Abstract algebras

Yanhua Wang
Shanghai University of Finance and Economics

2022.9

1. Chapter III. Rings

3.1 Rings

Sets

Definition

If a non-empty set R has two closed binary operations: addition and multiplication,
satisfying the following conditions, for $a, b, c \in R$
(1) $a + b = b + a$
(2) $(a + b) + c = a + (b + c)$
(3) There is an element $0 \in R$ such that $0 + a = a$.
(4) There exists an element $-a \in R$ such that $a + (-a) = 0$.
(5) $(ab)c = a(bc)$.
(6) $a(b + c) = ab + ac; (a + b)c = ac + bc$.
$(R, +, \cdot)$ is called a **ring.**

- A **ring** is an abelian group $(R, +)$ together with a second binary operation satisfying

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

Sets

- If $ab = ba, \forall a, b \in R$, we call R an abelian ring.

Sets

- If $ab = ba, \forall a, b \in R$, we call R an abelian ring.

Example

Let $R = \{0\}$ and $0+0 = 0, 0 \cdot 0 = 0$. Then R is a ring. R is called zero ring. It is obvious that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are rings with identity.

-

Sets

- If $ab = ba, \forall a, b \in R$, we call R an abelian ring.

Example

Let $R = \{0\}$ and $0+0 = 0, 0 \cdot 0 = 0$. Then R is a ring. R is called zero ring. It is obvious that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are rings with identity.

-

Definition

If there is an element $1_R \in R$ such that $1_R \neq 0$ and

$$1_R a = a 1_R, \forall a \in R,$$

we say R is a ring with unit or identity.

-

Sets

Example

Let $2\mathbb{Z} = \{2z | z \in \mathbb{Z}\}$ is a ring. There is no identity in $2\mathbb{Z}$.

-

Sets

Example

Let $2\mathbb{Z} = \{2z|z \in \mathbb{Z}\}$ is a ring. There is no identity in $2\mathbb{Z}$.

-

Example

$M_n(R)$ is a ring with addition and multiplication of matrix. This ring is called **Full-matrix ring.**

-

Example

Let $2\mathbb{Z} = \{2z | z \in \mathbb{Z}\}$ is a ring. There is no identity in $2\mathbb{Z}$.

-

Example

$M_n(R)$ is a ring with addition and multiplication of matrix. This ring is called **Full-matrix ring.**

-

Example

The continuous real-valued functions on an interval $[a, b]$ form a commutative ring by defining $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$.

-

Sets

Definition

A nonzero element $a \in R$ is called a *zero divisor* if there is a non-zero element b, such that $ab = 0$.

-

Sets

Definition

A nonzero element $a \in R$ is called a *zero divisor* if there is a non-zero element b, such that $ab = 0$.

-
- $\overline{2}, \overline{3} \in \mathbb{Z}_6$, we have $\overline{2} \cdot \overline{3} = 0$. So $\overline{2}$ and $\overline{3}$ are zero divisors.

Sets

Definition

A nonzero element $a \in R$ is called a *zero divisor* if there is a non-zero element b, such that $ab = 0$.

-
- $\overline{2}, \overline{3} \in \mathbb{Z}_6$, we have $\overline{2} \cdot \overline{3} = 0$. So $\overline{2}$ and $\overline{3}$ are zero divisors.
- There is no zero divisor in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Sets

Definition

A commutative ring with identity is called an *integral domain* if for any $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

-

Sets

Definition

A commutative ring with identity is called an *integral domain* if for any $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

-
- We have $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are integral domains.

Definition

A commutative ring with identity is called an *integral domain* if for any $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

-
- We have $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are integral domains.
- $\mathbb{Z}_6$ is not a integral domain.

Sets

Definition

A *divisor ring* R is a ring with identity in which every nonzero element in R is a unit (that is for each nonzero $a \in R$, there exists an unique element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.)

-

Sets

Definition

A *divisor ring* R is a ring with identity in which every nonzero element in R is a unit (that is for each nonzero $a \in R$, there exists an unique element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.)

-
- A commutative divisor ring is called a *field*.

Sets

Definition

A *divisor ring* R is a ring with identity in which every nonzero element in R is a unit (that is for each nonzero $a \in R$, there exists an unique element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.)

-
- A commutative divisor ring is called a *field*.
- $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields. $(\mathbb{Z}_n, +, \cdot)$ is a ring, but it is neither an integral domain nor a divisor ring.

Sets

Example

$(M_{2\times 2}(\mathbb{R}), +, \cdot)$ is a ring with identity E_2, which is not commutative. Moreover it is neither an integral domain nor a divisor ring, thus it is not a field.

-

Sets

Example

Let Q_8 be the quaternion group. We have

$$\mathcal{Q} = \{a + bI + cJ + dK | a, b, c, d \in \mathbb{R}\}$$

is a noncommutative divisor ring, called the ring of *quaternions*. $\mathcal{Q}$ is a divisor ring. In fact, for every $a + bI + cJ + dK$, we have $a - bI - cJ - dK$ such that

$$(a + bI + cJ + dK)(a - bI - cJ - dK) = a^2 + b^2 + c^2 + d^2.$$

This element can be zero only if a, b, c and d are all zero. So if $a + bI + cJ + dK \neq 0$,

$$(a + bI + cJ + dK)\left(\frac{a - bI - cJ - dK}{a^2 + b^2 + c^2 + d^2}\right) = 1$$

Proposition

Let R be a ring with a and b in R. Then
(1) $a0 = 0a = 0$;
(2) $a(-b) = (-a)b = -ab$;
(3) $(-a)(-b) = ab$;
(4) $\forall a \in R, -a = -1_R a = a(-1_R)$;
(5) $\forall a, b \in R$ *and* $n \in \mathbb{Z}$, $n(ab) = (an)b = a(nb)$;
(6) $(n1_R)a = a(n1_R) = na$;
(7) Given $a_1, a_2, \cdots, a_m$ *and* $b_1, b_2, \cdots, b_n \in \mathbb{R}$,

$$(a_1 + a_2 + \cdots + a_m)(b_1 + b_2 + \cdots + b_n) = \sum_{i=1}^{m} a_i \sum_{j=1}^{n} b_j.$$

-

- Proof: (1) $a0 = a(0+0) = a0 + a0$. Solving the equation, we have $a0 = 0$. Similarly, $0a = 0$.

- Proof: (1) $a0 = a(0+0) = a0 + a0$. Solving the equation, we have $a0 = 0$. Similarly, $0a = 0$.
- (2) Since $ab + a(-b) = a(b + (-b)) = a0 = 0$, $a(-b) = -ab$.
- (3) Following from (2), $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.
- (4) $a(-1_R) = -(a1_R) = -a = -(1_R a)$.
- (5) Prove by the mathematical induction. If $n = 0$, $0(ab) = 0 = (0a)b = a(0b)$. Assume that it is true for m, which is to say $m(ab) = (ma)b = a(mb)$. Then $(m+1)ab = mab + ab = (ma + a)b = a((m+1)b)$.

