Abstract Algebra
: Lecture 14

Leo

2024.11.7

Let R be an integral domain. Let $d \in R$, invertible or non-invertible. Let R^* be the set of invertible elements of R.

Definition 1. *Let $a = bc$. b is a factor of a and a is a multiple of b. If c is invertible, we can rewrite $a = bc$ as $a = bc^{-1}$. In this case we say a and b are associate. Denoted by $a \sim b$.*

Definition 2. *An element $d \in R$ is called irreducible if $d = ab$ then a or b is invertible.*

Definition 3. *An element $d \in R$ is called prime if $d|ab$ then $d|a$ or $d|b$.*

Remark 4. *Irreducible $\neq$ prime.*

Lemma 5. *In a ID, a prime is irreducible.*

证明. Let R be a ID, let $d \in R$ be a prime. Suppose $d = ab$, then $d|ab$, so $d|a$ or $d|b$, as d is prime. If $d|a$, then $a = dc$ for some $c \in R$, so $a = abc$. Since R is a ID, it shows $1 = bc$, i.e. b is a unit. Thus d is irreducible by definition. □

Remark 6. *An irreducible element is not necessarily a prime.*

Example 7. *Let $R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. Claim: (1). 2 is irreducible. (2). 2 is not prime.*
(1). Suppose $2 = (a + b\sqrt{-5}(c + d\sqrt{-5}))$ for some $a, b, c, d \in \mathbb{Z}$. Then taking complex conjugation, $2 = (a - b\sqrt{-5}(c - d\sqrt{-5}))$. $4 = (a^2 + 5b^2)(c^2 + 5d^2)$. Then $b = d = 0$, and $4 = a^2c^2$. So either $a^2 = 4$ and $c^2 = 1$ or $a^2 = 1$ and $c^2 = 4$. i.e. either $a = \pm 2$ and $c = \pm 1$ or $a = \pm 1$ and $c = \pm 2$. So 2 is irreducible.
(2). $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, but $2 \nmid 1 + \sqrt{-5}$ and $2 \nmid 1 - \sqrt{-5}$, so 2 is not prime.

Definition 8. *Let D be an ID. Then D is called a unique factorazition domain (UFD) if:*
(1). Each non-invertible element of D can be written as a product of finitely many irreducible elements. (Chain condition)
(2).And this factorazition is unique up to the order of the factors and multiplication by units.

Theorem 9. *Let D be a ID. Then D is a UFD if and only if:*
(1). Chain condition;
(2). Prime condition: every irreducible element is prime.

证明. First assume (1) and (2) hold. Let $a = p_1p_2 \dots p_s = q_1q_2 \dots q_t$. Where p_i, p_j are irreducibles. Then $p_1|q_1q_2 \dots q_t$, so $p_1|q_1$ or $p_1|q_2 \dots q_t$. Continue this arguement there exists i such that $p_1|q_i$. Similarly take p_2. Finally we get $a = p_1p_2 \dots p_s = q_1q_2 \dots q_t$. where $s = t$ and $p_i = q_i$ after reordering. Therefore D is a UFD.
Conversely, Let D be a UFD. Then we need to irreducible element is prime. Let $d \in D$ to be an irreducible element s.t. $d|ab$ where a, b are not invertible. Then $ab = dc$ for some $c \in D$. If c is invertible, then $d = abc^{-1} = a(bc^{-1})$, contradivtion. So c is not invertible.
Since D is a UFD, let $a = p_1p_2 \dots p_r$, $b = q_1q_2 \dots q_s$, $c = u_1u_2 \dots u_t$. $d \pm p_i$ or $d \pm q_j$, i.e. $d|a$ or $d|b$. Therefore d is a prime.

□

Definition 10. *An ID is called a Principal Ideal Domain (PID) if every ideal is principal.*

Theorem 11. *A PID is a UFD. A UFD is not nessecary a PID.*

Example 12. $\mathbb{Z}[x]$ *is a UFD .* $\mathbb{Z}[x]$ *is not a PID. Take* $(2, x)$*, this is not a principal ideal.*

Proposition 13. *Let D be a PID. And $p \in D - \{0\}$. Then:*
(1). p is a prime $\Leftrightarrow$ p is irreducible;
(2). (p) is a prime ideal $\Leftrightarrow$ (p) is a maximal ideal.

证明. Let p be irreducible. Then (p) is maximal. If (p) is not maximal, then there exists (q) such that $(p) \subsetneq (q)$. Then $p = aq$ for some $a \in D$. Since D is a PID, $(q) = (p)$ or $(q) = (1)$.
So $D/(p)$ is a field, so is ID, and (p) is a prime ideal, and p is a prime.
Conversely, (leave as an exercise). □

证明. (Proof of PID is UFD). Since irreducibility equivalent to prime by the proposition. We only need to prove that every non-zero non-unit element is a product of finitely many irreducible elements. If not we have:

$$(a) \subset (b) \subset (b_1) \subset (b_2) \subset \cdots$$

Let $I = \bigcup\limits_{0 \leqslant i < \infty} (b_i) \bigcup (a)$. Let $I = (d)$ ......(next time) □