

Rings,Fields

TS. Nguyễn Việt Đông

1

Rings,Fields

- 1. Rings, Integral Domains and Fields,
- 2. Polynomial and Euclidean Rings
- 3. Quotient Rings

2

1. Rings, Integral Domains and Fields

- 1.1.Rings
- 1.2. Integral Domains and Fields
- 1.3.Subrings and Morphisms of Rings

3

1. Rings, Integral Domains and Fields

- 1.1.Rings
- A *ring* $(R, +, \cdot)$ is a set R , together with two binary operations $+$ and \cdot on R satisfying the following axioms. For any elements $a, b, c \in R$,
 - (i) $(a + b) + c = a + (b + c)$. (associativity of addition)
 - (ii) $a + b = b + a$. (commutativity of addition)
 - (iii) there exists $0 \in R$, called the zero, such that $a + 0 = a$. (existence of an additive identity)
 - (iv) there exists $(-a) \in R$ such that $a + (-a) = 0$. (existence of an additive inverse)
 - (v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (associativity of multiplication)

4

1. Rings, Integral Domains and Fields

(vi) there exists $1 \in R$ such that

$1 \cdot a = a \cdot 1 = a$. (existence of multiplicative identity)

(vii) $a \cdot (b + c) = a \cdot b + a \cdot c$

and $(b + c) \cdot a = b \cdot a + c \cdot a$. (distributivity)

- Axioms (i)–(iv) are equivalent to saying that $(R, +)$ is an abelian group.
- The ring $(R, +, \cdot)$ is called a commutative ring if, in addition,
- (viii) $a \cdot b = b \cdot a$ for all $a, b \in R$. (commutativity of multiplication)

5

1. Rings, Integral Domains and Fields

- The integers under addition and multiplication satisfy all of the axioms above, so that $(\mathbb{Z}, +, \cdot)$ is a commutative ring. Also, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are all commutative rings. If there is no confusion about the operations, we write only R for the ring $(R, +, \cdot)$. Therefore, the rings above would be referred to as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or \mathbb{C} . Moreover, if we refer to a ring R without explicitly defining its operations, it can be assumed that they are addition and multiplication.
- Many authors do not require a ring to have a multiplicative identity, and most of the results we prove can be verified to hold for these objects as well. We must show that such an object can always be embedded in a ring that does have a multiplicative identity.

6

1. Rings, Integral Domains and Fields

- **Example 1.1.1.** Show that $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, where addition and multiplication on congruence classes, modulo n , are defined by the equations $[x] + [y] = [x + y]$ and $[x] \cdot [y] = [xy]$.
- *Solution.* It is well known that $(\mathbb{Z}_n, +)$ is an abelian group. Since multiplication on congruence classes is defined in terms of representatives, it must be verified that it is well defined. Suppose that $[x] = [x']$ and $[y] = [y']$, so that $x \equiv x' \pmod n$ and $y \equiv y' \pmod n$. This implies that $x = x' + kn$ and $y = y' + ln$ for some $k, l \in \mathbb{Z}$. Now $x \cdot y = (x' + kn) \cdot (y' + ln) = x' \cdot y' + (ky' + lx' + kln)n$, so $x \cdot y \equiv x' \cdot y' \pmod n$ and hence $[x \cdot y] = [x' \cdot y']$. This shows that multiplication is well defined.

7

1. Rings, Integral Domains and Fields

The remaining axioms now follow from the definitions of addition and multiplication and from the properties of the integers. The zero is $[0]$, and the unit is $[1]$. The left distributive law is true, for example, because

$$\begin{aligned} [x] \cdot ([y] + [z]) &= [x] \cdot [y + z] = [x \cdot (y + z)] \\ &= [x \cdot y + x \cdot z] \text{ by distributivity in } \mathbb{Z} \\ &= [x \cdot y] + [x \cdot z] = [x] \cdot [y] + [x] \cdot [z]. \end{aligned}$$

8

Example. The “linear equation” on \mathbb{Z}_m

$$[x]_m + [a]_m = [b]_m$$

where $[a]_m$ and $[b]_m$ are given, has a unique solution:

$$[x]_m = [b]_m - [a]_m = [b - a]_m$$

Let $m = 26$ so that the equation $[x]_{26} + [3]_{26} = [b]_{26}$ has a unique solution for any $[b]_{26}$ in \mathbb{Z}_{26} .

