Week 5(II)

Euclidean Domains

Defn. A Euclidean norm on an integral domain D is a function ν mapping the nonzero elements of D into nonnegative integers such that the following conditions are satisfied:

1. $\forall\ a, b \in D$ with $b \neq 0$, $\exists\ q, r \in D$ s.t. $a = bq + r$, where either $r = 0$ or $\nu(r) < \nu(b)$.
2. $\forall\ a, b \in D$, where neither b nor a is 0, $\nu(a) \leq \nu(ab)$.

Defn. An integral domain D is a Euclidean domain if there exists a Euclidean norm on D.

Example 1 $\mathbb{Z}$ and $F[x]$ are Euclidean domains.

Theorem Every Euclidean domain is a PID.

Proof. Let D be an Euclidean domain with norm ν and N be an ideal of D. If $N = \{0\}$, then $N =< 0 >$. Otherwise, let $b \in N$ and $\nu(b) = \min\{\ \nu(n) \mid n \in N \backslash \{0\}\}$. Now, $\forall\ a \in N$, $a = bq + r$. If $\nu(r) = 0$, then $a \in < b >$. Otherwise $r = a - bq \in N$. But, $\nu(r) < \nu(b)$.$\rightarrow\leftarrow$ ■

Corollary A Euclidean domain is a UFD.

Theorem Let D be a Euclidean domain. Then
$\nu(1) = \min\{\nu(a) \mid a \in D\backslash\{0\}\}$, moreover, $\nu(u) = \nu(1)$ if and only if u is a unit of D.

Proof. $\forall\ a \in D\backslash\{0\}$, $a = a \cdot 1$. Therefore $\nu(a) = \nu(a \cdot 1) \geq \nu(1)$.
($\Rightarrow$) Now, if $\nu(u) = \nu(1)$, then $\nu(u) = \nu(1) = \nu(uq + r)$ with either $\nu(r) < \nu(u)$ or $r = 0$. Since $\forall\ a \in D$, $\nu(a) \geq \nu(1)$, $\nu(r) < \nu(u) = \nu(1)$ not possible, $r = 0$. Thus, $1 = uq$, u is a unit.
($\Leftarrow$) If u is a unit, then $uu^{-1} = 1$. Hence $\nu(u) \leq \nu(1) \leq \nu(u)$. This implies that $\nu(u) = \nu(1)$. ■

有了 Euclidean norm 的概念, 就可以求兩個數的 gcd , 也就有了輾轉相除法 (Euclidean Algorithm)

Theorem (簡述) Let D be a Euclidean domain and let a and b be an nonzero elements of D. Then, if d is a gcd of a and b, then there exists λ and μ in D such that $d = \lambda a + \mu b$.

Proof. Omit.

Gaussian Integers

Defn. A Gaussian integer is a complex number $a + bi$, where $a, b \in \mathbb{Z}$. The norm of Gaussian integer $\alpha = a + bi$ is $N(\alpha) = a^2 + b^2$.

Lemma The set of Gaussian integers denoted by $\mathbb{Z}[i]$ has the following properties:

(a) $N(\alpha) \geq 0, \forall\ \alpha \in \mathbb{Z}[i]$.

(b) $N(\alpha) = 0$ iff $\alpha = 0$.

(c) $N(\alpha\beta) = N(\alpha)N(\beta)$.

Lemma $\mathbb{Z}[i]$ is an integral domain.

Proof. $\alpha\beta = 0$ iff $N(\alpha\beta) = N(\alpha)N(\beta) = 0 \Rightarrow N(\alpha) = 0$ or $N(\beta) = 0$ $\Rightarrow \alpha = 0$ or $\beta = 0$.

Theorem $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. Define the norm (Euclidean norm) be $\nu(\alpha) = N(\alpha)\ \forall\ \alpha \in \mathbb{Z}[i]$ and $\alpha \neq 0$. It suffices to prove that $N(\alpha)$ is a Euclidean norm.

Condition 2 $\forall\ \alpha, \beta \in \mathbb{Z}[i]\backslash\{0\}$, by the fact that $N(\alpha) \geq 1$ and $N(\beta) \geq 1$, we have $N(\alpha\beta) \geq N(\alpha)$ and $N(\alpha\beta) \geq N(\beta)$ respectively.

