

LECTURE NOTES
MA2314: FIELDS, RINGS AND MODULES (2017)

SERGEY MOZGOVOY

CONTENTS

1. Rings	2
1.1. Basic definitions	2
1.2. Ideals and quotient rings	4
1.3. Ring homomorphisms	7
1.4. Algebras	9
2. Integral domains	12
2.1. Basic definitions	12
2.2. UFD	13
2.3. PID	15
2.4. GCD and LCM	16
2.5. Euclidean domains	17
2.6. Field of fractions	19
2.7. Factorization in polynomial rings	20
2.8. Cyclotomic polynomials	22
3. Fields	24
3.1. Basic definitions	24
3.2. Field extensions	25
3.3. Splitting fields, Finite fields, Algebraically closed fields	27
3.4. Constructions with compass and straightedge	29
4. Symmetric polynomials	32
4.1. Discriminant	34
5. Modules	35
5.1. Definition and examples	35
5.2. Homomorphisms and submodules	36
5.3. Simple and indecomposable modules	38
5.4. Chinese remainder theorem	40
5.5. Modules over PID	41
5.6. Noetherian modules	43

1. RINGS

1.1. Basic definitions. Consider the set $\mathbb{Z}$ of integer numbers. It has two binary operations $+$ (addition) and $\cdot$ (multiplication) compatible with each other:

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca.$$

We will use this example as a motivation for a formal description of the above operations and their properties.

Definition 1.1. An abelian group is a pair $(A, +)$, where A is a set and $+: A \times A \rightarrow A$ is a map (written $(a, b) \mapsto a + b$) such that

- (1) (Associativity) $(a + b) + c = a + (b + c)$.
- (2) (Commutativity) $a + b = b + a$.
- (3) (Existence of zero) There exists an element $0 \in A$ such that $0 + a = a + 0 = a \forall a \in A$.
- (4) (Existence of negative) For any $a \in A$ there exists an element $b \in A$ such that $a + b = 0$. It is denoted by $-a$.

Example 1.2. The set of natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

has an obvious addition operation. But it is not a group: it does not contain negatives of nonzero elements. For example $-1 \notin \mathbb{N}$. The following are examples of abelian groups

- (1) The set $\mathbb{Z}$ of integer numbers.
- (2) The set $\mathbb{Q}$ of rational numbers.
- (3) The set $\mathbb{R}$ of real numbers.
- (4) The set $\mathbb{C}$ of complex numbers.

◇

Definition 1.3. A ring is a triple $(R, +, \cdot)$, where R is a set and $+: R \times R \rightarrow R$, $\cdot: R \times R \rightarrow R$ are binary operations such that

- (1) $(R, +)$ is an abelian group.
- (2) (Associativity of multiplication) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (3) (Existence of unity) $\exists 1 \in R$ such that $1a = a1 = a$ for all $a \in R$.
- (4) (Distributivity) $a(b + c) = ab + ac$, $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Definition 1.4. Let R be a ring. Then

- (1) R is called a commutative ring if for any $a, b \in R$: $ab = ba$.
- (2) R is called a division ring if for any nonzero $a \in R$ there exists $b \in R$ such that $ab = ba = 1$ (it is denoted by a^{-1} and is called the inverse of a).
- (3) R is called a field if it is a commutative ring and a division ring.

Example 1.5. We met already quite a few examples of rings.

- (1) The sets

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

are rings with respect to the natural operations of addition and multiplication. All of them are commutative. The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are also fields as all nonzero elements in them are invertible. The ring $\mathbb{Z}$ is not a field. For example, the element $2 \in \mathbb{Z}$ does not have inverse in $\mathbb{Z}$ as $1/2 \notin \mathbb{Z}$.

- (2) The sets of polynomials $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ are commutative rings. They are not fields.
- (3) The set $M_n(\mathbb{R})$ of $n \times n$ matrices with real coefficients is a ring. Addition and multiplication of matrices $A = (a_{ij})$, $B = (b_{ij})$ is given by

$$A + B = (c_{ij}), \quad c_{ij} = a_{ij} + b_{ij},$$

$$AB = (d_{ij}), \quad d_{ij} = \sum_{k=1}^n a_{ik}b_{kj}.$$

The zero element of this ring is the zero matrix. The unity element of this ring is the identity matrix

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$$

Similarly, the set $M_n(\mathbb{C})$ of $n \times n$ matrices with complex coefficients is a ring. For $n \geq 2$ they are not commutative. For example

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Therefore $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. For $n \geq 2$ they are also not division rings. For example, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is not invertible.

◇

Lemma 1.6. *If R is a ring then*

- (1) *The zero element is unique.*
- (2) *The negative of any element is unique.*
- (3) *The unity is unique.*

Proof. If $0'$ is another zero then $0 + 0' = 0$ and $0 + 0' = 0'$. Therefore $0 = 0'$. Assume that an element a has two negatives b, b' . Then

$$b = b + (a + b') = (b + a) + b' = 0 + b' = b'.$$

If $1'$ is another unity then $1 \cdot 1' = 1 = 1'$.

□

Lemma 1.7. *Let R be a ring. Then*

- (1) $0a = a0 = 0$.
- (2) $(-a)b = a(-b) = -ab$.

Proof.

$$0a + a = 0a + 1a = (0 + 1)a = 1a = a.$$

Therefore $0a = 0$. Similarly $a0 = 0$.

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

Therefore $(-a)b = -ab$. Similarly $a(-b) = -ab$.

□

1.2. Ideals and quotient rings. Let R be a ring.

Definition 1.8. A subset $I \subset R$ is called an ideal of R if

- (1) I is a subgroup of $(R, +)$, that is
 - (a) $0 \in I$.
 - (b) $a, b \in I \implies a + b \in I$.
 - (c) $a \in I \implies -a \in I$.
- (2) $a \in I, r \in R \implies ra \in I, ar \in I$

Remark 1.9. For any subsets $A, B \subset R$ define

$$A + B = \{a + b \mid a \in A, b \in B\}, \quad AB = \{ab \mid a \in A, b \in B\}.$$

Then the last condition can be written as $RI \subset I, IR \subset I$. ◇

Remark 1.10. Note that the subsets $\{0\} \subset R$ and $R \subset R$ are ideals. An ideal $I \subset R$ is called proper if it is a proper subset of R , that is, $I \neq R$. ◇

Example 1.11. For any $n \in \mathbb{Z}$ the set $I = \mathbb{Z}n$ is an ideal in the ring $\mathbb{Z}$:

- (1) $0n = 0 \in \mathbb{Z}n$.
 - (2) If $kn \in \mathbb{Z}n, ln \in \mathbb{Z}n$ then $kn + ln = (k + l)n \in \mathbb{Z}n$.
 - (3) If $kn \in \mathbb{Z}n$ then $-kn = (-k)n \in \mathbb{Z}n$.
 - (4) If $kn \in \mathbb{Z}$ and $r \in \mathbb{Z}$ then $r \cdot kn = (rk)n \in \mathbb{Z}n$.
- ◇

Lemma 1.12. All ideals of $\mathbb{Z}$ are of the form $\mathbb{Z}n$ for some $n \in \mathbb{Z}$.

Proof. Let $I \subset \mathbb{Z}$ be an ideal. If $I = \{0\}$ then $I = \mathbb{Z}0$. Assume that I is nonzero. Let n be the minimal positive element of I . We will prove that $I = \mathbb{Z}n$. Inclusion $\mathbb{Z}n \subset I$ is clear. Assume that $m \in I \setminus \mathbb{Z}n$. Dividing m by n with remainder we can write $m = qn + r$ for integers q, r with $0 \leq r < n$. Actually $0 < r < n$ as $m \notin \mathbb{Z}n$. As $m, n \in I$ also

$$r = m - qn = m - n - \dots - n \in I.$$

This contradicts to the minimality of n . □

1.2.1. Ideal generated by a set.

Lemma 1.13. Let R be a ring and let $(I_t)_{t \in T}$ be a collection of ideals in R . Then $\bigcap_{t \in T} I_t$ is an ideal in R .

Proof. Let $I = \bigcap_{t \in T} I_t$. Then

- (1) $0 \in I$ as $0 \in I_t \forall t \in T$.
 - (2) $a, b \in I \implies a, b \in I_t \forall t \in T \implies a + b \in I_t \forall t \in T \implies a + b \in I$.
 - (3) $a \in I \implies a \in I_t \forall t \in T \implies -a \in I_t \forall t \in T \implies -a \in I$.
 - (4) $a \in I, r \in R \implies a \in I_t \forall t \in T \implies ra, ar \in I_t \forall t \in T \implies ra, ar \in I$.
-

Definition 1.14. Let $F \subset R$ be a subset. Denote by (F) the smallest ideal of R that contains F , that is, the intersection of all ideals that contain F . It is called an ideal generated by F . If $F = \{f_1, \dots, f_n\}$, then we denote (F) also by $(f_1, \dots, f_n)$.

Remark 1.15. An ideal (F) can be described as a set of all finite sums

$$(F) = \{a_1 f_1 b_1 + \dots + a_k f_k b_k \mid k \geq 0, f_i \in F, a_i, b_i \in R\}.$$

If R is commutative then

$$(F) = \{a_1 f_1 + \dots + a_k f_k \mid k \geq 0, f_i \in F, a_i \in R\}.$$
◇

Example 1.16. An ideal generated by $n \in \mathbb{Z}$ is $(n) = \mathbb{Z}n = n\mathbb{Z}$. ◇

Remark 1.17. Given a commutative ring R and two elements $a, b \in R$, we say that a divides b (or b is a multiple of a) if there exists $c \in R$ such that $b = ac$. We write $a \mid b$ in this case. Note that $a \mid b$ if and only if $b \in (a)$. $\diamond$

1.2.2. *Quotient rings.* Let R be a ring and $I \subset R$ be an ideal. We will construct a quotient ring R/I as follows:

Define a binary relation $\sim$ on R (this is a subset of $R \times R$) by the rule

$$a \sim b \iff a - b \in I$$

(we say that a, b are congruent modulo I and write also $a \equiv b \pmod{I}$). This is an equivalence relation:

- (1) Reflexivity: $a \sim a$, because $a - a = 0 \in I$.
- (2) Symmetry: if $a \sim b$ then $b \sim a$, because if $a - b \in I$ then $b - a = -(a - b) \in I$.
- (3) Transitivity: $a \sim b, b \sim c \implies a \sim c$, because if $a - b \in I, b - c \in I$ then $(a - b) + (b - c) = a - c \in I$.

The equivalence class $[a]$ of an element $a \in R$ is given by

$$[a] = a + I = \{a + b \mid b \in I\}$$

and is also called a congruence class of a modulo I . The set of all equivalence classes is denoted by R/I .

Theorem 1.18. *The set R/I with an addition and multiplication*

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = ab + I$$

is a ring, called a quotient ring. Its zero element is $0 + I$ and its unity element is $1 + I$.

Proof. First of all we have to show that addition and multiplication are well defined. This means that we have to show that if $a \sim a'$ and $b \sim b'$ then

$$(a + I) + (b + I) = (a' + I) + (b' + I), \quad (a + I) \cdot (b + I) = (a' + I) \cdot (b' + I).$$

To show the first equality we have to show

$$(a + b) + I = (a' + b') + I$$

that is, $(a + b) - (a' + b') \in I$. But

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I.$$

To show the second equality we have to show

$$ab + I = a'b' + I$$

that is, $ab - a'b' \in I$. But

$$ab - a'b' = a(b - b') + (a - a')b' \in I$$

as $b - b' \in I$ and $a - a' \in I$.

Let us prove now that R/I is a ring. We check first that $(R/I, +)$ is an abelian group:

- (1) $(a + I + b + I) + c + I = (a + b + c) + I = a + I + (b + I + c + I)$.
- (2) $a + I + b + I = (a + b) + I = (b + a) + I = b + I + a + I$.
- (3) The element $0 + I = I \in R/I$ is zero: $a + I + 0 + I = (a + 0) + I = a + I$.
- (4) For any $(a + I) \in R/I$ there exists negative $(-a + I)$: $(a + I) + (-a + I) = (a - a) + I = 0 + I$.

Let us check the remaining axioms:

- (1) $((a + I) \cdot (b + I)) \cdot (c + I) = abc + I = (a + I) \cdot ((b + I) \cdot (c + I))$.
- (2) The element $1 + I \in R/I$ is the unity element: $(a + I)(1 + I) = a + I = (1 + I)(a + I)$.
- (3) (Distributivity)

$$\begin{aligned} (a + I)(b + I + c + I) &= (a + I)((b + c) + I) = (ab + ac) + I \\ &= (ab + I) + (ac + I) = (a + I)(b + I) + (a + I)(c + I). \end{aligned}$$

Similarly one can prove the second distributivity property.

□

Example 1.19. Consider the ring $\mathbb{Z}$ with an ideal $n\mathbb{Z}$. Then we can construct the quotient ring $\mathbb{Z}/n\mathbb{Z}$, called the ring of congruence classes of integers modulo n . It consists of n elements which are congruence classes of $0, 1, \dots, n-1$. For any $m \in \mathbb{Z}$, let $[m] = m + n\mathbb{Z}$ be the congruence class of m .

In the ring $\mathbb{Z}/2\mathbb{Z}$ we have $[1] + [1] = [0]$ and $[1] \cdot [1] = [1]$. In $\mathbb{Z}/3\mathbb{Z}$ we have $[2] \cdot [2] = [4] = [1]$ (as $4 \equiv 1 \pmod{3}$). This means that $[2]$ is invertible in $\mathbb{Z}/3\mathbb{Z}$. On the other hand, in $\mathbb{Z}/4\mathbb{Z}$ we have $[2] \cdot [2] = [4] = [0]$ (as $4 \equiv 0 \pmod{4}$). This means that $[2]$ is not invertible in $\mathbb{Z}/4\mathbb{Z}$. The difference between these two rings stems from the fact that 3 is prime and 4 is not. The general picture is described in the following theorem. $\diamond$

Theorem 1.20. *The ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.*

Proof. Necessary: assume that n is not prime. Then $n = km$ for some $1 < k, m < n$. In $\mathbb{Z}/n\mathbb{Z}$ we have $k, m \neq 0$, but $km = n = 0$. This means that k, m are zero divisors and $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Sufficient: assume that $n = p$ is a prime. Let $1 \leq k < p$ be a number that represents some nonzero element in $R = \mathbb{Z}/p\mathbb{Z}$. Then multiplication $k : R \rightarrow R$ (given by $[m] \mapsto [k][m]$) is injective: if not, then $[k][m] = 0$ for some $[m] \neq 0$. But this would imply that $p \mid km$ and therefore $p \mid k$ or $p \mid m$ (see the next result), a contradiction. As R is finite, the map $k : R \rightarrow R$ should be actually bijective. This implies that k is invertible. $\square$

Lemma 1.21. *Let p be a prime number and a, b be integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Let $I = \{n \in \mathbb{Z} \mid p \mid na\}$. Then $p, b \in I$. The set I is an ideal in $\mathbb{Z}$. Therefore $I = d\mathbb{Z}$ for some $d \geq 1$. As $p \in I = d\mathbb{Z}$, we conclude that $d \mid p$ and therefore $d = 1$ or $d = p$. If $d = 1$ then $p \mid d \cdot a = a$ and we are done. If $d = p$ then from $b \in I = p\mathbb{Z}$ we conclude that $p \mid b$. $\square$

1.3. Ring homomorphisms.

Definition 1.22. Let R be a ring. A subset $S \subset R$ is called a subring if S is itself a ring when addition and multiplication is restricted from R to S and if 1_R (the unity of R) is contained in S .

Remark 1.23. Given a ring R and a subset $S \subset R$, to verify that S is a subring of R we have to check the following axioms:

- (1) $a, b \in S \implies a + b \in S$.
- (2) $a, b \in S \implies ab \in S$.
- (3) $a \in S \implies -a \in S$.
- (4) $0, 1 \in S$.

◇

Remark 1.24. For example, there is a chain of subrings $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. But what about the ring $\mathbb{Z}/n\mathbb{Z}$? Is it a subring of $\mathbb{Z}$? The answer is not: all nonzero elements of $\mathbb{Z}/5\mathbb{Z}$ are invertible, but it would be rather difficult to find many invertible elements in $\mathbb{Z}$. It turns out that it works the other way around: there is a canonical map $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ that preserves the ring structures. This leads us to the following definition. ◇

Definition 1.25. A map $\varphi : R \rightarrow S$ between two rings is called a ring homomorphism if

- (1) $\varphi(a + b) = \varphi(a) + \varphi(b)$.
- (2) $\varphi(ab) = \varphi(a)\varphi(b)$.
- (3) $\varphi(1_R) = 1_S$.

A homomorphism φ is called an isomorphism if it is bijective.

Example 1.26. If $S \subset R$ is a subring, then the inclusion map

$$i : S \rightarrow R, \quad i(s) = s \quad \forall s \in S$$

is a ring homomorphism, called a canonical embedding. ◇

Example 1.27. Let $C[a, b]$ be the set of continuous functions $f : [a, b] \rightarrow \mathbb{R}$ on the closed interval $[a, b]$. This is a ring with addition and multiplication defined pointwise:

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x), \quad \forall x \in [a, b]$$

for any $f, g \in C[a, b]$. Let $x_0 \in [a, b]$. We define a ring homomorphism $\varphi : C[a, b] \rightarrow \mathbb{R}$ by

$$C[a, b] \ni f \mapsto f(x_0) \in \mathbb{R}.$$

It is called the evaluation map at the point x_0 . ◇

Lemma 1.28. Let R be a ring and $I \subset R$ be an ideal. The map $\pi : R \rightarrow R/I$ given by

$$a \mapsto a + I$$

is a ring homomorphism, called the canonical homomorphism of a quotient ring.

