Lecture Notes On Abstract Algebra (Week 4)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 7 (Sep 26, 2023): UFD

1.1 UFD

Throughout this lecture R will denote a commutative integral domain (i.e. a commutative ring with identity containing no zero-divisors).

Recall that a unit of R is an element that has an inverse with respect to multiplication. If a is any element of R and u is a unit, we can write

$$a = u(u^{-1}a).$$

This is not considered to be a proper factorization of a. For example we do not consider $5 = 1 \times 5$ or $5 = (-1)(-5)$ to be proper factorizations of 5 in $\mathbb{Z}$. Similarly we do not consider

$$x^2 + 2 = 2(\frac{1}{2}x^2 + 1)$$

to be a proper factorization of $x^2 + 2$ in $\mathbb{Q}[x]$.

Definition 1.1. *A nonzero element α in an integral domain R is called* **irreducible** (不可约) *if it is not a unit, and if whenever α is written as a product of two elements of R, one of which is a unit.*

π is irreducible $\Longleftrightarrow$ $\pi = ab$ implies either a or b is a unit.

Two elements r and s of R are called **associate** (相伴) to each other if $s = ur$ for some unit u of R. If r and s are associate, we write $r \sim s$. For example, $3x^2 + 6$ is associate to $x^2 + 2$ in $\mathbb{Q}[x]$, but $3x^2 + 6$ is NOT associate to $x^2 + 2$ in $\mathbb{Z}[x]$.

It's easy to see that

(1) u is a unit if and only if $u \sim 1$;

(2) the relation "$\sim$" is an equivalence relation.

Remark 1.1. 1. One can easily see that $s \sim r$ if and only if $(s) = (r)$ as principal ideals.

$$\boxed{a \sim b \Longleftrightarrow (a) = (b)}$$

2. If $a \sim \pi$ and π is irreducible, then a is irreducible.

Example 1.1. In $\mathbb{Z}$ the units are 1 and -1 and each non-zero non-unit element has two associates, namely itself and its negative. So 5 and -5 are associates, 6 and -6 are associates, and so on. The irreducible elements of $\mathbb{Z}$ are p and $-p$, for p prime.

Example 1.2. In $\mathbb{Q}[x]$, the units are the non-zero constant polynomials. The associates of a non-zero non-constant polynomial $f(x)$ are the polynomials of the form $af(x)$ where $a \in \mathbb{Q}^\times$. So x^2+2 is associate to $3x^2+6$, $\frac{1}{2}x^2+1$, etc.

Example 1.3. In Gaussian integers $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$, there are only four units: $\pm 1, \pm\sqrt{-1}$. We have $2 = (1-\sqrt{-1})(1+\sqrt{-1})$. Hence 2 is not irreducible. Since $1-\sqrt{-1} = -\sqrt{-1}(1+\sqrt{-1})$, $1-\sqrt{-1}$ and $1+\sqrt{-1}$ are associates. Actually, $1+\sqrt{-1}$ is irreducible. So $2 = -\sqrt{-1}(1+\sqrt{-1})^2$.

Definition 1.2. *An integral domain R is a* **unique factorization domain** *(UFD)* (唯一分解整环) *if the following conditions hold for each element α of R that is neither zero nor a unit.*

1. *Every α can be written as a product of a finite number of irreducible elements of R.*
2. *This can be done in an essentially unique way. If $\alpha = p_1 p_2 \cdots p_r$ and $\alpha = q_1 q_2 \cdots q_s$ are two expressions for α as products of irreducible elements, then $s = r$ and $q_1, q_2, \cdots, q_s$ can be reordered so that for each i, q_i is an associate of p_i.*

Remark 1.2. Note that UFD does not mean USB Flash Drive. A UFD is also called a *Gaussian domain*(高斯整环).

Example 1.4. The integer ring $\mathbb{Z}$ is a UFD. This is the *Fundamental Theorem of Arithmetic*. It's all because of the unique factorization property of $\mathbb{Z}$ that the Riemann zeta function has an expansion of infinite product:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}}, \ \Re(z) > 1$$

where p ranges over all prime numbers.

