Algebraic Structure (代数结构)
Chapter 2: Ring Fundamentals

Shengli Liu (刘胜利)

liu-sl@cs.sjtu.edu.cn
Lab of Cryptography and Information Security
密码与信息安全实验室
计算机科学与工程系
上海交通大学

Maximal Ideals

不特别说明，以后讨论的环均为有“1”环。

Definition 1.1 (maximal ideal)

A maximal ideal in the ring R is a proper ideal that is not contained in any strictly larger proper ideal.

Theorem 1.2

Every proper ideal I of the ring R is contained in a maximal ideal. Consequently, every ring has at least one maximal ideal.

Theorem 1.3

Let M be an ideal in the commutative ring R. Then M is a maximal ideal iff R/M is a field.

Maximal Ideals

不特别说明，以后讨论的环均为有“1”环。

Definition 1.1 (maximal ideal)

A maximal ideal in the ring R is a proper ideal that is not contained in any strictly larger proper ideal.

Theorem 1.2

Every proper ideal I of the ring R is contained in a maximal ideal. Consequently, every ring has at least one maximal ideal.

Theorem 1.3

Let M be an ideal in the commutative ring R. Then M is a maximal ideal iff R/M is a field.

Maximal Ideals

不特别说明，以后讨论的环均为有“1”环。

Definition 1.1 (maximal ideal)

A maximal ideal in the ring R is a proper ideal that is not contained in any strictly larger proper ideal.

Theorem 1.2

Every proper ideal I of the ring R is contained in a maximal ideal. Consequently, every ring has at least one maximal ideal.

Theorem 1.3

Let M be an ideal in the commutative ring R. Then M is a maximal ideal iff R/M is a field.

Proof.

- $\Rightarrow$ Suppose M is maximal. We know that R/M is a ring; When $a + M \neq M$, since M is maximal, the ideal $Ra + M$, is strictly larger than M, must be R. So $1 \in Ra + M$. If $1 = ra + m$ where $r \in R$ and $m \in M$, then

$$\begin{aligned}(r+M)(a+M) &= ra+M \\ &= (1-m)+M = 1+M\end{aligned}$$

- $\Leftarrow$ If R/M is a field, suppose $M \subset I$ and I is a ideal of R, there exist $a \in I, a \notin M$, and $M + a \neq M$ in R/M, there exist a inverse $M + x$ such that

$$(M+a)(M+x) = M+1 \Rightarrow M+ax = M+1$$

But $a \in I, M \subset I \Rightarrow ax \in I$. So $M + ax \subset I$, $1 \in I$, and $I = R$.

Proof.

- $\Rightarrow$ Suppose M is maximal. We know that R/M is a ring; When $a + M \neq M$, since M is maximal, the ideal $Ra + M$, is strictly larger than M, must be R. So $1 \in Ra + M$. If $1 = ra + m$ where $r \in R$ and $m \in M$, then

$$\begin{aligned}(r + M)(a + M) &= ra + M \\ &= (1 - m) + M = 1 + M\end{aligned}$$

- $\Leftarrow$ If R/M is a field, suppose $M \subset I$ and I is a ideal of R, there exist $a \in I, a \notin M$, and $M + a \neq M$ in R/M, there exist a inverse $M + x$ such that

$$(M + a)(M + x) = M + 1 \Rightarrow M + ax = M + 1$$

But $a \in I, M \subset I \Rightarrow ax \in I$. So $M + ax \subset I$, $1 \in I$, and $I = R$.

Prime Ideals

Definition 1.4 (prime ideal)

A prime ideal in a commutative ring is a proper ideal P such that for any $a, b \in R$, $ab \in P \Rightarrow a \in P \text{ or } b \in P$.

Theorem 1.5

If P is an ideal in the commutative ring R, then P is a prime ideal iff R/P is an integral domain.

Proof.

- $\Rightarrow$ Suppose P is prime. Since P is a proper ideal, R/P is a ring. If $(a+P)(b+P) = P$, then $ab \in P$ and $a \in P$ or $b \in P \Rightarrow (a+P) = P$ or $(b+P) = P$.
- $\Leftarrow$ If R/P is an integral domain, and $ab \in P$, then $(a+P)(b+P)$ is zero in R/P, so $a+P = P$ or $b+P = P$, i.e., $a \in P$ or $b \in P$.

Prime Ideals

Definition 1.4 (prime ideal)

A prime ideal in a commutative ring is a proper ideal P such that for any $a, b \in R$, $ab \in P \Rightarrow a \in P \text{ or } b \in P$.

Theorem 1.5

If P is an ideal in the commutative ring R, then P is a prime ideal iff R/P is an integral domain.

Proof.

- $\Rightarrow$ Suppose P is prime. Since P is a proper ideal, R/P is a ring. If $(a+P)(b+P) = P$, then $ab \in P$ and $a \in P$ or $b \in P \Rightarrow (a+P) = P$ or $(b+P) = P$.
- $\Leftarrow$ If R/P is an integral domain, and $ab \in P$, then $(a+P)(b+P)$ is zero in R/P, so $a+P = P$ or $b+P = P$, i.e., $a \in P$ or $b \in P$.

Prime Ideals

Definition 1.4 (prime ideal)

A prime ideal in a commutative ring is a proper ideal P such that for any $a, b \in R$, $ab \in P \Rightarrow a \in P \text{ or } b \in P$.

Theorem 1.5

If P is an ideal in the commutative ring R, then P is a prime ideal iff R/P is an integral domain.

Proof.