- (6) $(n1_R)a = a(1_R n) = na = n(a1_R) = na.$

- (6) $(n1_R)a = a(1_R n) = na = n(a1_R) = na.$
- (7) Prove by the mathematical induction. When $n = 1$,

$$
\begin{aligned}
&(a_1 + a_2 + \cdots + a_m)b = (a_1 + (a_2 + \cdots + a_m))b \\
=&a_1 b + (a_2 + \cdots + a_m)b = a_1 b + a_2 b + (a_3 + \cdots + a_m)b = \cdots \\
=&a_1 b + a_2 b + \cdots + a_m b = \sum_{i=1}^{m} a_i b
\end{aligned}
$$

Assume that it is true for $s - 1$. When $n = s$,

$$
\begin{aligned}
&(a_1 + a_2 + \cdots + a_m)(b_1 + b_2 + \cdots + b_s) \\
=&(a_1 + a_2 + \cdots + a_m)(b_1 + b_2 + \cdots + b_{s-1}) + (a_1 + a_2 + \cdots + a_m) \\
=&\sum_{i=1}^{m} a_i \sum_{j=1}^{s-1} b_j + \sum_{i=1}^{m} a_i b_s \\
=&\sum_{i=1}^{m} a_i \sum_{j=1}^{s} b_j.
\end{aligned}
$$

Proposition

Let D be a commutative ring with identity. The D is an integral domain if and only if for all nonzero elements $a \in D$ with $ab = ac$, we have $b = c$.

-

Proposition

Let D be a commutative ring with identity. The D is an integral domain if and only if for all nonzero elements $a \in D$ with ab=ac, we have b=c.

-
- Proof let D be an integral domain, then D has no zero divisors. Suppose that $ab = ac$ and $a \neq 0$, then $0 = a \cdot b - a \cdot c = a \cdot (b - c)$. Then $b - c = 0$, i.e. $b = c$.

Proposition

Let D be a commutative ring with identity. The D is an integral domain if and only if for all nonzero elements $a \in D$ with ab=ac, we have b=c.

-
- Proof let D be an integral domain, then D has no zero divisors. Suppose that $ab = ac$ and $a \neq 0$, then $0 = a \cdot b - a \cdot c = a \cdot (b - c)$. Then $b - c = 0$, i.e. $b = c$.
- Conversely, suppose that the cancellation law is true in D. That is, suppose that $ab = ac$ implies $b = c$. Let $ab = 0$. If $a \neq 0$, then $ab = 0 = a \cdot 0$ implies $b = 0$. Therefore, a can not be a zero divisor. So there is nonzero division, D is an integral domain.

Proposition

Every finite integral domain is a field.

-

Proposition

Every finite integral domain is a field.

-

Proof.

Let D be a finite integral domain, $D^* = D/\{0\}$. For each $a \in D^*$, define a map $\lambda_a : D^* \to D^*$ by $b \longmapsto ab$ for $a \in D$. Firstly, λ_a is well-defined since if $a \neq 0, b \neq 0$, then $ab \neq 0$ by D is integral domain. Next, λ_a is injective. Assume that $\lambda_a(b) = \lambda_a(c)$, i.e. $ab = ac$, then $b = c$ by the cancellation law. It is obvious that λ_a is surjective since D^* is a finite set, the map λ_a must also be surjective. Hence, for some $d \in D^*$, $\lambda_a(d) = ad = 1$, Therefore, a has a left inverse. Since D is commutative, d must be a right inverse for a. Consequently, D is a field. $\square$

-

Definition

The characteristic of a ring R is the least positive integer n such that $nr = 0$, for any $r \in R$. If no such integer exists, then the characteristic of R is defined to be 0. Denote as $char(R)$

-

Definition

The characteristic of a ring R is the least positive integer n such that $nr = 0$, for any $r \in R$. If no such integer exists, then the characteristic of R is defined to be 0. Denote as $char(R)$

-

Example

$\mathbb{Z}_p$ is a field if p is prime. Then $p\bar{a} = \bar{0}$, for $a \in \mathbb{Z}_p$, then $char(\mathbb{Z}_p) = p$. Moreover, we have

$$char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0.$$

-

Theorem

The characteristic of an integral domain is either prime or zero.

-

Theorem

The characteristic of an integral domain is either prime or zero.

-

Proof.

Let D be an integral domain, suppose that $char(D) = n, n \neq 0$. If n is not prime, then $n = a \cdot b$, where $1 < a < n, 1 < b < n$. Since $0 = n \cdot 1 = (a \cdot b)1 = (a \cdot 1)(b \cdot 1)$, note that D is integral domain, $a \cdot 1 = 0$ or $b \cdot 1 = 0$ If $a \cdot 1 = 0$, then $char(D) = a < n$. It is contradiction. The same for b. Hence, n must be prime. $\square$

-

3.2 Subrings and ideals

Subrings

Definition

Let $(R, +, \cdot)$be a ring. A *subring* S of R is a subset S of R such that $(S, +, \cdot)$ is a ring.

-

Subrings

Definition

Let $(R, +, \cdot)$be a ring. A *subring* S of R is a subset S of R such that $(S, +, \cdot)$ is a ring.

-

Example

The ring $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Notice that even though the original ring may have an identity, we do not require that its subring have an identity. We have the following chain of subrings: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

-

Proposition

Let R be a ring and S a subset of R. Then S is a subring of R if and only if the following conditions are satisfied.
(1) $S \neq \emptyset$.
(2) $r - s \in S$ *for all* $r, s \in S$.
(3) $rs \in S$ *for all* $r, s \in S$.

-

Proposition

Let R be a ring and S a subset of R. Then S is a subring of R if and only if the following conditions are satisfied.
(1) $S \neq \emptyset$.
(2) $r - s \in S$ for all $r, s \in S$.
(3) $rs \in S$ for all $r, s \in S$.

-

Proof.

If S is a subring, then $(S, +)$ is a subgroup of $(R, +)$, thus (1) and (2) hold. (3) is clear because S is a subring.
If S satisfy (1), (2) and (3), we have S is subgroup under "+" by (1) and (2). (3) means that S is closed under multiplication. S is a subset of R, so S is associative and distributive. Thus $(S, +, \cdot)$ is a subring of R. $\square$

Example

Let

$$R = M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

$$Tri = \left\{ \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \mid p, q, r \in \mathbb{R} \right\}.$$

Tri is a nonempty set. Let $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix}, \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \in T$, then

$$\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} = \begin{pmatrix} up & uq + vr \\ 0 & wr \end{pmatrix} \in T,$$

$$\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} - \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} = \begin{pmatrix} u - p & v - q \\ 0 & w - r \end{pmatrix} \in T$$

Then T is a subring of R.

Definition

A subring I of R is an ideal if $ar, ra \in I$, for $a \in I, r \in R$, or equivalent $rI \subseteq I, Ir \subseteq I$.

Example

$\{0\}$ and R are ideals of R. These two ideals are called trivial ideals.

-

Proposition

A nonempty set I of R is an ideal of R if
(1) $a, b \in I$, then $a - b \in I$.
(2) $a \in I, r \in R$, then $ar, ra \in I$.

Proof.

We have I is a commutative subgroup under "+" by (1). I is a subring by (1) and (2), and $ar, ra \in I$. Thus I of R is an ideal of R. $\square$

-

Example

$(\mathbb{Z}, + ,0)$. Take $n \neq 0, n \in \mathbb{Z}$.

$$I = \{rn \mid r \in \mathbb{Z}\} = \{\cdots, -2n, -n, 0, n, 2n \cdots\}$$

is an ideal of $\mathbb{Z}$ since $\mathbb{Z}I, I\mathbb{Z} \subseteq I$.
All ideals of $(\mathbb{Z}, +, 0)$ are $n\mathbb{Z}$ for every $n \neq 0$.

-

Example

Let$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in \mathbb{Z} \right\}$, then $I = \left\{ \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} | d \in \mathbb{Z} \right\}$ is an ideal of R.

