Finite Fields(有限體)

比起實數所形成的體, 有限體在近代應用的領域中扮演著更重要的角色

$(*)$ 有限體的元素個數必定是質數的次方 (Prime power).

Theorem 1 令 F 爲一個有限個元素的體, 則必存在一個質數 p, 使得 $ch(F) = p$.

Proof. 因爲 $|F| < +\infty$, 所以 $ch(F) \neq 0$. 令 $ch(F) = c$. 如果 c 不是質數, 令 $c = a \cdot b$, 於是, $c \cdot 1 = (a \cdot b) \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$. 因爲 $a \cdot 1$ 與 $b \cdot 1$ 皆在 F 中, 且不爲 0, 所以 F 有 zero divisor, $\rightarrow\leftarrow$. 因此, c 必定爲一質數. ■

Theorem 2 令 F 爲 $ch(F) = p$ 的有限體, 則 F 中必含有子體 $\mathbb{Z}_p$.

Proof. (說明) 這裡所謂的子體是與 $\mathbb{Z}_p$ 同構的子體.

Theorem 3 具有 $ch(F) = p$ 的有限體 F, $|F| = p^n$, for some $n \in \mathbb{Z}^+$.

Proof. 由定理 2, F 爲 $\mathbb{Z}_p$ 的 Finite extension, 令 $[F : \mathbb{Z}_p] = n$. 則 $\forall\ \alpha \in F$, $\alpha = \sum_{i=1}^{n} a_i \alpha_i$, 其中 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 爲佈於 $\mathbb{Z}_p$ 之向量空間 F 的基底, $a_i \in \mathbb{Z}_p$, $i = 1, 2, \cdots, n$. 因此 $|F| = p^n$. ■

Theorem 4 The multiplicative group $\langle F^*, \cdot \rangle$ of nonzero elements of a finite field F is cyclic.

Proof. Since $\langle F^*, \cdot \rangle$ is a finite abelian group, $F^* \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \mathbb{Z}_{d_t}$ where d_i's are primes. Let $m = \text{lcm}\{d_1, d_2, \cdots, d_t\}$. Then $m \leq \prod_{i=1}^{t} d_i$.

By direct counting $x^m = 1 \ \ \forall \ \ x \in F^*$, therefore $x^m - 1 = 0$ has at least $|F^*|$ zeros, i.e., $\prod_{i=1}^{t} d_i$ zeros. This implies that $m \geq \prod_{i=1}^{t} d_i$. Hence $m = \prod_{i=1}^{t} d_i$ and thus $d_1, d_2, \cdots, d_t$ are distinct primes. So $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \mathbb{Z}_{d_t}$ is a cyclic group. This concludes the proof. ■

Theorem 5 Let E be a field of p^n elements contained in an algebraic closure $\overline{\mathbb{Z}_p}$ of $\mathbb{Z}_p$. Then, the elements of E are precisely the zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Proof. Since $\langle E^*, \cdot \rangle$ is a group of order $p^n - 1$, $\forall \ \ \alpha \in E, \ \ \alpha^{p^n - 1} = 1$. Hence $\alpha^{p^n} = \alpha$. This implies that α is a zero of $x^{p^n} - x$. Also, $0^{p^n} - 0 = 0$, this shows that $\forall \ \ \alpha \in E$, α is a zero of $x^{p^n} - x$. Since $x^{p^n} - x$ can have at most p^n zeros, this concludes the proof. ■

Defn. An element α of a field is an nth root of unity if $\alpha^n = 1$. It is a primitive nth root of unity if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.

Thus the nonzero elements of a finite field F of p^n elements are all $(p^n - 1)$th roots of unity, i.e., $\alpha^{p^n - 1} = 1$. Moreover, if the group $\langle F^*, \cdot \rangle$ is generate by α, then α is a primitive $(p^n - 1)$th root of unity.

e.g. $\langle \mathbb{Z}_{11}, +, \cdot \rangle$ is a finite field and $\langle \mathbb{Z}_{11}^*, \cdot \rangle$ is a group generated by 2. "2" is a primitive 10th root of unity in $\mathbb{Z}_{11}$.