Proof. We have

$$\begin{aligned} \pi(a + b) &= (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b). \\ \pi(ab) &= ab + I = (a + I)(b + I) = \pi(a)\pi(b). \\ \pi(1) &= 1 + I. \end{aligned}$$

□

Example 1.29. Applying this lemma to $R = \mathbb{Z}$ and $I = n\mathbb{Z}$, we obtain a canonical homomorphism $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. ◇

Lemma 1.30. If $\varphi : R \rightarrow S$ is a ring homomorphism then

- (1) $\varphi(0) = 0$.
- (2) $\varphi(-a) = -\varphi(a)$.

Proof. 1. $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$. Therefore $\varphi(0) = 0$.

2. $\varphi(-a) + \varphi(a) = \varphi(-a + a) = \varphi(0) = 0$. Therefore $\varphi(-a) = -\varphi(a)$. □

Definition 1.31. Let $\varphi : R \rightarrow S$ be a ring homomorphism. Define

- (1) the kernel of φ by

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\} \subset R.$$

- (2) the image of φ by

$$\operatorname{im} \varphi = \{\varphi(a) \mid a \in R\} \subset S.$$

Lemma 1.32. Let $\varphi : R \rightarrow S$ be a ring homomorphism. Then

- (1) $\ker \varphi \subset R$ is an ideal.
(2) $\operatorname{im} \varphi \subset S$ is a subring.

Proof. 1. We have

- (1) $\varphi(0) = 0$. Therefore $0 \in \ker \varphi$.
(2) For any $a, b \in \ker \varphi$: $\varphi(a + b) = \varphi(a) + \varphi(b) = 0$. Therefore $a + b \in \ker \varphi$.
(3) For any $a \in \ker \varphi$: $\varphi(-a) = -\varphi(a) = 0$. Therefore $-a \in \ker \varphi$.
(4) For any $a \in \ker \varphi$, $r \in R$: $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$ and $\varphi(ar) = \varphi(a)\varphi(r) = 0$.
Therefore $ra, ar \in \ker \varphi$.

This proves that $\ker \varphi$ is an ideal in R .

2. We have $1_S \in \operatorname{im} \varphi$ as $\varphi(1_R) = 1_S$. Given two elements $\varphi(a), \varphi(b) \in \operatorname{im} \varphi$, we have

- (1) $\varphi(a) + \varphi(b) = \varphi(a + b) \in \operatorname{im} \varphi$.
(2) $-\varphi(a) = \varphi(-a) \in \operatorname{im} \varphi$.
(3) $\varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im} \varphi$.

This proves that $\operatorname{im} \varphi$ is a subring of S . □

Lemma 1.33. A ring homomorphism $\varphi : R \rightarrow S$ is injective if and only if $\ker \varphi = 0$ (we denote the zero ideal $\{0\}$ by 0).

Proof. Assume that φ is injective. If $\varphi(a) = 0$ then $\varphi(a) = \varphi(0) \implies a = 0$. Therefore $\ker \varphi = 0$.

Assume that $\ker \varphi = 0$. If $\varphi(a) = \varphi(b)$, then $\varphi(a - b) = 0 \implies a - b \in \ker \varphi \implies a - b = 0 \implies a = b$. Therefore φ is injective. □

Theorem 1.34 (Homomorphism Theorem). For any ring homomorphism $\varphi : R \rightarrow S$, there is a unique homomorphism $\bar{\varphi} : R/\ker \varphi \rightarrow S$ that makes the following diagram commute ($\varphi = \bar{\varphi} \circ \pi$)

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/\ker \varphi \\ & \searrow \varphi & \swarrow \bar{\varphi} \\ & S & \end{array}$$

It induces an isomorphism $\bar{\varphi} : R/\ker \varphi \rightarrow \operatorname{im} \varphi$.

Proof. Let $I = \ker \varphi$.

Uniqueness. From the requirement $\varphi = \bar{\varphi}\pi$ we obtain $\varphi(a) = \bar{\varphi}\pi(a) = \bar{\varphi}(a + I) \forall a \in R$. This means that for any equivalence class $a + I$ we require $\bar{\varphi}(a + I) = \varphi(a)$ and $\bar{\varphi}$ is uniquely determined.

Existence. For any equivalence class $a + I$, we define $\bar{\varphi}(a + I) = \varphi(a)$. This map is well-defined: if $a \sim b$ then $a - b \in I = \ker \varphi \implies \varphi(a - b) = 0 \implies \varphi(a) = \varphi(b)$. This map is a ring homomorphism:

- (1) $\bar{\varphi}(a + I + b + I) = \varphi(a + b) = \varphi(a) + \varphi(b) = \bar{\varphi}(a + I) + \bar{\varphi}(b + I)$.
(2) $\bar{\varphi}((a + I)(b + I)) = \bar{\varphi}(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(a + I)\bar{\varphi}(b + I)$.
(3) $\bar{\varphi}(1_R + I) = \varphi(1_R) = 1_S$.

For any $a \in R$ we have $\varphi(a) = \bar{\varphi}(a + I) = \bar{\varphi}\pi(a)$. Therefore $\varphi = \bar{\varphi}\pi$ and the diagram commutes.

Consider the map $\bar{\varphi} : R/I \rightarrow \operatorname{im} \varphi$. It is surjective as for any $\varphi(a) \in \operatorname{im} \varphi$ we have $\bar{\varphi}(a + I) = \varphi(a)$. It is also injective: if $\bar{\varphi}(a + I) = 0$, then $\varphi(a) = \bar{\varphi}(a + I) = 0 \implies a \in I$, therefore $a + I = I = 0 + I$. This means that $\bar{\varphi} : R/I \rightarrow \operatorname{im} \varphi$ is bijective and therefore an isomorphism. □

1.4. Algebras.

Definition 1.35. Let R be a commutative ring. A ring S is called an algebra over R if R is a subring of S and for any $r \in R$, $s \in S$: $rs = sr$.

Remark 1.36. For any ring S , define its center by

$$Z(S) = \{a \in S \mid ab = ba \ \forall b \in S\}.$$

If S is an algebra over R , then $R \subset Z(S)$. ◇

Remark 1.37. If R is a field and S is an algebra over R then S is a vector space over R . Assume that $(e_1, \dots, e_n)$ is a basis of S over R . Then all elements of S are of the form $x = \sum_{i=1}^n x_i e_i$, where $x_i \in R$. To define the multiplication on S , it is enough to describe the products $e_i e_j \in S$ for all i, j . Indeed, if $x = \sum x_i e_i$, $y = \sum y_j e_j$ with $x_i, y_j \in R$, then

$$xy = \left(\sum x_i e_i \right) \left(\sum y_j e_j \right) = \sum_{i,j} x_i y_j \cdot e_i e_j.$$

◇

1.4.1. The algebra of matrices. Let R be a commutative ring. Let $M_n(R)$ be the set of $n \times n$ matrices with coefficients in R . It is a ring with respect to the usual addition and multiplication: given matrices $A = (a_{ij})$, $B = (b_{ij})$ in $M_n(R)$, we define

$$A + B = (c_{ij}), \quad c_{ij} = a_{ij} + b_{ij}, \quad AB = (d_{ij}), \quad d_{ij} = \sum_{k=1}^n a_{ik} b_{kj}.$$

The ring $M_n(R)$ is an algebra over R . Indeed, R can be embedded into $M_n(R)$ by the rule

$$r \mapsto rI_n, \quad r \in R,$$

where I_n is an identity matrix in $M_n(R)$. Then R is a subring of $M_n(R)$ and its elements commute with all matrices

$$(rI_n)A = A(rI_n) = rA.$$

The algebra $M_n(R)$ over R is called the matrix algebra (or the matrix ring).

1.4.2. The algebra of quaternions. The algebra of quaternions $\mathbb{H}$ is an algebra over $\mathbb{R}$ with a basis $1, i, j, k$. The multiplication law is given on the basis by requiring that 1 is the identity and

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

Remark 1.38. This algebra was invented by Hamilton on October 16, 1843 while walking near the Broome Bridge, Dublin. This event is commemorated by a stone plaque near the bridge. For a long time quaternions were a mandatory exam topic in Dublin. ◇

Actually it is enough to require just

$$i^2 = j^2 = k^2 = ijk = -1.$$

Indeed, i, j, k are invertible and therefore $ijk = k^2$ implies $ij = k \implies kj = ij^2 = -i$ and so on. Given an element $x = a + bi + cj + dk \in \mathbb{H}$, we define the absolute value and the conjugate of x by

$$|x| = \sqrt{a^2 + b^2 + c^2 + d^2}, \quad \bar{x} = a - bi - cj - dk.$$

Then

$$x\bar{x} = (a + bi + cj + dk)(a - bi - ci - dk) = a^2 + b^2 + c^2 + d^2 = |x|^2$$

and similarly $\bar{x}x = |x|^2$. This implies that if $x \neq 0$ then

$$x \cdot \frac{\bar{x}}{|x|^2} = \frac{\bar{x}}{|x|^2} \cdot x = 1$$

and the element $\frac{\bar{x}}{|x|^2}$ is inverse to x . This means that all nonzero elements of $\mathbb{H}$ are invertible, that is, $\mathbb{H}$ is a division ring. It is non-commutative (for example $ij = k$ and $ji = -k$). The ring $\mathbb{H}$ is

an algebra over $\mathbb{R}$ if we embed $\mathbb{R} \subset \mathbb{H}$ by the rule $a \mapsto a1$ (note that the elements of $\mathbb{R}$ commute with the elements of $\mathbb{H}$). We can also embed $\mathbb{C} \subset \mathbb{H}$ by

$$a + bi \mapsto a1 + bi \in \mathbb{H}.$$

This makes $\mathbb{C}$ a subring of $\mathbb{H}$. But $\mathbb{H}$ is not an algebra over $\mathbb{C}$: $ij \neq ji$, that is, the element $i \in \mathbb{C}$ does not commute with elements of $\mathbb{H}$.

1.4.3. The algebra of polynomials. Let R be a commutative ring. Define the algebra $R[x]$ of polynomials in one variable x with coefficients in R to be the set of sequences

$$f = (f_0, f_1, f_2, \dots), \quad f_i \in R \quad \forall i \geq 0$$

such that all but a finite number of elements f_i are zero. We will write elements $f \in R[x]$ in a more customary form

$$f = f_0 + f_1x + f_2x^2 + \dots = \sum_{k \geq 0} f_k x^k.$$

Given two polynomials $f, g \in R[x]$, we define their sum $f + g \in R[x]$ by

$$f + g = \sum_{k \geq 0} (f_k + g_k) x^k$$

and define their product $fg \in R[x]$ by

$$fg = \sum_{k \geq 0} \left(\sum_{i=0}^k f_i g_{k-i} \right) x^k.$$

These operations define a structure of a ring on $R[x]$.

Remark 1.39. Note that

- (1) The zero element of $R[x]$ is a polynomial $0 = 0 + 0x + 0x^2 + \dots$.
- (2) The unity of $R[x]$ is a polynomial $1 = 1 + 0x + 0x^2 + \dots$.
- (3) The ring $R[x]$ is an algebra over R if we embed $R \subset R[x]$ by the rule $r \mapsto r + 0x + 0x^2 + \dots$.

◇

Definition 1.40. Let $f = f_0 + f_1x + \dots \in R[x]$ be a polynomial. Then

- (1) The element f_0 is called the constant term of f .
- (2) The number $\max \{k \geq 0 \mid f_k \neq 0\}$ is called the degree of f and is denoted by $\deg f$. If $f = 0$ then we define $\deg f = -\infty$.
- (3) If $n = \deg f$, then the element f_n is called the leading coefficient of f . If $f_n = 1$ then f is called a monic polynomial.

Remark 1.41. Let S be an algebra over R and let $f = \sum_{i \geq 0} f_i x^i \in R[x]$ be a polynomial. We define the evaluation of f at $s \in S$ (or the substitution of s into f) to be

$$f(s) = \sum_{i \geq 0} f_i s^i \in S.$$

◇

Theorem 1.42 (Evaluation of polynomials). *Let S be an algebra over a commutative ring R . Given an element $s \in S$, there exists a unique ring homomorphism $\varphi_s : R[x] \rightarrow S$ such that*

$$\varphi(a) = a \quad \forall a \in R, \quad \varphi_s(x) = s.$$

For any polynomial $f \in R[x]$, we have $\varphi_s(f) = f(s)$.

Proof. Let us prove the uniqueness. For any $f \in R[x]$, we have

$$\varphi_s(f) = \varphi_s \left(\sum_{k \geq 0} f_k x^k \right) = \sum_{k \geq 0} \varphi_s(f_k x^k) = \sum_{k \geq 0} \varphi_s(f_k) \varphi_s(x)^k = \sum_{k \geq 0} f_k s^k$$

and this proves that φ_s is uniquely determined. Conversely, if we define φ_s using this rule then $\varphi_s(a) = a \forall a \in R$ and $\varphi_s(x) = s$. Let us show that φ_s is a ring homomorphism. It is clear that it preserves the additive structures. Concerning the product, we have

$$\begin{aligned} \varphi_s(fg) &= \varphi_s \left(\sum_{k \geq 0} \left(\sum_{i=0}^k f_i g_{k-i} \right) x^k \right) = \sum_{k \geq 0} \left(\sum_{i=0}^k f_i g_{k-i} \right) s^k \\ &= \left(\sum_{i \geq 0} f_i s^i \right) \left(\sum_{j \geq 0} g_j s^j \right) = \varphi_s(f) \varphi_s(g). \end{aligned}$$

□

Remark 1.43. This proposition implies, that for any polynomial $f \in R[x]$ and for any element $r \in R$, we can evaluate $f(r) = \varphi_r(f) \in R$. Moreover, for any matrix $A \in M_n(R)$, we can evaluate $f(A) = \varphi_A(f) \in M_n(R)$ (recall that $M_n(R)$ is an algebra over R). ◇

Definition 1.44. Let S be an algebra over R and $f \in R[x]$. An element $s \in S$ is called a root (or a zero) of a polynomial f if $f(s) = 0$.

Remark 1.45. Define an algebra of polynomials in several variables inductively by the rule

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Such polynomials can be written in the form

$$f = \sum_{i_1, \dots, i_n \geq 0} f_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n},$$

where $f_{i_1 \dots i_n} \in R$ and all but a finite number of these elements are zero. ◇

Example 1.46. Consider a matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. Then $A - I = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $(A - I)^2 = 0$. This means that A is a root of a polynomial $p = (x - 1)^2 \in \mathbb{R}[x]$. Consider a ring homomorphism

$$\varphi_A : \mathbb{R}[x] \rightarrow M_2(\mathbb{R}), \quad f \mapsto f(A).$$

We proved that $p(A) = 0$, hence $p \in \ker \varphi_A$. As $\ker \varphi_A$ is an ideal, the entire ideal $(p) = \mathbb{R}[x]p$ generated by $p = (x - 1)^2$ is contained in $\ker \varphi_A$. One can show that actually $\ker \varphi_A = (p)$. ◇

2. INTEGRAL DOMAINS

2.1. Basic definitions.

Remark 2.1. There is the following chain of commutative ring classes

$$\begin{aligned} \text{Fields} \subset \text{Euclidean domains} \subset \text{Principal ideal domains} \\ \subset \text{Unique factorization domains} \subset \text{Integral domains} \subset \text{Commutative rings} \end{aligned}$$

We introduced already commutative rings and fields. Our goal will be to fill the gap. From now on all rings are assumed to be commutative. $\diamond$

Definition 2.2. Let R be a commutative ring.

- (1) R is called an integral domain if $ab = 0$ implies $a = 0$ or $b = 0$ for arbitrary $a, b \in R$.
- (2) An element $a \in R$ is called a zero divisor if there exists nonzero $b \in R$ such that $ab = 0$.
An element that is not a zero divisor is called a non-zero-divisor.
- (3) An element $a \in R$ is called an invertible element (or a unit) if there exists $b \in R$ such that $ab = 1$. The set of all units of R is denoted by $R^\times$.
- (4) Two elements $a, b \in R$ are called associates (we write $a \sim b$) if $a = ub$ for some $u \in R^\times$.

Remark 2.3. A commutative ring R is an integral domain $\iff$ nonzero elements of R are non-zero-divisors. $\diamond$

Example 2.4. The ring $\mathbb{Z}$ is an integral domain. The only invertible elements of $\mathbb{Z}$ are ± 1 . $\diamond$

Example 2.5. Any field is an integral domain. For any field $\mathbb{k}$ the ring $\mathbb{k}[x]$ is an integral domain. $\diamond$

Remark 2.6 (Cancellation). Assume that R is an integral domain and $a \in R$ is nonzero. If $ab = ac$ for some $b, c \in R$ then $b = c$. Indeed, $a(b - c) = 0$ and as a is not a zero divisor, we conclude that $b - c = 0$. Therefore $b = c$. $\diamond$

Lemma 2.7. Let R be an integral domain. Then two elements $a, b \in R$ are associates if and only if $(a) = (b)$ (if and only if $a \mid b$ and $b \mid a$).

Proof. If $b = ua$ with $u \in R^\times$, then $b \in (a)$ and $(b) \subset (a)$. Similarly, from $a = u^{-1}b$ we conclude $(a) \subset (b)$ and therefore $(a) = (b)$.

Conversely, if $(a) = (b)$ then $b = ua$, $a = vb$ for some $u, v \in R$. Therefore $a = vb = uva \implies a(1 - uv) = 0 \implies a = 0$ or $uv = 1$. If $a = 0$, then $b = ua = 0 = a$. If $uv = 1$ then u is invertible and a, b are associates. $\square$

2.2. UFD.

Definition 2.8. Let R be an integral domain.

- (1) An element $p \in R$ is called irreducible if $p \neq 0$, $p \notin R^\times$ and it can be written as a product only in a trivial way, that is, if $p = ab$ then $a \in R^\times$ or $b \in R^\times$.
- (2) An element $p \in R$ is called prime if $p \neq 0$, $p \notin R^\times$ and if $p \mid ab$ implies $p \mid a$ or $p \mid b$ for all $a, b \in R$.