Note that $J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | a, b \in \mathbb{Z} \right\}$ is not an ideal of $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z} \right\}$. Let $a, b, c, d, a_2, b_2 \in \mathbb{Z}$, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa_2 & b_2 \\ ca_2 & cb_2 \end{pmatrix} \neq J.$$

-

Example

R is a commutative, identity ring, $a \in R$,

$$I = \langle a \rangle = \{ar \mid r \in R\}$$

is an ideal of R. Since $0 = a0 \in \langle a \rangle$ and $a = a1 \in \langle a \rangle$, I is nonempty. If $ar_1 \in I, ar_2 \in I$, then $ar_1 - ar_2 = a(r_1 - r_2) \in I$. If $ar \in \langle a \rangle$, $s \in R$, we have $s(ar) = as(r) \in \langle a \rangle$. Thus $< a >$ is an ideal.

-

- Let R be a ring, $\forall a \in R$. Define

$$\begin{aligned}\mathcal{U} &= \{x_1ay_1 + x_2ay_2 + \cdots + x_may_m + sa + at + na | \\ &\quad x_i, y_i, s, t \in R, n \in \mathbb{Z}, i = 1, \cdots m\}.\end{aligned}$$

- Let R be a ring, $\forall a \in R$. Define

$$\begin{aligned}\mathcal{U} &= \{x_1 a y_1 + x_2 a y_2 + \cdots + x_m a y_m + sa + at + na | \\ &\quad x_i, y_i, s, t \in R, n \in \mathbb{Z}, i = 1, \cdots m\}.\end{aligned}$$

- $\mathcal{U}$ is an ideal.

- Let R be a ring, $\forall a \in R$. Define

$$\begin{aligned}\mathcal{U} &= \{x_1ay_1 + x_2ay_2 + \cdots + x_may_m + sa + at + na| \\ &\quad x_i, y_i, s, t \in R, n \in \mathbb{Z}, i = 1, \cdots m\}.\end{aligned}$$

- $\mathcal{U}$ is an ideal.
- In fact, if $u_1, u_2 \in \mathcal{U}$, $u_1 \pm u_2 \in \mathcal{U}$. For $r \in R$,

$$u = x_1ay_1 + x_2ay_2 + \cdots + x_may_m + sa + at + na,$$

then

$$\begin{aligned}& r(x_1ay_1 + x_2ay_2 + \cdots + x_may_m + sa + at + na) \\ = \;& rx_1ay_1 + rx_2ay_2 + \cdots + rx_may_m + rsa + rat + rna.\end{aligned}$$

Note that $rx_1, rx_2, \cdots, rx_m, rs, r, rn \in R$, $ru \in \mathcal{U}$. Similarly, $ur \in \mathcal{U}$.

Definition

Let R be a ring, $a \in R$, an ideal of the form

$$\begin{aligned}\langle a\rangle &= \{x_1ay_1 + x_2ay_2 + \cdots + x_may_m + sa + at + na \mid \\ &\quad x_i, y_i, s, t \in R, n \in \mathbb{Z}\}\end{aligned}$$

is called a *principal ideal.*

-

- (1) If R is a commutative ring, then

$$\langle a \rangle = \{ra + na | r \in R, n \in \mathbb{Z}\}.$$

- (1) If R is a commutative ring, then

$$\langle a\rangle = \{ra + na | r \in R, n \in \mathbb{Z}\}.$$

- (2) If R is a ring with identity, then

$$\langle a\rangle = \{\sum_i x_i a y_i | x_i, y_i \in R\}.$$

- (1) If R is a commutative ring, then

$$\langle a \rangle = \{ra + na | r \in R, n \in \mathbb{Z}\}.$$

- (2) If R is a ring with identity, then

$$\langle a \rangle = \{\sum_i x_i a y_i | x_i, y_i \in R\}.$$

- (3) If R is a commutative ring with identity , then

$$\langle a \rangle = \{ra | r \in R\}.$$

- Let R be a ring, $\forall a_1, a_2, \cdots, a_m \in R$. Define

$$\mathcal{I} = \{s_1 + s_2 + \cdots + s_m | s_i \in \langle a_i \rangle\},$$

Let $u = s_1 + s_2 + \cdots + s_m, u' = s'_1 + s'_2 + \cdots + s'_m \in \mathcal{I}$, then

$$u - u' = (s_1 - s'_1) + (s_2 - s'_2) + \cdots + (s_m - s'_m) \in \mathcal{I}.$$

Let $r \in R$, then $rs_i, rs'_i \in \langle a_i \rangle$ and

$ru = rs_1 + rs_2 + \cdots + rs_m \in \mathcal{I},\ ur = s_1 r + s_2 r + \cdots + s_m r \in \mathcal{I}$

Thus $\mathcal{I}$ is an ideal of R. Denote $\mathcal{I} = \langle a_1, a_2, \cdots, a_m \rangle$.

Theorem

There are only two ideals in a divisor ring i.e. trivial ideals.

-

Theorem

There are only two ideals in a divisor ring i.e. trivial ideals.

-

Proof.

Assume that I is an ideal of R. For $a \neq 0, a \in I$, there exists $a^{-1} \in R$ such that $a^{-1}a = aa^{-1} = 1$. Thus for any $b \in R$, $b = b1 \in I$, that means $I = R$. $\square$

-

Theorem

Every ideal in the ring of integers $\mathbb{Z}$ is a principle ideal.

-

Theorem

Every ideal in the ring of integers $\mathbb{Z}$ is a principle ideal.

-

Proof.

If $I = \langle 0 \rangle = \{0\}$, then I is a principle ideal. If $I \neq \{0\}$, then $I \subseteq \mathbb{Z}$. I is consisted by some integers in $\mathbb{Z}$. Let n be the smallest positive integer of I by the principle of well-ordering. For all $a \in I$, there exist $q, r \in \mathbb{Z}, 0 \leq r < n$, such that $a = nq + r$. That is $r = a - nq \in I$, but $r = 0$ since n is the least positive element in I. Therefore $a = nq$. So $I = \langle n \rangle$. $\square$

-

- Let $n \in \mathbb{Z}$. Note that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. If $na \in n\mathbb{Z}$, then $nab \in n\mathbb{Z}, b \in \mathbb{Z}$. All ideals of $\mathbb{Z}$ are $n\mathbb{Z}$. For example

$$
\begin{aligned}
\langle 4 \rangle &= \{\cdots - 8, -4, 0, 4, 8, \cdots\}, \\
\langle 2 \rangle &= \{\cdots - 4, -2, 0, 2, 4, \cdots\}.
\end{aligned}
$$

And $\langle 4 \rangle \subset \langle 2 \rangle$.

- Let R be a commutative ring with identity. Any expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 \cdots + a_nx^n,$$

where $a_i \in R$ and $a_n \neq 0$, is called a **polynomial** over R with indeterminate x. The elements $a_0, a_1, \cdots, a_n$ are called the coefficients of f. The coefficient a_n is called the leading coefficient.

- Let R be a commutative ring with identity. Any expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n,$$

where $a_i \in R$ and $a_n \neq 0$, is called a **polynomial** over R with indeterminate x. The elements $a_0, a_1, \cdots, a_n$ are called the coefficients of f. The coefficient a_n is called the leading coefficient.

- A polynomial is called **monic** if the leading coefficient is 1. If n is the largest nonnegative number for which $a_n \neq 0$, we say that the **degree** of f is n and write $\deg f(x) = n$. If no such n exists, then the degree of f is defined to be ∞.

- Denote the set of all polynomials with coefficients in a ring R by $R[x]$. $R[x]$ is a ring, we call it as **polynomial ring**.

