be a commutative ring, let $f, g \in A[X]$ be polynomials in one variable, of degree ≥ 0, and assume that the leading coefficient of g is a unit in A. Then there exist unique polynomials $q, r \in A[X]$ s.t.*

$$f = gq + r$$

and $\deg r < \deg g$

Proof. Write

$$f(X) = a_n X^n + \cdots + a_0$$
$$g(X) = b_d X^d + \cdots + b_0$$

where $n = \deg f$, $d = \deg g$ so that $a_n, b_d \neq 0$ and b_d is a unit in A. We use induction on n

if $n = 0$ and $\deg g > \deg f$, we let $q = 0$, $r = f$. If $\deg g = \deg f = 0$, then let $r = 0$ and $q = a_n b_d^{-1}$

Assume the theorem proved for polynomials of degree $< n$. We may assume $\deg g \leq \deg f$ (otherwise take $q = 0$ and $r = f$). Then

$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + f_1(X)$$

where $f_1(X)$ has degree $< n$. By induction, we can find q_1, r s.t.

$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + q_1(X) g(X) + r(X)$$

and $\deg r < \deg g$. Then we let

$$q(X) = a_n b_d^{-1} X^{n-d} + q_1(X)$$

For uniqueness, suppose that

$$f = q_1 g + r_1 = q_2 g + r_2$$

with $\deg r_1 < \deg g$ and $\deg r_2 < \deg g$. Subtracting yields

$$(q_1 - q_2)g = r_2 - r_1$$

Since the leading coefficient of g is assumed to be a unit, we have

$$\deg(q_1 - q_2)g = \deg(q_1 - q_2) + \deg g$$

Since $\deg(r_2 - r_1) < \deg g$, this relation can hold only if $q_1 - q_2 = 0$. Hence $r_1 = r_2$ □

Theorem 4.2. *Let k be a field. Then the polynomial ring in one variable $k[X]$ is principal*

Proof. Let $\mathfrak{a}$ be an ideal of $k[X]$ and assume $\mathfrak{a} \neq 0$. Let g be an element of $\mathfrak{a}$ of smallest degree ≥ 0. Let f be an element of $\mathfrak{a}$ s.t. $f \neq 0$. By the Euclidean algorithm we can find $q, r \in k[X]$ s.t.

$$f = qg + r$$

and $\deg r < \deg g$. But $r = f - qg$ whence $r \in \mathfrak{a}$. It follows that $r = 0$, hence that $\mathfrak{a}$ consists of all polynomials qg. □

A polynomial $f(X) \in k[X]$ is called **irreducible** if it has degree ≥ 1, and if one cannot write $f(X)$ as a product

$$f(X) = g(X)h(X)$$

with $g, h \in k[X]$ and both $g, h \notin k$. Elements of k are usually called **constant polynomials**. A polynomial is called **monic** if it has leading coefficient 1

Let A be a commutative ring and $f(X)$ a polynomial in $A[X]$. Let A be a subring of B. An element $b \in B$ is called a **root** or a **zero** of f in B if $f(b) = 0$.

Theorem 4.3. *Let k be a field and f a polynomial in one variable X in $k[X]$ of degree $n \geq 0$. Then f has at most n roots in k and if a is a root of f in k, then $X - a$ divides $f(X)$*

Proof. Suppose $f(a) = 0$. Find q, r s.t.

$$f(X) = q(X)(X - a) + r(X)$$

and $\deg r < 1$. Then

$$0 = f(a) = r(a)$$

Since $r = 0$ or r is a non-zero constant, we must have $r = 0$, whence $X - a$ divides $f(X)$. $\square$

Corollary 4.4. *Let k be a field and T an infinite subset of k. Let $f(X) \in k[X]$ be a polynomial in one variable. If $f(a) = 0$ for all $a \in T$, then $f = 0$*

Corollary 4.5. *Let k be a field, and let $S_1, \dots, S_n$ be infinite subsets of k. Let $f(X_1, \dots, X_n)$ be a polynomial in n variables over k. If $f(a_1, \dots, a_n) = 0$ for all $a_i \in S_i$ $(i = 1, \dots, n)$, then $f = 0$*

Proof. By induction. Let $n \geq 2$ and write

$$f(X_1, \dots, X_n) = \sum_j f_i(X_1, \dots, X_{n-1}) X_n^j$$

$\square$

Corollary 4.6. *Let k be an infinite field and f a polynomial in n variables over k . If f induces the zero function on $k^{(n)}$, then $f = 0$*