(註) primitive root 在 finite field 中扮演非常重要的角色, 把 field 中的元素以 α^k 的形式表示出來之後對乘法運算的簡化幫忙很大.

(例)　$GF(2^4)$: Finite field of order 2^4.　$GF(2^4) \cong \mathbb{Z}_2[x]/\langle 1+x+x^4 \rangle$

$$1 = 1000\ , \quad \alpha = 0100, \quad \alpha^2 = 0010\ , \quad \alpha^3 = 0001,$$
$$\alpha^4 = 1100\ , \quad \alpha^5 = 0110\ , \quad \alpha^6 = 0011\ , \quad \alpha^7 = 1101,$$
$$\alpha^8 = 1010\ , \quad \alpha^9 = 0101\ , \quad \alpha^{10} = 1110\ , \quad \alpha^{11} = 0111,$$
$$\alpha^{12} = 1111\ , \quad \alpha^{13} = 1011\ , \quad \alpha^{14} = 1001\ , \quad 0 = 0000,$$

Lemma 6　If F is a field of prime characteristic p with algebraic closure $\overline{F}$, then $x^{p^n} - x$ has p^n distinct zeros on $\overline{F}$.

Proof.　假如 $x^{p^n} - x = 0$ 在 $\overline{F}$ 中有重根, α, 亦即 $\alpha^{p^n} - \alpha = 0$, 則在 $D_x(x^{p^n} - x)$ 中 α 也是一個 zero. (微分的性質)

現在考慮 $x^{p^n-1} - 1 = 0$. (0 是一個根)

假設 $\alpha \neq 0$ 爲一重根, 則 $\alpha^{p^n-1} = 1$ 而且 $(p^n - 1)\alpha^{p^n-2} = 0$, 因爲 $\langle F^*, \cdot \rangle$ 爲一乘法群, 所以 $(p^n - 1) \cdot 1 \cdot \alpha^{p^n-2} = (-1) \cdot \frac{1}{\alpha} = 0$. 此爲不可能; 所以, 沒有重根. ■

Theorem 7　令 F 爲一有限體同時滿足 $ch(F) = p$, p 爲一質數. 則對於所有的 $n \in \mathbb{Z}^+$, $\alpha, \beta \in F$, $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$.

Proof.　利用歸納法.

當 $n = 1$ 時, $(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k} \ldots\ldots\ldots\ldots\ldots\ldots (1)$

由於對於所有的 $0 < k < p$, $p \mid \binom{p}{k}$, 所以 (1) 式可以改寫成

$(\alpha + \beta)^p = \alpha^p + \beta^p$, 亦即 $n = 1$ 時 $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$.

假設 $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$, 其中 $m < n$. 考慮 $(\alpha + \beta)^{p^{m+1}}$.

$(\alpha+\beta)^{p^{m+1}} = [(\alpha+\beta)^{p^m}]^p = (\alpha^{p^m}+\beta^{p^m})^p = (\alpha^{p^m})^p+(\beta^{p^m})^p = \alpha^{p^{m+1}}+\beta^{p^{m+1}}$.

所以 $n = m + 1$ 時, $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$, 定 理得證 ■

Theorem 8 (主要定理)

$\forall$ prime power p^n, there exists a finite field with p^n elements.

Proof. Let $\overline{\mathbb{Z}_p}$ be the algebraic closure of $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a finite field, $\overline{\mathbb{Z}_p}$ exists (by Theorem 31.17). Let $K \subseteq \overline{\mathbb{Z}_p}$ such that $K = \{x \in \overline{\mathbb{Z}_p} \mid x^{p^n} - x = 0\}$. Clearly, K is a field with p^n elements and we have the proof. ■

Corollary 9 If F is a finite field, then for every positive integer n, there is an irreducible polynomial in $F[x]$ of degree n.