Example 2.9. A positive $n \in \mathbb{Z}$ is irreducible if and only if it is prime (in the usual sense). $\diamond$

Remark 2.10. Any prime element is irreducible. Indeed, if $p = ab$ then $p \mid ab$, hence $p \mid a$ or $p \mid b$. Without loss of generality $p \mid a$, hence $a = cp$ for some $c \in R$. This implies $p = ba = bcp$ and $bc = 1$, hence $b \in R^\times$. We will see later that there are rings with irreducible elements that are not prime. $\diamond$

Definition 2.11. An integral domain R is called a unique factorization domain if

- (1) Any $a \in R \setminus \{0\}$ can be written as a product of a unit and irreducible elements, that is,

$$a = up_1, \dots, p_k$$

where $u \in R^\times$ and p_i are irreducible.

- (2) This representation is unique up to units and a permutation of factors. That is, if

$$a = vq_1, \dots, q_l$$

is another decomposition into a product of a unit and irreducibles, then $l = k$ and there exist a permutation $\sigma \in S_k$ and elements $u_i \in R^\times$ such that $q_i = u_i p_{\sigma i}$ for all i .

An integral domain satisfying just the first axiom is called a factorization domain.

Example 2.12.

- (1) The ring $\mathbb{Z}$ is a UFD.
- (2) Any field is a UFD for trivial reasons (all nonzero elements are invertible).
- (3) If K is a field, then $K[x]$ is a UFD as we will see later.

$\diamond$

Example 2.13. Let us consider a ring which is not a unique factorization domain. Let

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

We claim that the element 6 has two different factorizations into irreducible factors

$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i).$$

For any element $z = a + b\sqrt{5}i \in R$ we have

$$|z|^2 = a^2 + 5b^2 \in \mathbb{Z}$$

and if $z = z_1 z_2$ then $|z|^2 = |z_1|^2 |z_2|^2$. Therefore if $z \in R$ is invertible, then $|z|^2 \in \mathbb{Z}$ is invertible. This implies $|z| = 1$ and $z = \pm 1$. Assuming that we can write some of the elements $z = 2, 3, 1 \pm \sqrt{-5}$ as $z = z_1 z_2$ with $z_1, z_2 \notin R^\times$, we obtain that $|z|^2 = 4, 9, 6$ is equal to $|z_1|^2 \cdot |z_2|^2$ and therefore $|z_i|^2$ are equal to 2 or 3. But there are no such elements in R . This implies that $2, 3, 1 \pm \sqrt{-5}$ are irreducible. They are not associates of each other as $R^\times = \{\pm 1\}$. This implies that the above factorizations are not equivalent.

Equality

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

implies that $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$. But 2 does not divide $1 \pm \sqrt{-5}$. This means that 2 is not prime in the ring $\mathbb{Z}[\sqrt{-5}]$, although we have seen that 2 is irreducible. $\diamond$

Theorem 2.14. Let R be a factorization domain (satisfies just the first axiom of a UFD). Then R is a UFD if and only if every irreducible element of R is prime.

Proof. $\Rightarrow$. Let R be a UFD, $p \in R$ be irreducible and $p \mid ab$, that is, $ab = pc$ for some $a, b, c \in R$. We want to show that $p \mid a$ or $p \mid b$. Let

$$a = \prod a_i, \quad b = \prod b_i, \quad c = \prod c_i$$

be factorizations into irreducible elements. Then the element $ab = pc$ has two factorizations

$$\prod a_i \prod b_i = p \prod c_i.$$

From the uniqueness of factorizations we conclude that p equals (up to a unit) to one of a_i or b_j . This means that p divides a or b .

$\Leftarrow$. Assume that an element a has two decompositions into irreducibles

$$a = \prod_{i=1}^m p_i = \prod_{i=1}^n q_i.$$

By assumption all elements p_i are prime. Let $p = p_m$. Then p should divide one of q_i (we can assume that it is q_n). But q_n is irreducible, therefore $q_n = up$ for some $u \in R^\times$. Dividing both sides by p we obtain $\prod_{i=1}^{m-1} p_i = u \prod_{i=1}^{n-1} q_i$. By induction on m , these factorizations are the same up to the permutation of factors and multiplications by units. $\square$

2.3. PID.

Definition 2.15. Let R be a commutative ring.

- (1) An ideal $I \subset R$ is called principal if it can be generated by one element, that is $\exists a \in R$ such that $I = (a) = Ra$.
- (2) R is called a principal ideal domain if it is an integral domain and any ideal of R is a principal ideal.

Example 2.16. We have seen that any ideal in $\mathbb{Z}$ has a form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. This implies that $\mathbb{Z}$ is a principal ideal domain. $\diamond$

Lemma 2.17. Let R be a principal ideal domain. Then any irreducible element in R is prime.

Proof. Let $p \in R$ be irreducible and let $p \mid ab$. Assume that $p \nmid a$. The ideal (p, a) is a principal ideal, therefore $(p, a) = (d)$ for some $d \in R$. In particular $p \in (d)$ and $p = cd$ for some $c \in R$. As p is irreducible, we have $c \in R^\times$ or $d \in R^\times$. If $c \in R^\times$, then $(p) = (d) \ni a$ and $p \mid a$, a contradiction. If $d \in R^\times$, then $(a, p) = (d) = R$. Therefore $1 = ax + py$ for some $x, y \in R \implies b = abx + bpy \implies p \mid b$. $\square$

Theorem 2.18. Any PID is a UFD.

Proof. We have to show that a PID R is a factorization domain. The fact that R is a UFD will follow then from Theorem 2.14 and the fact that every irreducible element in R is prime according to the previous lemma.

Assume that a can not be represented as a product of irreducible elements (up to a unit). Then a is not a unit and not irreducible. Therefore we can decompose it as $a = a_1 b_1$ with $a_1, b_1 \notin R^\times$. Without loss of generality we can assume that a_1 does not have a factorization into a product. Continuing this argument, we obtain a sequence of elements satisfying $a_i = a_{i+1} b_{i+1}$ and therefore (strict inclusions here)

$$(a) \subset (a_1) \subset (a_2) \subset \dots$$

The union of these ideals is again an ideal. Moreover, it is a principal ideal (c) as R is a PID. We have $c \in (a_n)$ for some $n \geq 1$. Therefore $(a_n) = (c)$. This implies that $(a_n) = (a_{n+1})$, a contradiction. This proves the existence of a decomposition. $\square$

2.4. GCD and LCM. Let R be an integral domain.

Definition 2.19. The greatest common divisor of two elements $a, b \in R$ is an element $d \in R$ (denoted by $\gcd(a, b)$) such that

- (1) $d \mid a, d \mid b$.
- (2) If $c \mid a, c \mid b \implies c \mid d$.

The elements a, b are called coprime if $\gcd(a, b) = 1$.

Remark 2.20. A GCD of two elements does not exist in all rings, but we will see later that it exists in UFD. If d is a GCD of a, b then any its associate (that is, an element of the form ud for some $u \in R^\times$) is also a GCD of a, b . Conversely, if c, d are two GCD of a, b then $d \mid c$ and $c \mid d$. This means that c, d are associates. We denote by $\gcd(a, b)$ any of these associates. $\diamond$

Example 2.21. Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$ and an equation

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3 = 6$$

in R . Consider the elements

$$a = (1 + \sqrt{-5}) \cdot 2, \quad b = 6.$$

Then $d = 1 + \sqrt{-5}$ is a common divisor of a and b and also $c = 2$ is a common divisor of a and b . We also know that they are irreducible. However, neither of them is a greatest common divisor of a, b as $d \nmid c$ and $c \nmid d$. $\diamond$

Definition 2.22. The least common multiple of two elements $a, b \in R$ is an element $m \in R$ (denoted by $\text{lcm}(a, b)$) such that

- (1) $a \mid m, b \mid m$.
- (2) If $a \mid c, b \mid c$ then $m \mid c$.

Remark 2.23. Again we can show that a LCM of two elements a, b is determined only up to a unit. Any of them is denoted by $\text{lcm}(a, b)$. $\diamond$

Lemma 2.24. Let R be a principal ideal domain and $a, b \in R$. Then

- (1) $d = \gcd(a, b)$ if and only if $(a, b) = (d)$.
- (2) $m = \text{lcm}(a, b)$ if and only if $(a) \cap (b) = (m)$.

In particular GCD and LCM exist in principal ideal domains.

Proof. Let us prove just the first statement. Assume that $(d) = (a, b)$. Then $a, b \in (d) \implies d \mid a$ and $d \mid b$. If $c \mid a$ and $c \mid b$ then $a, b \in (c)$ and this implies $(d) = (a, b) \subset (c)$ and therefore $c \mid d$. This means that $d = \gcd(a, b)$. Conversely, if d' is a GCD of a, b then d' and d are associates and therefore $(d') = (d) = (a, b)$. $\square$

Lemma 2.25. Let R be a principal ideal domain. Then $a, b \in R$ are coprime if and only if there exist $x, y \in R$ such that $ax + by = 1$.

Proof. Condition that a, b are coprime means that $\gcd(a, b) = 1$. Condition that there $\exists x, y \in R$: $ax + by = 1$ means that $(a, b) = R = (1)$. Now we apply the previous lemma. $\square$

Theorem 2.26. GCD and LCM exist in unique factorization domains.

Proof. Any two elements a, b can be written in the form

$$a = u \prod_{i=1}^n p_i^{k_i}, \quad b = v \prod_{i=1}^n p_i^{l_i},$$

where $u, v \in R^\times$, $p_1, \dots, p_n$ are distinct prime elements (not associate to each other) and $k_i, l_i \geq 0$. Define

$$d = \prod_{i=1}^n p_i^{s_i}, \quad s_i = \min\{k_i, l_i\}, \quad m = \prod_{i=1}^n p_i^{t_i}, \quad t_i = \max\{k_i, l_i\}.$$

We claim that $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. Let us show this just for d . It is clear that $d \mid a$ and $d \mid b$. Assume that $c \mid a$ and $c \mid b$. Up to a unit, we can write $c = \prod_{i=1}^n p_i^{r_i}$, where $r_i \leq k_i$ and $r_i \leq l_i$. This implies $r_i \leq s_i$ and $c \mid d$. $\square$

2.5. Euclidean domains. Euclidean domains are rings where an analogue of the Euclidean division of integers (that is, division with a remainder) is possible.

Definition 2.27. An integral domain R is called a Euclidean domain if there exists a function

$$\delta : R \setminus \{0\} \rightarrow \mathbb{N} = \{0, 1, 2, \dots\}$$

(called a Euclidean function or a degree function) such that for any $a, b \in R \setminus \{0\}$ there exist elements $q, r \in R$ (quotient and remainder) such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.

Example 2.28. The ring $\mathbb{Z}$ with the degree function $\delta(n) = |n|$ is a Euclidean domain. $\diamond$

Example 2.29. For any field $\mathbb{k}$, the algebra of polynomials $\mathbb{k}[x]$ with the degree function $\delta(f) = \deg(f)$ is a Euclidean domain. This follows from the following result. $\diamond$

Theorem 2.30. Let R be a commutative ring and let $f, g \in R[x]$ with g a monic polynomial of degree d , that is, $g(x) = x^d + g_{d-1}x^{d-1} + \dots + g_0$. Then there exist unique polynomials $q, r \in R[x]$ such that $f = gq + r$ and $\deg r < d$.

Proof. Let us choose a polynomial $q \in R[x]$ such that the polynomial $r := f - gq$ has a minimal possible degree. Assume that $r = r_e x^e + \dots + r_0$ has degree $e \geq d$. Then

$$f - g(q + r_e x^{e-d}) = r - r_e g x^{e-d} = \sum_{i=0}^{e-1} r_i x^i - \sum_{i=0}^{d-1} r_e g_i x^{e-d+i}$$

has degree $< e$, a contradiction.

To prove the uniqueness, assume that $f = gq' + r'$ with $\deg r' < d$. Then $g(q - q') = r - r'$. If $q \neq q'$ then $\deg(g(q - q')) \geq \deg g = d$ and $\deg(r - r') < d$, a contradiction. Therefore $q = q'$, hence also $r = r'$. $\square$

Corollary 2.31. An element $a \in R$ is a root of a polynomial $f \in R[x]$ (that is, $f(a) = 0$) if and only if $(x - a)$ divides f .

Proof. We can divide with a remainder $f = (x - a)q + r$, where $\deg r < \deg(x - a) = 1$. This means that $r \in R$. If a is a root of f then $r = f(a) = 0$. Therefore $(x - a)$ divides f . Conversely, if $(x - a)$ divides f then clearly $f(a) = 0$. $\square$

Remark 2.32. If R is an integral domain, then a polynomial $f \in R[x]$ has at most $\deg f$ roots. Indeed, if $a \in R$ is a root of f , then we can write $f = (x - a)q$ with $\deg q = \deg f - 1$. Any root of f different from a is a root of q . By induction on degree, q has at most $\deg q = \deg f - 1$ roots. Therefore f has at most $\deg f$ roots.

This statement is false if R is not an integral domain. For example, the polynomial $x^2 - 1$ in $\mathbb{Z}_8[x]$ has four roots. $\diamond$

Example 2.33. The ring $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\} \subset \mathbb{C}$ is called the ring of Gaussian integers. It is a Euclidean domain with a degree function $\delta(x + yi) = |x + yi|^2 = x^2 + y^2$. Such degrees are precisely those natural numbers that can be written as a sum of two squares. $\diamond$

Lemma 2.34. The ring $\mathbb{Z}[i]$ of Gaussian integers is Euclidean.

Proof. Let $a, b \in \mathbb{Z}[i] \setminus \{0\}$. Consider the element $ab^{-1} = x + yi \in \mathbb{C}$. There exist $m, n \in \mathbb{Z}$ such that $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. Let $q = m + ni$ and

$$r = a - bq = b(ab^{-1} - q) = b((x - m) + (y - n)i).$$

We have

$$\delta(r) = |r|^2 = |b|^2 \cdot ((x - m)^2 + (y - n)^2) \leq |b|^2 \cdot (1/4 + 1/4) < |b|^2 = \delta(b).$$

$\square$

Theorem 2.35. *A Euclidean domain is a principal ideal domain and therefore also a unique factorization domain.*

Proof. Let R be a Euclidean domain with a degree function $\delta : R \setminus \{0\} \rightarrow \mathbb{N}$ and let $I \subset R$ be a nonzero ideal. Let $b \in I \setminus \{0\}$ have a minimal possible value $\delta(b)$. Then $(b) \subset I$ and we claim that $I = (b)$. If $a \in I \setminus (b)$, then we can write $a = bq + r$ with $r = 0$ or $\delta(r) < \delta(b)$. If $r = 0$, then $a = bq$ and $a \in (b)$, a contradiction. If $r \neq 0$ then $\delta(r) < \delta(b)$ and $r = a - bq \in I$, contradicting to the minimality of $\delta(b)$. This implies that $I = (b)$. $\square$

Example 2.36. This theorem implies in particular, that any polynomial ring $\mathbb{k}[x]$ over a field $\mathbb{k}$ is a principal ideal domain, hence a unique factorization domain. Therefore one has GCD and LCM in this ring. For example, the polynomials $x^2 + 1$, $x + 1$ over $\mathbb{Q}$ have $\gcd = 1$. On the other hand, the same polynomials over $\mathbb{Z}_2$ have $\gcd = x + 1$ (note that $x^2 + 1 = x^2 - 1 = (x - 1)(x + 1)$). $\diamond$

Remark 2.37 (Euclidean algorithm). As we have seen, any Euclidean domain R is a UFD and therefore its elements have the greatest common divisors. There is an algorithm, called the Euclidean algorithm, to find $\gcd(a, b)$ for any $a, b \in R$. This is a straightforward generalization of a similar algorithm for integers. Namely, we apply the following sequence of division with remainders, until we obtain the zero remainder:

$$\begin{array}{ll} a = q_1 b + r_1, & \delta(r_1) < \delta(b), \\ b = q_2 r_1 + r_2, & \delta(r_2) < \delta(r_1), \\ r_1 = q_3 r_2 + r_3, & \delta(r_3) < \delta(r_2), \\ \dots\dots\dots & \\ r_{k-2} = q_k r_{k-1} + r_k, & \delta(r_k) < \delta(r_{k-1}), \\ r_{k-1} = q_{k+1} r_k, & \delta(r_{k+1}) = 0. \end{array}$$

$\diamond$

Then

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{k-1}, r_k) = r_k.$$

This algorithm can also be used in order to find $x, y \in R$ such that $xa + yb = \gcd(a, b) = r_k$. Indeed, first we can write

$$r_1 = a - q_1 b.$$

Then

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 + q_1 q_2)b.$$

Continuing this process, we obtain an expression for r_k as a linear combination of a and b .

2.6. Field of fractions.

Remark 2.38. The ring $\mathbb{Z}$ of integers has non-invertible elements. If we allow to invert nonzero elements then we will end up with a field $\mathbb{Q}$ of rational numbers. Our goal is to formalize this construction for arbitrary integral domains. $\diamond$

Let R be an integral domain and let $S = R \setminus \{0\}$ (it is not a subring, but it is closed with respect to multiplication). Define a binary relation on $R \times S$ by the rule

$$(a, s) \sim (b, t) \iff at = bs.$$

(We think of a pair (a, s) as a fraction a/s). This is an equivalence relation:

- (1) Reflexivity: $(a, s) \sim (a, s)$.
- (2) Symmetry: $(a, s) \sim (b, t) \implies (b, t) \sim (a, s)$.
- (3) Transitivity: $(a, s) \sim (b, t) \wedge (b, t) \sim (c, v) \implies (a, s) \sim (c, v)$. Indeed, we have $at = bs$ and $bv = ct$. This implies $atv = bsv = cts$ and therefore $av = cs$, that is, $(a, s) \sim (c, v)$.