- $\Rightarrow$ Suppose P is prime. Since P is a proper ideal, R/P is a ring. If $(a+P)(b+P) = P$, then $ab \in P$ and $a \in P$ or $b \in P \Rightarrow (a+P) = P$ or $(b+P) = P$.
- $\Leftarrow$ If R/P is an integral domain, and $ab \in P$, then $(a+P)(b+P)$ is zero in R/P, so $a+P = P$ or $b+P = P$, i.e., $a \in P$ or $b \in P$.

Prime Ideals

Definition 1.4 (prime ideal)

A prime ideal in a commutative ring is a proper ideal P such that for any $a, b \in R$, $ab \in P \Rightarrow a \in P \text{ or } b \in P$.

Theorem 1.5

If P is an ideal in the commutative ring R, then P is a prime ideal iff R/P is an integral domain.

Proof.

- $\Rightarrow$ Suppose P is prime. Since P is a proper ideal, R/P is a ring. If $(a+P)(b+P) = P$, then $ab \in P$ and $a \in P$ or $b \in P \Rightarrow (a+P) = P$ or $(b+P) = P$.
- $\Leftarrow$ If R/P is an integral domain, and $ab \in P$, then $(a+P)(b+P)$ is zero in R/P, so $a+P = P$ or $b+P = P$, i.e., $a \in P$ or $b \in P$.

Prime Ideals

Definition 1.4 (prime ideal)

A prime ideal in a commutative ring is a proper ideal P such that for any $a, b \in R$, $ab \in P \Rightarrow a \in P \text{ or } b \in P$.

Theorem 1.5

If P is an ideal in the commutative ring R, then P is a prime ideal iff R/P is an integral domain.

Proof.

- $\Rightarrow$ Suppose P is prime. Since P is a proper ideal, R/P is a ring. If $(a+P)(b+P) = P$, then $ab \in P$ and $a \in P$ or $b \in P \Rightarrow (a+P) = P$ or $(b+P) = P$.
- $\Leftarrow$ If R/P is an integral domain, and $ab \in P$, then $(a+P)(b+P)$ is zero in R/P, so $a+P = P$ or $b+P = P$, i.e., $a \in P$ or $b \in P$.

Prime and maximal Ideals

Corollary 1.6

Let $f : R \mapsto S$ be an epimorphism of commutative rings. Then

- *If S is a field then $Kerf$ is a maximal ideal of R.*
- *If S is an integral domain then $Kerf$ is a prime ideal of R*

Proof.

By the first isomorphism theorem, S is isomorphic to $R/\mathrm{Ker}f$. Then the result follows from theorem 1.3 and 1.5 □

Prime and maximal Ideals

Corollary 1.6

Let $f : R \mapsto S$ be an epimorphism of commutative rings. Then

- *If S is a field then $Kerf$ is a maximal ideal of R.*
- *If S is an integral domain then $Kerf$ is a prime ideal of R*

Proof.

By the first isomorphism theorem, S is isomorphic to $R/\mathrm{Ker}f$. Then the result follows from theorem 1.3 and 1.5 □

Prime and maximal Ideals

Corollary 1.6

Let $f : R \mapsto S$ be an epimorphism of commutative rings. Then

- *If S is a field then $Kerf$ is a maximal ideal of R.*
- *If S is an integral domain then $Kerf$ is a prime ideal of R*

Proof.

By the first isomorphism theorem, S is isomorphic to $R/\mathrm{Ker}f$. Then the result follows from theorem 1.3 and 1.5 □

Prime and maximal Ideals

Corollary 1.7

In a commutative ring, a maximal ideal is prime.

A prime ideal may not be a maximal ideal.

Example 1.8

$\mathbb{Z}[x]$ is a ring. Then (2) and (x) are both prime ideals, but $(2) \subset (2, x)$ and $(x) \subset (2, x)$. Neither (2) nor (x) is maximal.

- Consider ring homomorphisms $\phi_1(f(x)) = f_0$, and $\phi_2(f(x)) = \sum (f_i \mod 2)x^i \in \mathbb{F}_2[x]$.
- Then $Ker(\phi_1) = (x)$ and $Ker(\phi_2) = (2)$.
- Both $\phi_1(\mathbb{Z}[x]) = \mathbb{Z}$ and $\phi_2(\mathbb{Z}[x]) = \mathbb{F}_2[x]$ are integer domains.

Prime and maximal Ideals

Corollary 1.7

In a commutative ring, a maximal ideal is prime.

A prime ideal may not be a maximal ideal.

Example 1.8

$\mathbb{Z}[x]$ is a ring. Then (2) and (x) are both prime ideals, but $(2) \subset (2, x)$ and $(x) \subset (2, x)$. Neither (2) nor (x) is maximal.

- Consider ring homomorphisms $\phi_1(f(x)) = f_0$, and $\phi_2(f(x)) = \sum (f_i \mod 2)x^i \in \mathbb{F}_2[x]$.
- Then $Ker(\phi_1) = (x)$ and $Ker(\phi_2) = (2)$.
- Both $\phi_1(\mathbb{Z}[x]) = \mathbb{Z}$ and $\phi_2(\mathbb{Z}[x]) = \mathbb{F}_2[x]$ are integer domains.

Polynomial Rings

Definition 2.1 (Polynomial Rings)

Let $R[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid a_i \in R, n \geq 0\}$ and R is a ring. Then $R[x]$ is a polynomial ring under the addition and multiplication of polynomials.

R是交换环，则$R[x]$是交换环；
R是有1环，则$R[x]$是有1环；
R是整环，则$R[x]$是整环；

Division Algorithm

If f and g are polynomials in $R[x]$,with g monic (首一), there are unique polynomials q and r in $R[X]$ such that $f = qg + r$ and $\deg r < \deg g$. If R is a field, g can be any nonzero polynomial.

Polynomial Rings

Definition 2.1 (Polynomial Rings)

Let $R[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_i \in R, n \geq 0\}$ and R is a ring. Then $R[x]$ is a polynomial ring under the addition and multiplication of polynomials.