It follows that the function $[x]_{26} \rightarrow [x]_{26} + [3]_{26}$ is a bijection of \mathbb{Z}_{26} to itself.

We can use this to define the Caesar’s **encryption**: the English letters are represented in a natural way by the elements of \mathbb{Z}_{26} : $A \rightarrow [0]_{26}$, $B \rightarrow [1]_{26}$, ..., $Z \rightarrow [25]_{26}$
 For simplicity, we write: $A \rightarrow 0$, $B \rightarrow 1$, ..., $Z \rightarrow 25$

- These letters are encrypted so that A is **encrypted** by the letters represented by $[0]_{26} + [3]_{26} = [3]_{26}$, i.e. D.
- Similarly B is encrypted by the letters represented by $[1]_{26} + [3]_{26} = [4]_{26}$, i.e. E, ... and finally Z is encrypted by $[25]_{26} + [3]_{26} = [2]_{26}$, i.e. C.
- In this way the message “MEET YOU IN THE PARK” is encrypted as

M	E	E	T		Y	O	U		I	N		T	H	E		P	A	R	K	
12	4	4	19		24	14	20		8	13		19	7	4		15	0	17	10	
↓	↓	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	↓
15	7	7	22		1	17	23		11	16		22	10	7		18	3	20	13	
P	H	H	W		B	R	X		L	Q		W	K	H		S	D	U	N	

- To **decrypt** a message, we use the inverse function:

$$[x]_{26} \rightarrow [x]_{26} - [3]_{26} = [x - 3]_{26}$$

P H H W is represented by 15 7 7 22



And hence decrypted by 12 4 4 19

The corresponding
decrypted message is M E E T

However this simple encryption method is easily detected.

- We can improve the encryption using the function

$$f: [x]_{26} \rightarrow [ax + b]_{26}$$

where a and b are constants chosen so that this function is a bijection

First we choose an **invertible** element a in \mathbb{Z}_{26} i.e. there exists a' in \mathbb{Z}_{26} such that

$$[a]_{26} [a']_{26} = [a a']_{26} = [1]_{26}$$

We write $[a']_{26} = [a]_{26}^{-1}$ if it exists.

The solution of the equation

$$[a]_{26} [x]_{26} = [c]_{26}$$

is $[x]_{26} = [a]_{26}^{-1} [c]_{26} = [a'c]_{26}$

We also say that the solution of the linear congruence

$$ax \equiv c \pmod{26}$$

is $x \equiv a'c \pmod{26}$

Now the inverse function of f is given by

$$[x]_{26} \rightarrow [a'(x - b)]_{26}$$

Example. Let $a = 7$ and $b = 3$, then the inverse of $[7]_{26}$ is $[15]_{26}$ since $[7]_{26}[15]_{26} = [105]_{26} = [1]_{26}$

Now the letter M is encrypted as

$$[12]_{26} \rightarrow [7 \cdot 12 + 3]_{26} = [87]_{26} = [9]_{26}$$

which corresponds to I. Conversely I is decrypted as

$$[9]_{26} \rightarrow [15 \cdot (9 - 3)]_{26} = [90]_{26} = [12]_{26}$$

which corresponds to M.

To obtain more secure encryption method, more sophisticated modular functions can be used

1. Rings, Integral Domains and Fields

- **Example 1.1.2.** Show that $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ is a commutative ring where $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

Solution. The set $\mathbb{Q}(\sqrt{2})$ is a subset of \mathbb{R} , and the addition and multiplication is the same as that of real numbers. First, we check that $+$ and \cdot are binary operations on $\mathbb{Q}(\sqrt{2})$. If $a, b, c, d \in \mathbb{Q}$, we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

since $(a + c)$ and $(b + d) \in \mathbb{Q}$. Also,

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

since $(ac + 2bd)$ and $(ad + bc) \in \mathbb{Q}$.