We denote the set of equivalence classes of such pairs by $Q(R)$ and denote the equivalence class of a pair (a, s) by $\frac{a}{s}$. Define addition and multiplication on $Q(R)$ by the rules

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

One can verify that these operations are well-defined and they equip $Q(R)$ with a ring structure. The zero element of $Q(R)$ is $\frac{0}{1}$. The unity of $Q(R)$ is $\frac{1}{1}$.

Theorem 2.39. *Let R be an integral domain. Then the ring $Q(R)$ is a field, called the field of fractions of R . The canonical map $i : R \rightarrow Q(R)$, $r \mapsto \frac{r}{1}$, is an injective ring homomorphism. If $f : R \rightarrow K$ is an injective ring homomorphism to a field K , then there exists a unique ring homomorphism $\bar{f} : Q(R) \rightarrow K$ that makes the following diagram commute ($f = \bar{f}i$)*

$$\begin{array}{ccc} R & \xrightarrow{i} & Q(R) \\ & \searrow f & \swarrow \bar{f} \\ & K & \end{array}$$

Proof. Let $\frac{a}{s} \in Q(R)$ be a nonzero element. Then $\frac{a}{s} \neq \frac{0}{1}$, that is, $a \neq 0$. This implies that $\frac{s}{a} \in Q(R)$. We have $\frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}$ and this means that $\frac{a}{s}$ is invertible. Therefore $Q(R)$ is a field.

The map $i : R \rightarrow Q(R)$ is obviously a ring homomorphism. For example, for $a, b \in R$

$$i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a + b}{1} = i(a + b).$$

To show that it is injective, assume that $a \in \ker i$. Then $\frac{a}{1} = \frac{0}{1}$. Then $a = 0$ and therefore $\ker i = 0$.

Uniqueness of $\bar{f}$. For any $a \in R$ we have $\bar{f}(\frac{a}{1}) = \bar{f}(i(a)) = f(a)$. If $s \in R \setminus \{0\}$ then $\bar{f}(\frac{s}{1})\bar{f}(\frac{1}{s}) = \bar{f}(\frac{1}{1}) = f(1) = 1$ and $\bar{f}(\frac{s}{1}) = f(s)$. Therefore $\bar{f}(\frac{1}{s}) = 1/f(s)$. This implies $\bar{f}(\frac{a}{s}) = \bar{f}(\frac{a}{1})\bar{f}(\frac{1}{s}) = f(a)/f(s)$ and uniqueness follows.

Existence of $\bar{f}$. We define $\bar{f}(\frac{a}{s}) = f(a)/f(s)$. One verifies easily that this map is well defined and is a ring homomorphism. The composition $(\bar{f}i)(a) = \bar{f}(\frac{a}{1}) = f(a)/f(1) = f(a)$. Therefore $f = \bar{f}i$. $\square$

Example 2.40. Consider an algebra of polynomials $\mathbb{k}[x]$ over a field $\mathbb{k}$. The field of quotients $Q(\mathbb{k}[x])$ is denoted by $\mathbb{k}(x)$ and is called the field of rational functions over $\mathbb{k}$. Its elements are fractions $\frac{f(x)}{g(x)}$, where f, g are polynomials over $\mathbb{k}$ and $g \neq 0$. $\diamond$

2.7. Factorization in polynomial rings. We know that if $\mathbb{k}$ is a field then $\mathbb{k}[x]$ is a UFD. This is not enough to show that $\mathbb{k}[x_1, \dots, x_n]$ is a UFD. Our goal will be to show that if R is a UFD then also $R[x]$ is a UFD. This will imply that $R[x_1, \dots, x_n]$ is a UFD.

Let R be a UFD. We know that any two elements $a, b \in R$ have a GCD. Similarly we can define the greatest common divisor of several elements $a_1, \dots, a_n$ which we denote by $\gcd(a_1, \dots, a_n)$.

Definition 2.41. Given a polynomial $f = \sum_{i=0}^n f_i x^i$ in $R[x]$, we define its content to be $d(f) = \gcd(f_0, \dots, f_n)$. We say that f is primitive if $d(f) = 1$.

Lemma 2.42 (Gauss's lemma). *Let R be a UFD and $f, g \in R[x]$. Then*

- (1) *If f, g are primitive then fg is primitive.*
- (2) *$d(fg) = d(f)d(g)$ (up to a unit).*

Proof. 1. Assume that fg is not primitive. Then there exists some prime $p \in R$ such that all coefficients of fg are divisible by p . For any polynomial $h \in R[x]$, we will denote by $\bar{h}$ its image in $R/(p)[x]$. Then $\overline{fg} = 0$ in $(R/pR)[x]$.

The ring R/pR is an integral domain. Indeed, if $a, b \in R$ are such that $[a][b] = 0$ in R/pR , then $ab \in pR \implies p \mid ab \implies p \mid a$ or $p \mid b \implies [a] = 0$ or $[b] = 0$ in R/pR .

This implies that $(R/pR)[x]$ is also an integral domain. From $\bar{f} \cdot \bar{g} = \overline{fg} = 0$ we obtain that $\bar{f} = 0$ or $\bar{g} = 0$. This means that p divides all the coefficients of f or all the coefficients of g , that is, either f or g is not primitive, a contradiction.

2. Indeed, let $a = d(f)$ and $b = d(g)$. Then $f = af^*$ and $g = bg^*$ for primitive $f^*, g^* \in R[x]$. Therefore

$$d(fg) = d(abf^*g^*) = abd(f^*g^*) = ab = d(f)d(g),$$

where $d(f^*g^*) = 1$ as f^*g^* is primitive. □

Corollary 2.43. *Let R be a UFD and $f \in R[x]$ be a non-constant irreducible polynomial. Then f is irreducible in $Q(R)[x]$.*

Proof. Assume that $f = gh$, where $g, h \in Q(R)[x]$ have positive degrees. We can write

$$g = \frac{a}{b}g^*, \quad h = \frac{c}{d}h^*,$$

where $a, b, c, d \in R$ and $g^*, h^* \in R[x]$ are primitive. Then $f = \frac{ac}{bd}g^*h^*$ and

$$bd \cdot d(f) = ac \cdot d(g^*h^*) = ac.$$

This implies that $\frac{ac}{bd} = d(f) \in R$ and

$$f = \frac{a}{b}g^* \cdot \frac{c}{d}h^* = d(f)g^*h^*.$$

This contradicts to the irreducibility of f in $R[x]$. □

Corollary 2.44. *Let $f, g, h \in \mathbb{Q}[x]$ be monic and $f = gh$. If $f \in \mathbb{Z}[x]$, then $g, h \in \mathbb{Z}[x]$.*

Proof. Let $g = \frac{a}{b}g^*, h = \frac{c}{d}h^*$, where $a, b, c, d \in \mathbb{Z}$ and $g^*, h^* \in \mathbb{Z}[x]$ are primitive. Then $f = \frac{ac}{bd}g^*h^*$ and, comparing contents, we get $\frac{ac}{bd} = 1$ (f is monic, hence primitive). Comparing the leading coefficients in $g^* = \frac{b}{a}g$, we obtain $\frac{b}{a} \in \mathbb{Z}$ and similarly $\frac{d}{c} \in \mathbb{Z}$. From $\frac{bd}{ac} = 1$ we conclude $\frac{b}{a} = \frac{d}{c} = 1$ (up to a sign). This implies $g = g^* \in \mathbb{Z}[x]$ and $h = h^* \in \mathbb{Z}[x]$. □

Theorem 2.45. *If R is a UFD then $R[x]$ is a UFD. The irreducible elements of $R[x]$ are*

- (1) *Irreducible elements of R .*
- (2) *Primitive polynomials in $R[x]$ that are irreducible in $Q(R)[x]$.*

Proof. We can embed $R[x]$ into $Q(R)[x]$, where $Q(R)$ is a field of fractions of R . We know that $Q(R)[x]$ is a UFD. Let us show that elements described in the statement of the theorem are irreducible in $R[x]$. All irreducible elements in R are also irreducible in $R[x]$. Also any primitive $p \in R[x]$ that is irreducible in $Q(R)[x]$ is irreducible in $R[x]$: it can not be written as product of two polynomials having positive degree, and if it is equal to cf for $c \in R$ and $f \in R[x]$ then $d(p) = 1 = d(c)d(f) = cd(f) \implies c \in R^\times \implies p$ is irreducible.

Let us show that every polynomial in $R[x]$ can be factorized into a product of irreducibles in $R[x]$. Given $f \in R[x]$, we can factorize it as a product $f = \prod q_i$ of irreducible polynomials in $Q(R)[x]$. We can write $q_i = c_i p_i$, where $c_i \in Q(R)$ and $p_i \in R[x]$ is a primitive polynomial irreducible in $Q(R)[x]$. Then

$$f = c \prod p_i,$$

where $c = \prod c_i \in Q(R)$. The product $\prod p_i$ is a primitive polynomial in $R[x]$ by the Gauss lemma. If $c = \frac{a}{b}$ then we can write $bf = a \prod p_i$ and comparing the GCD of coefficients on both sides we obtain $b \mid a$, that is $c = \frac{a}{b} \in R$. Now we decompose c into a product of irreducible elements. We have seen that polynomials p_i are irreducible in $R[x]$. This proves the existence of a factorization into irreducibles. This shows also that every irreducible element in $R[x]$ is of the form described in the statement of the theorem.

To show the uniqueness, we have to prove that any irreducible polynomial $p \in R[x]$ is prime. This is clear if $p \in R$. If $\deg p > 0$ then p is a primitive polynomial, irreducible in $Q(R)[x]$. Assume that $p \mid fg$ in $R[x]$. As p is irreducible in $Q(R)[x]$, it is also prime in $Q(R)[x]$. Therefore $p \mid f$ or $p \mid g$ in $Q(R)[x]$. Without loss of generality $p \mid f$ in $Q(R)[x]$. Then there exist $a, b \in R \setminus 0$ and primitive $h \in R[x]$ such that

$$f = \frac{a}{b} hp.$$

Then $bf = ahp$ and $d(bf) = bd(f) = ad(hp) = a$ (as h and p are primitive). This means that $\frac{a}{b} = d(f) \in R$, $\frac{a}{b}h \in R[x]$, and $p \mid f$ in $R[x]$. Therefore p is prime in $R[x]$ and this finishes the proof of the uniqueness of factorizations. $\square$

Theorem 2.46 (Eisenstein's criterion). *Let $f = \sum_{i=0}^n f_n x^n \in \mathbb{Z}[x]$ be a degree n polynomial and p be a prime number such that*

- (1) $p \mid f_0, \dots, f_{n-1}$,
- (2) $p \nmid f_n$,
- (3) $p^2 \nmid f_0$.

Then f is irreducible in $\mathbb{Q}[x]$.

Proof. We can assume that f is primitive (divide f by its content, if necessary). We will show that f is irreducible in $\mathbb{Z}[x]$ (by the previous theorem this will imply that f is also irreducible in $\mathbb{Q}[x]$). Assuming the converse, we can write $f = gh$, for some non-constant $g, h \in \mathbb{Z}[x]$. Then modulo p , we obtain $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{Z}_p[x]$. By our assumption $\bar{f}_i = 0$ for $0 \leq i < n$ and therefore $\bar{f} = \bar{f}_n x^n$, where $\bar{f}_n \neq 0$ in $\mathbb{Z}_p$. This implies $\bar{g} = \bar{b}x^k$, $\bar{h} = \bar{c}x^l$, where $k = \deg g > 0$, $l = \deg h > 0$ and $b, c \in \mathbb{Z}_p$ are nonzero. This implies that the constant terms of g, h are divisible by p and therefore f_0 is divisible by p^2 . A contradiction. $\square$

2.8. Cyclotomic polynomials.

Definition 2.47.

- (1) An element $\xi \in \mathbb{C}$ is called a root of unity if $\xi^n = 1$ for some $n \geq 1$. In this case $\xi = e^{2\pi i k/n}$ for some $0 \leq k < n$.
- (2) Given $n \geq 1$, an element $\xi \in \mathbb{C}$ is called an n -th root of unity if $\xi^n = 1$.
- (3) For any root of unity ξ , define $\text{ord } \xi = \min \{n \geq 1 \mid \xi^n = 1\}$.
- (4) An element ξ is called a primitive n -th root of unity if $\xi^n = 1$ and $\xi^k \neq 1$ for $1 \leq k < n$. Equivalently, $\text{ord } \xi = n$.

Remark 2.48. An element $\xi = e^{2\pi i k/n}$ is an n -th primitive root of unity if and only if $\gcd(k, n) = 1$. Indeed, if $d = \gcd(k, n) > 1$, then $\xi^{n/d} = e^{2\pi i k/d} = 1$ as $k/d \in \mathbb{Z}$. This implies that $\text{ord } \xi < n$. Conversely, if $\gcd(k, n) = 1$ and $\xi^m = 1$ for some $1 \leq m < n$, then $n \mid km \implies n \mid m$, a contradiction. $\diamond$

Remark 2.49. Let ξ be a d -th primitive root of unity. Then $\xi^n = 1$ if and only if $d \mid n$. Indeed, $\xi = e^{2\pi i k/d}$ with $\gcd(k, d) = 1$. Therefore $1 = \xi^n = e^{2\pi i kn/d} \implies d \mid kn \implies d \mid n$. Every n -th root of unity is a primitive root for a unique $d \mid n$. $\diamond$

Let

$$\Phi_d(x) = \prod_{\text{ord } \xi = d} (x - \xi).$$

By the previous discussion

$$x^n - 1 = \prod_{\xi^n = 1} (x - \xi) = \prod_{d \mid n} \prod_{\text{ord } \xi = d} (x - \xi) = \prod_{d \mid n} \Phi_d(x).$$

We obtain by induction (and Gauss lemma) that $\Phi_d(x) \in \mathbb{Z}[x]$. This polynomial is called a d -th cyclotomic polynomial.

Example 2.50. We have $\Phi_1(x) = x - 1$. For any prime p , we have $d \mid p$ if and only if $d = 1$ or $d = p$. This implies

$$x^p - 1 = (x - 1)\Phi_p(x),$$

hence

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1.$$

We have

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x),$$

hence $\Phi_4(x) = x^2 + 1$.

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x),$$

hence

$$\Phi_6(x) = \frac{(x^3 - 1)(x^3 + 1)}{(x^3 - 1)\Phi_2(x)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1.$$

$\diamond$

Theorem 2.51 (Kronecker). *The polynomial $\Phi_d(x)$ is irreducible for every $d \geq 1$.*

Let us prove first a simpler version.

Lemma 2.52 (Gauss). *For every prime p , the polynomial*

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

is irreducible.

Proof (Eisenstein). Applying the substitution $x = y + 1$, we obtain

$$\Phi_p(y + 1) = \frac{(y + 1)^p - 1}{y + 1 - 1} = \frac{(y + 1)^p - 1}{y}.$$

The coefficient of y^{p-1} is one. The coefficient of y^{k-1} is $\binom{p}{k}$ for $1 \leq k < p$ and is divisible by p . The coefficient of y^0 is $\binom{p}{1} = p$ is not divisible by p^2 . By Eisenstein criterium our polynomial is irreducible. $\square$

Proof of Theorem 2.51 (Dedekind). Let $f(x)$ be in an irreducible factor of $\Phi_n(x)$. It has integer coefficients by Gauss's lemma. We will prove that if ξ is a root of f and p is prime, coprime to n , then $f(\xi^p) = 0$. This implies by induction that if $(m, n) = 1$, then $f(\xi^m) = 0$. As ξ is a root of f , it is a root of Φ_n and is a primitive n -th root of 1. If $f(\xi^m) = 0$ for all $(m, n) = 1$, then all primitive n -th roots of 1 are roots of f , hence $\Phi_n = f$ and Φ_n is irreducible.

For any two polynomials $f, g \in \mathbb{Z}[x]$, we have

$$(f + g)^p = \sum_{i=0}^p \binom{p}{i} f^i g^{p-i} \equiv f^p + g^p \pmod{p}.$$

Applying this to the sum of monomials $f = \sum_{i=0}^d f_i x^i \in \mathbb{Z}[x]$, we obtain

$$f(x)^p \equiv \sum_{i=0}^d f_i^p x^{ip} \equiv \sum_{i=0}^d f_i x^{ip} = f(x^p) \pmod{p},$$

where we used $a^p \equiv a \pmod{p}$ for $a \in \mathbb{Z}$ (Fermat's little theorem).

Let g be an irreducible polynomial such that $g(\xi^p) = 0$. If $f = g$, then we are done, hence we assume that $f \neq g$. As ξ is a root of $g(x^p)$, we obtain that f divides $g(x^p)$. Therefore, modulo p , $\bar{f}(x)$ divides $\bar{g}(x^p) = \bar{g}(x)^p$. Hence $\bar{f}(x), \bar{g}(x)$ have a non-trivial common factor $\bar{h}(x)$. As $f(\xi) = 0$ and $g(\xi^p) = 0$, both polynomials divide $x^n - 1$, hence also fg divides $x^n - 1$. This implies that $\bar{h}^2$ divides $x^n - 1$ in $\mathbb{F}_p[x]$. But $x^n - 1 \in \mathbb{F}_p[x]$ does not have multiple factors (the derivative nx^{n-1} is non-zero and coprime to $x^n - 1$). A contradiction. $\square$

3. FIELDS

3.1. Basic definitions. Recall that a field is a commutative ring such that every its nonzero element is invertible. We know the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Also we know that for any prime integer p , the quotient ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field. The next lemma gives an important source of new fields.