R是交换环，则$R[x]$是交换环；
R是有1环，则$R[x]$是有1环；
R是整环，则$R[x]$是整环；

Division Algorithm

If f and g are polynomials in $R[x]$,with g monic (首一), there are unique polynomials q and r in $R[X]$ such that $f = qg + r$ and $\deg r < \deg g$. If R is a field, g can be any nonzero polynomial.

Polynomial Rings

Definition 2.1 (Polynomial Rings)

Let $R[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid a_i \in R, n \geq 0\}$ and R is a ring. Then $R[x]$ is a polynomial ring under the addition and multiplication of polynomials.

R是交换环，则$R[x]$是交换环；
R是有1环，则$R[x]$是有1环；
R是整环，则$R[x]$是整环；

Division Algorithm

If f and g are polynomials in $R[x]$,with g monic (首一), there are unique polynomials q and r in $R[X]$ such that $f = qg + r$ and $\deg r < \deg g$. If R is a field, g can be any nonzero polynomial.

Polynomial Rings

Theorem 2.2 (Remainder Theorem)

If $f \in R[X]$ and $a \in R$, then for some unique polynomial $q(X)$ in $R[X]$ we have

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

hence $f(a) = 0$ iff $X - a$ divides $f(X)$.

Proof.

We can write $f(X) = q(X)(X - a) + r(X)$ where r is a constant. so $r = f(a)$ and $f(a) = 0$ iff $X - a$ divides $f(X)$. □

Polynomial Rings

Theorem 2.2 (Remainder Theorem)

If $f \in R[X]$ and $a \in R$, then for some unique polynomial $q(X)$ in $R[X]$ we have

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

hence $f(a) = 0$ iff $X - a$ divides $f(X)$.

Proof.

We can write $f(X) = q(X)(X - a) + r(X)$ where r is a constant. so $r = f(a)$ and $f(a) = 0$ iff $X - a$ divides $f(X)$. □

Polynomial Rings

Theorem 2.3

If R is an integral domain, then a nonzero polynomial f in $R[X]$ of degree n has at most n roots in R.

Proof.

We prove it by induction, if $deg(f) = 1$, then it is obvious. If the result holds in $deg(f) = n - 1$. Then when $deg(f) = n$ and it has no roots, the result is right, otherwise f at least has a root a, we can write $f(X) = (X - a)g(X)$ while $deg(g) = n - 1$, since $g(X)$ has at most $n - 1$ roots, then $f(X)$ has most n roots in R. □

Example 2.4

Let $R = \mathbb{Z}_8$, which is not an integral domain. The polynomial $f(X) = X^3$ has four roots in R, namely $\{0, 2, 4, 6\}$

Polynomial Rings

Theorem 2.3

If R is an integral domain, then a nonzero polynomial f in $R[X]$ of degree n has at most n roots in R.

Proof.

We prove it by induction, if $deg(f) = 1$, then it is obvious. If the result holds in $deg(f) = n - 1$. Then when $deg(f) = n$ and it has no roots, the result is right, otherwise f at least has a root a, we can write $f(X) = (X - a)g(X)$ while $deg(g) = n - 1$, since $g(X)$ has at most $n - 1$ roots, then $f(X)$ has most n roots in R. □

Example 2.4

Let $R = \mathbb{Z}_8$, which is not an integral domain. The polynomial $f(X) = X^3$ has four roots in R, namely $\{0, 2, 4, 6\}$

Polynomial Rings

Theorem 2.3

If R is an integral domain, then a nonzero polynomial f in $R[X]$ of degree n has at most n roots in R.

Proof.

We prove it by induction, if $deg(f) = 1$, then it is obvious. If the result holds in $deg(f) = n - 1$. Then when $deg(f) = n$ and it has no roots, the result is right, otherwise f at least has a root a, we can write $f(X) = (X - a)g(X)$ while $deg(g) = n - 1$, since $g(X)$ has at most $n - 1$ roots, then $f(X)$ has most n roots in R. □

Example 2.4

Let $R = \mathbb{Z}_8$, which is not an integral domain. The polynomial $f(X) = X^3$ has four roots in R, namely $\{0, 2, 4, 6\}$

Unique Factorization

Let R be an integral domain.
设R为整环。若$a, b \in R$，且存在$c \in R$使得$a = bc$，则称b为a的因子，记为$b|a$。若e不是a的因子，则记为$e \nmid a$。

Definition 3.1

1. **unit** A unit in a integral domain R is an element with multiplicative inverse.
2. **Associate** The elements a and b are associates if $a = ub$ for some unit u.
3. **Irreducible** If $a \neq 0$ and a is not a unit, a is said to be irreducible if $a = bc$, then b or c must be a unit.
4. **Prime** If $a \neq 0$ and a is not a unit, a is said to be prime if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Fact 3.2

Unique Factorization

Let R be an integral domain.
设R为整环。若$a, b \in R$，且存在$c \in R$使得$a = bc$，则称b为a的因子，记为$b|a$。若e不是a的因子，则记为$e \nmid a$。

Definition 3.1

1. **unit** A unit in a integral domain R is an element with multiplicative inverse.
2. **Associate** The elements a and b are associates if $a = ub$ for some unit u.
3. **Irreducible** If $a \neq 0$ and a is not a unit, a is said to be irreducible if $a = bc$, then b or c must be a unit.
4. **Prime** If $a \neq 0$ and a is not a unit, a is said to be prime if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Fact 3.2

Unique Factorization

Let R be an integral domain.
设R为整环。若$a, b \in R$，且存在$c \in R$使得$a = bc$，则称b为a的因子，记为$b|a$。若e不是a的因子，则记为$e \nmid a$。