Let k be a finite field with q elements. Let $f(X_1, \dots, X_n)$ be a polynomial in n variables over k. Write

$$f(X_1, \dots, X_n) = \sum a_{\bar{v}} X_1^{v_1} \dots X_n^{v_n}$$

If $a_{\bar{v}} \neq 0$ we recall that the monomial $M_{\bar{v}}(X)$ **occurs** in f. Suppose this is the case, and that in this monomial $M_{\bar{v}}(X)$ some variable X_i occurs with an exponent $v_i \geq q$. We can write

$$X_i^{v_i} = X_i^{q+\mu}$$

If we replace $X_i^{v_i}$ by $X_i^{\mu+1}$ in this monomial, then we obtain a new polynomial which gives rise to the same function as f. The degree of this new polynomial is at most equal to the degree of f

Performing the above operation a finite number of times, for all the monomials occuring in f and all the variables $X_1, \dots, X_n$ we obtain some polynomial f^* giving rise to the same function as f, but whose degree in each variable is $< q$

Corollary 4.7. *Let k be a finite field with q elements. Let f be a polynomial in n variables over k s.t. the degree of f in each variable is $< q$. If f induces the zero function on k^n, then $f = 0$*

Let f be a polynomial in n variables over the finite field k. A polynomial g whose degree in each variable is $< q$ will be said to be **reduced**. There exists a unique reduced polynomial f^* which gives the same function as f on k^n

Let k be a field. By a **multiplicative subgroup** of k we shall mean a subgroup of the group k^* (non-zero elements of k)

Theorem 4.8. *Let k be a field and let U be a finite multiplicative subgroup of k. Then U is cyclic*

Proof. **??** Write U as a product of subgroups $U(p)$ for each prime p, where $U(p)$ is a p-group. □

Corollary 4.9. *If k is a finite field, then k^* is cyclic*

An element ζ in a field k s.t. there exists an integer $n \geq 1$ s.t. $\zeta^n = 1$ is called a **root of unity**, or n-th root of unity. Thus the set of n-th roots of unity is the set of roots of the polynomial $X^n - 1$. There are at most n such roots, and they form a group, which is cyclic by Theorem 4.8

The group of roots of unity is denoted by $\boldsymbol{\mu}$. The group of roots of unity in a field K is denoted by $\boldsymbol{\mu}(K)$

A field k is said to be **algebraically closed** if every polynomial in $k[X]$ of degree ≥ 1 has a root in k. If k is algebraically closed then the irreducible polynomials in $k[X]$ are the polynomials of degree 1. In such a case, the unique factorization of a polynomial f of degree ≥ 0 can be written in the form

$$f(X) = c\prod_{i=1}^{r}(X - \alpha_i)^{m_i}$$

Let A be a commutative ring. We define a map

$$D : A[X] \to A[X]$$

if $f(X) = a_n X^n + \cdots + a_0$ with $a_i \in A$, we define the **derivative**

$$Df(X) = f'(X) = \sum_{v=1}^{n} v a_v X^{v-1}$$

Let K be a field and f a non-zero polynomial in $K[X]$. Let a be a root of f in K. We can write

$$f(X) = (X - a)^m g(X)$$

with some polynomial $g(X)$ relatively prime to $X - a$. We call m the **multiplicity** of a in f, and say that a is a **multiple root** if $m > 1$

Proposition 4.10. *Let K, f be as above. The element a of K is a multiple root of f iff it is a root and $f'(a) = 0$*

Proposition 4.11. *Let $f \in K[X]$. If K has characteristic 0, and f has degree ≥ 1, then $f' \neq 0$. Let K have characteristic $p > 0$ and f have degree ≥ 1. Then $f' = 0$ iff in the expression for $f(X)$ given by*

$$f(X) = \sum_{v=1}^{n} a_v X^v$$

p divides each integer v s.t. $a_v \neq 0$

Since the binomial coefficients $\binom{p}{v}$ are divisible by p for $1 \leq v \leq p-1$ we see that if K has characteristic p, then for $a, b \in K$ we have

$$(a+b)^p = a^p + b^p$$

Since obviously $(ab)^p = a^p b^p$ the map

$$x \mapsto x^p$$

is a homomorphism of K into itself, which has trivial kernel, hence is injective. Iterating, we conclude that for each integer $r \geq 1$, the map $x \mapsto x^{p^r}$ is an endomorphism of K, called the **Frobenius endomorphism**.

