Week 2-4 (II)

Ideal

Defn. Let R be a ring with unity 1. An dditive subgroup N of R is an ideal if for each element $a \in R$ and $b \in N$, $ab \in N$ and $ba \in N$.

$(*)$ Ideal 在環中所扮演的角色就像 Normal subgroup 在群中所扮演的角色類似; 有了 ideal N, 才可以定義 Factor ring.

$R/N : (a+N)(b+N) = ab+N$ well-defined.

Example $\mathbb{Z}$ 中的 ideal 是 $n\mathbb{Z}$ 的形式.

Example $\mathbb{R}[x]$ 中的 ideal 是 $\{f(x)q(x) \mid q(x) \in \mathbb{R}[x]\}$ 的形式, 其中 $f(x) \in \mathbb{R}[x]$.

Lemma Let R be a commutative ring with 1. Then, for each $a \in R$, $< a >= \{ax \mid x \in R\}$ is an ideal of R, $< a >$ is also called a principal ideal of R.

Corollary Every ideal of Z is a principal ideal.

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

Proof. Let R be an ideal $\neq \{0\}$ of $F[x]$ and $f(x)$ is a polynomial in R with minimum degree but not a zero polynomial. We claim that for each element $g(x) \in R$, $f(x) \mid g(x)$. Suppose not. By division algorithm (holds for $F[x]$), $g(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $r(x) \neq 0$ and $deg(r(x)) < deg(f(x))$. If $r(x) = 0$, done. Otherwise, if $r(x) \neq 0$, since $g(x) \in R$ and $f(x)q(x) \in R$, we have $r(x) \in R$. This is a contradiction. We have the proof. ■

Defn. A proper ideal N of a ring R is an ideal which is different form R. $\{0\}$ and R are trivial ideals of R. An ideal M is maximal if there does not exist an ideal N, s.t. $M \subsetneq N \subsetneq R$. An ideal P is a prime ideal of R if for every element $ab \in P$ implies that $a \in P$ or $b \in P$.

Proposition Let R be a commutitive ring with 1, and N be an ideal of R which contains a unit. Then $N = R$.

Proof. 自己證.

Corollary Every field contains no nontrivial proper ideal.

Theorem Let φ be a ring homomorphism from R into R'. Let N be an ideal of R and N' be an ideal of R'. Then

(a) $\varphi[N]$ is an ideal of $\varphi[R]$. (注意, 不是 R' 的 ideal)

(b) $\varphi^{-1}[N']$ is an ideal of R.

Proof. 自己證明.

Theorem $\varphi : R \to R/N$ defined by $\varphi(x) = x + N$ is a homomorphism from R onto R/N. (N is an ideal of R)

Note that $Ker\varphi = N$ and φ is called a canonical homomorphism.

Theorem Let R be a commutative ring with 1. Then R/M is a field if and only if M is a maximal ideal of R.

Proof. ($\Rightarrow$) Suppose not. $\exists$ ideal N, $M \subsetneq N \subsetneq R$. 由上述 canoninical homo. $\varphi[N]$ 是 R/M 的一個 ideal, 而且 $\varphi[N] \neq \{M\}$, $\varphi[N]$ 也不等於 R/M, 所以 $\varphi[N]$ 是一個 proper ideal, 這個結論與 R/M 是 field 矛盾. 所以 M 必然是 maximal ideal.

($\Leftarrow$) 因爲 R 是 commutative ring with 1, 所以 R/M 也是一個 commutative ring 具有乘法單位元素 $1 + M$. 現在, 我們證明 R/M 中的每一個非零 ("M") 元素 $a + M$ 都有乘法反元素, 這裡 $a \notin M$.
由於 $a + M \in R/M$, 所以 $< a + M >$ 是 R/M 的一個 ideal, 於是 $\varphi^{-1}[< a + M >]$ 是 R 的一個 ideal. ($\varphi : R \to R/M$ 爲 homo.) 因爲 $1 + M \notin < a + M >$, 所以 $\varphi^{-1}[< a + M >] \subsetneq R$, 又因爲 $a \notin M$, 所以 $M \subsetneq \varphi^{-1}[< a + M >]$, 因此 M 不是 maximal ideal. $\rightarrow\leftarrow$
所以 R/M 是 field. ■

同理, 我們可以證明

Theorem Let R be a commutativering with 1. Then R/N is an integral domain if and only if N is a prime ideal.