Definition 3.1

1. **unit** A unit in a integral domain R is an element with multiplicative inverse.
2. **Associate** The elements a and b are associates if $a = ub$ for some unit u.
3. **Irreducible** If $a \neq 0$ and a is not a unit, a is said to be irreducible if $a = bc$, then b or c must be a unit.
4. **Prime** If $a \neq 0$ and a is not a unit, a is said to be prime if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Fact 3.2

Unique Factorization

Let R be an integral domain.
设R为整环。若$a, b \in R$，且存在$c \in R$使得$a = bc$，则称b为a的因子，记为$b|a$。若e不是a的因子，则记为$e \nmid a$。

Definition 3.1

1. **unit** A unit in a integral domain R is an element with multiplicative inverse.
2. **Associate** The elements a and b are associates if $a = ub$ for some unit u.
3. **Irreducible** If $a \neq 0$ and a is not a unit, a is said to be irreducible if $a = bc$, then b or c must be a unit.
4. **Prime** If $a \neq 0$ and a is not a unit, a is said to be prime if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Fact 3.2

Unique Factorization

Let R be an integral domain.
设R为整环。若$a, b \in R$，且存在$c \in R$使得$a = bc$，则称b为a的因子，记为$b|a$。若e不是a的因子，则记为$e \nmid a$。

Definition 3.1

1. **unit** A unit in a integral domain R is an element with multiplicative inverse.
2. **Associate** The elements a and b are associates if $a = ub$ for some unit u.
3. **Irreducible** If $a \neq 0$ and a is not a unit, a is said to be irreducible if $a = bc$, then b or c must be a unit.
4. **Prime** If $a \neq 0$ and a is not a unit, a is said to be prime if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Fact 3.2

- a is prime iff (a) is a prime ideal (excluding (0)).

Unique Factorization

Lemma 3.3

If a is prime, then a is irreducible, but not conversely.

Proof.

- If a is prime and $a = bc$, then $a|bc$, so $a|b$ or $a|c$. If $a|b$, we denote by $b = ad$, then $b = ad = bcd$, so $cd = 1$ and therefore c is a unit.
- If a is irreducible, we need to find an example that a is not prime. Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, then 2 in R is irreducible but not prime. Because suppose $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$; then $4 = (a^2 + 3b^2)(c^2 + 3d^2)$, then $a^2 + 3b^2 \neq 2$, so $a^2 + 3b^2 \neq 2 = 1$ or 4. Let $a^2 + 3b^2 = 1$, then $a = \pm 1, b = 0$。So 2 is irreducible. But $2 \mid 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and $2 \nmid (1 \pm \sqrt{-3})$, so 2 is not prime.

□

Unique Factorization

Lemma 3.3

If a is prime, then a is irreducible, but not conversely.

Proof.

- If a is prime and $a = bc$, then $a|bc$, so $a|b$ or $a|c$. If $a|b$, we denote by $b = ad$, then $b = ad = bcd$, so $cd = 1$ and therefore c is a unit.
- If a is irreducible, we need to find an example that a is not prime. Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, then 2 in R is irreducible but not prime. Because suppose $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$; then $4 = (a^2 + 3b^2)(c^2 + 3d^2)$, then $a^2 + 3b^2 \neq 2$, so $a^2 + 3b^2 \neq 2 = 1$ or 4. Let $a^2 + 3b^2 = 1$, then $a = \pm 1, b = 0$。 So 2 is irreducible. But $2 \mid 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and $2 \nmid (1 \pm \sqrt{-3})$, so 2 is not prime.

□

Unique Factorization

Lemma 3.3

If a is prime, then a is irreducible, but not conversely.

Proof.

- If a is prime and $a = bc$, then $a|bc$, so $a|b$ or $a|c$. If $a|b$, we denote by $b = ad$, then $b = ad = bcd$, so $cd = 1$ and therefore c is a unit.
- If a is irreducible, we need to find an example that a is not prime. Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, then 2 in R is irreducible but not prime. Because suppose $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$; then $4 = (a^2 + 3b^2)(c^2 + 3d^2)$, then $a^2 + 3b^2 \neq 2$, so $a^2 + 3b^2 \neq 2 = 1$ or 4. Let $a^2 + 3b^2 = 1$, then $a = \pm 1, b = 0$。So 2 is irreducible. But $2 \mid 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and $2 \nmid (1 \pm \sqrt{-3})$, so 2 is not prime.

$\square$

Unique Factorization

素元与不可约元在惟一分解的意义下合二为一。

Definition 3.4 (unique factorization domain)

A unique factorization domain is an integral domain R satisfying the following properties:

- **Existence** Every nonzero element a in R can be expressed as $a = up_1 \ldots p_n$, where u is a unit, the p_i are irreducible and $n \in \mathbb{N}$.
- **Uniqueness** If a has another factorization, say $a = vq_1 \ldots q_m$, where v is a unit and the q_i are irreducible, then $n = m$ and, after reordering if necessary, p_i and q_i are associates for each i.

Theorem 3.5

In a unique factorization domain, a is irreducible iff a is prime.

Unique Factorization

素元与不可约元在惟一分解的意义下合二为一。

Definition 3.4 (unique factorization domain)

A unique factorization domain is an integral domain R satisfying the following properties:

- **Existence** Every nonzero element a in R can be expressed as $a = up_1 \ldots p_n$, where u is a unit, the p_i are irreducible and $n \in \mathbb{N}$.
- **Uniqueness** If a has another factorization, say $a = vq_1 \ldots q_m$, where v is a unit and the q_i are irreducible, then $n = m$ and, after reordering if necessary, p_i and q_i are associates for each i.

Theorem 3.5

In a unique factorization domain, a is irreducible iff a is prime.