14

1. Rings, Integral Domains and Fields

- We now check that axioms (i)–(viii) of a commutative ring are valid in $\mathbb{Q}(\sqrt{2})$.
 - (i) Addition of real numbers is associative.
 - (ii) Addition of real numbers is commutative.
 - (iii) The zero is $0 = 0 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
 - (iv) The additive inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, since $(-a)$ and $(-b) \in \mathbb{Q}$.
 - (v) Multiplication of real numbers is associative.
 - (vi) The multiplicative identity is $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
 - (vii) The distributive axioms hold for real numbers and hence hold for elements of $\mathbb{Q}(\sqrt{2})$.
 - (viii) Multiplication of real numbers is commutative.

15

1. Rings, Integral Domains and Fields

- 1.2. Integral Domains and Fields
- One very useful property of the familiar number systems is the fact that if $ab = 0$, then either $a = 0$ or $b = 0$. This property allows us to cancel nonzero elements because if $ab = ac$ and $a \neq 0$, then $a(b - c) = 0$, so $b = c$. However, this property does not hold for all rings. For example, in \mathbb{Z}_4 , we have $[2] \cdot [2] = [0]$, and we cannot always cancel since $[2] \cdot [1] = [2] \cdot [3]$, but $[1] \neq [3]$.
- If $(R, +, \cdot)$ is a commutative ring, a nonzero element $a \in R$ is called a *zero divisor* if there exists a nonzero element $b \in R$ such that $a \cdot b = 0$. A nontrivial commutative ring is called an *integral domain* if it has no zero divisors.

16

1. Rings, Integral Domains and Fields

- A *field* is a ring in which the nonzero elements form an abelian group under multiplication. In other words, a field is a nontrivial commutative ring R satisfying the following extra axiom.
 - (ix) For each nonzero element $a \in R$ there exists $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$.
- The rings $\mathbb{Q}, \mathbb{R},$ and \mathbb{C} are all fields, but the integers do not form a field.
- **Proposition 1.2.1.** *Every field is an integral domain; that is, it has no zero divisors.*

17

1. Rings, Integral Domains and Fields

- **Theorem 1.2.2.** *A finite integral domain is a field.*
- *Proof.* Let $D = \{x_0, x_1, x_2, \dots, x_n\}$ be a finite integral domain with x_0 as 0 and x_1 as 1. We have to show that every nonzero element of D has a multiplicative inverse.

If x_i is nonzero, we show that the set $x_i D = \{x_i x_0, x_i x_1, x_i x_2, \dots, x_i x_n\}$ is the same as the set D . If $x_i x_j = x_i x_k$, then, by the cancellation property, $x_j = x_k$. Hence all the elements $x_i x_0, x_i x_1, x_i x_2, \dots, x_i x_n$ are distinct, and $x_i D$ is a subset of D with the same number of elements. Therefore, $x_i D = D$. But then there is some element, x_j , such that $x_i x_j = x_1 = 1$.

Hence $x_j = x_i^{-1}$, and D is a field

18

1. Rings, Integral Domains and Fields

- **Theorem 1.2.3.** *\mathbb{Z}_n is a field if and only if n is prime.*
- *Proof.* Suppose that n is prime and that $[a] \cdot [b] = [0]$ in \mathbb{Z}_n . Then $n|ab$. So $n|a$ or $n|b$ by Euclid's Lemma.

Hence $[a] = [0]$ or $[b] = [0]$, and \mathbb{Z}_n is an integral domain. Since \mathbb{Z}_n is also finite, it follows from Theorem 1.2.2 that \mathbb{Z}_n is a field.

Suppose that n is not prime. Then we can write $n = rs$, where r and s are integers such that $1 < r < n$ and $1 < s < n$. Now $[r] = [0]$ and $[s] = [0]$ but $[r] \cdot [s] = [rs] = [0]$. Therefore, \mathbb{Z}_n has zero divisors and hence is not a field.