- Denote the set of all polynomials with coefficients in a ring R by $R[x]$. $R[x]$ is a ring, we call it as **polynomial ring**.

Example

Let $p(x) = 3 + 3x^3$ and $q(x) = 4 + 4x^2 + 4x^4$ be polynomials in $\mathbb{Z}_{12}[x]$. Then

$$\begin{aligned} p(x) + q(x) &= 7 + 4x^2 + 3x^3 + 4x^4 \\ p(x)q(x) &= 0. \end{aligned}$$

This example tells us that we can not expect $R[x]$ to be an integral domain if R is not an integral domain.

-

- Let F be a field. A principal ideal in $F[x]$ is an ideal $\langle p(x) \rangle$ generated by some polynomial $p(x)$, that is,

$$\langle p(x) \rangle = \{p(x)q(x) | q(x) \in F[x]\}.$$

- Let F be a field. A principal ideal in $F[x]$ is an ideal $\langle p(x) \rangle$ generated by some polynomial $p(x)$, that is,

$$\langle p(x) \rangle = \{p(x)q(x) | q(x) \in F[x]\}.$$

- For example, the polynomial $x^2 \in F[x]$ generates the ideal $\langle x^2 \rangle$ consisting of all polynomials with no constant term or term of degree 1.

Theorem

Let F be a field. Then every ideal in $F[x]$ is a principal ideal.

-

Theorem

Let F be a field. Then every ideal in $F[x]$ is a principal ideal.

-
- Proof: Let I be an ideal of $F[x]$. If I is the zero ideal, the theorem is easily true. Suppose that I is a nontrivial ideal in $F[x]$, and let $p(x) \in I$ be a nonzero element of minimal degree. If $\deg p(x) = 0$, then $p(x)$ is a nonzero constant and 1 must be in I. Since 1 generates all of $F[x]$, $\langle 1 \rangle = I = F[x]$ and I is again a principal ideal.

- Now assume that $\deg p(x) \geq 1$ and let $f(x)$ be any element in I. By the division algorithm there exist $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = p(x)q(x) + r(x)$ and $\deg r(x) < \deg p(x)$. Since $f(x), p(x) \in I$ and I is an ideal, $r(x) = f(x) - p(x)q(x)$ is also in I. However, since we chose $p(x)$ to be of minimal degree, $r(x)$ must be the zero polynomial. Since we can write any element $f(x) \in I$ as $p(x)q(x)$ for some $q(x) \in F[x]$, it must be the case that $I = \langle p(x) \rangle$.

3.3 Ring homomorphisms

Definition

Let R and S be rings, a map $\phi : R \longrightarrow S$ is a ring homomorphism, if for all $a, b \in R$,

$$\begin{aligned} \phi(a+b) &= \phi(a)+\phi(b), \\ \phi(ab) &= \phi(a)\phi(b). \end{aligned}$$

The kernel of a ring homomorphism to be the set

$$Ker\phi = \{a \mid \phi(a) = 0, a \in R\}.$$

If $\phi : R \longrightarrow S$ is a bijection, then ϕ is called an isomorphism of rings.

- If there is an isomorphism $\phi : R \longrightarrow S$, we say R is isomorphic to S, denote $R \cong S$.

Examples:

Example

Let $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n : a \longmapsto a(\mod n)$ be a map. Then ϕ is a ring homomorphism, since

$$\begin{aligned} \phi(a+b) &= \phi(a)+\phi(b) \\ &= (a+b)(\mod n) \\ &= a(\mod n)+b(\mod n) \\ &= \phi(a)+\phi(b) \end{aligned}$$

and

$$\phi(ab) = ab(\mod n) = a(\mod n)b(\mod n) = \phi(a)\phi(b).$$

-

Example

Let $C[a,b]$ be the ring of continuous real-valued functions on an interval $[a,b]$. For a fixed $\alpha \in [a,b]$, we define a map

$$\begin{array}{rcl} \phi_\alpha : C[a,b] & \longrightarrow & \mathbb{R}, \\ f & \longmapsto & f(\alpha). \end{array}$$

This is a ring homomorphism since

$$\begin{array}{rcl} \phi_\alpha(f+g) & = & (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g), \\ \phi_\alpha(fg) & = & (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g). \end{array}$$

Ring homomorphisms of the type ϕ_α are called evaluation homomorphism.

Example

Let $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{R} \right\}$ be a subring of the matrix ring $M_2(\mathbb{R})$. Now define a map

$$\begin{aligned} \phi : R &\longrightarrow \mathbb{C}, \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} &\longrightarrow a + bi. \end{aligned}$$

Then ϕ is a ring homomorphism.

-

Proposition

Let $\phi : R \longrightarrow S$ be a ring homomorphism.
(1) If R is a commutative ring, then $\phi(R)$ is commutative.
(2) $\phi(0_R) = 0_S$.
(3) Let $1_R, 1_S$ be the identities for R and S. If ϕ is surjective, then $\phi(1_R) = 1_S$.
(4) If R is a field and $\phi(R) \neq 0$, then $\phi(R)$ is a field.

-

Proof.

(1) Let $a, b \in R$ and $ab = ba$. Then

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a).$$

S is commutative.
(2) Note that ϕ is a group homomorphism under addition, then $\phi(0_R) = 0_S$.
(3) Let $\phi(r) = 1_S$ by ϕ surjective. Then $1_S = \phi(r) = \phi(r1_R) = \phi(r)\phi(1_R) = 1_S\phi(1_R) = \phi(1_R)$. Thus $\phi(1_R) = 1_S$.
(4) R is a field, $1_R \in R$. Let $\phi(r) \in \phi(R)$, then $\phi(r) = \phi(r1_R) = \phi(r)\phi(1_R)$ for any $r \in R$, then $\phi(1_R)$ is the identity in $\phi(R)$. $\phi(R)$ is commutative since R is commutative. Let $a \in R, \phi(a) \in \phi(R)$, then $\phi(1_R) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$. Thus, for every $\phi(a) \in \phi(R)$, $\phi(a)^{-1} = \phi(a^{-1})$. $\square$

Proposition

The kernel of any ring homomorphism $\phi : R \to S$ *is an ideal in* R*.*

-

Proposition

The kernel of any ring homomorphism $\phi : R \to S$ is an ideal in R.

-

Proof.

Note that $ker\phi$ is a subgroup of R. For all $a \in ker\phi, r \in R$, we have

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0,$$
$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0.$$

So $ra, ar \in ker\phi$. □

-

Theorem

Let I be an ideal of R. The factor group R/I is a ring with multiplication defined by

$$(r + I)(s + I) = rs + I. \quad (1)$$

-

Theorem

Let I be an ideal of R. The factor group R/I is a ring with multiplication defined by

$$(r+I)(s+I) = rs + I. \tag{1}$$

-
- proof: Let $r+I, s+I \in R/I$, then R/I is an abelian group since
$$(r+I) + (s+I) = r+s+I.$$
We will show that the multiplication is well-defined. That is the product $(r+I)+(s+I) = r+s+I$ is independent of the choice of coset.