Unique Factorization

素元与不可约元在惟一分解的意义下合二为一。

Definition 3.4 (unique factorization domain)

A unique factorization domain is an integral domain R satisfying the following properties:

- **Existence** Every nonzero element a in R can be expressed as $a = up_1 \dots p_n$, where u is a unit, the p_i are irreducible and $n \in \mathbb{N}$.
- **Uniqueness** If a has another factorization, say $a = vq_1 \dots q_m$, where v is a unit and the q_i are irreducible, then $n = m$ and, after reordering if necessary, p_i and q_i are associates for each i.

Theorem 3.5

In a unique factorization domain, a is irreducible iff a is prime.

Unique Factorization

素元与不可约元在惟一分解的意义下合二为一。

Definition 3.4 (unique factorization domain)

A unique factorization domain is an integral domain R satisfying the following properties:

- **Existence** Every nonzero element a in R can be expressed as $a = up_1 \ldots p_n$, where u is a unit, the p_i are irreducible and $n \in \mathbb{N}$.
- **Uniqueness** If a has another factorization, say $a = vq_1 \ldots q_m$, where v is a unit and the q_i are irreducible, then $n = m$ and, after reordering if necessary, p_i and q_i are associates for each i.

Theorem 3.5

In a unique factorization domain, a is irreducible iff a is prime.

Unique Factorization

Proof.

Since prime implies irreducible, so we don't need to prove this. Assume a is irreducible, and let $a \mid bc$, Then we have $ad = bc$ for some $d \in R$. We factor d, b and c into irreducibles to obtain

$$aud_1 \dots d_r = vb_1 \dots b_s wc_1 \dots c_t$$

where u, v and w are units and d_i, b_i and c_i are irreducible. By uniqueness of factorization, a, which is irreducible, must be an associate of some b_i or c_i. Thus a divides b or a divides c. $\square$

Unique Factorization

Definition 3.6

Let R be an integral domain. Let $A \subset R$, with $0 \notin A$. The element d is a greatest common divisor (gcd) of A if d divides each a in A, and whenever e divides each a in A, we have $e|d$.

Fact 3.7

If $d'|d$ and $d|d'$, so that d and d' are associates.

在相伴的意义下，最大公因子是惟一的。

Unique Factorization

Definition 3.6

Let R be an integral domain. Let $A \subset R$, with $0 \notin A$. The element d is a greatest common divisor (gcd) of A if d divides each a in A, and whenever e divides each a in A, we have $e|d$.

Fact 3.7

If $d'|d$ and $d|d'$, so that d and d' are associates.

在相伴的意义下，最大公因子是惟一的。

Unique Factorization

Definition 3.6

Let R be an integral domain. Let $A \subset R$, with $0 \notin A$. The element d is a greatest common divisor (gcd) of A if d divides each a in A, and whenever e divides each a in A, we have $e|d$.

Fact 3.7

If $d'|d$ and $d|d'$, so that d and d' are associates.

在相伴的意义下，最大公因子是惟一的。

Unique Factorization

Let R be an integral domain. Let $A \subseteq R$.

Definition 3.8

The elements of A are said to be relatively prime if 1 is a $\gcd$ of A.

Definition 3.9

The nonzero element m is a least common multiple (lcm) of A if each a in A divides m, and whenever $a|e$ for each $a \in A$, we have $m|e$.

在环R中，如果$a|b$，当且仅当理想$(b) \leq (a)$。元素间的整除关系等价于元素的所生成的理想间的包含关系！

Unique Factorization

Let R be an integral domain. Let $A \subseteq R$.

Definition 3.8

The elements of A are said to be relatively prime if 1 is a $\gcd$ of A.

Definition 3.9

The nonzero element m is a least common multiple (lcm) of A if each a in A divides m, and whenever $a|e$ for each $a \in A$, we have $m|e$.

在环R中，如果$a|b$，当且仅当理想$(b) \leq (a)$。元素间的整除关系等价于元素的所生成的理想间的包含关系！

Unique Factorization

Let R be an integral domain. Let $A \subseteq R$.

Definition 3.8

The elements of A are said to be relatively prime if 1 is a $\gcd$ of A.

Definition 3.9

The nonzero element m is a least common multiple (lcm) of A if each a in A divides m, and whenever $a|e$ for each $a \in A$, we have $m|e$.

在环R中，如果$a|b$，当且仅当理想$(b) \leq (a)$。元素间的整除关系等价于元素的所生成的理想间的包含关系！

Unique Factorization

Theorem: Let R be an integral domain, Then:

- If R is a UFD, then R satisfies the ascending chain condition on principal ideals, in other words,
  if $a_1, a_2, \ldots \in R$ and $< a_1 > \subsetneq < a_2 > \subsetneq \ldots$, then the sequence is finite.
  真因子链$a_1, a_2, \cdots$是有限的。（注：真因子为非平凡因子）
- If R satisfies the ascending chain condition on principal ideals, then every nonzero element of R can be factored into irreducibles.
- If every nonzero element of R can be factored into irreducibles, and every irreducible element of R is prime, then R is a UFD.
- UFD$\Rightarrow$ 真因子链有限。
- 整环R中，(1)真因子链有限 $\Rightarrow$ (2)任一元素都可分解为有限个不可约元的乘积；
  (3) 条件：任意不可约元都是素元。
- $(1)(3) \Leftrightarrow$整环R是UFD$\Leftrightarrow$ (2)(3)。

Unique Factorization

Theorem: Let R be an integral domain, Then:

- If R is a UFD, then R satisfies the ascending chain condition on principal ideals, in other words,
  if $a_1, a_2, \ldots \in R$ and $< a_1 > \subsetneq < a_2 > \subsetneq \ldots$, then the sequence is finite.
  真因子链$a_1, a_2, \cdots$是有限的。（注：真因子为非平凡因子）
- If R satisfies the ascending chain condition on principal ideals, then every nonzero element of R can be factored into irreducibles.
- If every nonzero element of R can be factored into irreducibles, and every irreducible element of R is prime, then R is a UFD.