19

1. Rings, Integral Domains and Fields

Example 2.1.2. *Is $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ an integral domain or a field?*

Solution. From Example 1.1.2 we know that $\mathbb{Q}(\sqrt{2})$ is a commutative ring. Let $a + b\sqrt{2}$ be a nonzero element, so that at least one of a and b is not zero. Hence $a - b\sqrt{2} \neq 0$ (because $\sqrt{2}$ is not in \mathbb{Q}), so we have

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2}.$$

This is an element of $\mathbb{Q}(\sqrt{2})$, and so is the inverse of $a + b\sqrt{2}$. Hence $\mathbb{Q}(\sqrt{2})$ is a field (and an integral domain).

20

1. Rings, Integral Domains and Fields

- 1.3.SUBRINGS AND MORPHISMS OF RINGS
- If $(R, +, \cdot)$ is a ring, a nonempty subset S of R is called a *subring* of R if for all $a, b \in S$:
 - $a + b \in S$.
 - $-a \in S$.
 - $a \cdot b \in S$.
 - $1 \in S$.
- Conditions (i) and (ii) imply that $(S, +)$ is a subgroup of $(R, +)$ and can be replaced by the condition $a - b \in S$.

21

1. Rings, Integral Domains and Fields

- For example, \mathbb{Z}, \mathbb{Q} , and \mathbb{R} are all subrings of \mathbb{C} . Let D be the set of $n \times n$ real diagonal matrices. Then D is a subring of the ring of all $n \times n$ real matrices, $M_n(\mathbb{R})$, because the sum, difference, and product of two diagonal matrices is another diagonal matrix. Note that D is commutative even though $M_n(\mathbb{R})$ is not.
- Example 1.3.1. Show that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subring of \mathbb{R} . *Solution.* Let $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Then
 - $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
 - $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
 - $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
 - $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

22

1. Rings, Integral Domains and Fields

- A *homomorphism* between two rings is a function between their underlying sets that preserves the two operations of addition and multiplication and also the element 1. Many authors use the term *morphism* instead of *homomorphism*.
- More precisely, let $(R, +, \cdot)$ and $(S, +, \cdot)$ be two rings. The function $f: R \rightarrow S$ is called a *ring morphism* if for all $a, b \in R$:
 - $f(a + b) = f(a) + f(b)$.
 - $f(a \cdot b) = f(a) \cdot f(b)$.
 - $f(1) = 1$.
- A *ring isomorphism* is a bijective ring morphism. If there is an isomorphism between the rings R and S , we say R and S are *isomorphic rings* and write $R \cong S$.

23

1. Rings, Integral Domains and Fields

- Example 1.3.2.** Show that $f: \mathbb{Z}_{24} \rightarrow \mathbb{Z}_4$, defined by $f([x]_{24}) = [x]_4$ is a ring morphism.
- Proof.* Since the function is defined in terms of representatives of equivalence classes, we first check that it is well defined. If $[x]_{24} = [y]_{24}$, then $x \equiv y \pmod{24}$ and $24 \mid (x - y)$. Hence $4 \mid (x - y)$ and $[x]_4 = [y]_4$, which shows that f is well defined. We now check the conditions for f to be a ring morphism.
 - $f([x]_{24} + [y]_{24}) = f([x + y]_{24}) = [x + y]_4 = [x]_4 + [y]_4$.
 - $f([x]_{24} \cdot [y]_{24}) = f([xy]_{24}) = [xy]_4 = [x]_4 \cdot [y]_4$.
 - $f([1]_{24}) = [1]_4$.

24

2. Polynomial and Euclidean Rings

- 2.1. Polynomial Rings
- 2.2. Euclidean Rings

25

2. Polynomial and Euclidean Rings

- 2.1. Polynomial Rings
- If R is a commutative ring, a *polynomial* $p(x)$ in the indeterminate x over the ring R is an expression of the form $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, where $a_0, a_1, a_2, \dots, a_n \in R$ and $n \in \mathbb{N}$. The element a_i is called the *coefficient* of x^i in $p(x)$. If the coefficient of x^i is zero, the term $0x^i$ may be omitted, and if the coefficient of x^i is one, $1x^i$ may be written simply as x^i . Two polynomials $f(x)$ and $g(x)$ are called *equal* when they are identical, that is, when the coefficient of x^n is the same in each polynomial for every n . In particular, $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = 0$ is the zero polynomial if and only if $a_0 = a_1 = a_2 = \dots = a_n = 0$