4.2 Polynomials Over a Factorial Ring

5 Algebraic Extensions

5.1 Finite and Algebraic Extensions

Let F be a field. If F is a subfield of a field E, then we also say that E is an **extension field** of F. We may view E as a vector space over F, and we say E is **finite** or **infinite** extension of F according as the dimension of this vector space is finite or infinite.

Let F be a subfield of a field E. An element α of E is said to be **algebraic** over F if there exists elements $a_0, \ldots, a_n \in F$, not all equal to 0, s.t.

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

If $\alpha \neq 0$, and α is algebraic, then we can always find elements a_i as above s.t. $a_0 \neq 0$

Let X be a variable over F. We can also say that α is algebraic over F if the homomorphism

$$F[X] \to E$$

which is the identity on F and maps X on α has a non-zero kernel. In that case the kernel is an ideal which is principal, generated by a single polynomial $p(X)$, which we may assume has leading coefficient 1. We then have an isomorphism

$$F[X]/(p(X)) \cong F[\alpha]$$

and since $F[\alpha]$ is entire, it follows that $p(X)$ is irreducible. Having normalized $p(X)$ so that its leading coefficient is 1, we see that $p(X)$ is uniquely determined by α and will be called the **irreducible polynomial of α over F**, denoted by $\mathrm{irr}(\alpha, F, X)$

An extension E of F is said to be **algebraic** if every element of E is algebraic over F

Proposition 5.1. *Let E be a finite extension of F. Then E is algebraic over F*

Proof. Let $\alpha \in E, \alpha \neq 0$. The powers of α

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

cannot be linearly independent over F for all positive integers n, otherwise the dimension of E over F would be infinite. A linear relation between these powers shows that α is algebraic over F. $\square$

If E is an extension of F, we denote by

$$[E : F]$$

the dimension of E as a vector space over F.

Proposition 5.2. *Let k be a field and $F \subset E$ extension fields of k. Then*

$$[E : k] = [E : F][F : k]$$

if $\{x_i\}_{i \in I}$ is a basis for F over k and $\{y_j\}_{j \in J}$ is a basis for E over F, then $\{x_i y_j\}_{(i,j) \in I \times J}$ is a basis for E over k

Proof. Let $z \in E$. By hypothesis there exist elements $\alpha_j \in F$, almost all $\alpha_j = 0$, s.t.

$$z = \sum_{j \in J} \alpha_j y_j$$

For each $j \in J$ there exists elements $b_{ji} \in k$, almost all of which are equal to 0, s.t.

$$\alpha_j = \sum_{i \in I} b_{ji} x_i$$

and hence

$$z = \sum_j \sum_i b_{ji} x_i y_j$$

This shows that $\{x_i y_j\}$ is a family of generators for E over k. We must show that it is linearly independent. Let $\{c_{ij}\}$ be a family of elements of k, almost all of which are 0, s.t.

$$\sum_j \sum_i c_{ij} x_i y_j = 0$$

Then for each j

$$\sum_i c_{ij} x_i = 0$$

since the elements y_j are linearly independent over F. Hence $c_{ij} = 0$ □

Corollary 5.3. *The extension E of k is finite iff E is finite over F and F is finite over k*

A **tower** of fields is a sequence

$$F_1 \subset F_2 \subset \cdots \subset F_n$$

of extension fields. The tower is called **finite** iff each step is finite

Let k be a field, E an extension field, and $\alpha \in E$. We denote by $k(\alpha)$ the smallest subfield of E containing both k and α. It consists of all quotients $f(\alpha)/g(\alpha)$ where f, g are polynomials with coefficients in k and $g(\alpha) \neq 0$.

Proposition 5.4. *Let α be algebraic over k. Then $k(\alpha) = k[\alpha]$, and $k(\alpha)$ is finite over k. The degree $[k(\alpha) : k]$ is equal to the degree of* $\mathrm{irr}(\alpha, k, X)$

Let E, F be extensions of a field k. If E and F are contained in some field L then we denote by EF the smallest subfield of L containing both E and F, and call it the **compositum** of E and F, in L.