Theorem

Let I be an ideal of R. The factor group R/I is a ring with multiplication defined by

$$(r+I)(s+I) = rs + I. \tag{1}$$

-
- proof: Let $r+I, s+I \in R/I$, then R/I is an abelian group since
$$(r+I)+(s+I) = r+s+I.$$
We will show that the multiplication is well-defined. That is the product $(r+I)+(s+I) = r+s+I$ is independent of the choice of coset.
- If $r' \in r+I, s' \in s+I$, then $r's' \in rs+I$. Since $r', s' \in r+I$, there exist $a, b \in I$ such that $r' = r+a$ and $s' = s+b$. The multiplication $r's' = rs + as + rb + ab$. is in $r+I$ since

- The multiplication satisfy associative law and distributive laws because

$$((r+I)(s+I))(t+I) = (rs+I)(t+I) = (rs)t+I = rst+I,$$
$$(r+I)((s+I)(t+I)) = (r+I)(st+I) = r(st)+I = rst+I.$$

and

$$((r+I)+(s+I))(t+I) = (r+s+I)(t+I) = (r+s)t+I,$$
$$(r+I)((s+I)+(t+I)) = (r+I)(s+t+I) = r(s+t)+I.$$

Definition

Let R be a ring, and I be an ideal of R, ring R/I is called factor ring or quotient ring.

-

Theorem

Let I be an ideal of R. The map $\psi : R \to R/I$ defined by $\psi(r) = r + I$ is a ring homomorphism of R onto R/I with kernel I.

-

Theorem

Let I be an ideal of R. The map $\psi : R \to R/I$ defined by $\psi(r) = r + I$ is a ring homomorphism of R onto R/I with kernel I.

-

Proof.

It is obvious that $\psi : R \to R/I$ is a group homomorphism. Let $r, s \in R$, then

$$\psi(rs) = \psi(r)\psi(s) = (r + I)(s + I) = rs + I.$$

Thus ψ is a ring homomorphism. If $r \in I$, then

$$\psi(r) = r + I = I = 0 + I = \bar{0} \in R/I.$$

$\square$

Definition

The map $\psi : R \to R/I$ is called *natural homomorphism* or *canonical homomorphism.*

-

Theorem

First Isomorphism Theorem for Rings: *Let* $\phi : R \to S$ *be a ring homomorphism. Then* $Ker\phi$ *is an ideal of* R*. If* $\psi : R \to R/ker\phi$ *is the canonical homomorphism, then there exists an isomorphism* $\eta : R/Ker\phi \to \phi(R)$ *such that* $\phi = \eta\psi$*.*

-

Theorem

First Isomorphism Theorem for Rings: *Let $\phi : R \to S$ be a ring homomorphism. Then $Ker\phi$ is an ideal of R. If $\psi : R \to R/ker\phi$ is the canonical homomorphism, then there exists an isomorphism $\eta : R/Ker\phi \to \phi(R)$ such that $\phi = \eta\psi$.*

-
- Proof: By the First Isomorphism Theorem for groups, there exist a well-defined additive group homomorphism $\eta : R/Ker\phi \to \phi(R)$ defined by $\eta(r + Ker\phi) = \phi(r)$. And η preserve multiplication since

$$\eta((r+I)(s+I)) = \eta(rs+I) = \phi(rs) = \phi(r)\phi(s),$$
$$\eta(r+I)\eta(s+I) = \phi(r)\phi(s).$$

Theorem

Second Isomorphism Theorem for rings: *Let I be a subring of a ring R and J an ideal of R. Then $I \cap J$ is an ideal of I, and*

$$I/I \cap J \cong (I+J)/J.$$

-

Theorem

Second Isomorphism Theorem for rings: *Let I be a subring of a ring R and J an ideal of R. Then $I \cap J$ is an ideal of I, and*

$$I/I \cap J \cong (I + J)/J.$$

-

Theorem

Third Isomorphism Theorem: *Let R be a ring and I and J be ideals of R where $J \subset I$. Then*

$$R/I \cong \frac{R/J}{I/J}. \tag{2}$$

-

Theorem

Correspondence Theorem of rings: *Let I be an ideal of a ring R. Then $S \longrightarrow S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R containing I correspond to ideals of R/I.*

-

Theorem

Correspondence Theorem of rings: *Let I be an ideal of a ring R. Then $S \longrightarrow S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R containing I correspond to ideals of R/I.*

-

Proof.

The correspondence between subgroups applies here. All one has to do is verify that S is a subring if and only if S/I is. Assume that S is a subring containing I as an ideal, then there is a factor ring S/I. Conversely, if S/I is a subring of R/I, then S is a subring of R. $\square$

-

3.4 Maximal ideals and prime ideals

Definition

A proper ideal M of a ring R is a maximal ideal of R if the ideal M is not a proper subset of any ideal of R except R itself.

-

Definition

A proper ideal M of a ring R is a maximal ideal of R if the ideal M is not a proper subset of any ideal of R except R itself.

-

Example

$2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. But $4\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ since $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$.

-

Theorem

Let R be a commutative ring with identity and M an ideal in R. Then M is a maximal ideal of R if and only if R/M is a field.

-

Theorem

Let R be a commutative ring with identity and M an ideal in R. Then M is a maximal ideal of R if and only if R/M is a field.

-
- Proof: Let M be a maximal ideal in R. If R is a commutative ring, then R/M must also be a commutative ring. Clearly, $1+M$ acts as an identity for R/M. We must also show that every nonzero element in R/M has an inverse. If $a+M$ is a nonzero element in R/M, then $a \notin M$. Define $I = \{ra + m | r \in R, m \in M\}$. We will show that I is an ideal in R. The set I is nonempty since $0a + 0 = 0 \in I$. If $r_1 a + m_1, r_2 a + m_2 \in I$, then

$$(r_1 a + m_1) - (r_2 a + m_2) = (r_1 - r_2) + (m_1 - m_2) \in I.$$

- Also, for any $s \in R$, then $s(ra + m) = sra + sm \in I$ since $sm \in M$, $(ra + m)s = ras + ms = rsa + sm \in I$ by R commutativity. Hence, I is an ideal. Therefore, I is an ideal properly containing M. Since M is a maximal ideal, $I = R$. consequently, by the definition of I there must be an $m \in M$ and an element $b \in R$ such that $1 = ab + m$. Therefore,

$$1 + M = ab + M = ba + M = (a + M)(b + M).$$

- Conversely, suppose that M is an ideal and R/M is a field. Since R/M is a field, it must contain at least two elements: $0+M = M$ and $1+M$. Hence, M is a proper ideal of R. Let I be any ideal properly containing M. We need to show that $I = R$. Choose $a \in I$ but $a \notin M$. Since $a + M$ is a nonzero element in a field, there exists an element $b + M \in R/M$ such that $(a+M)(b+M) = ab+M = 1+M$. Consequently, there exists an element $m \in M$ such that $ab + m = 1$ and $1 \in I$. Therefore, $r1 = r \in I$ for all $r \in R$. Consequently, $I = R$

Example

Let p be prime, $p\mathbb{Z}$ be an ideal in $\mathbb{Z}$. Then $p\mathbb{Z}$ is a maximal ideal since $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is a field.

-

Definition

A proper ideal P in a commutative ring R is called a prime ideal if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

-

Definition

A proper ideal P in a commutative ring R is called a prime ideal if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

-

Example

It is easy to check that the set $P = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ is an ideal in $\mathbb{Z}_{12}$. This ideal is prime and maximal ideal.

-

Example

Let $\mathbb{Z}_2[x]$ be the polynomial ring over $\mathbb{Z}_2$. Then $\langle x^2+1\rangle$ is not a prime ideal. Since

$$(x+1)(x+1) = x^2+1 \in \langle x^2+1\rangle,$$

but $x+1 \notin \langle x^2+1\rangle$. So $\langle x^2+1\rangle$ is not a prime ideal of $\mathbb{Z}_2[x]$.

-

Proposition

Let n be a positive integer. Then $\langle n \rangle$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime.