26

2. Polynomial and Euclidean Rings

- If n is the largest integer for which $a_n \neq 0$, we say that $p(x)$ has *degree* n and write $\deg p(x) = n$. If all the coefficients of $p(x)$ are zero, then $p(x)$ is called the *zero polynomial*, and its degree is not defined. The set of all polynomials in x with coefficients from the commutative ring R is denoted by $R[x]$. That is, $R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R, n \in \mathbb{N}\}$.
- This forms a ring $(R[x], +, \cdot)$ called the *polynomial ring with coefficients from R* when addition and multiplication of the polynomials

27

2. Polynomial and Euclidean Rings

- For example, in $\mathbb{Z}_5[x]$, the polynomial ring with coefficients in the integers modulo 5, we have $(2x^3 + 2x^2 + 1) + (3x^2 + 4x + 1) = 2x^3 + 4x + 2$ and $(2x^3 + 2x^2 + 1) \cdot (3x^2 + 4x + 1) = x^5 + 4x^4 + 4x + 1$. When working in $\mathbb{Z}_n[x]$, the coefficients, but not the exponents, are reduced
- **Proposition 2.2.2** If R is an integral domain and $p(x)$ and $q(x)$ are nonzeropolynomials in $R[x]$, then $\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$

28

2. Polynomial and Euclidean Rings

- 2.2. Euclidean Rings
 - An integral domain R is called a **Euclidean ring** if for each nonzero element $a \in R$, there exists a nonnegative integer $\delta(a)$ such that:
 - (i) If a and b are nonzero elements of R , then $\delta(a) \leq \delta(ab)$.
 - (ii) For every pair of elements $a, b \in R$ with $b \neq 0$, there exist elements $q, r \in R$ such that $a = qb + r$ where $r = 0$ or $\delta(r) < \delta(b)$. (division algorithm)
- Ring \mathbb{Z} of integers is a euclidean ring if we take $\delta(b) = |b|$, the absolute value of b , for all $b \in \mathbb{Z}$. A field is trivially a euclidean ring when $\delta(a) = 1$ for all nonzero elements a of the field.
- Ring of polynomials, with coefficients in a field, is a euclidean ring when we take $\delta(g(x))$ to be the degree of the polynomial $g(x)$.

29

2. Polynomial and Euclidean Rings

- **EUCLIDEAN ALGORITHM**
 - The division algorithm allows us to generalize the concepts of divisors and greatest common divisors to any euclidean ring. Furthermore, we can produce a euclidean algorithm that will enable us to calculate greatest common divisors.
 - If a, b, q are three elements in an integral domain such that $a = qb$, we say that b divides a or that b is a factor of a and write $b|a$. For example, $(2 + i)|(7 + i)$ in the gaussian integers, $\mathbb{Z}[i]$, because $7 + i = (3 - i)(2 + i)$.
- Proposition 2.2.1.** Let a, b, c be elements in an integral domain R .
- (i) If $a|b$ and $a|c$, then $a|(b + c)$.
 - (ii) If $a|b$, then $a|br$ for any $r \in R$.
 - (iii) If $a|b$ and $b|c$, then $a|c$.

30

2. Polynomial and Euclidean Rings

- By analogy with \mathbb{Z} , if a and b are elements in an integral domain R , then the element $g \in R$ is called a *greatest common divisor* of a and b , and is written $g = \gcd(a, b)$, if the following hold:
 - (i) $g|a$ and $g|b$.
 - (ii) If $c|a$ and $c|b$, then $c|g$.
- The element $l \in R$ is called a *least common multiple* of a and b , and is written $l = \text{lcm}(a, b)$, if the following hold:
- (i) $a|l$ and $b|l$.
 - (ii) If $a|k$ and $b|k$, then $l|k$.