Definition 1.3. *Let $a, b \in R$. If $a = bc$ for some $c \in R$, then we say b is a* **divisor** *of a or say that a is a multiple of b, denoted by $b \mid a$. If $b \mid a$ and a, b are not associates, we say b is a* **proper divisor** (真因子) *of a. If b is not a divisor of a, we write $b \nmid a$.*

One can see that $2+\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$ is a divisor of 10. Eventually 10 is a multiplier of $2+\sqrt{-6}$. But $2+\sqrt{-6}$ is not a divisor of 5.

Remark 1.3. 1. It's clear that $a \mid b$ if and only if $b \in (a)$, or $(b) \subseteq (a)$. Consequently, if $a, b \neq 0$, then $(a) = (b)$ if and only if $a \mid b$ and $b \mid a$, or equivalently $a \sim b$.

2. An irreducible element can not be factored as a product of two proper divisors.

Definition 1.4. *Let $a, b \in R$. An element d is called a* **greatest common divisor** *(gcd for short)* (最大公因子) *of a and b if $d \mid a$ and $d \mid b$; and if c is an element such that $c \mid a$ and $c \mid b$, then $c \mid d$.*

If d' is another gcd of a and b, then $d' \mid d$ and $d \mid d'$ by the definition of gcd. Hence $d \sim d'$. Thus, the gcd of two elements is uniquely determined up to units if it exists. We denote any gcd of a and b as (a, b). If $(a, b) \sim 1$, we say a and b are **relatively prime** (or **coprime**) (互素). Two coprime elements have no common divisor other than units.

Let

$$a = up_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},\ b = vp_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

be the decompositions of a, b as irreducible divisors. Here u, v are units and $p_1, p_2, \cdots, p_r$ are distinct irreducible elements. All $e_i, f_i \geq 0$ and $e_i + f_i \geq 1$. Then

$$\prod_{i=1}^{r} p_i^{\min\{e_i, f_i\}}$$

is a greatest common divisor of a and b.

Properties of UFD

1. every element has only finite many non-associate proper divisors;
2. two elements always have a gcd;
3. $(ca, cb) \sim c(a, b)$;
4. if $(a, b) \sim 1, (a, c) \sim 1$, then $(a, bc) \sim 1$.

Remark 1.4. If d is a gcd of a, b in a UFD, then $(a, b) = (d)$ is not necessarily true. For example, $\mathbb{Z}[x, y]$ is a UFD and x, y are relatively prime, but $(x, y) \neq (1)$.

The Ring $\mathbb{Z}[\sqrt{-6}]$ is Not A UFD Note that

$$\mathbb{Z}[\sqrt{-6}] = \left\{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\right\}.$$

It's easy to show that $\mathbb{Z}[\sqrt{-6}]$ is a domain. We claim that $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.
The proof of this claim will involve a number of steps.

1. We define a function $\delta : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}_{\geq 0}$ by $\delta(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ denotes the complex conjugate of $\alpha \in \mathbb{C}$. Thus

$$\delta(a + b\sqrt{-6}) = (a + b\sqrt{-6})(a - \sqrt{-6}) = a^2 + 6b^2. \tag{1}$$

Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$. Then

$$\delta(\beta) = \delta(\alpha)\delta(\beta).$$

So δ is multiplicative.

2. Suppose $\alpha \in \mathbb{Z}[\sqrt{-6}]^\times$ and let β be its inverse. Then $\delta(\alpha\beta) = \delta(1) = 1 = \delta(\alpha)\delta(\beta)$. Since $\delta(\alpha)$ and $\delta(\beta)$ are positive integers this means $\delta(\alpha) = \delta(\beta) = 1$. So $\delta(\alpha) = 1$ whenever α is a unit.

On the other hand $\delta(a + b\sqrt{-6}) = 1$ implies $a^2 + 6b^2 = 1$ for integers a and b which means $b = 0$ and $a = \pm 1$. So $\alpha \in \mathbb{Z}[\sqrt{-6}]$ is a unit if and only if $\delta(\alpha) = 1$ and hence $\mathbb{Z}[\sqrt{-6}]^\times = \{1, -1\}$.