-

Proposition

Let n be a positive integer. Then $\langle n\rangle$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime.

-

Proof.

If n is not prime, then n is 1 or a composite number. If $n = 1$, then $\langle n\rangle = \mathbb{Z}$, it is not a prime ideal. If $n = ab$ for $1 < a < n, 1 < b < n$, then $n \in \langle n\rangle$, but $a \notin \langle n\rangle, b \notin \langle n\rangle$. So $\langle n\rangle$ is not a prime ideal.
Conversely, if n is a prime number, and $ab \in \langle n\rangle$, then $n|ab$, thus $n|a$ or $n|b$, that is $a \in \langle n\rangle$ or $b \in \langle n\rangle$. $\square$

-

Proposition

Let R be a commutative ring with identity 1_R. Then P is a prime ideal in R if and only if R/P is an integral domain.

-

Proposition

Let R be a commutative ring with identity 1_R. Then P is a prime ideal in R if and only if R/P is an integral domain.

-
- Proof: Assume that P is an ideal in R and R/P is an integral domain. Suppose that $ab \in P$. If $a + P, b + P \in R/P$ such that
$$(a + P)(b + P) = 0 + P = P,$$
then either $a + P = P$ or $b + P = P$. This means that either $a \in P$ or $b \in P$, which shows that P must be prime.

Proposition

Let R be a commutative ring with identity 1_R. Then P is a prime ideal in R if and only if R/P is an integral domain.

-
- Proof: Assume that P is an ideal in R and R/P is an integral domain. Suppose that $ab \in P$. If $a + P, b + P \in R/P$ such that
$$(a + P)(b + P) = 0 + P = P,$$
then either $a + P = P$ or $b + P = P$. This means that either $a \in P$ or $b \in P$, which shows that P must be prime.
- Conversely, suppose that P is prime and
$$(a + P)(b + P) = ab + P = 0 + P = P.$$
Then $ab \in P$. If $a \notin P$, then b must be in P by the definition of a prime ideal. Hence, $b + P = 0 + P$ and R/P is an integral

Example

Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$. The factor ring $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is an integral domain only when n is prime. It is actually a field. Hence, the nonzero prime ideals in $\mathbb{Z}$ are the ideals $p\mathbb{Z}$ for p a prime.

-

Corollary

Every maximal ideal in a commutative ring with identity is also a prime ideal.

-

Corollary

Every maximal ideal in a commutative ring with identity is also a prime ideal.

-
- Remark: If there is no identity in the ring R, the corollary is not true. For example, $4\mathbb{Z}$ is a maximal ideal of $2\mathbb{Z}$, but $4\mathbb{Z}$ is not a prime ideal of $2\mathbb{Z}$.

Theorem

Let F be a field and suppose that $p(x) \in F[x]$. Then the ideal generated by $p(x)$ is maximal if and only if $p(x)$ is irreducible.

-

Theorem

Let F be a field and suppose that $p(x) \in F[x]$. Then the ideal generated by $p(x)$ is maximal if and only if $p(x)$ is irreducible.

-
- Proof: Suppose that $p(x)$ generates a maximal ideal of $F[x]$. Then $\langle p(x) \rangle$ is also a prime ideal of $F[x]$. Since a maximal ideal must be properly contained inside $F[x]$, $p(x)$ cannot be a constant polynomial. Let us assume that $p(x)$ factors into product of two polynomials, say $p(x) = f(x)g(x)$, where $\deg f(x) < \deg(p(x), \deg g(x) < \deg(p(x)$. Since $\langle p(x) \rangle$ is a prime ideal, one of these factors, say $f(x)$, is in $\langle p(x) \rangle$ and therefore be a multiple of $p(x)$. But this would imply that $\langle p(x) \rangle \subset \langle f(x) \rangle$, which is impossible since $\langle p(x) \rangle$ is maximal.

- Conversely, suppose that $p(x)$ is irreducible over $F[x]$. Let I be an ideal in $F[x]$ containing $\langle p(x) \rangle$. Then I is a principal idea, hence, $I = \langle f(x) \rangle$ for some $f(x) \in F[x]$. Since $p(x) \in I$, it must be the case that $p(x) = f(x)g(x)$ for some $g(x) \in F[x]$. However, $p(x)$ is irreducible; hence, either $f(x)$ or $g(x)$ is a constant polynomial. If $f(x)$ is constant, then $I = F[x]$ and we are done. If $g(x)$ is a constant, then $f(x)$ is a constant multiple of I and $I = \langle p(x) \rangle$. Thus, there are no proper ideals of $F[x]$ that properly contain $\langle p(x) \rangle$.

1.4 Extension fields

Definition

Let E is a field. A subfield F is a subset of E and F is a field. A field E is an *extension field* of a field F if F is a subfield of E. The field F is called the *base field.* We write $F \subseteq E$ or E/F.

-

Definition

Let E is a field. A subfield F is a subset of E and F is a field. A field E is an *extension field* of a field F if F is a subfield of E. The field F is called the *base field.* We write $F \subseteq E$ or E/F.

-
- Given a field extension E/F, the larger field E can be considered as a vector space over F. The elements of E are the vectors and the elements of F are scalars. For example, $\mathbb{C} = \{a + bi | a, b \in \mathbb{Q}, i^2 = -1\}$ is a vector space over $\mathbb{Q}$, and $\mathbb{C}$ is a extension field of $\mathbb{Q}$.

Definition

If an extension field E of a field F is a finite dimensional vector space over F of dimension n, then we say that E is a finite extension of degree n over F. We write $[E : F] = n$ to indicate the dimension of E over F.

-

Definition

If an extension field E of a field F is a finite dimensional vector space over F of dimension n, then we say that E is a finite extension of degree n over F. We write $[E : F] = n$ to indicate the dimension of E over F.

-

Example

Let
$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}.$$
Then $\mathbb{Q}(\sqrt{2})$ is a extension field of $\mathbb{Q}$, the basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$, and
$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

-

Example

If we consider the polynomial

$$p(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3).$$

$(x^2 - 2)$ and $(x^2 - 3)$ are irreducible in $\mathbb{Q}$.
Let

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Q}(\sqrt{2})\}.$$

Then $p(x)$ is reducible in E.

-

- E is a extension field of $\mathbb{Q}(\sqrt{2})$, the basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{3}\}$, and

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2.$$

- E is a extension field of $\mathbb{Q}(\sqrt{2})$, the basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{3}\}$, and

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2.$$

- Furthermore,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} | a, b, c, d \in \mathbb{Q}\},$$

then

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

Theorem

Telescope Formula: If E is a finite extension of F and K is a finite extension of E, then K is a finite extension of F and

$$[K:F] = [K:E][E:F]. \tag{3}$$

-

- Proof: Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for E as a vector space over F and $\{\beta_1, \cdots, \beta_m\}$ be a basis for K as a vector space over E. We claim that $\{\alpha_i \beta_j\}$ is a basis for K over F.

- Proof: Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for E as a vector space over F and $\{\beta_1, \cdots, \beta_m\}$ be a basis for K as a vector space over E. We claim that $\{\alpha_i\beta_j\}$ is a basis for K over F.
- We will first show that these vectors span K. Let $u \in K$. Then $u = \sum_{j=1}^{m} b_j\beta_j$ and $b_j = \sum_{i=1}^{n} a_{ij}\alpha_i$, where $b_j \in E$ and $a_{ij} \in F$. Then

$$u = \sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij}\alpha_i)\beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j).$$

So the mn vectors $\alpha_i\beta_j$ must span K over F.