31

2. Polynomial and Euclidean Rings

- **Euclidean Algorithm.**
- Let a, b be elements of a euclidean ring R and let b be nonzero. By repeated use of the division algorithm, we can write
- $$a = bq_1 + r_1 \text{ where } \delta(r_1) < \delta(b)$$
- $$b = r_1q_2 + r_2 \text{ where } \delta(r_2) < \delta(r_1)$$
- $$r_1 = r_2q_3 + r_3 \text{ where } \delta(r_3) < \delta(r_2)$$
- ...
- $$r_{k-2} = r_{k-1}q_k + r_k \text{ where } \delta(r_k) < \delta(r_{k-1})$$
- $$r_{k-1} = r_kq_{k+1} + 0.$$
- If $r_1 = 0$, then $b = \gcd(a, b)$; otherwise, $r_k = \gcd(a, b)$.

32

2. Polynomial and Euclidean Rings

Furthermore, elements $s, t \in R$ such that $\gcd(a, b) = sa + tb$ can be found by starting with the equation $r_k = r_{k-2} - r_{k-1}q_k$ and successively working up the sequence of equations above, each time replacing r_i in terms of r_{i-1} and r_{i-2} .

- **Example 2.1.1.** Find the greatest common divisor of 713 and 253 in \mathbb{Z} and find two integers s and t such that $713s + 253t = \gcd(713, 253)$.

Solution. By the division algorithm,

we have (i) $713 = 2 \cdot 253 + 207$ $a = 713, b = 253, r_1 = 207$

(ii) $253 = 1 \cdot 207 + 46$ $r_2 = 46$

(iii) $207 = 4 \cdot 46 + 23$ $r_3 = 23$

$46 = 2 \cdot 23 + 0. r_4 = 0$

33

2. Polynomial and Euclidean Rings

- The last nonzero remainder is the greatest common divisor. Hence

$$\gcd(713, 253) = 23.$$

We can find the integers s and t by using equations (i)–(iii). We have

$$23 = 207 - 4 \cdot 46 \text{ from equation (iii)}$$

$$= 207 - 4(253 - 207) \text{ from equation (ii)}$$

$$= 5 \cdot 207 - 4 \cdot 253$$

$$= 5 \cdot (713 - 2 \cdot 253) - 4 \cdot 253 \text{ from equation (i)}$$

$$= 5 \cdot 713 - 14 \cdot 253.$$

- Therefore, $s = 5$ and $t = -14$.

34

2. Polynomial and Euclidean Rings

- **Example 2.2.2.** Find the inverse of $[49]$ in the field \mathbb{Z}_{53}
- *Solution.* Let $[x] = [49]^{-1}$ in \mathbb{Z}_{53} . Then $[49] \cdot [x] = [1]$; that is, $49x \equiv 1 \pmod{53}$. We can solve this congruence by solving the equation $49x - 1 = 53y$, where $y \in \mathbb{Z}$. By using the euclidean algorithm we have

$$53 = 1 \cdot 49 + 4 \text{ and } 49 = 12 \cdot 4 + 1.$$

Hence

$$\gcd(49, 53) = 1 = 49 - 12 \cdot 4 = 49 - 12(53 - 49)$$

$$= 13 \cdot 49 - 12 \cdot 53.$$

Therefore, $13 \cdot 49 \equiv 1 \pmod{53}$ and $[49]^{-1} = [13]$ in \mathbb{Z}_{53} .

35

3. Ideals and quotient rings

- 3.1. Ideals
- 3.2. Quotient rings

36

3. Ideals and quotient rings

- 3.1. Ideals.

A nonempty subset I of a ring R is called an ideal of R if the following conditions are satisfied for all $x, y \in I$ and $r \in R$:

- (i) $x - y \in I$.
- (ii) $x \cdot r$ and $r \cdot x \in I$.

Condition (i) implies that $(I, +)$ is a subgroup of $(R, +)$. In any ring R , R itself is an ideal, and $\{0\}$ is an ideal.