Lemma 3.1. *Let K be a field and $p \in K[x]$ be irreducible. Then $K[x]/(p)$ is a field.*

Proof. Let $f \in K[x]$ be such that $[f] \neq 0$ in $K[x]/(p)$. If $d = \gcd(f, p)$, then $d \mid p$, hence $d = p$ or $d = 1$ (up to a unit). If $d = p$ then $p \mid f \implies f \in (p) \implies [f] = 0$, a contradiction. If $d = 1$, then there exist $u, v \in K[x]$ such that $fu + pv = 1$. This implies that $[f][u] = 1$ in $K[x]/(p)$. Therefore $[f]$ is invertible and $K[x]/(p)$ is a field. $\square$

Definition 3.2. Let L be a field. A subring $K \subset L$ is called a subfield if K is a field (when equipped with an induced ring structure). The field L is called a field extension of K . We write L/K in this case.

Lemma 3.3. *Let L be a field. An intersection of a collection of subfields of L is a subfield.*

Proof. Let $(K_i)_{i \in I}$ be a collection of subfield of L and let $K = \bigcap_{i \in I} K_i$. It is clear that $0, 1 \in K$. For any $a, b \in K$ we have $a, b \in K_i \forall i \in I$. Therefore $a + b, ab \in K_i \forall i \in I$. This implies $a + b, ab \in K$. Therefore $K \subset L$ is a subring. Finally, if $a \in K$ is nonzero, then $a^{-1} \in K_i \forall i \in I$. Therefore $a^{-1} \in K$. This means that $K \subset L$ is a subfield. $\square$

Remark 3.4. Given a field K and a subset $S \subset K$, the intersection of all subfields of K that contain S is a subfield called a subfield generated by S . It is the minimal subfield that contains S .

The subfield of K generated by $\emptyset$ (or by $\{0, 1\}$) is called the prime subfield of K . It is the smallest subfield contained in K . $\diamond$

Definition 3.5. Let K be a field. We define its characteristic $\text{char } K$ to be the minimal integer $p \geq 2$ such that

$$p \cdot 1 := \underbrace{1 + \cdots + 1}_p = 0$$

if such p exists and zero otherwise.

Theorem 3.6. *The characteristic of a field K is either zero or a prime number. The prime subfield of K is*

- (1) $\mathbb{Q}$ if $\text{char } K = 0$.
- (2) $\mathbb{F}_p$ if $p = \text{char } K$ is prime.

Proof. Consider a map $f : \mathbb{Z} \rightarrow K$ defined for $n \geq 0$ by

$$f(n) = n \cdot 1 := \underbrace{1 + \cdots + 1}_n$$

and $f(-n) = -f(n)$. This is a ring homomorphism. Indeed, for any $m, n \geq 0$, we have

$$\begin{aligned} f(m+n) &= \underbrace{1 + \cdots + 1}_{m+n} = \underbrace{(1 + \cdots + 1)}_m + \underbrace{(1 + \cdots + 1)}_n = f(m) + f(n), \\ f(mn) &= \underbrace{1 + \cdots + 1}_{mn} = \underbrace{(1 + \cdots + 1)}_m \cdot \underbrace{(1 + \cdots + 1)}_n = f(m) \cdot f(n) \end{aligned}$$

and similarly for any $m, n \in \mathbb{Z}$. Ideal $\ker f \subset \mathbb{Z}$ can be written as $\ker f = (p)$ for some $p \geq 0$.

If $p = 0$ then f is injective and therefore $n \cdot 1 \neq 0$ for any $n > 0$. This means that $\text{char } K = 0$. Injective map $f : \mathbb{Z} \rightarrow K$ can be extended to $f : \mathbb{Q} \rightarrow K$. We obtain a subfield $\mathbb{Q} \subset K$ generated by $0, 1$. This implies that $\mathbb{Q}$ is a prime subfield of K .

If $p > 0$ then p is the minimal positive integer such that $p \cdot 1 = 0$ in K . Therefore $\text{char } K = p$. Moreover, there is an injective ring homomorphism $\mathbb{Z}/(p) = \mathbb{Z}/\ker f \rightarrow K$. Therefore $\mathbb{Z}/(p)$ is an integral domain. If p is not prime, then there exist $1 < a, b < p$ such that $ab = p$. Then the corresponding congruence classes $\bar{a}, \bar{b} \in \mathbb{Z}/(p)$ are nonzero and $\bar{a}\bar{b} = 0$. This contradicts to the fact that $\mathbb{Z}/(p)$ is an integral domain. We conclude that p is prime and therefore $\mathbb{Z}/(p)$ is a field. It is a subfield of K generated by $0, 1$. Therefore it is a prime subfield of K . $\square$

3.2. Field extensions.

Definition 3.7. Let L/K be a field extension and $a_1, \dots, a_n \in L$. We denote by $K(a_1, \dots, a_n) \subset L$ the subfield generated by K and $a_1, \dots, a_n$ and denote by $K[a_1, \dots, a_n] \subset L$ the subring generated by K and $a_1, \dots, a_n$:

$$\left\{ \sum b_{i_1, \dots, i_n} a_1^{i_1} \dots a_n^{i_n} \mid b_{i_1, \dots, i_n} \in K \right\}.$$

Extension L/K is called simple if there exists an element $a \in L$ such that $L = K(a)$.

Example 3.8.

- (1) Consider the field extension $\mathbb{C}/\mathbb{R}$. Then $\mathbb{R}(i) = \mathbb{R}[i] = \mathbb{C}$.
- (2) Let K be a field and $L = K(x)$ be the field of rational functions over K . Then the ring generated by K and x is the ring of polynomials $K[x]$. The field generated by K and x is $K(x) = L$.
- (3) Let us show that $\mathbb{Q}[\sqrt{2}]$ is a field and therefore $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. Any element of $\mathbb{Q}[\sqrt{2}]$ is of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Its inverse is

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} = \frac{a}{a^2 + 2b^2} - \frac{b}{a^2 + 2b^2} \sqrt{2} \in \mathbb{Q}[2].$$

Therefore all nonzero elements of $\mathbb{Q}[\sqrt{2}]$ are invertible in $\mathbb{Q}[\sqrt{2}]$ and it is a field. ◇

Definition 3.9. Let L/K be a field extension.

- (1) L can be considered in a natural way as a vector space over K : it is an abelian group and the scalar multiplication $K \times L \rightarrow L$ can be defined using multiplication in L . Define the degree of the field extension

$$[L : K] = \dim_K L \in \mathbb{N} \cup \{\infty\}.$$

- (2) L/K is called a finite field extension if $[L : K] < \infty$.

Example 3.10. We have $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, $K(x) : K = \infty$, $\mathbb{R} : \mathbb{Q} = \infty$. ◇

Remark 3.11. Let K be a finite field and let $p = \text{char } K$. We know that $\mathbb{F}_p \subset K$. Let $n = [K : \mathbb{F}_p]$ and $(e_1, \dots, e_n)$ be a basis of K over $\mathbb{F}_p$. Then every element in K can be uniquely written in the form

$$b_1 e_1 + \dots + b_n e_n$$

for some $b_1, \dots, b_n \in \mathbb{F}_p$. Therefore the number of elements of K equals p^n . This means that the number of elements of a finite field is always a power of a prime number. One can show that for any $n \geq 1$ there exists a unique (up to an isomorphism) field having p^n elements. It is denoted by $\mathbb{F}_{p^n}$. ◇

Definition 3.12. Let L/K be a field extension. An element $a \in L$ is called algebraic over K if there exists a nonzero polynomial $f \in K[x]$ such that $f(a) = 0$. Otherwise a is called transcendental.

Example 3.13.

- (1) The element $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$. It is a root of the polynomial $x^2 + 1 \in \mathbb{R}[x]$.
- (2) The element $\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ is algebraic over $\mathbb{Q}$. It is a root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$.
- (3) The element $x \in K(x)$ is transcendental over K .
- (4) The element $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (Lindemann, 1882). ◇

Theorem 3.14. Let L/K be a field extension and $a \in L$ be algebraic over K . Then

- (1) Among all monic polynomials in $K[x]$ that have root a there exists a unique polynomial p having minimal degree. It is called the minimal polynomial of a over K .
- (2) The minimal polynomial $p \in K[x]$ of a is irreducible. If a is a root of $f \in K[x]$, then $p \mid f$.
- (3) There is an isomorphism of fields

$$K[x]/(p) \rightarrow K[a] = K(a), \quad f \mapsto f(a).$$

(4) We have $[K(a) : K] = \deg p$. If $d = \deg p$, then $(1, a, \dots, a^{d-1})$ is a basis of $K(a)$ over K .

Proof. 1. Consider the ring homomorphism $\varphi_a : K[x] \rightarrow L$ given by $f \mapsto f(a)$. As a is algebraic, the kernel $\ker \varphi_a \subset K[x]$ is a non-trivial principal ideal. Let $p \in K[x]$ be the monic polynomial such that $\ker \varphi_a = (p)$. If $f \in K[x]$ is another monic polynomial that has root a , then $f \in (p)$ and $p \mid f$. This implies that $\deg p \leq \deg f$ and if $\deg p = \deg f$ then $p = f$.

2. We have $K[x]/(p) \subset L$ and therefore $K[x]/(p)$ is an integral domain. This implies that p is irreducible. Indeed, if $p = fg$ then $\overline{f}\overline{g} = 0$ in $K[x]/(p) \implies \overline{f} = 0$ or $\overline{g} = 0 \implies p \mid f$ or $p \mid g$ and this means that $p = f$ or $p = g$ up to a unit. We have seen already that if $f \in K[x]$ has root a then $p \mid f$.

3. The kernel of the map $\varphi_a : K[x] \rightarrow L$ is (p) and its image is $K[a]$. This implies that $K[x]/(p) \simeq K[a]$. We know that $K[x]/(p)$ is a field as p is irreducible. Therefore $K[a]$ is a field and $K(a) = K[a]$.

4. The basis of $K[x]/(p)$ is given by $(1, x, \dots, x^{d-1})$. Therefore the basis of $K[a] = K(a)$ is given by $(1, a, \dots, a^{d-1})$. $\square$

Lemma 3.15. *Let L/K be a finite field extension. Then any element $a \in L$ is algebraic over K .*

Proof. Let $n = [L : K] = \dim_K L$. Then the $n + 1$ elements $1, a, \dots, a^n$ are linearly dependent over K . Therefore there exist elements $f_0, \dots, f_n \in K$ not all of which are zero such that

$$f_0 + f_1 a + \dots + f_n a^n = 0.$$

Let $f = \sum_{i=0}^n f_i x^i \in K[x]$. Then $f \neq 0$ and $f(a) = 0$. $\square$

Example 3.16. This lemma implies that any complex number $a \in \mathbb{C}$ is algebraic over $\mathbb{R}$. Moreover, the elements $1, a, a^2$ are linearly dependent over $\mathbb{R}$, hence there exists a nonzero polynomial

$$f = f_2 x^2 + f_1 x + f_0 \in \mathbb{R}[x]$$

such that $f(a) = 0$. This means that every complex number a is a root of a quadratic polynomial with real coefficients. $\diamond$

Lemma 3.17. *Let L/K be a field extension and $a \in L$ be transcendental. Then $K(a) \simeq K(x)$.*

Proof. Consider a ring homomorphism $\varphi : K[x] \rightarrow L$, $f \mapsto f(a)$. This map is injective as a is otherwise algebraic. All nonzero elements in $K[x]$ are mapped to the invertible elements in L , therefore we can extend φ to a ring homomorphism $K(x) = Q(K[x]) \rightarrow L$. This map is injective and its image is a field generated by K and a , that is, $K(a)$. Therefore $K(x) \simeq K(a)$. $\square$

Theorem 3.18. *Consider finite field extensions $K \subset L \subset M$. Then*

$$[M : K] = [M : L] \cdot [L : K].$$

Proof. Let $r = [L : K]$, $s = [M : L]$, let $l_1, \dots, l_r$ be a basis of L/K and let $m_1, \dots, m_s$ be a basis of M/L . We claim that the products $l_i m_j$ form a basis of M/K . Given $x \in M$ we can write

$$x = \sum_{j=1}^s y_j m_j, \quad y_j \in L$$

and we can write

$$y_j = \sum x_{ij} l_i, \quad x_{ij} \in K.$$

Therefore

$$x = \sum y_j m_j = \sum_{i,j} x_{ij} l_i m_j$$

and this means that $l_i m_j$ generate M/K . To prove that they are linearly independent assume that we have elements $x_{ij} \in K$ such that $\sum_{i,j} x_{ij} l_i m_j = 0$. As $m_1, \dots, m_s$ are linearly independent over L , we conclude that $\sum_{i,j} x_{ij} l_i = 0$ for every j . As l_i are linearly independent over K , we conclude that $x_{ij} = 0$ for all i, j . This implies that

$$\{l_i m_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a basis of M/K and therefore $[M : K] = rs$. $\square$

3.3. Splitting fields, Finite fields, Algebraically closed fields.

Definition 3.19. A field K is called algebraically closed if every non-constant polynomial in $K[x]$ has at least one root over K . Equivalently, any polynomial in $K[x]$ splits over K , that is, it is a product of linear polynomials.

Theorem 3.20 (Fundamental Theorem of Algebra). *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

Remark 3.21. If K is an algebraically closed field and L/K is a finite field extension then $L = K$. Indeed, we know that every $a \in L$ is algebraic over K . Let $p \in K[x]$ be the minimal polynomial of a . Then p is a product of linear polynomials with coefficients in K , hence $a \in K$. We conclude that $L = K$. $\diamond$

Definition 3.22. Let K be a field.

- (1) We say that a nonconstant polynomial $f \in K[x]$ splits over a field extension L/K if there exist $a \in K$ and $c_1, \dots, c_n \in L$ such that

$$f(x) = a(x - c_1) \dots (x - c_n).$$

- (2) A field extension L/K is called a splitting field of $f \in K[x]$ if f splits over L and $L = K(c_1, \dots, c_n)$, where $c_1, \dots, c_n \in L$ are the roots of f .

Theorem 3.23. *Let K be a field and $f \in K[x]$ be a polynomial of degree $n \geq 1$. Then there exists a (unique up to an isomorphism) splitting field L of f over K . Moreover, $[L : K] \leq n!$.*

Proof. We will only prove existence. Let $p = \sum_{i=0}^d p_i x^i$ be an irreducible divisor of f . Let $L' = K[x]/(p)$, $I = (p)$, and $a = x + I \in L'$. Then

$$p(a) = p_0 + p_1(x + I) + \dots + p_d(x + I)^d = (p_0 + p_1x + \dots + p_dx^d) + I = p(x) + I = I.$$

Therefore $p(a) = 0$ in L' . This implies that $f(a) = 0$ and we can write

$$f(x) = (x - a)g(x)$$

for some polynomial $g \in L'[x]$ of degree $n - 1$. By induction on n , there exists a splitting field L of g over L' of degree $[L : L'] \leq (n - 1)!$. This is also a splitting field of f over K . Note that

$$[L' : K] = \deg p \leq \deg f = n.$$

Therefore

$$[L : K] = [L : L'] \cdot [L' : K] \leq (n - 1)! \cdot n = n!.$$

$\square$

Theorem 3.24. *Every finite field has p^n elements, for some prime p and integer $n \geq 1$. For every prime p and integer $n \geq 1$, there exists a (unique up to an isomorphism) field with p^n elements. It is denoted by $\mathbb{F}_{p^n}$.*

Proof. Let K be a finite field of characteristic p . Then p is prime and K contains a prime subfield $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. If $n = [K : \mathbb{F}_p]$, then $\#K = p^n$.

Let K be a field with $q = p^n$ elements. Then the set $K^\times = K \setminus \{0\}$ of invertible elements is a group with respect to multiplication. It has $q - 1$ elements, hence $a^{q-1} = 1$ for all $a \in K^\times$. This implies that $a^q = a$ for all $a \in K$. Therefore all elements of K are roots of the polynomial $x^q - x$, hence $x^q - x = \prod_{a \in K} (x - a)$. This implies that K is a splitting field of $x^q - x$ over $\mathbb{F}_p$, hence is unique.

Let us prove existence of a field with $q = p^n$ elements. Let K be the splitting field of $x^q - x$ over $\mathbb{F}_p$. We claim that K is the set of q distinct roots of $x^q - x$, hence contains q elements. Let $L \subset K$ be the set of all roots of $f(x) = x^q - x$. Then L is a subfield of K :

- (1) $0, 1 \in L$ as $0^q = 0$ and $1^q = 1$.
- (2) If $a, b \in L$, then $a^q = a, b^q = b \implies (ab)^q = a^q b^q = ab \implies ab \in L$.
- (3) If $0 \neq a \in L$, then $a^q = a \implies (a^{-1})^q = a^{-q} = a^{-1} \implies a^{-1} \in L$.

- (4) Let $a, b \in L$. We have $(a + b)^q = a^q + b^q$ (binomial coefficients $\binom{q}{k}$ are divisible by p if $0 < k < q$). This implies $(a + b)^q = a^q + b^q = a + b \implies a + b \in L$.

As L is a field containing all roots of $x^q - x$ (and nothing else), it is the splitting field of this polynomial, hence $K = L$. We only need to show that $f(x) = x^q - x$ does not have multiple roots. Indeed, assume that $f(x) = (x - a)^2 \cdot g(x)$ for some $g \in K[x]$ and $a \in K$. We can formally define a derivative of polynomials. Then $f'(x) = 2(x - a)g(x) + (x - a)^2 g'(x)$ and $f'(a) = 0$. But $f'(x) = qx^{q-1} - 1 = -1$ as $q = p^n = 0$ in K . A contradiction. We conclude that all roots of $x^q - x$ are distinct, hence $\#K = \#L = q$. $\square$

Lemma 3.25. *Let K be a field. The following conditions are equivalent.*

- (1) *Any non-constant polynomial in $K[x]$ has at least one root over K .*
- (2) *Any polynomial in $K[x]$ splits over K , that is, it is a product of linear polynomials.*
- (3) *Any irreducible polynomial over K is linear.*
- (4) *Any algebraic element over K is contained in K .*
- (5) *If L/K is a finite field extension, then $L = K$.*

A field K satisfying these properties is called an algebraically closed field.