- We must show that $\{\alpha_i\beta_j\}$ are linearly independent. Suppose that there exist $c_{ij} \in F$ such that

$$u = \sum_{i,j} c_{ij}(\alpha_i\beta_j) = \sum_{i,j}(c_{ij}\alpha_i)\beta_j) = 0.$$

Since the $\beta_j's$ are linearly independent over E, it must be the case that

$$\sum_{i,j} c_{ij}\alpha_i = 0,$$

for all j. However, the α_j are also linearly independent over F. Therefore, $c_{ij} = 0$ for all i and j, which completes the proof.

Corollary

If F_i is a field for $i = 1, \cdots, k$ and F_{i+1} is a finite extension of F_i, then F_k is a finite extension of F_1 and

$$[F_k : F_1] = [F_k : F_{k-1}] \cdots [F_2 : F_1] \tag{4}$$

-

- If E is a field extension of F and $\alpha_1, \cdots, \alpha_n$ are contained in E, we denote the smallest field containing F and $\alpha_1, \cdots, \alpha_n$ by $F(\alpha_1, \cdots, \alpha_n)$. If $E = F(\alpha)$ for some $\alpha \in E$, then E is a *simple extension* of F.
- Let $E = F(\alpha)$ be a simple extension of F. Note that $a \in E$, then $a^k \in E$ for $k \in \mathbb{N}$. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots \in F[x]$, then

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n + \cdots \in E.$$

If $g(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n + \cdots \neq 0$, then $g(\alpha)^{-1} \in E$. Thus

$$E = \{f(\alpha)g(\alpha)^{-1} | f(x), g(x) \in F[x], g(\alpha) \neq 0\}.$$

- Let $F[x]$ be the polynomial ring over field F, $F[a]=\{f(a)|f(x)\in F[x]\}$, $F[\alpha_1,\alpha_2,\cdots,\alpha_s] = \{f(\alpha_1,\alpha_2,\cdots,\alpha_s)|f(x_1,x_2,\cdots,x_s) \in F(x_1,x_2,\cdots,x_s)\}$.

- Let $F[x]$ be the polynomial ring over field F, $F[a] = \{f(a) | f(x) \in F[x]\}$, $F[\alpha_1, \alpha_2, \cdots, \alpha_s] = \{f(\alpha_1, \alpha_2, \cdots, \alpha_s) | f(x_1, x_2, \cdots, x_s) \in F(x_1, x_2, \cdots, x_s)\}$.
- If $E = F(\alpha_1, \alpha_2, \cdots \alpha_s)$ be a extension of F, then $E = F(\alpha_1)(\alpha_2) \cdots (\alpha_s)$. Thus

$$\begin{aligned} E &= \{f(\alpha_1, \alpha_2, \cdots, \alpha_n) g(\alpha_1, \alpha_2, \cdots, \alpha_n)^{-1} | \\ &\quad f(x), g(x) \in F[x], g(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0\}. \end{aligned}$$

- Let $F[x]$ be the polynomial ring over field F, $F[a] = \{f(a)|f(x) \in F[x]\}$, $F[\alpha_1, \alpha_2, \cdots, \alpha_s] = \{f(\alpha_1, \alpha_2, \cdots, \alpha_s)|f(x_1, x_2, \cdots, x_s) \in F(x_1, x_2, \cdots, x_s)\}$.
- If $E = F(\alpha_1, \alpha_2, \cdots \alpha_s)$ be a extension of F, then $E = F(\alpha_1)(\alpha_2)\cdots(\alpha_s)$. Thus

$$\begin{aligned} E &= \{f(\alpha_1, \alpha_2, \cdots, \alpha_n)g(\alpha_1, \alpha_2, \cdots, \alpha_n)^{-1}| \\ &\quad f(x), g(x) \in F[x], g(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0\}. \end{aligned}$$

- Then $F(\alpha)$ is a factor field of $F[\alpha]$, $F(\alpha_1, \alpha_2, \cdots, \alpha_s)$ is a factor field of $F[\alpha_1, \alpha_2, \cdots, \alpha_s)$.

- Let F be a field $\mathbb{Q}$. Consider the simple extension $\mathbb{Q}[\pi]$. Then

$$\mathbb{Q}(\pi) = \{f(\pi)g(\pi)^{-1} | f(x), g(x) \in \mathbb{Q}[x], g(\pi) \neq 0\}$$

$\mathbb{Q}(\pi)$ is the factor field of ring $\mathbb{Q}[\pi]$.

- Exercise: Show that
  (1) $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.
  (2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

- Exercise: Show that
  (1) $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.
  (2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
- Recall that $(\sqrt{2})^{-1} = \frac{1}{2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. In fact,

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}[\sqrt{2}](\sqrt{3}) \\ &= \{a + b\sqrt{3} | a, b \in \mathbb{Q}(\sqrt{2})\}. \end{aligned}$$

- Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Since neither 0 nor 1 is a root of this polynomial, we know that $p(x)$ is irreducible over $\mathbb{Z}_2$. We will construct a field extension of $\mathbb{Z}_2$ containing an element α such that $p(\alpha) = 0$.

- Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Since neither 0 nor 1 is a root of this polynomial, we know that $p(x)$ is irreducible over $\mathbb{Z}_2$. We will construct a field extension of $\mathbb{Z}_2$ containing an element α such that $p(\alpha) = 0$.
- The ideal $\langle p(x) \rangle$ generated by $p(x)$ is maximal. Hence, $\mathbb{Z}_2/\langle p(x) \rangle$ is a field. Let $f(x) + \langle p(x) \rangle$ be an arbitrary element of $\mathbb{Z}_2/\langle p(x) \rangle$. By the division algorithm,

$$f(x) = (x^2 + x + 1)q(x) + r(x),$$

where the degree of $r(x)$ is less than the degree of $x^2 + x + 1$.

- $$f(x) + \langle x^2 + x + 1 \rangle = r(x) + \langle x^2 + x + 1 \rangle.$$

  The only possibilities for $r(x)$ are then $0, 1, x$ and $1 + x$. Consequently, $\mathbb{Z}_2/\langle p(x) \rangle$ is a field with four elements and must be a field extension of $\mathbb{Z}_2$, $E = \mathbb{Z}_2/\langle p(x) \rangle$ containing a zero α of $p(x)$.

- $$f(x) + \langle x^2 + x + 1\rangle = r(x) + \langle x^2 + x + 1\rangle.$$

  The only possibilities for $r(x)$ are then $0, 1, x$ and $1 + x$. Consequently, $\mathbb{Z}_2/\langle p(x)\rangle$ is a field with four elements and must be a field extension of $\mathbb{Z}_2$, $E = \mathbb{Z}_2/\langle p(x)\rangle$ containing a zero α of $p(x)$.
- The field $\mathbb{Z}_2(\alpha)$ consists of elements

$$\begin{aligned} 0 + 0\alpha &= 0, \\ 1 + 0\alpha &= 1, \\ 0 + 1\alpha &= \alpha, \\ 1 + 1\alpha &= 1 + \alpha. \end{aligned}$$

- Notice that $\alpha^2 + \alpha + 1 = 0$. Hence, if we compute

  $$(1+\alpha)^2 = (1+\alpha)(1+\alpha) = 1+\alpha+\alpha+(\alpha)^2 = \alpha+(1+\alpha+(\alpha)^2) = \alpha.$$

- Notice that $\alpha^2 + \alpha + 1 = 0$. Hence, if we compute

  $$(1+\alpha)^2 = (1+\alpha)(1+\alpha) = 1+\alpha+\alpha+(\alpha)^2 = \alpha+(1+\alpha+(\alpha)^2) = \alpha.$$

- Let $a + b\alpha$ be the inverse of α, then

  $$1 = \alpha(a + b\alpha) = a\alpha + b\alpha^2 = a\alpha + b(-1 - \alpha) = (a - b)\alpha - b,$$

  Thus $a = -1 = 1, b = -1 = 1$. So the inverse of α is $1 + \alpha$.