Proof.($\Rightarrow$) Suppose not. Then there exists two elements a and b not in N such that $ab \in N$. This implies that in R/N, there exist two elements $a+N$ and $b+N$ which not $N(R/N$ 中的 $0)$, but $(a+N)(b+N) = N$. This implies that R/N is not an integral domain.
($\Leftarrow$) Let $ab \in N$. Then $(a+N)(b+N) = N$ implies $a \in N$ or $b \in N$ (since R/N is an integral domain.) ■

Corolllary Every maximal ideal of R is a prime ideal.

Theorem An ideal $< p(x) > \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is <u>irreducible</u> over F.

Proof. ($\Rightarrow$) Suppose not. $p(x) = f(x)g(x)$ where
$1 \leq \deg(fx) < deg(p(x))$ and $1 \leq \deg(g(x)) < deg(p(x))$. This implies that $< p(x) > \subsetneq < f(x) > \subsetneq F[x]. \rightarrow\leftarrow$
($\Leftarrow$) Suppose not. $\exists$ N (ideal of $F[x]$), s.t. $< p(x) > \subsetneq N \subsetneq F[x]$. Since every ideal of $F[x]$ is a principal ideal, $N =< g(x) >$. Now, $p(x) \in < g(x) >$, $p(x) = g(x)q(x)$. Since $p(x)$ is irreducible, either $g(x)$ or $q(x)$ is of degree 0. If $deg(g(x)) = 0$, then $N = F[x]$. On the other hand, if $q(x)$ is of degree 0, let $q(x) = c \neq 0$, then $g(x) = \frac{1}{c}p(x)$. Hence $< g(x) > = < p(x) >$, $< p(x) >$ is maximal. ■

Theorem Let $p(x)$ be an irreducible poly. in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x)$, $s(x) \in F[x]$, then either $p(x) \mid r(x)$ or $p(x) \mid s(x)$.

Proof. $< p(x) >$ is a maximal ideal of $F[x]$. Hence $< p(x) >$ is a prime ideal of $F[x]$. This implies that if $r(x)s(x) \in < p(x) >$, then either $r(x) \in < p(x) >$ or $s(x) \in < p(x) >$. This concludes the proof. ■

目標

令 F 爲一體而 $f(x)$ 爲 $F[x]$ 中的一個非常數多項式。證明存在有一個體 $E \geq F$ 這滿足 E 中存在有一個元素 α 使得 $f(\alpha) = 0$.

例 $x^2 + 1 \in \mathbb{Q}[x]$, $\mathbb{Q}(i)$ (包含 $\mathbb{Q}$ 及 i 的體) 存在, 其中 $\mathbb{Q}(i) \geq \mathbb{Q}$, 而且 $i^2 + 1 = 0$.

證明的概念

1. 令 $p(x) \mid f(x)$ 而且 $p(x)$ 是 irreducible. (Note : $f(x) \in F[x]$)
2. 令 $E = F[x]/ < p(x) >$. (這是一個 field, 因爲 $< p(x) >$ 是 maximal ideal.)
3. 令 $\alpha = x + < p(x) > \in E$, 則 $f(\alpha) = f(x) + < p(x) > = < p(x) >$ is a zero in E.
4. F is isomorphic to a subfield of E. ($\forall\ c_1 \neq c_2 \in F$, $c_1 + < p(x) > \neq\ c_2 + < p(x) >$)
   F 中的"0"可以看成 E 中的 $< p(x) >$. ($\varphi : F \overset{1-1}{\underset{onto.}{\longrightarrow}} E$)

$(*)$ F is embedded in E.

Unique Factorization Domain (UFD)

Defn. Let R be a commutative ring with unity and $a, b \in R$. If $\exists\ c \in R$. s.t. $b = ac$, then a divides b (or a is a factor of b), denoted by $a \mid b$.

Defn. An element u of a commutative ring with unity R is a unit of R if u divides 1, that u has a multiplicative inverse in R. Two elements $a, b \in R$ are associates in R if $a = bu$ where u is a unit.

Example Let $a, b \in \mathbb{Q}$, 3 and 5 are associates.

Defn. A nonzero element p is not a unit of an integral domain D is irreducible of D if every factorization $p = ab$ in D has the property that either a or b is a unit.