Condition 1 (比較複雜)

令 $\alpha = a_1 + a_2 i$, $\beta = b_1 + b_2 i$, $\beta \neq 0$, 因此 $N(\beta) \geq 1$。

我們要證明對於任選兩個元素 α, β, 都存在兩個 $\mathbb{Z}[i]$ 中的元素 σ 及 ρ 使得 $\alpha = \beta\sigma + \rho$, 其中不是 $N(\rho) = 0$ 亦即 $\rho = 0$, 就是 $N(\rho) < N(\beta) = b_1^2 + b_2^2$.

由於 $\alpha, \beta \in \mathbb{Z}[i]$, 所以必存在一個 $r + si \in \mathbb{Q}[i]$ 使得 $\alpha = \beta(r + si)$, $r, s \in \mathbb{Q}$, 假設 $q_1, q_2 \in \mathbb{Z}$, 滿足 $|r - q_1| \leq \frac{1}{2}$ 且 $|s - q_2| \leq \frac{1}{2}$, 則 $N((r + si) - (q_1 + q_2 i)) = N((r - q_1) - (s - q_2)i) \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$, 於是,

令 $\sigma = q_1 + q_2 i$, 則 ρ 可以選成 $\alpha - \beta\sigma$, 於是,

$N(\rho) = N(\alpha - \beta\sigma) = N(\beta(\frac{\alpha}{\beta} - \sigma)) = N(\beta)N(\frac{\alpha}{\beta} - \sigma) \leq N(\beta) \cdot \frac{1}{2} < N(\beta)$,

因此 $N(\rho) < N(\beta)$. ■

以下介紹在 $\mathbb{Z}[i]$ 中不可分解的概念.

Defn. Let D be an integral domain. A multiplicative norm N on D is a function mapping D into the integers $\mathbb{Z}$ such that

1. $N(\alpha) = 0$ iff $\alpha = 0$.
2. $N(\alpha\beta) = N(\alpha)N(\beta)\ \forall\ \alpha, \beta \in D$.

Theorem If D is an integral domain with a multiplicative norm N, then $N(1) = 1$ and $|N(u)| = 1$ for every unit u in D. If, furthermore, every α such that $|N(\alpha)| = 1$ is a unit in D, then an element π in D with $|N(\pi)| = p$ for a prime $p \in \mathbb{Z}$, is irreducible of D.

Proof. $N(1) = N(1 \cdot 1) = N(1) \cdot N(1) \Rightarrow N(1) = 1$

Let u be a unit in D, then $N(uu^{-1}) = N(1) = 1$. Since $N(u)$ is an integer $|N(u)| = 1$. Now, since the units of D are exactly the elements of norm ± 1, every element x satisfying $|N(x)| = 1$ implies that x is a unit. Let $\pi \in D$ be such that $|N(\pi)| = p$ where p is a prime. Assume that $\pi = \alpha\beta$, then $p = |N(\pi)| = |N(\alpha\beta)| = |N(\alpha)N(\beta)| = |N(\alpha)||N(\beta)|$. So, either $|N(\alpha)| = 1$ or $|N(\beta)| = 1$ which implies that either α or β is a unit. ■

Example $N(a+bi) = a^2 + b^2$ for each $a + bi \in \mathbb{Z}[i]$ is a multiplicative norm. Since $1 + 2i$ has norm $N(1 + 2i) = 5$, $1 + 2i$ is irreducible in $\mathbb{Z}[i]$. But $3 + i$ is not in $\mathbb{Z}[i]$, since $3 + i = (1 - i)(1 + 2i)$.

Example $\mathbb{Z}[i]$ is a UFD.(Review)

Example (Not a UFD)

Let $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$. Let $N(a + b\sqrt{5}i) = a^2 + 5b^2$. Consider $21 = 3 \cdot 7 = (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i)$.

注意：3, 7, $1 \pm 2\sqrt{5}i$ 都是 irreducibles!

1. $3 = \alpha\beta$ ($7 = \alpha\beta$)

   $N(3) = N(\alpha)N(\beta) = 9$, 當 $N(\alpha) = 9$, 則 $N(\beta) = 1$, 於是 β 是 unit.

   當 $N(\alpha) = 3$, 令 $\alpha = a + b\sqrt{5}i$, 所以 $N(\alpha) = a^2 + 5b^2$=3, 無整數解. 所以3是 irreducible, 同理可討論7也是 irreducible.

2. $1 + 2\sqrt{5}i = \gamma\delta$ (同理 $1 - 2\sqrt{5}i = \gamma\delta$.)

   $N(1 + 2\sqrt{5}i) = 21 = N(\gamma\delta) = N(\gamma)N(\delta)$. $N(\gamma) = 1$ 則 γ 爲 unit, similary $N(\delta) = 1$. $N(\gamma) = 3$ or 7 , 同 1 所以 $1 + 2\sqrt{5}i$爲 irreducible.