- UFD$\Rightarrow$ 真因子链有限。
- 整环R中，(1)真因子链有限 $\Rightarrow$ (2)任一元素都可分解为有限个不可约元的乘积；
  (3) 条件：任意不可约元都是素元。
- $(1)(3) \Leftrightarrow$整环R是UFD$\Leftrightarrow$ (2)(3)。

Unique Factorization

Theorem: Let R be an integral domain, Then:

- If R is a UFD, then R satisfies the ascending chain condition on principal ideals, in other words, if $a_1, a_2, \ldots \in R$ and $< a_1 > \subsetneq < a_2 > \subsetneq \ldots$, then the sequence is finite. 真因子链$a_1, a_2, \cdots$是有限的。（注：真因子为非平凡因子）
- If R satisfies the ascending chain condition on principal ideals, then every nonzero element of R can be factored into irreducibles.
- If every nonzero element of R can be factored into irreducibles, and every irreducible element of R is prime, then R is a UFD.

- UFD$\Rightarrow$ 真因子链有限。
- 整环R中，(1)真因子链有限 $\Rightarrow$ (2)任一元素都可分解为有限个不可约元的乘积；
  (3) 条件：任意不可约元都是素元。
- $(1)(3) \Leftrightarrow$整环R是UFD$\Leftrightarrow$ (2)(3)。

Principal ideal domain

Fact 3.10

Thus R is UFD iff R satisfies the ascending chain condition and every irreducible element of R is prime.

Definition 3.11

A principal ideal domain (PID) is an integral domain in which every ideal is principal, that is, generated by a single element.

Principal ideal domain

Fact 3.10

Thus R is UFD iff R satisfies the ascending chain condition and every irreducible element of R is prime.

Definition 3.11

A principal ideal domain (PID) is an integral domain in which every ideal is principal, that is, generated by a single element.

Principal ideal domain

Theorem 3.12

Every principal ideal domain is a unique factorization domain. For short, PID implies UFD.

Proof:

- If $< a_1 > \subsetneq < a_2 > \subsetneq \cdots$, let $I = \bigcup_i < a_i >$. Then I is an ideal.
- Let $I =< b >$, then $b \in < a_n >$ for some n. Hence $I \subseteq < a_n >$.
- We have $< a_i > \subseteq I \subseteq < a_n > \subseteq < a_i >$ for $i \geq n$.
- Therefore $< a_i > = < a_n >$ for $i \geq n$. Acc on principal ideals is satisfied.

Principal ideal domain

Theorem 3.12

Every principal ideal domain is a unique factorization domain. For short, PID implies UFD.

Proof:

- If $< a_1 > \subsetneq < a_2 > \subsetneq \cdots$, let $I = \bigcup_i < a_i >$. Then I is an ideal.
- Let $I =< b >$, then $b \in < a_n >$ for some n. Hence $I \subseteq < a_n >$.
- We have $< a_i > \subseteq I \subseteq < a_n > \subseteq < a_i >$ for $i \geq n$.
- Therefore $< a_i > = < a_n >$ for $i \geq n$. Acc on principal ideals is satisfied.

Principal ideal domain

Theorem 3.12

Every principal ideal domain is a unique factorization domain. For short, PID implies UFD.

Proof:

- If $< a_1 >\subsetneq< a_2 >\subsetneq \cdots$, let $I = \bigcup_i < a_i >$. Then I is an ideal.
- Let $I =< b >$, then $b \in< a_n >$ for some n. Hence $I \subseteq< a_n >$.
- We have $< a_i >\subseteq I \subseteq< a_n >\subseteq< a_i >$ for $i \geq n$.
- Therefore $< a_i >=< a_n >$ for $i \geq n$. Acc on principal ideals is satisfied.

Principal ideal domain

Theorem 3.12

Every principal ideal domain is a unique factorization domain. For short, PID implies UFD.

Proof:

- If $< a_1 >\subsetneq< a_2 >\subsetneq \cdots$, let $I = \bigcup_i < a_i >$. Then I is an ideal.
- Let $I =< b >$, then $b \in< a_n >$ for some n. Hence $I \subseteq< a_n >$.
- We have $< a_i >\subseteq I \subseteq< a_n >\subseteq< a_i >$ for $i \geq n$.
- Therefore $< a_i >=< a_n >$ for $i \geq n$. Acc on principal ideals is satisfied.

Principal ideal domain

Theorem 3.12

Every principal ideal domain is a unique factorization domain. For short, PID implies UFD.

Proof:

- If $< a_1 > \subsetneq < a_2 > \subsetneq \cdots$, let $I = \bigcup_i < a_i >$. Then I is an ideal.
- Let $I = < b >$, then $b \in < a_n >$ for some n. Hence $I \subseteq < a_n >$.
- We have $< a_i > \subseteq I \subseteq < a_n > \subseteq < a_i >$ for $i \geq n$.
- Therefore $< a_i > = < a_n >$ for $i \geq n$. Acc on principal ideals is satisfied.

Principal ideal domain

- Let a be an irreducible. Then $< a >$ is a proper ideal.
- By acc on principal ideals, $< a > \subseteq M$ for some M a maximal principal ideal.
- Let $M =< b >$, then $b|a$, and b is not a unit, so b is an associate of a, hence $< b >=< a >$.
- M is a prime ideal, so is $< a >$. Hence a is prime.