3. Note that

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}). \tag{2}$$

We have $10 = \delta(2+\sqrt{-6})$. If $2+\sqrt{-6}$ is not irreducible in $\mathbb{Z}[\sqrt{-6}]$ then it factorizes as $\alpha_1\alpha_2$ where α_1 and α_2 are non-units. Then we must have $\delta(\alpha_1) = 2, \delta(\alpha_2) = 5$ or $\delta(\alpha_1) = 5, \delta(\alpha_2) = 2$. In either case would means $2 = c^2 + 6d^2$ for integers c and d which is impossible. So $2 + \sqrt{-6}$ is irreducible in $\mathbb{Z}[\sqrt{-6}]$. Similarly $2 - \sqrt{-6}$ is also irreducible.

$$\boxed{x^2 + 6y^2 = 2 \text{ has no solutions in } \mathbb{Z} \Longrightarrow 2 \pm \sqrt{-6} \text{ is irreducible in } \mathbb{Z}[\sqrt{-6}].}$$

If 5 is irreducible, then $5 = \beta_1\beta_2$ where β_1 and β_2 are not units. Then we must have $\delta(\beta_1) = \delta(\beta_2) = 5$. This would means that $5 = c^2 + 6d^2$ for some integers c and d which is impossible. So 5 is irreducible. Similarly 2 is irreducible as well.

4. Since any two of $2, 5, 2 + \sqrt{-6}, 2 - \sqrt{-6}$ are not associates, we conclude from (2) that the factorizations of 10 above are genuinely different, and hence $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.

Exercises

1. Let π be a nonzero element of a domain R and $\pi \notin R^\times$. Show that π is irreducible if and only if (π) is a maximal element among principal ideals. Furthermore, if R is a principal ideal domain, then π is irreducible if and only if (π) is a maximal ideal.
2. Show that the ring $\mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{10}]$ are not UFD.
3. Show that $\mathbb{Z}[x]$ is a UFD, but not a principal ideal domain.
4. Show that the formal power series $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ has the following expansion of infinite product:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - p^{-s}\right)^{-1},$$

where p ranges over all prime numbers.

1.2 Criterions for Unique Factorization

Before discussing the criterions for testing UFD, we need the following definitions.

Definition 1.5. *A nonzero element π of R is called a* **prime** (素元) *if π is not a unit and if $\pi \mid ab$ implies either $\pi \mid a$ or $\pi \mid b$.*

Basic Facts on Prime Elements

1. π is prime $\Longleftrightarrow$ $\pi \mid ab$ implies $\pi \mid a$ or $\pi \mid b$.
2. π is prime $\Longleftrightarrow$ (π) is a prime ideal.
3. π, π_1 are primes and $\pi \mid \pi_1 \Longrightarrow \pi \sim \pi_1$.
4. A prime element is always irreducible.

Remark 1.5. 1. Let $\pi \notin R^\times$ and $\pi \neq 0$. Then π is a prime element if and only if $\pi \nmid a$ and $\pi \nmid b$ implies $\pi \nmid ab$. It's obvious that the associates of a prime are still primes.

2. A prime element is always irreducible.

   Actually, if $\pi \in R$ is a prime, then $\pi \neq 0$ and $\pi \notin R^\times$. Assume $\pi = ab$. Then $\pi \mid ab$ and thus $\pi \mid a$ or $\pi \mid b$. WLOG we assume $\pi \mid a$. There will be some $c \in R$ such that $a = c\pi$. Hence $\pi = bc\pi$. So $bc = 1$, yielding b is a unit. Consequently π is irreducible.

3. Irreducible elements in a UFD are primes.

   In fact, let π be irreducible and $\pi \mid ab$, then there exists some $c \in R$ such that $ab = \pi c$. Since π is an irreducible element and R is uniquely factored, π (or its associates) must appear in the decomposition of a or b. This implies $\pi \mid a$ or $\pi \mid b$. Thus π is a prime.

4. Generally an irreducible element may not be a prime. For example, we know 2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$, but 2 is not a prime in $\mathbb{Z}[\sqrt{-6}]$, since $2 \mid (2+\sqrt{-6})(2-\sqrt{-6})$, but $2 \nmid (2+\sqrt{-6})$, $2 \nmid (2-\sqrt{-6})$.

The following theorem demonstrates a criterion for testing UFD.

Theorem 1.1. *Let R be a domain. Then R is a UFD if and only if the following conditions are satisfied:*

1. (Divisors chain condition) *R contains no infinite sequences of elements $a_1, a_2, \ldots$ such that a_{i+1} is a proper divisor of a_i.*

   In other words, if $a_1, a_2, \ldots$ is a sequence of elements in R such that $a_{i+1} \mid a_i$ for all $i \geq 1$, then there exists some positive integer m such that $a_k \sim a_m$ for all $k \geq m$.

