Algebra

2008.10.2

3.3 FACTORIZATION IN COMMUTATIVE RINGS

Definition 1. *An ideal P in a ring R is said to be* **prime** *if $P \neq R$ and for any ideals A ,B in R*

$$AB \subset P \quad \Rightarrow \quad A \subset P \quad or \quad B \subset P$$

Definition 2. *An integral domain R is a* **unique factorization domain** *(UFD) provided that:*

(i) every nonzero nounit element a *of R can be written* $\mathrm{a} = c_1 c_2 \dots c_n$ *, with $c_1, \dots, c_n$ irreducible.*

(ii) If $\mathrm{a} = c_1 c_2 \dots c_n$ *and* $\mathrm{a} = d_1 d_2 \dots d_m$ *(c_i, d_i irreducible), then $n = m$ and for some perutation σ of $\{1, 2, \dots, n\}$, c_i and $d_{\sigma(i)}$ are associates for every i.*

Example. $\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

$$4 = 2 \times 2 = (\sqrt{5} + 1)(\sqrt{5} - 1)$$

$2, \sqrt{5} + 1, \sqrt{5} - 1$ are irreducible. $\mathbb{Z}[\sqrt{5}]$ is not UFD. Notice that $2, \sqrt{5} + 1, \sqrt{5} - 1$ are not prime in $\mathbb{Z}[\sqrt{5}]$.

Lemma 1. *Let R be UFD then an irreducible element is a prime.*

Proof. Let $a \in R$ be irreducible, suppose $a \mid bc$ and $a \nmid b$. Hence $ad = bc$ for some $d \in R$. 將 ad 和 bc 展開, 因爲 a 是 prime, 且 $a \nmid b$, 則 a 就出現在 c 的展開中。也就是 $a \mid c$。 □

Theorem 1. *Let R be an Integral domain. Then R is UFD if and only if*

(i)*(**Ascending chain condition**)for any principal ideals*

$$(a_1) \subseteq (a_2) \subseteq (a_2) \subseteq \ldots,$$

there exists $n \in \mathbb{N}$ sit $(a_1) = (a_2)$ for $i \geq n$;

(ii)*(**Primeness condition**)every irreducible element is a prime.*

Proof. Note that $(a) \subseteq (b) \Leftrightarrow b \mid a$ and $(a) = (b) \Leftrightarrow a, b$ are associates.

($\Rightarrow$) (i)Suppose $(a_1) \subseteq (a_2) \subseteq (a_2) \subseteq \ldots$, without loss of generality, 將相同的去掉, 只比較不同的, 即 $(a_1) \subsetneq (a_2) \subsetneq (a_2) \subsetneq \ldots$. By UFD, $a_1 = c_1 c_2 \ldots c_n$ with c_i irreducible. By note, $(a_i) \subsetneq (a_{i+1})$, 由前往後, 一一去掉相同的因子, 最後會只剩下 c_k 因子, 則 $(a_i) = (a_n)$ for $i \leq n$. (ii)This is an immediate consequence of previous lemma.

($\Leftarrow$) (i)Set $T = \{a \in R \mid a \neq 0$, a is not a unit and a is not a product of finite irreducible elements$\}$, if $T = \phi$, then we are done. Suppose $T \neq \phi$, pick $a_1 \in T$, then a_1 must be reducible. Hence $a_1 = a_2 c$ where $a_2 \in T, c \in R$ is not a unit. Thus $(a_1) \subsetneq (a_2)$. Following this way, we find $(a_1) \subsetneq (a_2) \subsetneq \ldots$, a contradiction to ACC. (ii)Suppose $c_1 c_2 \ldots c_n = d_1 d_2 \ldots d_m$ with c_i, d_i irreducible. Since c_1 is prime(primeness), $c_1 \mid d_i$ for some i, say $i = 1$, $d_i \mid c_1$ then c_1, d_1 are associates, say $c_1 = d_1$. Then $c_1(c_2 c_3 \ldots c_n - d_2 d_3 \ldots d_m) = 0$, $c_1 \neq 0$(R is an integral domain). Thus $c_2 c_3 \ldots c_n = d_2 d_3 \ldots d_m$. (ii) follows by induction on n. □

Theorem 2. *Every principal ideal domain(PID) R is a unique factorization domain(UFD).*

Proof. (i)(**Ascending chain condition**) Suppose $(a_1) \subsetneq (a_2) \subsetneq (a_2) \subsetneq \ldots$ are ideals. Then $\bigcup_{i \geq 1} (a_i)$ is an ideal. By PID, $\bigcup_{i \geq 1} (a_i) = (b)$ for some $b \in R$, say $b \in (a_n)$ for some n, thus $(b) \subseteq (a_n)$. Hence $(a_i) = (b)$ for $i = n$. (ii)(**Primeness**) Pick an irreducible element $\in R$. We prove (a) is a "maximal ideal". Suppose $(a) \subsetneq (b) \subsetneq (R)$ for some $b \in R$. Then $b \mid a$ and

a, b are not associates. b is not a unit. Hence $a = bc$ for c not a unit. This is a contradiction, thus a is irredicible. Hence $\big(a\big)$ is a prime ideal, and we know a is prime in R. $\square$