Proof. Let $|F| = q = p^r$ where $ch(F) = p$. Then, there is a field $K \leq \overline{F}$ containing $\mathbb{Z}_p$ (up to isomorphism) and containing precisely of the zeros of $x^{p^{rn}} - x$. (Theorem 5) Now, $\forall$ $\alpha \in F$ $\alpha^{p^{rn}} - \alpha = (\alpha^{p^r})^n - \alpha = \alpha^{p^r \cdot p^{nr-r}} - \alpha = \cdots = \alpha - \alpha = 0$. Hence, $F \leq K$, 同時 $[K : F] = n$. 又因爲一個 Finite extension 必爲一個 simple extension, 所以 $K = F(\beta)$. 於是 $irr(\beta, F)$ 爲一 n 次 irreducible polynomial over F.■

Theorem 10 Let p be a prime and $n \in \mathbb{Z}^+$. If E and E' are fields of order p^n, then $E \simeq E'$. (元素個數相等的有限體同構)

Proof. Both fields contain precisely the zeros of $x^{p^n} - x \in \mathbb{Z}_p[x]$ and also $E \simeq \mathbb{Z}_p[x]/\langle f(x) \rangle \simeq E'$ where $f(x)$ is irreducible polynomial of $\mathbb{Z}_p[x]$ of degree n. ■

(Ex.)1. Show that every irreducible polynomial in $\mathbb{Z}_p[x]$ is a divisior of $x^{p^n} - x$ for some n.

2. Show that $x^{p^n} - x$ is the product of all monic irreducible polynomial in $\mathbb{Z}_p[x]$ of a degree d dividing n.

Constructible Numbers

Defn. A real number α is constructible if we can construct a line segment of length $|\alpha|$ in a finite number of steps from this given segment of unit length by using a straightedge (without measurement) and a compass.

Theorem The field F of constructible real numbers consists precisely of all real numbers that we can obtain from $\mathbb{Q}$ by taking square roots of positive numbers a finite number of times and applying a finite number of field operations.

Corollary If γ is constructive, then $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^t$ for some $t \in \mathbb{Z}^+ \cup \{0\}$.

1. **Corollary**(Theorem) Doubling the cube is impossible.

2. **Theorem** Trisecting the angle is impossible.

3. **Theorem** Squaring the circle is impossible.

Proof.

1. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

2. 三等分 60° 爲不可能, 因爲 $cos20^\circ$ 無法作圖.

3. π 不是代數數. ■

如果 F 爲佈於 $\mathbb{Z}_p$ 的有限體, 則 $|F| = p^n$, 其中 $n \in \mathbb{Z}^+$.

(p.1) $\forall\ \alpha \in F,\ \alpha^{p^n} - \alpha = 0$.

實際上, 一定存在一個 $M(x)$, $deg(M(x)) < p^n$, $M(x) \in \mathbb{Z}_p[x]$ 且 $M(\alpha) = 0$.

Defn. The minimal polynomial over $\mathbb{Z}_p$ of β is the lowest degree monic poly. $M(x) \in \mathbb{Z}_p[x]$ s.t. $M(\beta) = 0$

e.g. $x^{16} - x$

$= x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ (?)

$$\begin{aligned} 0 &\rightarrow x \\ 1 &\rightarrow x+1 \\ \alpha^5 &\rightarrow x^2+x+1 \\ \alpha &\rightarrow x^4+x+1 \\ \alpha^3 &\rightarrow x^4+x^3+x^2+x+1 \\ \alpha^{14} &\rightarrow x^4+x^3+1 \end{aligned}$$

$$\begin{aligned} (\alpha^5)^2+\alpha^5+1 &= \alpha^{10}+\alpha^5+1 = \alpha^5(\alpha^5+1)+1 = (\alpha^2+\alpha)(\alpha^2+\alpha+1)+1 \\ &= \alpha^4+\alpha^2+\alpha^2+\alpha+1 = \alpha^4+\alpha+1 = 0 \end{aligned}$$

(M1) M(x) is irreducible.