2. (Primeness condition) *Every irreducible element of R is a prime.*

By Theorem 1.1, $\mathbb{Z}[\sqrt{-6}]$ is not a UFD, because it does not satisfy the primeness condition. Actually, 2 is irreducible, but not a prime, in $\mathbb{Z}[\sqrt{-6}]$. Note that $\mathbb{Z}[\sqrt{-6}]$ satisfies the divisor chain condition (why?).

Remark 1.6. Note that principle ideal $(a) \subseteq (b)$ if and only if $b \mid a$. Hence the **Divisor Chain Condition (DCC)** on elements is equivalent to the **Ascending Chain Condition (ACC)** on principal ideals: every ascending chain of principal ideals is stable (if $(a_1) \subseteq (a_2) \subseteq \cdots$ is an ascending chain of principal ideals, then there exists some positive integer m such that $(a_k) = (a_m)$ for all $k \geq m$).

Divisor chain on elements $\Longleftrightarrow$ Ascending chain on principal ideals

The primeness condition can be replaced by the GCD condition to achieve another criterion for testing UFD.

Theorem 1.2. *Let R be a domain. Then R is a UFD if and only if the following conditions are satisfied:*

1. (Divisors chain condition) *R contains no infinite sequences of elements $a_1, a_2, \cdots$ such that a_{i+1} is a proper divisor of a_i.*

2. (GCD condition) *Any two elements of R have a greatest common divisor (gcd).*

Remark 1.7. The GCD condition implies the primeness condition.

$$
\begin{aligned}
\text{UFD} &\iff \text{DCC on elements} + \text{Primeness condition} \\
&\iff \text{ACC on principal ideals} + \text{Primeness condition} \\
&\iff \text{DCC on elements} + \text{GCD condition} \\
&\iff \text{ACC on principal ideals} + \text{GCD condition}
\end{aligned}
$$

Exercises

1. Show that $\mathbb{Z}[\sqrt{-5}]$ satisfies DCC on elements, but $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
2. The following exercise shows that a subring of a UFD is not necessarily a UFD.

   Let
   $$R = \{f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}.$$
   Show that

   (1) R is a subring of $\mathbb{Q}[x]$;

   (2) $2 \in R$ is not invertible;

   (3) the ascending chain of principal ideals $(x) \subsetneq (\frac{x}{2}) \subsetneq (\frac{x}{2^2}) \subsetneq \cdots \subsetneq (\frac{x}{2^n}) \subsetneq$ is not stable;

   (4) R is not a UFD.
3. Let p be a prime of the form $4n+1$ and let q be a prime such that the Legendre symbol $\left(\frac{q}{p}\right) = -1$. Show that $\mathbb{Z}[\sqrt{pq}]$ is not a UFD.

2 Lecture 8 (Sep 28, 2023): PID and Euclidean Domain

2.1 A PID is a UFD

Recall we have defined what is principal ideal ring. A (commutative) domain R is called a **principal ideal domain** (PID for short) if every ideal of R is principal. For example, $\mathbb{Z}$ is a PID, which is the simplest kind of rings.

Basic Properties of PID

1. The prime ideals are of the form: (0), (π), where π is a prime element.
2. Every nonzero prime ideal is maximal in a PID.

   In fact, let (π) be a prime ideal in a PID R and $(\pi) \subsetneq (\gamma)$. Then
   $$\pi = \gamma u$$
   for some $u \in R$ and u is not a unit. Notices that π is a prime element and $\pi \mid \gamma u$. We have $\pi \mid \gamma$ or $\pi \mid u$.

   If $\pi \mid \gamma$, then $\gamma = \pi v$ for some $v \in R$. Thus $\pi = \pi u v$, yielding $uv = 1$. Hence u is a unit, contradiction. So $\pi \mid u$, $u = \pi w$ for some $w \in R$. This means $\gamma w = 1$. Hence γ is a unit and $(\gamma) = R$. Consequently (π) is maximal.