Principal ideal domain

- Let a be an irreducible. Then $< a >$ is a proper ideal.
- By acc on principal ideals, $< a > \subseteq M$ for some M a maximal principal ideal.
- Let $M =< b >$, then $b|a$, and b is not a unit, so b is an associate of a, hence $< b >=< a >$.
- M is a prime ideal, so is $< a >$. Hence a is prime.

Principal ideal domain

- Let a be an irreducible. Then $< a >$ is a proper ideal.
- By acc on principal ideals, $< a > \subseteq M$ for some M a maximal principal ideal.
- Let $M =< b >$, then $b|a$, and b is not a unit, so b is an associate of a, hence $< b >=< a >$.
- M is a prime ideal, so is $< a >$. Hence a is prime.

Principal ideal domain

- Let a be an irreducible. Then $< a >$ is a proper ideal.
- By acc on principal ideals, $< a > \subseteq M$ for some M a maximal principal ideal.
- Let $M =< b >$, then $b|a$, and b is not a unit, so b is an associate of a, hence $< b >=< a >$.
- M is a prime ideal, so is $< a >$. Hence a is prime.

Principal ideal domain

Theorem 3.13

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Rightarrow$

- Let R be a PID. Then R is a UFD.
- If $< p >$ is a prime ideal, then $< p > \subseteq < q >$ for some maximal ideal $< q >$.
- $q|p$ and q is not unit, hence p and q are associate.
- $< p > = < q >$, both of which are maximal ideals.

Principal ideal domain

Theorem 3.13

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Rightarrow$

- Let R be a PID. Then R is a UFD.
- If $< p >$ is a prime ideal, then $< p > \subseteq < q >$ for some maximal ideal $< q >$.
- $q|p$ and q is not unit, hence p and q are associate.
- $< p > = < q >$, both of which are maximal ideals.

Principal ideal domain

Theorem 3.13

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Rightarrow$

- Let R be a PID. Then R is a UFD.
- If $< p >$ is a prime ideal, then $< p > \subseteq < q >$ for some maximal ideal $< q >$.
- $q|p$ and q is not unit, hence p and q are associate.
- $< p > = < q >$, both of which are maximal ideals.

Principal ideal domain

Theorem 3.13

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Rightarrow$

- Let R be a PID. Then R is a UFD.
- If $< p >$ is a prime ideal, then $< p > \subseteq < q >$ for some maximal ideal $< q >$.
- $q|p$ and q is not unit, hence p and q are associate.
- $< p > = < q >$, both of which are maximal ideals.

Principal ideal domain

Theorem 3.13

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Rightarrow$

- Let R be a PID. Then R is a UFD.
- If $< p >$ is a prime ideal, then $< p > \subseteq < q >$ for some maximal ideal $< q >$.
- $q|p$ and q is not unit, hence p and q are associate.
- $< p > = < q >$, both of which are maximal ideals.

Principal ideal domain

Theorem 3.14

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof: $\Leftarrow$Let I be an ideal of R. If $I = \{0\}$, obviously I is a principal ideal. Now let $I \neq \{0\}$. $\forall a \in I$, we have $a = up_1p_2 \dots p_t$ due to the fact that R is UFD. Let n is the minimum for t, and $up_1p_2 \dots p_n \in I$. Induction on n:

- If $n = 0$, $I = R = (1)$.
- Suppose that the result holds for all $r < n$, now we prove the case of n.
  - First we prove that $I \subseteq (p_1)$. Suppose that $b \in I$ but $b \notin (p_1)$. $R/(p_1)$ is a field since (p_1) is a maximal ideal. Then $\exists c \in R$ such that $bc = 1+(p_1)$, i.e., $bc-dp_1 = 1$. Hence $bcp_2 \dots p_n - dp_1p_2 \dots p_n = p_2 \dots p_n \in I$. Contradiction to the minimum of n.
  - Let $J = \{x \mid xp_1 \in I\}$. Then J is an ideal and $Jp_1 = I$.
  - J has a minimum $n-1$ (among the numbers of irreducibles in factorization of each element), so $J = (w)$ for some $w \in R$.
  - $I = (p_1w)$.

Principal ideal domain

Theorem 3.14

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Leftarrow$Let I be an ideal of R. If $I = \{0\}$, obviously I is a principal ideal. Now let $I \neq \{0\}$. $\forall a \in I$, we have $a = up_1p_2 \dots p_t$ due to the fact that R is UFD. Let n is the minimum for t, and $up_1p_2 \dots p_n \in I$. Induction on n:

- If $n = 0$, $I = R = (1)$.
- Suppose that the result holds for all $r < n$, now we prove the case of n.
  - First we prove that $I \subseteq (p_1)$. Suppose that $b \in I$ but $b \notin (p_1)$. $R/(p_1)$ is a field since (p_1) is a maximal ideal. Then $\exists c \in R$ such that $bc = 1 + (p_1)$, i.e., $bc - dp_1 = 1$. Hence $bcp_2 \dots p_n - dp_1p_2 \dots p_n = p_2 \dots p_n \in I$. Contradiction to the minimum of n.
  - Let $J = \{x \mid xp_1 \in I\}$. Then J is an ideal and $Jp_1 = I$.
  - J has a minimum $n-1$ (among the numbers of irreducibles in factorization of each element), so $J = (w)$ for some $w \in R$.
  - $I = (p_1w)$.

Principal ideal domain

Theorem 3.14

R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal.