Let k be a subfield of E and let $\alpha_1, \ldots, \alpha_n \in E$. We denote by

$$k(\alpha_1, \ldots, \alpha_n)$$

the smallest subfield of E containing k and $\alpha_1, \ldots, \alpha_n$. Its elements consist of all quotients

$$\frac{f(\alpha_1, \ldots, f_n)}{g(\alpha_1, \ldots, \alpha_n)}$$

where f, g are polynomials in n variables with coefficients in k, and

$$g(\alpha_1, \dots, \alpha_n) \neq 0$$

We observe that E is the union of all its subfields $k(\alpha_1, \dots, \alpha_n)$ as $(\alpha_1, \dots, \alpha_n)$ ranges over finite subfamilies of elements of E. We could define the **compositum of an arbitrary subfamily of subfields of a field** L as the smallest subfield containing all fields in the family. We say that E is **finitely generated** over k if there is a finite family of elements $\alpha_1, \dots, \alpha_n$ of E s.t.

$$E = k(\alpha_1, \dots, \alpha_n)$$

Proposition 5.5. *Let E be a finite extension of k. Then E is finitely generated*

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of E as vector space over k. Then certainly

$$E = k(\alpha_1, \dots, \alpha_n)$$

□

If $E = k(\alpha_1, \dots, \alpha_n)$ is finitely generated, and F is an extension of k, both F, E contained in L, then

$$EF = F(\alpha_1, \dots, \alpha_n)$$

and EF is finitely generated over F

$$\begin{tikzcd}
 & EF \arrow[dl, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & F \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

Lines slanting up indicate an inclusion relation between fields. We also call the extension EF of F the **translation** of E to F, or also the **lifting** of E to F

Let α be algebraic over the field k. Let F be an extension of k, and assume $k(\alpha)$, F both contained in some field L. Then α is algebraic over F. Consider the irreducible polynomial for α.

Suppose that we have a tower of fields

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \dots, \alpha_n)$$

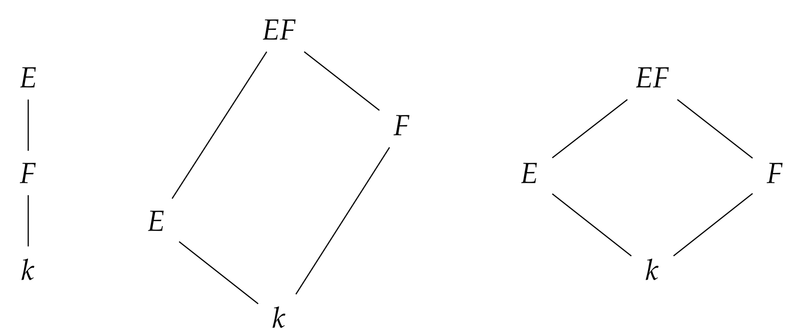
each one generated from the preceding field by a single element. Assume that each α_i is algebraic over k, $i = 1, \dots, n$. As a special case of our preceding remark, we note that α_{i+1} is algebraic over $k(\alpha_1, \dots, \alpha_i)$. Hence each step of the tower is algebraic

Proposition 5.6. *Let $E = k(\alpha_1, \dots, \alpha_n)$ be a finitely genrated extension of a field k, and assume α_i algebraic over k for each $i = 1, \dots, n$. Then E is finite algebraic over k*

Proof. E is finite by Proposition 5.4 and Corollary 5.3. Algebraic by Proposition 5.1 $\square$

Let $\mathcal{C}$ be a certain class of extension fields $F \subset E$. $\mathcal{C}$ is **distinguished** if it satisfies the following conditions

1. Let $k \subset F \subset E$ be a tower of fields. The extension $k \subset E$ is in $\mathcal{C}$ iff $k \subset F$ is in $\mathcal{C}$ and $F \subset E$ is in $\mathcal{C}$
2. if $k \subset E$ is in $\mathcal{C}$, if F is any extension of k, and E, F are both contained in some field, then $F \subset EF$ is in $\mathcal{C}$
3. if $k \subset F$ and $k \subset E$ are in $\mathcal{C}$ and F, E are subfields of a common field, then $k \subset FE$ is in $\mathcal{C}$



It is convenient to write E/F instead of $F \subset E$ to denote an extension

Proposition 5.7. *The class of algebraic extensions is distinguished, and so is the class of finite extensions*