Table: Addition Table of $\mathbb{Z}_2(\alpha)$

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Table: Multiplication Table of $\mathbb{Z}_2(\alpha)$

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Definition

An element α in an extension field E over F is *algebraic* over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$.

-

Definition

An element α in an extension field E over F is *algebraic* over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$.

-

Definition

An element in E that is not algebraic over F is *transcendental* over F.

-

Definition

An element α in an extension field E over F is *algebraic* over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$.

-

Definition

An element in E that is not algebraic over F is *transcendental* over F.

-

Definition

An extension field E of a field F is an algebraic extension of F if every element in E is algebraic over F.

-

- Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ since they are zeros of the polynomials $x^2 - 2$ and $x^2 + 1$, respectively.

- Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ since they are zeros of the polynomials $x^2 - 2$ and $x^2 + 1$, respectively.
- Clearly π and e are algebraic over the real numbers. However, it is a nontrivial fact that they are transcendental over $\mathbb{Q}$.

- Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ since they are zeros of the polynomials $x^2 - 2$ and $x^2 + 1$, respectively.
- Clearly π and e are algebraic over the real numbers. However, it is a nontrivial fact that they are transcendental over $\mathbb{Q}$.
- Numbers in $\mathbb{R}$ that are algebraic over $\mathbb{Q}$ are in fact quite rare. Almost all real numbers are transcendental over $\mathbb{Q}$.

- Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ since they are zeros of the polynomials $x^2 - 2$ and $x^2 + 1$, respectively.
- Clearly π and e are algebraic over the real numbers. However, it is a nontrivial fact that they are transcendental over $\mathbb{Q}$.
- Numbers in $\mathbb{R}$ that are algebraic over $\mathbb{Q}$ are in fact quite rare. Almost all real numbers are transcendental over $\mathbb{Q}$.
- In many cases we do not know whether or not a particular number is transcendental; for example, it is still not known whether $\pi + e$ is transcendental or algebraic.

Example

We will show that $\sqrt{2+\sqrt{3}}$ is algebraic over $\mathbb{Q}$. If $\alpha = \sqrt{2+\sqrt{3}}$, then $\alpha^2 = 2+\sqrt{3}$. Hence, $\alpha^2 - 2 = \sqrt{3}$ and $(\alpha^2-2)^2 = 3$. Since $\alpha^4 - 4\alpha^2 + 1 = 0$, it must be true that α is a zero of the polynomial $x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$.

-

Definition

A complex number that is algebraic over $\mathbb{Q}$ is an **algebraic number**. A **transcendental number** is an element of $\mathbb{C}$ that is transcendental over $\mathbb{Q}$.

-

Proposition

A field extension of finite degree is algebraic.

Proof.

Let E be a finite extension of F and let $x \in E$. By hypothesis, $[E : F] = n$, E has finite dimension n as a vector space over F. Consequently, the set $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ is linearly dependent, and there are elements $a_0, a_1, \cdots, a_n \in F$ not all zero, such that $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. So α is a root of the nonzero polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, and E is therefore algebraic over F. $\square$

-

Theorem

Let E be an extension field of a field F and $\alpha \in E$ with α algebraic over F . Then there is a unique irreducible monic polynomial $p(x) \in F(x)$ of smallest degree such that $p(\alpha) = 0$. If $f(x)$ is another polynomial in $F[x]$ such that $f(\alpha) = 0$, then $p(x)$ divides $f(x)$.

-

- Proof: Let $\phi_\alpha : F[x] \longrightarrow E$ be the evaluation homomorphism. The kernel of ϕ_α is a principal ideal generated by some $p(x) \in F[x]$ with deg $p(x) \geq 1$. We know that such a polynomial exists, since $F[x]$ is a principal ideal domain and α is algebraic. The ideal $\langle p(x) \rangle$ consists exactly of those elements of $F[x]$ having α as a zero. If $f(\alpha) = 0$ and $f(x)$ is not the zero polynomial, then $f(x) \in \langle p(x) \rangle$ and $p(x)$ divides $f(x)$. So $p(x)$ is a polynomial of minimal degree having α as a zero. Any other polynomial of the same degree having α as a zero must have the form $bp(x)$ for some $b \in F$.

- Proof: Let $\phi_\alpha : F[x] \longrightarrow E$ be the evaluation homomorphism. The kernel of ϕ_α is a principal ideal generated by some $p(x) \in F[x]$ with deg $p(x) \geq 1$. We know that such a polynomial exists, since $F[x]$ is a principal ideal domain and α is algebraic. The ideal $\langle p(x) \rangle$ consists exactly of those elements of $F[x]$ having α as a zero. If $f(\alpha) = 0$ and $f(x)$ is not the zero polynomial, then $f(x) \in \langle p(x) \rangle$ and $p(x)$ divides $f(x)$. So $p(x)$ is a polynomial of minimal degree having α as a zero. Any other polynomial of the same degree having α as a zero must have the form $bp(x)$ for some $b \in F$.
- Suppose now that $p(x) = r(x)s(x)$. Since $p(\alpha) = 0, r(\alpha)s(\alpha) = 0$, consequently, either $r(\alpha) = 0$ or $s(\alpha) = 0$, which contradicts the fact that deg$p(x) \geq 1$. Therefore, $p(x)$ must be irreducible.

Definition

Let E be an extension field of F and $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ of the last theorem is called the **minimal polynomial** for α over F. The degree of $p(x)$ is the degree of α over F.

-

Definition

Let E be an extension field of F and $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ of the last theorem is called the **minimal polynomial** for α over F. The degree of $p(x)$ is the degree of α over F.

-

Example

Let $f(x) = x^2 - 2$ and $g(x) = x^4 - 4x^2 + 1$. They are the minimal polynomials of $\sqrt{2}$ and $\sqrt{2+\sqrt{3}}$, respectively.

-

- The minimal polynomials of i in $\mathbb{Q}$ and $\mathbb{R}$ is x^2+1. We have

$$\mathbb{Q}[i] = \mathbb{Q}[x]/\langle x^2+1\rangle, \quad \mathbb{R}[i] \cong \mathbb{R}[x]/\langle x^2+1\rangle.$$

- The minimal polynomials of i in $\mathbb{Q}$ and $\mathbb{R}$ is x^2+1. We have

$$\mathbb{Q}[i] = \mathbb{Q}[x]/\langle x^2+1\rangle, \quad \mathbb{R}[i] \cong \mathbb{R}[x]/\langle x^2+1\rangle.$$

- Let

$$\begin{aligned} f(x) &= ((x-\sqrt{3})^2-2)((x+\sqrt{3})^2-2) \\ &= (x-\sqrt{3}-\sqrt{2})(x-\sqrt{3}+\sqrt{2}) \\ &\quad (x+\sqrt{3}-\sqrt{2})(x+\sqrt{3}+\sqrt{2}) \\ &= x^4-10x^2+1. \end{aligned}$$

Then $f(\sqrt{2}+\sqrt{3})=0$. The minimal polynomials of $\sqrt{2}+\sqrt{3}$ is $f(x)=x^4-10x^2+1$.