Proof. $1 \implies 2$. Let $f \in K[x]$ have degree n and $c \in K$ be its root. Then $f(x) = (x - c)g(x)$ for some polynomial $g \in K[x]$ of degree $n - 1$. By induction on n , we can write $g(x) = a(x - c_1) \dots (x - c_{n-1})$. Therefore

$$f(x) = a(x - c)(x - c_1) \dots (x - c_{n-1}).$$

$2 \implies 3$. Let $p \in K[x]$ be an irreducible polynomial. By assumption it is a product of linear polynomials. Therefore p is linear.

$3 \implies 4$. Let L/K be a field extension and $a \in L$ be algebraic over K . Then the minimal polynomial of a over K is irreducible. By assumption it is linear. This implies that $a \in K$.

$4 \implies 5$. Let L/K be a finite field extension. Then any element $a \in L$ is algebraic. By assumption $a \in K$. This implies that $L = K$.

$5 \implies 1$. We can assume that $f \in K[x]$ is irreducible. Then the field $K[x]/(f)$ is finite over K . By assumption $L = K[x]/(f) = K$ and therefore

$$\deg f = [L : K] = 1,$$

that is, f is linear. $\square$

Theorem 3.26 (Fundamental Theorem of Algebra). *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

Proof. Let

$$f(z) = z^n + f_{n-1}z^{n-1} + \dots + f_0$$

be a non-constant polynomial over $\mathbb{C}$ that does not have roots over $\mathbb{C}$. There exist $r > 0$ such that for all $z \in \mathbb{C}$ with $|z| > r$, we have

$$|f(z)| > |f(0)|.$$

Let $D_r = \{z \in \mathbb{C} \mid |z| \leq r\}$. Then

$$\inf_{z \in \mathbb{C}} |f(z)| = \inf_{z \in D_r} |f(z)| = |f(z_0)| > 0$$

for some $z_0 \in D_r$ (as D_r is compact). If $f(z) \neq 0$ for all $z \in \mathbb{C}$, then $1/f(z)$ is holomorphic and bounded over $\mathbb{C}$:

$$|f(z)| \geq |f(z_0)| \implies \frac{1}{|f(z)|} \leq \frac{1}{|f(z_0)|} < +\infty.$$

By the Liouville's Theorem such function should be constant. Therefore $f(z)$ is constant. A contradiction. $\square$

3.4. Constructions with compass and straightedge. In this section we discuss constructions on the plane $\mathbb{R}^2$ using a compass and a straightedge. We will usually identify $\mathbb{R}^2$ with $\mathbb{C}$. Our goal is to understand the set $K \subset \mathbb{C}$ of points that can be constructed using a compass and a straightedge starting from the points 0 and 1. The following problems were studied already in Ancient Greece:

- (1) Duplication of a cube (construct $a > 0$ such that $a^3 = 2 \cdot 1^3 = 2$).
- (2) Trisection of an arbitrary angle (given an angle $\varphi \in [0, 2\pi]$ construct an angle $\varphi/3$, that is, given a point $e^{i\varphi} \in \mathbb{C}$, construct a point $e^{i\varphi/3}$).
- (3) Quadrature of a circle (construct $a > 0$ such that a square with sides of length a has an area of a radius one circle, that is, $a^2 = \pi$)

We will show that these constructions are not possible with a compass and a straightedge.

Definition 3.27. Let $K \subset \mathbb{C}$ be a subset.

- (1) A line through two distinct points in K is called an elementary K -constructible line.
- (2) A circle that has some point in K and a center in K is called an elementary K -constructible circle.
- (3) All elementary K -constructible lines and circles are called elementary K -constructible objects.
- (4) A point in the intersection of two different elementary K -constructible objects is called an elementary K -constructible point.

Lemma 3.28. Let L/K be a field extension and $\text{char } K \neq 2$. Then the following conditions are equivalent

- (1) $[L : K] = 2$.
- (2) $L = K[a]$ for some $a \in L \setminus K$ such that $a^2 \in K$.

Such fields extension is called quadratic.

Proof. 1 $\implies$ 2. Let $b \in L \setminus K$. Its minimal polynomial has degree 2 and can be written in the form

$$p(x) = x^2 + cx + d = (x + c/2)^2 + (d - c^2/4), \quad c, d \in K.$$

From $p(b) = 0$ we obtain

$$(b + c/2)^2 = c^2/4 - d.$$

Therefore the element $a = b + c/2 \in L \setminus K$ satisfies

$$a^2 = c^2/4 - d \in K$$

and we have $L = K[a]$.

2 $\implies$ 1. The minimal polynomial of a over K is $p(x) = x^2 - a^2$. Therefore

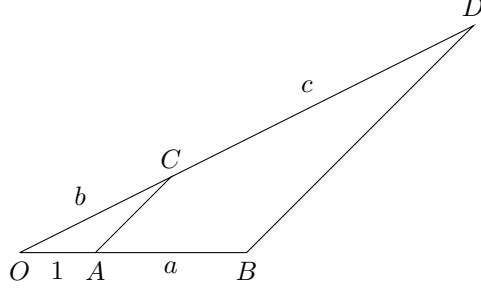
$$[L : K] = [K[a] : K] = \deg p = 2.$$

□

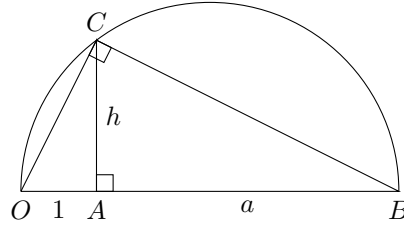
Theorem 3.29. The following subsets of $\mathbb{C}$ coincide

- (1) The smallest subset $K \subset \mathbb{C}$ that contains 0, 1 and all its elementary constructible points.
- (2) The minimal subfield $L \subset \mathbb{C}$ that contains all its square roots.

Proof. $L \subset K$: To prove this we need to show that K is a field closed under taking square roots. Then $L \subset K$ as L is the minimal field with this property. Let us show first that K is a field. Given $z, w \in \mathbb{C}$, one can construct a parallelogram with vertices 0, $z, w, z + w$. Therefore one can construct $z + w$. It is easy to construct $-z$. To construct zw or z/w , we represent $z = ae^{i\varphi}$ and $w = be^{i\psi}$, where $a, b \in \mathbb{R}$ are the lengths of z, w and $\varphi, \psi \in [0, 2\pi]$ are the angles between z, w and the x -axis. Then $zw = abe^{i(\varphi+\psi)}$ and similarly for z/w . One can easily add and subtract angles. Therefore we just have to multiply and divide real positive numbers. In the following picture the lines AC and BD are parallel and therefore $\frac{a}{1} = \frac{c}{b}$, that is, $c = ab$. This implies that if we know real $a, b > 0$, then we can construct $c = ab$. And if we know real $b, c > 0$, then we can construct $a = \frac{c}{b}$. This implies that K is a field.



Let us show that K is stable under taking square roots. We have to prove that given $z = ae^{i\varphi}$, we can also construct $\sqrt{a}e^{i\varphi/2}$. It is easy to construct a bisector of an angle. Therefore we can construct an angle $\varphi/2$. To construct $\sqrt{a}$, consider the following picture, where we start with intervals OA and AB , construct a circle with the diameter OB , and raise a perpendicular to OB at the point A . The angle OCB is right.



We have

$$(1^2 + h^2) + (a^2 + h^2) = OC^2 + BC^2 = OB^2 = (1 + a)^2$$

which implies $h^2 = a$, that is, $h = \sqrt{a}$.

$\mathbf{K} \subset \mathbf{L}$: To prove this we will show that $L \ni 0, 1$ is closed under elementary constructions. Then $K \subset L$ as K is the minimal set with this property. First, we claim that $z \in L$ if and only if $\operatorname{Re} z, \operatorname{Im} z \in L \cap \mathbb{R}$. If $L \subset \mathbb{C}$ is closed under taking square roots, then so is its conjugate $\bar{L}$ and the intersection $L \cap \bar{L}$ (if $x^2 = a$ for $a \in L \cap \bar{L}$ then $x \in L \cap \bar{L}$). From the minimality of L , we obtain $L = L \cap \bar{L} \implies L = \bar{L}$. This implies that if $z = x + iy \in L \implies \bar{z} = x - iy \in L \implies x = \frac{1}{2}(z + \bar{z}) \in L$ and $iy = \frac{1}{2}(z - \bar{z}) \in L$. Note that $i \in L$ as $i^2 = -1 \in L$. Therefore $y \in L$. Conversely, if $x, y \in L \cap \mathbb{R}$ then also $x + iy \in L$.

An elementary L -constructible circle consists of points $x + iy$ satisfying

$$(x - a)^2 + (y - b)^2 = c^2$$

for some $a, b, c \in L \cap \mathbb{R}$. An elementary L -constructible line through the points $x_1 + iy_1 \in L$ and $x_2 + iy_2 \in L$ (with $x_1 \neq x_2, y_1 \neq y_2$) has an equation

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}.$$

It can be written in the form

$$ax + by + c = 0,$$

where $a = y_2 - y_1 \in L \cap \mathbb{R}$, $b = x_1 - x_2 \in L \cap \mathbb{R}$ and $c = ax_1 + by_1 \in L \cap \mathbb{R}$. Intersection points of L -constructible circles and lines have coordinates (x, y) , where x, y are solutions of linear and quadratic equations with coefficients in $L \cap \mathbb{R}$. By assumption, L is closed under taking square roots and therefore under taking quadratic extensions or taking roots of quadratic equations. This implies that $x, y \in L$ and therefore $x + iy \in L$. Therefore L is closed under elementary constructions and $K \subset L$. $\square$

Remark 3.30. The points of $K = L$ from the previous theorem are called constructible points. The angle $\varphi \in [0, 2\pi]$ is called constructible if the point $e^{i\varphi}$ on the unit circle is constructible. $\diamond$

Corollary 3.31. *If $a \in \mathbb{C}$ is constructible, then it is algebraic over $\mathbb{Q}$ and its minimal polynomial has degree 2^k for some $k \geq 0$.*

Proof. By the previous theorem, there exists a chain of field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_n$$

such that $a \in K_n$ and $[K_i : K_{i-1}] = 2$ for $1 \leq i \leq n$. Then

$$[K_n : \mathbb{Q}] = \prod_{i=1}^n [K_i : K_{i-1}] = 2^n.$$

This implies that K_n is a finite field extension of $\mathbb{Q}$. Therefore a is algebraic over $\mathbb{Q}$. If $p \in \mathbb{Q}[x]$ is the minimal polynomial of a , then

$$\deg p = [\mathbb{Q}[a] : \mathbb{Q}]$$

is a divisor of $[K_n : \mathbb{Q}] = 2^n$ as

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}[a]] \cdot [\mathbb{Q}[a] : \mathbb{Q}].$$

Therefore $\deg p$ is a power of 2. □

Corollary 3.32. *The following constructions are impossible with a compass and a straightedge*

- (1) *Duplication of a cube.*
- (2) *Trisection of an arbitrary angle.*
- (3) *Quadrature of a circle.*

Proof. 1. Assume that we can construct $a > 0$ such that $a^3 = 2$. The minimal polynomial of $a = 2^{1/3}$ over $\mathbb{Q}$ is $x^3 - 2$. Its degree is 3 which is not a power of 2. Therefore a is not constructible.

2. Assume that we can trisect an arbitrary angle. One can construct angles $\pi/3$ and $\varphi = 2\pi/3$. Therefore the point $e^{i\varphi} = e^{2\pi i/3}$ is constructible. We will show that the angle $\varphi/3$ is not constructible, that is, the point $z = e^{i\varphi/3} = e^{2\pi i/9}$ is not constructible. We have

$$z^9 = e^{9 \cdot 2\pi i/9} = e^{2\pi i} = 1.$$

Therefore z is a root of the polynomial

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1).$$

It is clear that $z^3 \neq 1$. Therefore z is a root of the polynomial $p(x) = x^6 + x^3 + 1$. This polynomial is irreducible. To see this we apply the Eisenstein's criterion to the polynomial

$$p(x+1) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$$

with prime 3. The irreducibility of p implies that p is a minimal polynomial of z . Its degree is 6 which is not a power of 2. Therefore z is not constructible.

3. If the quadrature of the circle is possible, then the value $a > 0$ satisfying $a^2 = \pi$ is algebraic. This implies that a^2 is also algebraic. But by the theorem of Lindemann (1882) π is not algebraic. □

4. SYMMETRIC POLYNOMIALS

Let $\mathbb{k}$ be a field. For every permutation $\sigma \in S_n$, define a map

$$\sigma : \mathbb{k}[x_1, \dots, x_n] \rightarrow \mathbb{k}[x_1, \dots, x_n], \quad f \mapsto \sigma f = f(x_{\sigma 1}, \dots, x_{\sigma n}).$$

This defines an action of the group S_n on the algebra $\mathbb{k}[x_1, \dots, x_n]$. A polynomial $f \in \mathbb{k}[x_1, \dots, x_n]$ is called symmetric if $\sigma f = f$ for all $\sigma \in S_n$. The set

$$\Lambda_n = \mathbb{k}[x_1, \dots, x_n]^{S_n}$$

of all symmetric polynomials is a subalgebra of $\mathbb{k}[x_1, \dots, x_n]$.

Example 4.1.

- (1) For every $1 \leq k \leq n$, the polynomial

$$e_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}$$

is a symmetric polynomial (of degree k) in Λ_n , called an elementary symmetric polynomial. For example,

$$\begin{aligned} e_1 &= x_1 + x_2 + \dots + x_n, \\ e_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3 + \dots + x_{n-1} x_n, \\ e_n &= x_1 \dots x_n. \end{aligned}$$

We can write

$$\prod_{i=1}^n (x - x_i) = x^n - e_1 x^{n-1} + e_2 x^{n-2} + \dots + (-1)^n e_n.$$

- (2) For every $k \geq 1$, the polynomial

$$h_k = \sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} x_{i_1} \dots x_{i_k}$$

is a symmetric polynomial (of degree k) in Λ_n , called a complete symmetric polynomial. For example,

$$\begin{aligned} h_1 &= x_1 + x_2 + \dots + x_n, \\ h_2 &= x_1^2 + x_1 x_2 + x_2^2 + x_1 x_3 + \dots + x_{n-1} x_n + x_n^2. \end{aligned}$$

- (3) For every $k \geq 1$, the polynomial

$$p_k = x_1^k + \dots + x_n^k$$

is a symmetric polynomial (of degree k) in Λ_n , called a power sum.

◇

Theorem 4.2. *The elements $e_1, \dots, e_n$ generate Λ_n over $\mathbb{k}$ and are algebraically independent. This means that every element in Λ_n is a polynomial in $e_1, \dots, e_n$ and if*

$$f(e_1, \dots, e_n) = \sum_{i_1, \dots, i_n \geq 0} f_{i_1, \dots, i_n} e_1^{i_1} \dots e_n^{i_n} = 0, \quad f_{i_1, \dots, i_n} \in \mathbb{k},$$

then $f = 0$.

Proof. Consider the lexicographic order on $\mathbb{N}^n$:

$$(i_1, \dots, i_n) > (j_1, \dots, j_n) \iff \exists k \geq 1 : i_l = j_l \ \forall l < k, \quad i_k > j_k.$$

Let f be a symmetric polynomial and let $x_1^{i_1} \dots x_n^{i_n}$ be the highest monomial in f (with a non-zero coefficient) wrt lexicographic order. Then $i_1 \geq i_2 \geq \dots \geq i_n$ (as otherwise we can exchange some of i_k and get a higher monomial). The highest monomial in

$$(1) \quad e_1^{i_1 - i_2} e_2^{i_2 - i_3} \dots e_n^{i_n}$$

is

$$x_1^{i_1 - i_2} (x_1 x_2)^{i_2 - i_3} \dots (x_1 \dots x_n)^{i_n} = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}.$$

We can subtract (1) from f (with an appropriate coefficient) in order to kill the highest monomial. The highest monomial of the new polynomial has a smaller degree (with respect to the lexicographic order) and we can assume by induction that the new polynomial can be expressed as a polynomial of $e_1, \dots, e_n$.

Let us show that $e_1, \dots, e_n$ are algebraically independent. The highest monomial of $e_1^{k_1} \dots e_n^{k_n}$ is

$$x_1^{k_1} (x_1 x_2)^{k_2} \dots (x_1 \dots x_n)^{k_n} = x_1^{\sum_{i \geq 1} k_i} x_2^{\sum_{i \geq 2} k_i} \dots$$

This implies that if $e_1^{k_1} \dots e_n^{k_n} \neq e_1^{l_1} \dots e_n^{l_n}$, then the corresponding highest monomials are different. Given a non-trivial linear combination of products $e_1^{k_1} \dots e_n^{k_n}$ over $\mathbb{k}$, consider the highest monomials of all $e_1^{k_1} \dots e_n^{k_n}$ (having non-zero coefficients). The highest of them appears only once, hence has a non-zero coefficient and the whole linear combination is nonzero. This implies that the products $e_1^{k_1} \dots e_n^{k_n}$ are linearly independent and the elements $e_1, \dots, e_n$ are algebraically independent. $\square$

Remark 4.3. In the same way we can show that $h_1, \dots, h_n$ generate Λ_n and are algebraically independent. Similarly (if $\mathbb{k}$ has characteristic zero) $p_1, \dots, p_n$ generate Λ_n and are algebraically independent. $\diamond$

Remark 4.4. For example in Λ_2 , we have $e_1 = h_1 = p_1 = x_1 + x_2$ and

$$e_2 = x_1 x_2, \quad h_2 = x_1^2 + x_1 x_2 + x_2^2, \quad p_2 = x_1^2 + x_2^2.$$

This implies

$$h_2 = e_1^2 - e_2 = \frac{1}{2}(p_1^2 + p_2), \quad p_2 = e_1^2 - 2e_2.$$

$\diamond$

Remark 4.5. Consider generating functions

$$E(t) = \sum_{k \geq 0} e_k t^k = \prod_{i=1}^n (1 + x_i t),$$

$$H(t) = \sum_{k \geq 0} h_k t^k = \prod_{i=1}^n (1 + x_i t + x_i^2 t^2 + \dots) = \prod_{i=1}^n \frac{1}{1 - x_i t}.$$

Then

$$H(t)E(-t) = 1.$$

$$\log H(t) = \sum_{i=1}^n \log \frac{1}{1 - x_i t} = \sum_{i=1}^n \sum_{k \geq 1} \frac{x_i^k t^k}{k} = \sum_{k \geq 1} \frac{p_k}{k} t^k.$$

$\diamond$

4.1. Discriminant. Let $f \in \mathbb{k}[x]$ and $L/\mathbb{k}$ be its splitting field, so that $f(x) = a \prod_{i=1}^n (x - x_i)$, where $x_i \in L$ are the roots of f . Define the discriminant of f

$$\Delta = a^{2n-2} \prod_{i < j} (x_i - x_j)^2$$

which is symmetric in $x_1, \dots, x_n$. Note that Δ is zero if and only if f has a multiple root. Let us show that $\Delta \in \mathbb{k}$. By the previous result Δ is a polynomial in $e_1, \dots, e_n$, where

$$f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} + \dots + (-1)^n e_n.$$

This means that Δ is a polynomial in the coefficients of f , hence $\Delta \in \mathbb{k}$.