3. Two elements in a PID always have a greatest common divisor. This is, a PID satisfies the GCD condition.

   Actually, let a, b be elements of R which is a PID, then $(a) + (b) = (d)$ for some $d \in R$. Hence $(a) \subseteq (d), (b) \subseteq (d)$ and there exist $u, v \in R$ such that

   $$d = au + bv.$$

   It follows that $d \mid a, d \mid b$. Consequently $d' \mid d$ for every common divisor d' of a and b. Therefore d is a greatest common divisor of a and b.

Theorem 2.1. *A PID is a UFD.*

Proof. We already know that the GCD condition holds for a PID. It suffices to check the ascending chain condition on principal ideals: every ascending chain of principal ideals is stable.

Let $(a_1) \subseteq (a_2) \subseteq \cdots$ be an ascending chain of ideals in R. Set $I = \bigcup_{i \geq 1} (a_i)$. Then I is an ideal of R. Hence there is some $\alpha \in R$ such that $I = (\alpha)$. Since $\alpha \in \bigcup_{i \geq 1} (a_i)$, $\alpha \in (a_m)$ for some $m \geq 1$. But $(\alpha) \supseteq (a_i)$ for all i. So $(\alpha) \subseteq (a_i) \subseteq (\alpha)$ for all $i \geq m$. It follows $(a_i) = (\alpha) = (a_m)$ for all $i \geq m$. This shows the ideal chain is stable. □

Remark 2.1. The converse of Theorem 2.1 is not true. For example, $\mathbb{Z}[x]$ is a UFD, but $\mathbb{Z}[x]$ is not principal.

Corollary 2.1. *Every irreducible element of a PID is prime.*

2.2 A Euclidean Domain is a PID

Notice that R^* denotes the set of nonzero elements of R.

Definition 2.1. *A domain R is called* **Euclidean** (欧几里得整环) *if there exist a map $\delta : R^* \to \mathbb{Z}_{\geq 0}$ such that for $a \in R, b \in R^*$, there exist $q, r \in R$ satisfying*

$$a = bq + r,$$

where $r = 0$ or $\delta(r) < \delta(b)$. The map δ is called a Euclidean function *on R.*

Example 2.1. The integer ring $\mathbb{Z}$ becomes a Euclidean domain if we define $\delta(a) = \begin{cases} a, & \text{if } a \geq 0, \\ -a & \text{if } a < 0. \end{cases}$

Example 2.2. If F is a field, we know that the division algorithm holds in the polynomial ring $F[x]$: for $f(x), g(x) \in F[x]$, $g(x) \neq 0$, there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Hence $F[x]$ is Euclidean.

Example 2.3. The ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is called the *ring of Gaussian integers*, where $i = \sqrt{-1}$. For $\alpha = a + bi \in \mathbb{Z}[i]$, we put

$$\delta(\alpha) = \alpha\overline{\alpha} = |\alpha|^2, \text{ or } \delta(a + bi) = a^2 + b^2.$$

Then $\delta(\alpha) \in \mathbb{Z}_{\geq 0}$ and δ is multiplicative: $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$, even for all $\alpha, \beta \in \mathbb{Q}[i]$ (the field of fractions of $\mathbb{Z}[i]$).

Assume $\beta \neq 0$. Then $\frac{\alpha}{\beta} = u + vi \in \mathbb{Q}[i]$. Choose $a, b \in \mathbb{Z}$ such that

$$|a - u| \leq \frac{1}{2}, \quad |b - v| \leq \frac{1}{2}.$$

That is, $\frac{\alpha}{\beta} = (a + bi) + (s + ti)$, where $a + bi \in \mathbb{Z}[i], s + ti \in \mathbb{Q}[i]$ with $|s|, |t| \leq \frac{1}{2}$. Hence $\delta(s + ti) = s^2 + t^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Put $\gamma = (a + bi)\beta, \varepsilon = (s + ti)\beta$. Then

$$\alpha = \beta\gamma + \varepsilon,$$

where $\varepsilon = \alpha - \beta\gamma \in \mathbb{Z}[i]$. Note that

$$\delta(\varepsilon) = \delta(s + ti)\delta(\beta) \leq \frac{1}{2}\delta(\beta) < \delta(\beta).$$

Therefore the Gaussian integers is Euclidean.

Remark 2.2. The Euclidean function in a ring suggests an algorithm that could calculate some form of greatest common divisor, as we do in $\mathbb{Z}$.