(M2) If $f(x) \in \mathbb{Z}_p[x]$ and $f(\beta) = 0$, then $M(x) \mid f(x)$. Let

$f(x) = M(x)q(x) + r(x)$ where $r(x) = 0$ or $deg(r(x)) < deg(M(x))$. If $r(x) \neq 0$, then $r(\beta) = 0$. $\rightarrow\leftarrow$ ■

(M3) $M(x) \mid x^{p^n} - x$.

(M4) $deg(M(x)) \leq n$.

Proof. $[F : \mathbb{Z}_p] = n$ *Rightarrow* $\{1, \beta, \beta^2, \cdots, \beta^n\}$ is linear independent. Let $\sum_{i=0}^{n} b_i \beta^i = 0$ (線性組合). Then $f(\beta) = 0$ where $f(x) = \sum_{i=0}^{n} b_i x^i$. Thus, $M(x) \mid f(x)$. $deg(M(x)) \leq n$. ■

(M5) The minimal polynomial of a primitive element of F has degree n. (Such a polynomial is called a primitive polynomial.)

Proof. Let β be a primitive element of F, i.e., $F^* = \langle\beta\rangle$. Let $M(x)$ be the minimal polynomial of β and $deg(M(x)) = d$. Then $F = \mathbb{Z}_p[z]/langleM(x)\rangle$ is a field with p^d elements. Since $\beta \in F$, $\langle\beta\rangle \subseteq F^*$, $n \geq d$. By (M4) $d \leq m$, hence $d = n$. ■

Theorem All finite fields with the same number of elements are isomorphic.

Proof. Let F_1, F_2 be two finite fields with p^n elements and let α be a primitive element of F_1 with minimal polynomial M(x). By (M3) $M(x) \mid x^{p^n} - x$. This implies that there exists an element $\beta \in F_2$ where minimal polynomial is $M(x)$.

Now, F_1 can be considered as a field consist of all polynomials in α of degree $\leq$"$n - 1$" (modulo $M(x)$) and F_2 can be considered as a

field consist of all polynomials in β of degree $\leq$"$n-1$" (modulo $M(\beta)$). Therefore $\varphi : F_1 \to F_2$ defined by $\varphi(f(\alpha)) = f(\beta)$ is an isomorphism.

e.g.

Defined by x^3+x+1	Defined by x^3+x^2+1
$000 = 0$	$000 = 0$
$100 = \alpha^0$	$100 = \beta^0$
$010 = \alpha$	$010 = \beta$
$001 = \alpha^2$	$001 = \beta^2$
$110 = \alpha^3$	$101 = \beta^3$
$011 = \alpha^4$	$111 = \beta^4$
$111 = \alpha^5$	$110 = \beta^5$
$101 = \alpha^6$	$011 = \beta^6$
(不同)	

α 的 minimal polynomial 是 x^3+x+1

β 的 minimal polynomial 也是 x^3+x+1

$((\beta^3)^3+\beta^3+1) = \beta^9+\beta^3+1 = \beta^2+\beta^3+1 = 0$. $\alpha \to \beta^3$ generates an isomorphism.

(M6) Let $|F| = p^n$. Then $\alpha \to \alpha^p$ generates an isomorphism onto itself. (α and α^p 具有相同的 minimal polynomial!)

Proof. $[f(\alpha)]^p = f(\alpha^p)$ (?) ■

e.g. $(\beta^4+\beta^3+\beta+1)^2=(\beta^2)^4+(\beta^2)^3+(\beta^2)+1=\beta^8+\beta^6+\beta^2+1.$

$0,1,2,3,4,\cdots,14$

$\downarrow$

α^0 的 M.P. 爲 $x+1$

α^1 的 M.P. 爲 $(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$

α^3 的 M.P. 爲 $(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9)$

α^5 的 M.P. 爲

$(x+\alpha^5)(x+\alpha^{10})=x^2+\alpha^5x+\alpha^{10}x+\alpha^{15}=x^2+(\alpha^{10}+\alpha^5)x+\alpha^{15}$