Let $n = 2$ and $f = x^2 - e_1 x + e_2 = x^2 + bx + c$. Then we get the usual discriminant

$$\Delta = (x_1 - x_2)^2 = e_1^2 - 4e_2 = b^2 - 4c.$$

Let $n = 3$ and assume for simplicity that

$$f = x^3 - e_1 x^2 + e_2 x - e_3 = x^3 + bx + c,$$

that is, $e_1 = x_1 + x_2 + x_3 = 0$. As Δ has degree 6, we have

$$\Delta = ue_3^2 + ve_2^3,$$

for some $u, v \in \mathbb{Z}$. If $x_3 = 0$, then $x_1 + x_2 = 0$ and

$$x_1^2 x_2^2 (x_1 - x_2)^2 = vx_1^3 x_2^3,$$

hence $v = -4$. If $x_1 = x_2 = 1$, $x_3 = -2$, then

$$0 = 4u - 4(1 - 2 - 2)^3,$$

hence $u = -27$. We obtain

$$\Delta = -27e_3^2 - 4e_2^3 = -27c^2 - 4b^3.$$

Example 4.6. Let us compute the discriminant of $x^n - 1$. Let $\xi = e^{2\pi i/n}$. Then

$$\begin{aligned} \Delta &= \prod_{0 \leq i < j < n} (\xi^i - \xi^j)^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\xi^i - \xi^j) = (-1)^{\binom{n}{2}} \prod_{i=0}^{n-1} \prod_{j \neq i} \xi^i (1 - \xi^{j-i}) \\ &= (-1)^{\binom{n}{2}} \prod_{i=0}^{n-1} \xi^i \prod_{k \neq 0} (1 - \xi^k) = (-1)^{\binom{n}{2}} \xi^{\binom{n}{2}} n^n = (-1)^{\binom{n}{2}} e^{\pi i(n-1)} n^n = \pm n^n. \end{aligned}$$

where we used the fact that $\prod_{k \neq 0} (x - \xi^k) = \frac{x^n - 1}{x - 1} = 1 + x + \dots + x^{n-1}$ and substituted $x = 1$. A discriminant of f is a polynomial in the coefficients of f . This implies that the discriminant of $x^n - 1$ is still $\pm n^n$ if we consider $x^n - 1$ as a polynomial in $\mathbb{F}_p[x]$. In particular, if $p \mid n$, then $\Delta = 0$ and $x^n - 1$ has multiple roots over $\mathbb{F}_p$. If $p \nmid n$, then $\Delta \neq 0$ and $x^n - 1$ does not have multiple roots over $\mathbb{F}_p$. The last statement also follows from the fact that $x^n - 1$ and its derivative nx^{n-1} are non-zero and coprime, hence $x^n - 1$ can not have multiple factors (and in particular multiple roots). $\diamond$

5. MODULES

5.1. Definition and examples. Modules over rings generalize the notion of a vector space over a field.

Definition 5.1. Let R be a ring. A module over R (or an R -module) is an abelian group $(M, +)$ together with a map

$$R \times M \rightarrow M, \quad (a, m) \mapsto a \cdot m = am,$$

called a multiplication, such that for all $a, b \in R$ and $m, n \in M$

- (1) $a(bm) = (ab)m$,
- (2) $1m = m$,
- (3) $a(m + n) = am + an$,
- (4) $(a + b)m = am + bm$.

Remark 5.2. If R is a field, then an R -module is usually called an R -vector space or a vector space over R . $\diamond$

Example 5.3. Any ring R is a module over itself. More generally, for any $n \geq 1$, the product R^n is an R -module with multiplication defined by $a(x_1, \dots, x_n) = (ax_1, \dots, ax_n)$. $\diamond$

Example 5.4. Let $I \subset \mathbb{R}$ be an ideal. Then I is a module over R with a natural multiplication $R \times I \ni (a, b) \mapsto ab \in I$. $\diamond$

Example 5.5. Let $f : R \rightarrow S$ be a ring homomorphism and M be an S -module. Then M can be considered also as an R -module. Multiplication is given by

$$a \cdot m = f(a) \cdot m, \quad a \in R, m \in M.$$

We say that the R -module structure on M is obtained by restriction of scalars. In particular, S is a module over R with multiplication given by

$$a \cdot s = f(a) \cdot s, \quad a \in R, s \in S.$$

If $I \subset R$ is an ideal, then there is a canonical ring homomorphism $\pi : R \rightarrow R/I$. Therefore R/I is an R -module, with multiplication given by $a(b + I) = ab + I$. $\diamond$

Remark 5.6. Let M be an R -module, 0_R be the zero element of R and 0_M be the zero element of M . Then

- (1) $0_R m = 0_M$ for any $m \in M$.
- (2) $(-1)m = -m$ for any $m \in M$.
- (3) $a0_M = 0_M$ for any $a \in R$.

Indeed,

$$0_R m + 0_R m = (0_R + 0_R)m = 0_R m.$$

Therefore $0_R m = 0_M$. Similarly,

$$(-1)m + m = (-1 + 1)m = 0_R m = 0_M.$$

Therefore $(-1)m = -m$. Finally

$$a0_M + a0_M = a(0_M + 0_M) = a0_M.$$

Therefore $a0_M = 0_M$. $\diamond$

Example 5.7. Let M be an abelian group. Then M is automatically a $\mathbb{Z}$ -module. Indeed, for any $k \geq 0$ and $m \in M$, define

$$k \cdot m = \underbrace{m + \dots + m}_{k \text{ summands}}$$

and $(-k)m = -km$. Note that this is a unique possible structure of a $\mathbb{Z}$ -module on M because we should have $1 \cdot m = m$, $2 \cdot m = (1 + 1)m = m + m$ and generally $(k + 1)m = km + m$. $\diamond$

5.2. Homomorphisms and submodules.

Definition 5.8. Let R be a ring and M, N be R -modules.

- (1) A map $f : M \rightarrow N$ is called a homomorphism of R -modules (or R -linear) if
 - (a) $f(m + m') = f(m) + f(m')$ for any $m, m' \in M$.
 - (b) $f(am) = af(m)$ for any $a \in R, m \in M$.
- (2) A bijective homomorphism $f : M \rightarrow N$ is called an isomorphism.
- (3) A homomorphism $f : M \rightarrow M$ is called an endomorphism. A bijective endomorphism $f : M \rightarrow M$ is called an automorphism.
- (4) The set of all R -module homomorphism $f : M \rightarrow N$ is denoted by $\text{Hom}_R(M, N)$.
- (5) The set of all R -module endomorphisms $f : M \rightarrow M$ is denoted by $\text{End}_R(M) = \text{Hom}_R(M, M)$.

Lemma 5.9. Let M, N be two R -modules. Then

- (1) $\text{Hom}_R(M, N)$ is an abelian group, with an addition defined by

$$(f + g)m = f(m) + g(m), \quad f, g \in \text{Hom}_R(M, N), \quad m \in M.$$

- (2) $\text{End}_R(M) = \text{Hom}(M, M)$ is a ring, with an addition defined as above and a multiplication defined by composition

$$(fg)m = f(g(m)), \quad f, g \in \text{Hom}_R(M, N), \quad m \in M.$$

Example 5.10. Let K be a field and $V = K^n$ be a vector space of dimension n . Given a matrix $A = (a_{ij}) \in M_n(K)$, we can associate with it a linear map

$$f_A : V \rightarrow V, \quad x = (x_1, \dots, x_n)^t \mapsto Ax = \left(\sum_j a_{1j}x_j, \dots, \sum_j a_{nj}x_j \right)^t.$$

The map

$$M_n(K) \rightarrow \text{End}_K(V), \quad A \mapsto f_A$$

is an isomorphism of rings. Given a linear map $f : V \rightarrow V$, one reconstructs the matrix $A = (a_{ij}) \in M_n(K)$ by the rule $fe_j = \sum_i a_{ij}e_i$, where $(e_1, \dots, e_n)$ is the standard basis of $V = K^n$. We will often identify $A \in M_n(K)$ and $f_A \in \text{End}_K(V)$. $\diamond$

Remark 5.11. If M is an abelian group, then the ring $\text{End}_{\mathbb{Z}}(M)$ is denoted by $\text{End}(M)$. If M is an R -module, then there is a ring homomorphism

$$\varphi : R \rightarrow \text{End}(M), \quad \varphi(a)(m) = am, \quad a \in R, \quad m \in M.$$

For example

$$\varphi(ab)m = (ab)m = a(bm) = \varphi(a)(bm) = \varphi(a)(\varphi(b)m)$$

and therefore $\varphi(ab) = \varphi(a) \circ \varphi(b)$. Conversely, given an abelian group M and a ring homomorphism $\varphi : R \rightarrow \text{End}(M)$, we can equip M with an R -module structure

$$a \cdot m = \varphi(a)(m) \in M, \quad a \in R, \quad m \in M. \quad \diamond$$

Example 5.12. Let V be a vector space over a field K . Given a K -linear map $A \in \text{End}_K(V)$, the evaluation map

$$K[x] \rightarrow \text{End}_K(V), \quad f \mapsto f(A)$$

is a ring homomorphism, hence V gets a structure of a $K[x]$ -module

$$f \cdot v = f(A)(v), \quad f \in K[x], \quad v \in V.$$

Conversely, if V is a $K[x]$ -module (extending the K -vector space structure on V), then multiplication by x induces a K -linear map $A : V \rightarrow V$. $\diamond$

Definition 5.13. Let M be an R -module. A subset $N \subset M$ is called a submodule if N is a subgroup and for any $a \in R, m \in N$ we have $am \in N$ (that is, $RN \subset N$).

Example 5.14. Let R be a commutative ring. Then the submodules of R are precisely the ideals of R . $\diamond$

Lemma 5.15. *Let $f : M \rightarrow N$ be a homomorphism of R -modules. Then*

- (1) *The set $\ker f = \{m \in M \mid f(m) = 0\}$ is a submodule of M .*
- (2) *The set $\operatorname{im} f = \{f(m) \mid m \in M\}$ is a submodule of N .*
- (3) *f is injective if and only if $\ker f = 0$.*

Remark 5.16. Given an R -module M and a submodule $N \subset M$, one can define the quotient M/N of abelian groups (similar to the construction of the quotient ring R/I for an ideal $I \subset R$). Define an equivalence relation on M by

$$m \sim m' \iff m - m' \in N.$$

The equivalence class of $m \in M$ is

$$[m] = m + N = \{m + n \mid n \in N\}.$$

The set of equivalence classes is denoted by M/N . It has a structure of an abelian group defined by

$$[m] + [m'] = [m + m'].$$

◇

Theorem 5.17. *Let M be an R -module and $N \subset M$ be a submodule. Then*

- (1) *The quotient group M/N has a structure of an R -module defined by*

$$a \cdot [m] = [am], \quad a \in R, m \in M.$$

- (2) *The natural map $\pi : M \rightarrow M/N$, $m \mapsto [m]$, is a homomorphism of R -modules.*
- (3) *If $f : M \rightarrow M'$ is a homomorphism of R -modules, then there exists a unique homomorphism $\bar{f} : M/\ker f \rightarrow M'$ that makes the following diagram commute ($\bar{f} \circ \pi = f$)*

$$\begin{array}{ccc} M & \xrightarrow{\pi} & M/\ker f \\ & \searrow f & \swarrow \bar{f} \\ & M' & \end{array}$$

The map $\bar{f}$ induces an isomorphism $\bar{f} : M/\ker f \xrightarrow{\sim} \operatorname{im} f$.

5.3. Simple and indecomposable modules.

Definition 5.18. Let R be a ring and M be a nonzero R -module.

- (1) A module M is called simple (or irreducible) if it does not contain any submodules except zero and itself.
- (2) A module M is called indecomposable if it can not be written as an (internal) direct sum of nonzero submodules, that is, there are no nonzero submodules $N, N' \subset M$ such that $N \cap N' = 0$ and $N + N' = M$.
- (3) A submodule $N \subsetneq M$ is called maximal, if there are no submodules $N \subsetneq L \subsetneq M$.

Remark 5.19. Any simple module is indecomposable. ◇

Remark 5.20. Given two R -modules N, N' , define a new R -module $N \oplus N'$, called an (external) direct sum of N and N' , to be the product of abelian groups $N \times N'$ equipped with a multiplication

$$a(n, n') = (an, an'), \quad a \in R, n \in N, n' \in N'.$$

A module M is indecomposable if and only if it is not isomorphic to a direct sum $N \oplus N'$ for some nonzero modules N, N' . ◇

Example 5.21. If K is a field, then K is a simple module over itself. ◇

Example 5.22. Let R be a PID and $p \in R$ be irreducible. Then

- (1) The module $(p) \subset R$ is maximal: if $(p) \subset (a) \subset R \implies a \mid p \implies a = 1$ or $a = p$ (up to a unit) $\implies (a) = R$ or $(a) = (p)$. The quotient $R/(p)$ is a field and is a simple module over $R/(p)$ and over R .
- (2) The module $M = R/(p^2)$ is not simple. It has a submodule $N = (p)/(p^2)$. The quotient M/N is isomorphic to $R/(p)$. Note that $N = (p)/(p^2)$ is also isomorphic to $R/(p)$:

$$R/(p) \rightarrow (p)/(p^2), \quad a \mapsto ap.$$

- (3) The module $M = R/(p^2)$ is indecomposable. Indeed, for any submodule $N \subset M$, there exists an ideal $(p^2) \subset (a) \subset R$ such that $N = (a)/(p^2)$. We obtain from $a \mid p^2$ that $a = 1, p$ or p^2 (up to a unit). Therefore the only submodules of $M = R/(p^2)$ are $0 = (p^2)/(p^2) \subset (p)/(p^2) \subset (1)/(p^2) = M$. If $N_1 \oplus N_2 = M$ then $N_1 \subset N_2$ or $N_2 \subset N_1$. Assuming the former without loss of generality, we obtain $N_1 = N_1 \cap N_2 = 0$, hence M is indecomposable.
- (4) Let $p, q \in R$ be coprime. Then $M = R/(pq)$ is an (internal) direct sum of $N_1 = (p)/(pq) \subset M$ and $N_2 = (q)/(pq)$: let $a \in R$ be such that $[a] \in N_1 \cap N_2$. Then $p \mid a$ and $q \mid a \implies pq \mid a \implies [a] = 0$ in $R/(pq)$. Therefore $N_1 \cap N_2 = 0$. There exist $u, v \in R$ such that $1 = up + vq \implies 1 \in N_1 + N_2 \implies N_1 + N_2 = R/(pq) = M$.

This proves that $M = R/(pq)$ is not indecomposable. Note that $R/(q) \simeq (p)/(pq) = N_1$, $[a]_q \mapsto [ap]_{pq}$ and similarly $R/(p) \simeq (q)/(pq) = N_2$. This implies that $R/(pq) \simeq R/(p) \oplus R/(q)$ (external direct sum). ◇

Lemma 5.23 (Schur's lemma). *For any simple R -module M , the endomorphism ring $\text{End}_R(M)$ is a division ring, that is, any endomorphism $M \rightarrow M$ is either zero or invertible.*

Proof. Assume that $f : M \rightarrow M$ is nonzero. Then $\ker f \subset M$ is a submodule not equal to M . Therefore $\ker f = 0$ and f is injective. On the other hand $\text{im } f \subset M$ is a submodule not equal to zero. Therefore $\text{im } f = M$ and f is surjective. This implies that f is bijective and therefore invertible. □

Corollary 5.24. *Let R be an algebra over an algebraically-closed field K . If M is a simple R -module, finite-dimensional over K , then $\text{End}_R(M) = K$.*

Proof. We know that $S = \text{End}_R(M)$ is a division ring. As M is f.d., $\text{End}_K(M)$ is also f.d. For every $a \in S$, the elements $1, a, \dots, a^n \in S \subset \text{End}_K(M)$ are linearly dependent over K for large n . Therefore there exists monic $f \in K[x]$ with $f(a) = 0$. As K is algebraically closed, we can write

$f = \prod_i (x - c_i)$ with $c_i \in K$. Then $f(a) = \prod_i (a - c_i) = 0$. The ring S is an integral domain and $a - c_i \in S$ for all i . Therefore $a - c_i = 0$ for some i , hence $a = c_i \in K$.