5.2 Algebraic Closure

Let E be an extension of a field F and let

$$\sigma : F \to L$$

be an embedding (i.e. an injective homomorphism) of F into L. Then σ induces an isomorphism of F with its image σF, which is sometimes written F^σ. An embedding τ of E in L will be said to be **over** σ if the restriction of τ to F is equal to σ. We also say that τ **extends** σ. If σ is the identity then we say that τ is an embedding of E **over** F

$$\begin{tikzcd} E \arrow[r, "\tau"] & L \\ F \arrow[u, "\text{inc}"] \arrow[r, "\sigma"'] & L \arrow[u, "\text{id}"'] \end{tikzcd} \qquad \begin{tikzcd} E \arrow[rr, "\tau"] & & L \\ & F \arrow[ul, "\text{inc}"] \arrow[ur, "\text{inc}"'] & \end{tikzcd}$$

6 Real Fields

6.1 Ordered Fields

Let K be a field. An **ordering** of K is a subset P of K having the following properties

ORD 1. Given $x \in K$, we have either $x \in P$,or $x = 0$ or $-x \in P$, and these three possibilities are mutually exclusive

ORD 2. If $x, y \in P$, then $x + y, xy \in P$

K is **ordered by** P, and we call P the set of **positive elements**

Suppose K is ordered by P. Since $1 \neq 0$ and $1 = 1^2 = (-1)^2$, we see that $1 \in P$. By **ORD 2**, it follows that $1 + \cdots + 1 \in P$, whence K has characteristic 0. If $x \in P$ and $x \neq 0$, then $xx^{-1} = 1 \in P$ implies that $x^{-1} \in P$

Let E be a field. Then a product of sums of squares in E is a sum of squares. If $a, b \in E$ are sum of squares and $b \neq 0$, then a/b is a sum of squares

Consider complex number:)

Let $x, y \in K$. We define $x < y$ to mean that $y - x \in P$. If $x < 0$ we say that x is **negative**.

If K is ordered and $x \in K$, $x \neq 0$, then x^2 is positive

If E has characteristic $\neq 2$, and -1 is a sum of squares in E, then every element $a \in E$ is a sum of squares, because $4a = (1+a)^2 - (1-a)^2$

If K is a field with an ordering P, and F is a subfield, then obviously, $P \cap F$ defines an ordering of F, which is called the **induced** ordering

Let K be an ordered field and let F be a subfield with the induced ordering. We put $|x| = x$ if $x > 0$ and $|x| = -x$ if $x < 0$. An element $\alpha \in K$ is **infinitely large** over F if $|\alpha| \geq x$ for all $x \in F$. It is **infinitely small** over F if $0 \leq |\alpha| \leq |x|$ for all $x \in F$, $x \neq 0$. α is infinitely large if and only if α^{-1} is infinitely small. K is **archimedean** over F if K has no elements which are infinitely large over F. An intermediate field F_1, $K \supset F_1 \supset F$ is **maximal archimedean over** F in K if it is archimedean over F and no other intermediate field containing F_1 is archimedean over F. We say that F is **maximal archimedean in** K if it is maximal archimedean over itself in K

Let K be an ordered field and F a subfield. Let K be an ordered field and F a subfield. Let $\mathfrak{o}$ be the set of elements of K which are not infinitely large over F. Then $\mathfrak{o}$ is a ring and that for any $\alpha \in K$, we have α or $\alpha^{-1} \in \mathfrak{o}$. Hence $\mathfrak{o}$ is what is called a valuation ring, containing F. Let $\mathfrak{m}$ be the ideal of all $\alpha \in K$ which are infinitely small over F. Then $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{o}$, because any element in $\mathfrak{o}$ which is not in $\mathfrak{m}$ has an inverse in $\mathfrak{o}$. We call $\mathfrak{o}$ the **valuation ring determined by the ordering of** K/F

Proposition 6.1. *Let K be an ordered field and F a subfield. Let $\mathfrak{o}$ be the valuation ring determined by the ordering of K/F, and let $\mathfrak{m}$ be its maximal ideal. Then $\mathfrak{o}/\mathfrak{m}$ is a real field.*

Proof. Otherwise, we could write

$$-1 = \sum \alpha_i^2 + a$$

with $\alpha_i \in \mathfrak{o}$ and $a \in \mathfrak{m}$. Since $\sum \alpha_i^2$ is positive and a is infinitely small, such a relation is clearly impossible $\square$