Theorem 2.2. *Every Euclidean domain is a PID, hence a UFD.*

Proof. Let R be Euclidean with Euclidean function δ. The zero ideal is obviously principal. Let I be a nonzero ideal. The set $\{\delta(x) \mid x \neq 0\}$ has a minimal element. Choose $d \in I$ so that

$$\delta(d) = \min\{\delta(x) \mid x \neq 0\}.$$

We claim $I = (d)$. Actually, for any $a \in I$, there exist $q, r \in R$ such that $a = dq + r$ with $r = 0$ or $r \neq 0$ and $\delta(r) < \delta(d)$. If $r \neq 0$, the $\delta(r) < \delta(d)$ and $r = a - dq \in I$. This contradicts the choice of d. Thus $r = 0$ and $a = dq \in (d)$. Consequently $I = (d)$. Therefore R is a PID. □

From Theorem 2.2, we know that a Euclidean domain possesses the property of unique factorization. Hence, we can define gcd of two elements in a Euclidean domain. Actually, the map δ in a Euclidean domain can helps us to find a gcd of two elements if we use the division algorithm repeatedly. This is the situation in $\mathbb{Z}$, where we use the *Euclidean algorithm* to find the gcd of two integers. This is why a Euclidean domain so named. On the other hand, in a UFD, we can certainly define a gcd. But we can not find it out by some explicit steps as we do in $\mathbb{Z}$, since generally division algorithm does not hold even in a UFD (see Remark 2.4).

Corollary 2.2. *Let F be a field. Then the polynomial ring ring $F[x]$ in one variable is a Euclidean domain, hence a PID.*

Corollary 2.3. *The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, hence a PID.*

Remark 2.3. 1. The converse of Theorem 2.2 is not true: a PID is not necessarily Euclidean. If fact, the domain $R = \mathbb{Z}[\omega]$ is a UFD (also a PID), where $\omega = \frac{1+\sqrt{-19}}{2}$. But it is not a Euclidean domain. For an elementary proof of this fact, you are referred to

Oscar A. Campoli, *A Principal Ideal Domain That Is Not a Euclidean Domain*, American Mathematical Monthly, Vol. 95, No. 9 (Nov, 1988), 868-871.

2. The ring $\mathbb{R}[x,y]/(x^2+y^2+1)$ is a PID that is not Euclidean.

Theorem 2.3. *If R is a UFD, so is the polynomial ring $R[x]$.*

Corollary 2.4. *Let R be a UFD and let $x_1, \cdots, x_n$ be indeterminates. Then $R[x_1, \cdots, x_n]$ is a UFD.*

Since every field is a PID, we have

Corollary 2.5. *The polynomial ring $F[x_1, \cdots, x_n]$ over a field F in several indeterminates $x_1, \cdots, x_n$ is a UFD.*

Facts on UFD

1. If R is a UFD, then the polynomial ring $R[x]$ is also a UFD.
2. If R is a UFD or a field, then $R[x_1, \cdots, x_n]$ is a UFD.
3. The Eisenstein Criterion (艾森斯坦判别法) on irreducible polynomials is still true for $R[x]$ if R is a UFD.

If F is a field, we know the polynomial ring $F[x_1, \cdots, x_n]$ is a UFD. But the quotients of such a polynomial ring usually don't admit unique factorization. For instance, $\mathbb{R}[x,y]$ modulo the ideal (x^2+y^2-1). Then $x^2=(1-y)(1+y)$ and likewise $y^2=(1-x)(1+x)$.

$$\{\text{Euclidean Domain}\} \subsetneq \{\text{PID}\} \subsetneq \{\text{UFD}\}.$$

Remark 2.4. Let $|m|$ be a square-free integer and

$$R_m = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{if } m \equiv 2,3 (\text{mod } 4), \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}], & \text{if } m \equiv 1 (\text{mod } 4). \end{cases}$$

which is the ring of algebraic integers of the quadratic number field $\mathbb{Q}(\sqrt{m})$. A very interesting question is when R_m is UFD and when R_m is Euclidean. This question has a close relation with the algebraic property and number-theoretic property of the algebraic number field $\mathbb{Q}(\sqrt{m})$. The domain R_m that are UFD are all known for negative m, they are not yet all known for positive m. But those m for which it is known are the following:

$$\begin{aligned} m = &-163, -67, -43, -19, -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, \\ &33, 37, 41, 53, 57, 61, 69, 73, 77, 89, 93, 97. \end{aligned}$$