Alternative proof: Let $f : M \rightarrow M$ be an R -homomorphism. As a linear operator on a K -vector space, f admits an eigenvector $v \in M$ with an eigenvalue $\lambda \in K$ (as K is algebraically closed). Then $f' = f - \lambda \text{Id} \in \text{End}_R(M)$, $f'(v) = f(v) - \lambda v = 0 \implies \ker f' \neq 0$. But $\ker f' \subset M$ is a submodule and M is simple, hence $\ker f' = M \implies f' = 0$. This implies $f = \lambda \text{Id}$. $\square$

Lemma 5.25. *Let M be an R -module and $N \subset M$ be a submodule. Then $N \subset M$ is maximal if and only if M/N is simple.*

Proof. Consider a canonical homomorphism $\pi : M \rightarrow M/N$. There is a bijection between the submodules $N \subset L \subset M$ and the submodules of M/N given by $L \mapsto \pi(L) = L/N \subset M/N$. The inverse is given by

$$M/N \supset L' \mapsto \pi^{-1}(L') \subset M.$$

The submodule $N \subset M$ is maximal $\iff N$ and M are the only submodules $N \subset L \subset M \iff 0$ and M/N are the only submodules of $M/N \iff M/N$ is simple. $\square$

Lemma 5.26. *Let R be a commutative ring and M be a simple R -module. Then there exists a maximal ideal $I \subset R$ such that $M \simeq R/I$.*

Proof. Let $m \in M$ be a nonzero element. Consider a homomorphism of R -modules

$$f : R \rightarrow M, \quad f(r) = rm.$$

Then $\text{im } f \subset M$ is a nonzero submodule and therefore $\text{im } f = M$. Let $I = \ker f$. Then I is a submodule and therefore an ideal of R . There is an isomorphism

$$R/I \simeq \text{im } f = M.$$

As M is simple, we obtain by the previous lemma that $I \subset R$ is a maximal submodule and a maximal ideal. $\square$

Definition 5.27. Let R be a ring and M be an R -module. A composition series of a module M is a chain of submodules

$$0 = M_0 \subset M_1 \subset \dots \subset M_n = M$$

such that the modules M_i/M_{i-1} are simple for $1 \leq i \leq n$. The modules M_i/M_{i-1} are called the subquotients of the composition series. The number n is called the length of the composition series.

Theorem 5.28 (Jordan-Hölder Theorem). *Let M be an R -module that has at least one composition series. Then any two composition series of M have the same length and have isomorphic subquotients (up to a permutation). The length of a composition series is called the length of M .*

Example 5.29. Let R be a PID and $p, q \in R$ be two irreducible elements, not associate to each other. Then $M = R/(pq) \simeq R/(p) \oplus R/(q)$ has the following filtrations:

$$\begin{aligned} M_0 &= 0, & M_1 &= R/(p), & M_2 &= M, \\ M'_0 &= 0, & M'_1 &= R/(q), & M'_2 &= M. \end{aligned}$$

The corresponding subquotients are

$$\begin{aligned} M_1/M_0 &\simeq R/(p), & M_2/M_1 &\simeq R/(q), \\ M'_1/M'_0 &\simeq R/(q), & M'_2/M'_1 &\simeq R/(p). \end{aligned}$$

The tuples of subquotients are the same up to a permutation. $\diamond$

5.4. Chinese remainder theorem. We have seen that given a PID R and coprime elements $p, q \in R$, we have

$$R/(pq) \simeq R/(p) \oplus R/(q).$$

We will generalize this statement by proving the Chinese Remainder Theorem. In its classical form, formulated in the 3rd century AD by Sunzi (not to be confused with Sun Tzu, the author of “The art of war”) it is

Theorem 5.30. *Let $n_1, \dots, n_k$ be positive, pairwise coprime integers. Then for any integers $a_1, \dots, a_k$, there exists an integer a such that*

$$a \equiv a_i \pmod{n_i}, \quad \forall i = 1, \dots, k.$$

There exists a unique such integer with $0 \leq a < n = n_1 \dots n_k$.

This theorem can be formulated as a statement that the map

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}, \quad a + n\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, \dots, a + n_k\mathbb{Z})$$

is an isomorphism (of rings or of abelian groups).

Proof. The above map is injective. Indeed, if $[a] = a + n\mathbb{Z}$ is mapped to zero, then $n_i \mid a$ for all i , hence $n = \prod_i n_i \mid a$ as the elements n_i are pairwise coprime. This implies that $[a] = 0$. Injectivity of the map implies bijectivity as the groups on both sides have the same number of elements. $\square$

We can generalize the above result to arbitrary PID.

Theorem 5.31. *Let R be a PID and $n_1, \dots, n_k$ be pairwise coprime elements (that is, $\gcd(n_i, n_j) = 1$ for $i \neq j$). Then the map*

$$R/(n) \rightarrow R/(n_1) \times \dots \times R/(n_k), \quad a + (n) \mapsto (a + (n_1), \dots, a + (n_k)),$$

is an isomorphism of rings (or R -modules), where $n = n_1 \dots n_k$.

Remark 5.32. In particular, we see that for any coprime $p, q \in R$, we have an isomorphism $R/(pq) \simeq R/(p) \oplus R/(q)$ of R -modules. $\diamond$

This statement, in its own right, can be generalized as follows

Theorem 5.33. *Let R be a commutative ring and $I_1, \dots, I_k$ be ideals of R that are pairwise coprime: $I_i + I_j = R$, $i \neq j$. Then the map*

$$\varphi : R/I \rightarrow R/I_1 \times \dots \times R/I_k, \quad a + I \mapsto (a + I_1, \dots, a + I_k),$$

is an isomorphism of rings (or R -modules), where $I = \bigcap_i I_i$. Moreover $I = I_1 I_2 \dots I_k$.

Proof. The kernel of the map

$$R \rightarrow R/I_1 \times \dots \times R/I_k$$

is $\bigcap_i I_i = I$. This implies injectivity of φ . Let us prove surjectivity. For any $i \neq j$, we can find $e_{ij} \in I_i$ and $e_{ji} \in I_j$ such that $1 = e_{ij} + e_{ji}$. Then, for any i , we have

$$1 = \prod_{j \neq i} (e_{ij} + e_{ji}) \in I_i + \prod_{j \neq i} e_{ji}.$$

Let $e_i \in I_i$ and $f_i = \prod_{j \neq i} e_{ji} \in \prod_{j \neq i} I_j$ be such that $1 = e_i + f_i$. Given elements $[a_i] \in R/I_i$ for all i , we claim that $a = \sum_j f_j a_j$ satisfies $a \equiv a_i \pmod{I_i}$ for all i . Indeed,

$$a - a_i = a - (e_i + f_i)a_i = \sum_{j \neq i} f_j a_j - e_i a_i \in I_i$$

as $e_i \in I_i$ and $f_j \in I_i$ for $j \neq i$. Therefore $a \equiv a_i \pmod{I_i}$ for all i and the map φ is surjective.

We also have to show that $\bigcap_i I_i = \prod_i I_i$. Inclusion $\prod_i I_i \subset \bigcap_i I_i$ is trivial. On the other hand, let $a \in \bigcap_i I_i$. Then by induction $a \in J = I_1 \dots I_{k-1}$. Therefore

$$a = a(e_k + f_k) \in JI_k + I_k J = \prod_i I_i$$

as $e_k \in I_k$, $f_k \in \prod_{j \neq k} I_j = J$ and $a \in I_k$. This proves that $\bigcap_i I_i \subset \prod_i I_i$. $\square$

5.5. Modules over PID. Consider the following two fundamental results of linear algebra and the theory of finite abelian groups. In linear algebra one proves that every square matrix over $\mathbb{C}$ is conjugate to its Jordan canonical form which is a direct sum of Jordan blocks

$$J_{n,\lambda} = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix} \quad \lambda \in \mathbb{C}, \quad n \geq 1.$$

The fundamental theorem of finitely generated abelian groups states that every such group is isomorphic to a direct sum

$$\mathbb{Z}^k \oplus \mathbb{Z}/(p_1^{n_1}) \oplus \dots \oplus \mathbb{Z}/(p_r^{n_r}),$$

where $k \geq 0$, $p_i \in \mathbb{Z}$ are prime numbers and $n_i \geq 1$. In particular, every finite abelian group is isomorphic to

$$\mathbb{Z}/(p_1^{n_1}) \oplus \dots \oplus \mathbb{Z}/(p_r^{n_r}).$$

We will see that these two results are essentially equivalent, if seen from an appropriate point of view, and then we will give a general unified proof.

Given a vector space $V = K^n$ over a field K and a linear operator $A \in \text{End}_K(V) = M_n(K)$, we can equip V with a structure of a $K[x]$ -module (we denote it by V_A)

$$f \cdot v = f(A)(v), \quad f \in K[x], \quad v \in V.$$

Conversely, if V is a $K[x]$ -module, then it is a K -vector space and we can define

$$A \in \text{End}_K(V), \quad A(v) = x \cdot v, \quad v \in V.$$

Example 5.34. Consider the $K[x]$ -module $V = K[x]/(x - \lambda)^n$, where $\lambda \in K$ and $n \geq 1$. Choose the basis $(x - \lambda)^{n-1}, \dots, (x - \lambda)^2, (x - \lambda), 1$ of V . In this basis we have

$$A(x - \lambda)^k = x(x - \lambda)^k = (x - \lambda)^{k+1} + \lambda(x - \lambda)^k$$

for $k < n - 1$ and $A(x - \lambda)^{n-1} \equiv \lambda(x - \lambda)^{n-1} \pmod{(x - \lambda)^n}$. Therefore the matrix of A in this basis is exactly the Jordan block $J_{n,\lambda}$. $\diamond$

Let W be another K -vector space, $B \in \text{End}_K(W)$ and W_B be the corresponding $K[x]$ -module. Then an isomorphism $g : V_A \rightarrow W_B$ of $K[x]$ -modules can be identified with a K -linear isomorphism $g : V \rightarrow W$ such that $gA = Bg$:

$$gA(v) = g(x \cdot v) = x \cdot g(v) = Bg(v), \quad v \in V.$$

This means that $B = gAg^{-1}$ and the corresponding matrices are conjugate if $V = W = K^n$. The statement that a matrix $A \in M_n(K)$ (with $K = \mathbb{C}$) is conjugate to a direct sum of Jordan blocks $J_{n_1,\lambda_1}, \dots, J_{n_r,\lambda_r}$ can be translated now to the statement that the $K[x]$ -module V_A is isomorphic to a direct sum of $K[x]$ -modules

$$K[x]/(x - \lambda_1)^{n_1} \oplus \dots \oplus K[x]/(x - \lambda_r)^{n_r}.$$

The polynomials $(x - \lambda)^n$ are powers of irreducible polynomials $x - \lambda \in K[x]$ and these are the only irreducible (or prime) elements in $K[x]$ (up to a unit) if $K = \mathbb{C}$ or K is algebraically closed. In the same way for abelian groups we had summands $\mathbb{Z}/(p^n)$, where p is prime. This shows that both statements are essentially equivalent, with the first statement being about modules over $K[x]$ and the second statement about modules over $\mathbb{Z}$ (that is, abelian groups). Both of them follow from the general result we will prove next.

Definition 5.35. Let M be an R -module.

- (1) A family of elements $(m_i)_{i \in I}$ in M generates M if every element of M can be written in the form

$$\sum_{i \in I} a_i m_i, \quad a_i \in R$$

with all but finitely many a_i equal zero.

- (2) M is called finitely generated over R if there exists a finite family $(m_1, \dots, m_k)$ of elements in M that generates M .

Theorem 5.36. *Let R be a PID. A finitely generated R -module is isomorphic to a direct sum*

$$R^k \oplus R/(p_1^{n_1}) \oplus \dots \oplus R/(p_r^{n_r}),$$

where $k \geq 0$, $p_i \in R$ are prime and $n_i \geq 1$. The modules R and $R/(p^n)$ are indecomposable.

Proof. Let M be a finitely generated R -module with generators $x_1, \dots, x_m$. Then there is a surjective homomorphism $\psi : R^m \rightarrow M$ (where $R^m \ni e_i \mapsto x_i$). The kernel $\ker \psi \subset R^m$ is finitely generated (see below). Therefore there is a surjective homomorphism $\phi : R^n \rightarrow \ker \psi$ and we obtain a sequence of maps

$$R^n \xrightarrow{\varphi} R^m \xrightarrow{\psi} M,$$

where $\text{im } \varphi = \ker \psi$ so that

$$\text{coker } \varphi := R^m / \text{im } \varphi = R^m / \ker \psi \simeq M.$$

We can represent φ as an $m \times n$ matrix with coefficients in R . By changing the bases in R^m and R^n we can put this matrix to the form, called a Smith normal form,

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & 0 \\ \dots & \dots & \dots & a_r & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

with nonzero $a_1 \mid a_2 \mid \dots \mid a_r$ and $r \leq m, n$. The elements a_i are unique (up to a unit). The algorithm is somewhat involved for general PID, but in the case of Euclidean domains one can use the usual Gaussian elimination on rows and columns to get the required form. I omit the details. We obtain then

$$M \simeq R^m / \text{im } \varphi = R/(a_1) \oplus \dots \oplus R/(a_r) \oplus R^{m-r}.$$

If $a \in R$ is nonzero and $a = \prod_i p_i^{k_i}$ is a factorization into irreducible (distinct) factors, then

$$R/(a) \simeq R/(p_1^{k_1}) \oplus R/(p_2^{k_2}) \oplus \dots$$

by the Chinese Remainder theorem. We obtain the required decomposition of the module M .

Let us see that R is indecomposable. If $N_1 = (a) \subset R$, $N_2 = (b) \subset R$ and $N_1, N_2 \neq 0$, then $0 \neq ab \in N_1 \cap N_2$, hence $N_1 \cap N_2 \neq 0$ and $R \neq N_1 \oplus N_2$. Similarly one can show that $R/(p^n)$ is indecomposable. $\square$

5.6. Noetherian modules. In the proof of the theorem we used the fact that a submodule of R^n is finitely generated if R is a PID. Let us discuss this in more detail.

Definition 5.37. Let R be a ring.

- (1) An R -module M is called Noetherian if every submodule of M is finitely generated.
- (2) The ring R is called Noetherian if it is Noetherian as a (left) R -module over itself.

Example 5.38. A PID R is Noetherian. Indeed, every submodule of R is an ideal, hence a principal ideal, generated by one element. $\diamond$

Lemma 5.39. Let R be a ring and M be an R -module. The following conditions are equivalent

- (1) Every submodule of M is finitely generated.
- (2) Every increasing chain of submodules

$$M_1 \subset M_2 \subset \dots \subset M$$

stabilizes, that is, $M_n = M_{n+1} = \dots$ for $n \gg 0$.

Proof. $1 \implies 2$. Consider an increasing chain

$$M_1 \subset M_2 \subset \dots \subset M$$

and let $N = \bigcup_{n \geq 1} M_n \subset M$. Then N is a submodule of M and by assumption it is finitely generated. Let $x_1, \dots, x_k$ be generators of N . Then $x_i \in M_{n_i}$ for some $n_i \geq 1$. Taking $n = \max_i n_i$, we obtain $x_i \in M_n$ for all i , hence $N \subset M_n$ and $M_n = M_{n+1} = \dots$.

$2 \implies 1$. Let $N \subset M$ be a submodule and let $x_0 = 0 \in N$. Assuming that elements $x_0, \dots, x_k$ in N are constructed, let $M_k \subset N$ be the module generated by them. If $M_k = N$ then N is finitely generated and we are done. If $M_k \neq N$, let $x_{k+1} \in N \setminus M_k$ and continue the procedure. In this way we obtain a chain of modules

$$M_1 \subset M_2 \subset \dots \subset N \subset M$$

with $M_k \neq M_{k+1}$ for all $k \geq 1$. A contradiction. $\square$

Lemma 5.40. Let M be an R -module and $N \subset M$ be a submodule. Then M is Noetherian $\iff N$ and M/N are Noetherian.

Proof. Let M be Noetherian. If $L \subset N$ is a submodule, then $L \subset M$, hence L is finitely generated and N is Noetherian. Let $L \subset M/N$ be a submodule and let $\pi : M \rightarrow M/N$ be the projection. The module $L' = \pi^{-1}(L) \subset M$ is finitely generated, hence also $L = \pi(L')$ is finitely generated and M/N is Noetherian.

Assume that N and M/N are Noetherian and let $L \subset M$. Then $L \cap N \subset N$ is finitely generated and $L/(L \cap N) \simeq (L + N)/N \subset M/N$ is finitely generated. This implies that L is also finitely generated. $\square$

Corollary 5.41. If M, N are Noetherian R -modules, then $M \oplus N$ is also Noetherian.

Proof. Let $M' = M \oplus N$. Then $N \subset M'$ and $M'/N \simeq M$ are Noetherian. We conclude that M' is Noetherian. $\square$

Corollary 5.42. If R is a Noetherian ring, then the module R^n is Noetherian for all $n \geq 1$.

Proof. The module R^n is a direct sum of copies of R . $\square$

Corollary 5.43. If R is a PID, then every submodule of R^n is finitely generated.

Proof. We have seen that R is Noetherian. Therefore R^n is also Noetherian. This means that every submodule of R^n is finitely generated. $\square$

Lemma 5.44. Let M be a Noetherian module over a ring R and $f : M \rightarrow M$ be a surjective homomorphism. Then f is an isomorphism.

Proof. Consider the chain of modules $\ker f \subset \ker f^2 \subset \dots \subset M$. As M is Noetherian, this chain stabilizes $\implies \exists n \geq 1, \ker f^n = \ker f^{2n} \implies \text{im } f^n \cap \ker f^n = 0$. Indeed, if $f^n(x) \in \ker f^n \implies f^{2n}(x) = 0 \implies x \in \ker f^{2n} = \ker f^n \implies f^n(x) = 0$. As f is surjective: $\text{im } f^n = M \implies \ker f^n = \text{im } f^n \cap \ker f^n = 0 \implies \ker f = 0 \implies f$ is injective. $\square$