Proof:$\Leftarrow$Let I be an ideal of R. If $I = \{0\}$, obviously I is a principal ideal. Now let $I \neq \{0\}$. $\forall a \in I$, we have $a = up_1p_2 \dots p_t$ due to the fact that R is UFD. Let n is the minimum for t, and $up_1p_2 \dots p_n \in I$. Induction on n:

- If $n = 0$, $I = R = (1)$.
- Suppose that the result holds for all $r < n$, now we prove the case of n.
  - First we prove that $I \subseteq (p_1)$. Suppose that $b \in I$ but $b \notin (p_1)$. $R/(p_1)$ is a field since (p_1) is a maximal ideal. Then $\exists c \in R$ such that $bc = 1+(p_1)$, i.e., $bc-dp_1 = 1$. Hence $bcp_2 \dots p_n-dp_1p_2 \dots p_n = p_2 \dots p_n \in I$. Contradiction to the minimum of n.
  - Let $J = \{x \mid xp_1 \in I\}$. Then J is an ideal and $Jp_1 = I$.
  - J has a minimum $n-1$ (among the numbers of irreducibles in factorization of each element), so $J = (w)$ for some $w \in R$.
  - $I = (p_1w)$.

Principal Ideal Domains and Euclidean Domains

Theorem 4.1

Let R be a PID, with A a nonempty subset of R. Then d is a greatest common divisor of A iff d is a generator of (A).

Proof:

- **1.** Let d be a $\gcd$ of A, and assume that

$$(A) = (b) = \left\{\sum r_i a_i \mid r_i \in R, a_i \in A\right\}.$$

  - Then d divides every $a \in A$, so d divides all finite sums $\sum r_i a_i$, in particular d divides b,hence $(b) \subseteq (d)$,that is, $(A) \subseteq (d)$.
  - But if $a \in A$ then $a \in (b)$, so that b divides a. Since d is a $\gcd$ of A, it follows that b divides d, so (d) is contained in $(b) = (A)$.

  We conclude that $(A) = (d)$, proving that d is a generator of (A).

Principal Ideal Domains and Euclidean Domains

Proof:

- **2.** Conversely,assume that d generates $< A >$. If $a \in A$ then a is a multiple of d,so that $d|a$. Since d can be expressed as $\sum r_i a_i$,any element that divides everything in A divides d, so that d is a gcd of A.

Principal Ideal Domains and Euclidean Domains

Corollary 4.2

If d is a $\gcd$ of A, where A is a nonempty subset of the PID R,then d can be expressed as a finite linear combination $\sum r_i a_i$ of elements of A with coefficients in R.

Definition 4.3 (Euclidean domain)

Let R be an integral domain. R is said to be a Euclidean domain (ED) if there is a function Ψ from $R \setminus \{0\}$ to the nonnegative integers satisfying the following property:

- If a and b are elements of R,with $b \neq 0$, then a can be expressed as $bq + r$ where either $r = 0$ or $\Psi(r) < \Psi(b)$.
- We can replace "$r = 0$ or $\Psi(r) < \Psi(b)$" by simply "$\Psi(r) < \Psi(b)$" if we define $\Psi(0)$ to be $-\infty$.

Theorem 4.4

If R is a Euclidean domain, then R is a principal ideal domain. For short, ED implies PID.

Proof:

- Let I be an ideal of R. If $I = \{0\}$ then I is principal,so assume $I \neq \{0\}$. Then $\{\Psi(b) : b \in I, b \neq 0\}$ is a nonempty set of nonnegative integers, and therefore has a smallest element n.
- Let b be any element of I such that $\Psi(b) = n$; we claim that $I =< b >$. For if a belongs to I then we have $a = bq + r$ where $r = 0$ or $\Psi(r) < \Psi(b)$. Now $r = a - bq \in I$ (because a and b belong to I),so if $r \neq 0$ then $\Psi(r) < \Psi(b)$ is impossible by minimality of $\Psi(b)$. Thus b is a generator of I.

Rings of Fractions

Definition 5.1

Let S be a subset of the ring R; we say that S is multiplicative if $0 \notin S$, $1 \in S$, and whenever a and b belong to S, we have $ab \in S$.

Example: $S = R \setminus \{0\}$.

If S is a multiplicative subset of the commutative ring R, we define the following equivalence relation on $R \times S$:

- $(a, b) \sim (c, d)$ iff for some $s \in S$ we have $s(ad - bc) = 0$.

Rings of Fractions

Definition 5.2

Define the fraction $\frac{a}{b}$ to be the equivalence class of the pair (a, b).

- The set of all equivalence classes is denoted by $S^{-1}R$, and is called (in view of what we are about to prove) the ring of fractions of R by S.

Rings of Fractions

- addition: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
- multiplication: $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$
- additive identity: $\frac{0}{1}$
- additive inverse: $-(\frac{a}{b}) = \frac{-a}{b}$
- multiplicative identity: $\frac{1}{1}$

Theorem 5.3

If R is an integral domain,so is $S^{-1}R$. If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is a field (the field of fractions or quotient field of R) and R can be embedded in its quotient field.

Fact 5.4

The quotient field F of an integral domain R is the smallest field containing R.

Proof: We may regard R as a subset of F,so that F is a field containing R.

But if L is any field containing R, then all fractions a/b, $a, b \in R$, must belong to L. Thus $F \subseteq L$.

Irreducible Polynomials

Definition 6.1 (Irreducible Polynomials)

Let R be a integral domain, and $R[X]$ is a integral domain,

- We will refer to an irreducible element of $R[X]$ as an irreducible polynomial.
- A polynomial that is not irreducible is said to be reducible or factorable.

Example 6.2

- X^2+1 is irreducible in $\mathbb{R}[X]$ where $\mathbb{R}$ is the field of real numbers
- X^2+1 is reducible in $\mathbb{C}[X]$ where $\mathbb{C}$ is the field of complex numbers.

作业

Page. 164，习题4-1：5
Page. 181，习题4-3：1(4)(6)，19
Page. 190，习题4-4：1，7