A still smaller set occurs when we ask whether the domain R_m is Euclidean (i.e. whether there is an algorithm that could calculate some form of greatest common divisor, as we do in the integers), this set is fully known, and only the following fields are Euclidean:

$$m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Note that when R_m is not Euclidean this does not imply that there are no greatest common divisors, but only that there is no algorithm to calculate them! We have mention that a Euclidean domain is always a UFD. But in the domain $\mathbb{Z}[\sqrt{-6}]$ (which is not a UFD, hence non-Euclidean), the concept of greatest common divisor exists. For instance, 2 and $1+\sqrt{-6}$ have greatest common divisor 1, but we can not apply the Euclidean algorithm to find it.

Recap: Facts on UFD

1. A domain is UFD if and only if it satisfies divisors chain condition and primeness condition.
2. A domain is UFD if and only if it satisfies divisors chain condition and GCD condition.
3. Every element of UFD has only finite many proper divisors.
4. Every irreducible of a UFD is prime.
5. Two elements of a UFD always have a gcd.
6. If R is UFD, so it the polynomial ring $R[x]$.
7. If F is a field or UFD, then the polynomial rings $F[x_1, x_2, \cdots, x_n]$ are UFD.
8. The ring $\mathbb{Z}[\sqrt{-6}], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{10}]$ are not UFD.
9. The ring $\mathbb{Z}[x]$ is a UFD, but not a PID.
10. The ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a UFD, but not a Euclidean domain. The ring $\mathbb{R}[x, y]/(x^2 + y^2 + 1)$ is also a principal ideal domain that is not Euclidean.

Exercises

1. Let π, π_1 be prime elements of a domain R and $\pi \mid \pi_1$. Show that π and π_1 are associate.
2. Explain that a subring of a UFD may not be a UFD.
3. Let R be a PID and $a \in R^*$. Shoe that $R/(a)$ is a field if a is a prime and $R/(a)$ is not a domain if a is not a prime.
4. Let R be a PID and R' a domain containing R as a subring. Show that if d is a gcd of a and b in R, then d is also a gcd of a and b in R'.
5. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain wrt the function $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.
6. Let R be a PID and R' a domain containing R as a subring. Show that if d is a gcd of a and b in R, then d is also a gcd of a and b in R'.
7. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain wrt the function $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.
8. Let $\tau = \frac{1+\sqrt{-7}}{2}$. Show that $\mathbb{Z}[\tau]$ is a Euclidean domain wrt the function $\delta(\alpha) = \alpha\overline{\alpha}$, where $\alpha \in \mathbb{Z}[\tau]$ and $\overline{\alpha}$ denotes its complex conjugate.
9. (Schönemann's Irreducibility Criterion) Let $f(x) \in \mathbb{Z}[x]$ have degree $n > 0$ and assume that there is a prime p and an integer a such that

$$f(x) = (x - a)^n + pF(x), F(x) \in \mathbb{Z}[x].$$

If $F(a) \not\equiv 0 \bmod p$, then $f(x)$ is irreducible modulo p^2.

2.3 Quiz 2

1. (4分) 写出环 $\mathbb{C}[x]/(x^4-1)$ 的所有素理想.
2. (4分) 设 α 为幺环 R 的元, 且有正整数 n 使得 $\alpha^n = 0$. 证明

$$u = 1 + \alpha + \alpha^2 + \cdots + \alpha^{2023}$$

   可逆.

3. (4分) 设 τ 是二元多项式环 $\mathbb{C}[x,y]$ 到一元多项式环 $\mathbb{C}[t]$ 的同态, 满足 $\tau(x) = t^2, \tau(y) = t^3$, 且对于 $a \in \mathbb{C}$, $\tau(a) = a$. 求 $\ker \tau$.
4. (4分) 证明: $(5, 2+\sqrt{-6})$ 是 $\mathbb{Z}[\sqrt{-6}]$ 的极大理想.
5. (4分) 设 R 为整环, $\pi \in R$ 非零且不可逆. 证明: π 为 R 的不可约元的充要条件是 (π) 为 R 的所有主理想构成的集合中的极大元.

Homework Exercise 4, 5, 12, 14, 16, 17, 18, 23, 24 on page 157-159.