- **Proposition 3.1.1.** *Let a be an element of commutative ring R . The set $\{ar \mid r \in R\}$ of all multiples of a is an ideal of R called the principal ideal generated by a . This ideal is denoted by (a) .*

37

3. Ideals and quotient rings

- For example, $(n) = n\mathbb{Z}$, consisting of all integer multiples of n , is the principal ideal generated by n in \mathbb{Z} .
- The set of all polynomials in $\mathbb{Q}[x]$ that contain $x^2 - 2$ as a factor is the principal ideal $(x^2 - 2) = \{(x^2 - 2) \cdot p(x) \mid p(x) \in \mathbb{Q}[x]\}$ generated by $x^2 - 2$ in $\mathbb{Q}[x]$.
- The set of all real polynomials that have zero constant term is the principal ideal $(x) = \{x \cdot p(x) \mid p(x) \in \mathbb{R}[x]\}$ generated by x in $\mathbb{R}[x]$. It is also the set of real polynomials with 0 as a root.
- The set of all real polynomials, in two variables x and y , that have a zero constant term is an ideal of $\mathbb{R}[x, y]$. However, this ideal is not principal.

38

3. Ideals and quotient rings

- However, every ideal is principal in many commutative rings; these are called *principal ideal rings*.
- **Theorem 3.1.1.** *A euclidean ring is a principal ideal ring.*
- **Corollary 3.1.2.** *\mathbb{Z} is a principal ideal ring, so is $F[x]$, if F is a field.*
- **Proposition 3.1.3.** *Let I be ideal of the ring R . If I contains the identity 1, then I is the entire ring R .*

39

3. Ideals and quotient rings

- 3.2. Quotient rings.
- **Theorem 3.2.1.** *Let I be an ideal in the ring R . Then the set of cosets forms a ring $(R/I, +, \cdot)$ under the operations defined by*

$$(I + r_1) + (I + r_2) = I + (r_1 + r_2)$$
and

$$(I + r_1)(I + r_2) = I + (r_1 r_2).$$
This ring $(R/I, +, \cdot)$ is called the quotient ring (or factor ring) of R by I

40

3. Ideals and quotient rings

Example 3.2.1. If $I = \{0, 2, 4\}$ is the ideal generated by 2 in \mathbb{Z}_6 , find the tables for the quotient ring \mathbb{Z}_6/I .

Solution. There are two cosets of \mathbb{Z}_6 by I : namely,

$$I = \{0, 2, 4\} \text{ and } I + 1 = \{1, 3, 5\}. \text{ Hence } \mathbb{Z}_6/I = \{I, I + 1\}.$$

The addition and multiplication tables given in Table 10.1 show that the quotient ring \mathbb{Z}_6/I is isomorphic to \mathbb{Z}_2 .

TABLE 10.1. Quotient Ring $\mathbb{Z}_6/\{0, 2, 4\}$

+	I	I + 1	·	I	I + 1
I	I	I + 1	I	I	I
I + 1	I + 1	I	I + 1	I	I + 1

41

3. Ideals and quotient rings

- **Theorem 3.2.2. Morphism Theorem for Rings.** If $f: R \rightarrow S$ is a ring morphism, then $R/\text{Ker} f$ is isomorphic to $\text{Im} f$.
- This result is also known as the first isomorphism theorem for rings.
- *Proof.* Let $K = \text{Ker} f$. It follows from the morphism theorem for groups, that $\psi: R/K \rightarrow \text{Im} f$, defined by $\psi(K + r) = f(r)$, is a group isomorphism. Hence we need only prove that ψ is a ring morphism. We have $\psi\{(K + r)(K + s)\} = \psi\{K + rs\} = f(rs) = f(r)f(s) = \psi(K + r)\psi(K + s)$

42

3. Ideals and quotient rings

- Example 3.2.1. Prove that $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.
- Solution. Consider the ring morphism $\psi: \mathbb{Q}[x] \rightarrow \mathbb{R}$ defined by $\psi(f(x)) = f(\sqrt{2})$. The kernel is the set of polynomials containing $x^2 - 2$ as a factor, that is, the principal ideal $(x^2 - 2)$. The image of ψ is $\mathbb{Q}(\sqrt{2})$, so by the morphism theorem for rings, $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.
- In this isomorphism, the element $a_0 + a_1x \in \mathbb{Q}[x]/(x^2 - 2)$ is mapped to $a_0 + a_1\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Addition and multiplication of the elements $a_0 + a_1x$ and $b_0 + b_1x$ in $\mathbb{Q}[x]/(x^2 - 2)$ correspond to the addition and multiplication of the real numbers $a_0 + a_1\sqrt{2}$ and $b_0 + b_1\sqrt{2}$.

43