Defn. (UFD)

An integral domain D is a UFD if

1. Every element of D that is neither 0 or a unit can be factored into a product of finite number of irreducibles.
2. If $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are two factorizations of $x \in D$ into irreducibles, then $r = s$ and (after renumbering) p_i and q_i are associates $i = 1, 2, \cdots, r$.

Lemma Let R be a commutative ring and let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of ideals in R. Then $N = \overset{\cup}{_{i=1}} N_i$ is an ideal of R.

Proof. 自已 check.

Lemma (Ascending chain condition for a PID)

Let D be a PID. If $N_1 \subseteq N_2 \subseteq \cdots$ is ascending chain of ideals in D, then there exists a positive integer r such that $N_r = N_s$ for all $s \geq r$.

Proof. By above lemma $N = \overset{\cup}{_{i=1}} N_i$ is an ideal of D. Since D is a PID, $N =< c >$ for some $c \in D$. By the definition of N, there exists a r, s.t. $c \in N_r$. Now, for $s \geq r$, $< c > \subseteq N_r \subseteq N_s \subseteq N =< c >$.
Hence, $N_r = N_s$ ■

Theorem Let D be a PID. Then every element that in neither 0 nor a unit in D is a product of irreducibles.

Proof. Consider $a \neq 0$ which is not a unit. If a is an irreducible, then we are done. Otherwise, $a = a_1 b_1$ where a_1 and b_1 is a unit. If both a_1 and b_1 are irreducibles, then we are done. Otherwise, let a_1 be the one which is not irreducible. Then $< a > \subsetneq < a_1 >$ (?)
And then $< a > \subset < a_1 > \subset < a_2 > \subset \cdots$. Since D is a PID, the ascending chain condition holds. Thus $< a > \subset < a_1 > \subset \cdots \subset < a_r >$ and clearly a_r is irreducible.

Now, $a = a_r \cdot c_1$ where a_r is irreducible and c_1 is not a unit. By above process, we have that $a = a_r \cdot c_{r'} \cdot d_1$ where $c_{r'}$ is irreducible and d_1 is not unit. Due to the fact that D is a PID, the factorization has finite products and the last element is an irreducible, this concludes the proof. ■

Lemma An ideal $< p >$ in a PID is maximal iff p is an irreducible.

Lemma In a PID, if an irreducible $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Corollary If p is an irreducible in a PID and $p \mid a_1 a_2 \cdots a_n$ for $a_i \in D$, then $p \mid a_i$ for at least one i.

代數中的 Primes

Defn. A nonzero nonunit element p of an integral domain D is a prime if, $\forall\ a, b \in D$, $p \mid ab$ implies either $p \mid a$ or $p \mid b$.

Theorem Every PID is a UFD.

Proof. 由前面的定理知道, 在一個 PID 中, 每個元素都可以 寫成有限個 irreducibles 的乘積, 所以只要證明唯一性即可。
令 $a \in D$, $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. 從 p_1 開始考慮; $p_1 \mid a$, 所以 $p_1 \mid q_1 q_2 \cdots q_s$. 因此 $p_1 \mid q_j$. 因爲 p_1、q_j 都是 irreducible, 所以 $q_j = p_1 u_1$, u_1 爲 unit. 爲了方便說明, 令 q_j 爲 q_1(排列), 於是 $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. 因爲 D 是 integral domain, 所以 $p_2 p_3 \cdots p_r = \mu_1 q_2 q_3 \cdots q_s$. 繼續上述步驟我們可以推得 $r = s$.(units 不影響分解的唯一性.) ■

重要概念 並非每個 UFD 都是 PID!

Example Let $F[x, y]$ be the set of polynomials with two indeterminates x and y where F is a field. Then $F[x, y]$ is a

commutative ring with 1, moreover, $F[x, y]$ is an integral domain. Now, let N be the set of all polynomial in $F[x, y]$ such that its constant term is "0". Then N is an ideal of $F[x, y]$. But, N is not a principal ideal of $F[x, y]$. Note that $F[x, y]$ is a UFD, by Corollary 45.30.

$(*)$ If F is a field and x_1,x_2,$\cdots$,x_n are indeterminates, then $F[x_1, x_2, \cdots, x_n]$ is a UFD. This is a direct consequence of the most fundamental theorem:

Theorem (45.29) If D is a UFD, then $D[x]$ is a UFD.

Proof. Omit.