Application to Number Theory

Theorem (費馬 $p = a^2 + b^2$ 定理)

Let p be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for some integers a, b if and only if $p \equiv 1 (\text{mod } 4)$.

Proof.($\Rightarrow$) Since p is odd, a^2 and b^2 must be of different parity, i.e., one even and one odd. Let $a = 2r$ and $b = 2s + 1$. Then $a^2 + b^2 \equiv 1(\text{mod } 4)$.
($\Leftarrow$) 比較困難些

因爲 p 是質數, 所以 $< \mathbb{Z}_p^* , \cdot >$ 是一個 $p-1$ 個元素的循環群, 現在 $4 \mid p-1$, 所以有一個元素 n, $n^4 = 1$ 但是 $n^2 \neq 1$, 所以 $n^2 \equiv -1(\text{mod } p)$, 這表示 $p \mid n^2 + 1$.

現在把 p, n^2+1 看成 $\mathbb{Z}[i]$ 的元素, 於是 $p \mid (n+i)(n-i)$; 因爲 p 在 $\mathbb{Z}[i]$ 中是 irreducible, 所以 $p \mid n+i$ or $p \mid n-i$. 如果 $p \mid n+i$, 則 $n+i = p \cdot (a+bi)$, $a+bi \in \mathbb{Z}[i]$, 於是 $pb = 1$, 此爲不可能. 同理, $p \mid n-i$ 也不可能; 所以 p 不可能是 irreducible.

令 $p = (a+bi)(c+di)$, $a+bi$ 與 $c+di$ 皆不是 unit.

$N(p) = N(a+bi)N(c+di) \Rightarrow p^2 = (a^2+b^2)(c^2+d^2)$.

由於 $N(a+bi)$ 與 $N(c+di)$ 皆不爲 1, 所以 $a^2+b^2 \neq 1$ 且 $c^2+d^2 \neq 1$. 又因爲 $p^2 = (a+bi)(a-bi)(c+di)(c-di)$, $p = (x+yi)(z+wi)$; 最後, 因爲 $p \in \mathbb{Z}$, 所以 $(x+yi)$ 與 $z+wi$ 必爲共軛, 亦即 $z = x$, $w = -y$. 由此推得 $p = (a+bi)(a-bi) = a^2+b^2$ $(a = c, b = d)$ ■

($*$) 質數的形式當然不只有 $4k+1$ 的部份, 除了 2 之外尚有一大堆的質數是 $4k+3$ 的形式, 如7, 11, 19, $\cdots$; 然而, 這些質數就等法以兩個整數的平方和來表示。費馬 $p = a^2 + b^2$ 定理是以代數方法來研究數論一個非常典型的例子。

(補充) Ideal 的應用

Let F be a finite field, say $F =< \mathbb{Z}_2 , +, \cdot >= GF[2]$. Then $F[x]$ is a principal ideal domain.

Defn. A code $\mathcal{C}$ of length n is a set of n-vectors in F^n. If $\mathcal{C}$ itself forms a linear space (vector space), then $\mathcal{C}$ is a linear code.

Defn. A code $\mathcal{C}$ of length n is a cyclic code if $\mathcal{C}$ itself is a linear code and for each $(a_0, a_1, \cdots, a_{n-1}) \in \mathcal{C}$, $(a_1, a_2, \cdots, a_{n-1}, a_0)$ is also in $\mathcal{C}$.

Consider $F[x]/ < x^n - 1 >= F[x]/ < x^n + 1 >$. It is a principal ideal ring (not necessarily be a domain). Now, let $g(x) \in F[x]/ < x^n + 1 >$, $< g(x) >$ is an ideal of $F[x]/ < x^n + 1 >$ and also $< g(x) >$ is a principal ideal.

$(*)$ $g(x) \mid x^n + 1$.

Theorem $< g(x) >$ is a cyclic code of length n.

e.g. n=7, $g(x) = x^3 + x + 1$

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1). \ (?)$$

$\{011, 101, 110, 000\}$ 爲一長度 3 的循環碼。以多項式來表示爲 $\{0, 1 + x, x + x^2, 1 + x^2\}$, 它可以想成是在 $\mathbb{Z}_2[x]/ < x^3 + 1 >$ 中由 $g(x) = 1 + x$ 而生成的數碼.

$(*)$ You got to live with what you have!

但是, 要別人好, 就要比別人用功, 不是嗎?