§5.2 有限域.

F为域且$|F|<+\infty$，则称F为有限域.

记号：$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

命题1：设F为有限域. 则1)$\exists$素数p s.t. F为$\mathbb{F}_p$的扩域，从而$\mathrm{char}F = p$.

2) 若K/F为有限扩张且$|F|=q$. 则$|K| = q^n$, $n=[K:F]$.

证：1) $\varphi: \mathbb{Z} \to F$, $n \to n\cdot 1$ 环同态. $\ker\varphi = p\mathbb{Z}$. $p>0$且为素数.

$\therefore \bar{\varphi}: \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \to F$, $n+p\mathbb{Z} \to n\cdot 1$ 为单同态 $\Rightarrow F/\mathbb{F}_p$为域扩张.

2) 设$n=[K:F]$, $\alpha_1, \cdots \alpha_n \in K$为一组F-基. 则$\forall \alpha \in K$, α可唯一写成$\sum_{i=1}^{n} c_i\alpha_i$, $c_i \in F$

$\therefore |K| = q^n$. □

命题2：设F为有限域，$q=|F|=p^n$. 则

1) $\alpha^q = \alpha \quad \forall \alpha \in F$.

2) $X^q - X = \prod_{\alpha\in F}(X-\alpha)$

3) F是X^q-X在$\mathbb{F}_p$上的分裂域.

证：1) $U(F) = F\setminus\{0\}$为交换群且$|U(F)| = q-1$.

$\forall \alpha \in F\setminus\{0\}$. $\alpha^{q-1}=1 \Rightarrow \alpha^q = \alpha \quad \forall \alpha \in F$.

2) X^q-X为首1 (1)) $\Rightarrow X^q - X = \prod_{\alpha\in F}(X-\alpha)$.

3) $F = \mathbb{F}_p(\alpha_1, \cdots \alpha_q)$ 其中$F=\{\alpha_1, \cdots \alpha_q\}$.

$\Rightarrow$ F是X^q-X在$\mathbb{F}_p$上的分裂域. □

推论1：设F_1, F_2为有限域且$|F_1|=|F_2|$ 则$F_1 \cong F_2$.

证：设$q=|F_1|=|F_2|=p^n$. 则由命题2：F_1, F_2为X^q-X在$\mathbb{F}_p$上的分裂域 $\Rightarrow F_1 \cong F_2$.

$K/\mathbb{F}_p$为域扩张，$n>0$.

令 $F=\{\alpha\in K \mid \alpha^{p^n}-\alpha=0\}$ 断言：$F/\mathbb{F}_p$ 为扩域

证：$\forall\ \alpha\in\mathbb{F}_p,\ \alpha^p=\alpha \Rightarrow \alpha^{p^n}=\alpha \Rightarrow \alpha\in F \ \therefore \mathbb{F}_p\subseteq F$

$\forall\ \alpha_1,\alpha_2\in F,\ (\alpha_1-\alpha_2)^{p^n}=\alpha_1^{p^n}-\alpha_2^{p^n}=\alpha_1-\alpha_2\Rightarrow\alpha_1-\alpha_2\in F$

$(\alpha_1\alpha_2)^{p^n}=\alpha_1^{p^n}\alpha_2^{p^n}=\alpha_1\alpha_2\Rightarrow\alpha_1\alpha_2\in F$

$\therefore$ F 为子环.

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

$\therefore$ F 为子域.

定理1：设 F 为有限域，$n>0$，则 $\exists$ 域扩张 K/F s.t. $[K:F]=n$，且 K 在同构意义下唯一.

证：设 $|F|=q$. 由命题1知 $q=p^m$，p 为素数，$m=[F:\mathbb{F}_p]$.

令 L 为 $X^{q^n}-X$ 在 F 上的分裂域. 记 $K=\{\alpha\in L \mid \alpha^{q^n}-\alpha=0\}$

$=\{\alpha\in L\mid \alpha^{p^{mn}}-\alpha=0\}$

$\forall\ \alpha\in F.\ \alpha^q-\alpha=0\Rightarrow\alpha^{q^n}-\alpha=0\Rightarrow\alpha\in K\Rightarrow F\subseteq K$.

由前述断言 $\Rightarrow$ K 为域 $\Rightarrow$ K/F 为域扩张.

$(X^{q^n}-X)'=q^n\cdot X^{q^n-1}-1=-1\Rightarrow \gcd(X^{q^n}-X,\ (X^{q^n}-X)')=1$

$\therefore$ $X^{q^n}-X$ 在 L 中无重根 $\therefore$ $|K|=q^n$

命题1 $\Rightarrow$ $|K|=q^{[K:F]}\Rightarrow[K:F]=n$.

设 $\tilde{K}/F$ 为域扩张 s.t. $[\tilde{K}:F]=n$. 则 $|\tilde{K}|=q^n=|K|$

由推论2，$\tilde{K}\cong K$. □

设 $q=p^n$，p 为素数. 令 $F=\mathbb{F}_p$ 则定理1 $\Rightarrow$ q 元有限域存在且唯一(同构意义下)

记号：$\mathbb{F}_q$ 表示 q 元有限域.

定理2：设 $q=p^n$，p 为素数.

1) $U(\mathbb{F}_q)=\mathbb{F}_q\setminus\{0\}$ 为 $q-1$ 阶循环群.

2) $\mathrm{Frob}_p:\mathbb{F}_q\longrightarrow\mathbb{F}_q$，$\alpha\longrightarrow\alpha^p$ 为自同构且 $\mathrm{Frob}_p|_{\mathbb{F}_p}=\mathrm{id}$，并且

$\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)=\langle \mathrm{Frob}_p\rangle$，$|\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)|=n$.

3) 设 $F \subseteq \mathbb{F}_q$ 为子域且 $|F| = p^d$，则 $d \mid n$. 反之，若 $d \mid n$ 则 $\exists!$ 子域 $F \subseteq \mathbb{F}_q$ s.t. $|F| = p^d$.

证：① BA II P58 定理11可知.

2) $\forall \alpha_1, \alpha_2 \in \mathbb{F}_q$, $Frob_p(\alpha_1+\alpha_2) = (\alpha_1+\alpha_2)^p = \alpha_1^p + \alpha_2^p = Frob_p(\alpha_1) + Frob_p(\alpha_2)$.

$Frob_p(\alpha_1\alpha_2) = (\alpha_1\alpha_2)^p = \alpha_1^p\alpha_2^p = Frob_p(\alpha_1)Frob_p(\alpha_2)$

$Frob_p(1) = 1^p = 1$

$\therefore Frob_p$ 为同态 $\because \mathbb{F}_q$ 为有限集且 $Frob_p$ 为单的 $\therefore Frob_p$ 为同构.

$\forall \alpha \in \mathbb{F}_p$, $\alpha^p = \alpha \Rightarrow Frob_p(\alpha) = \alpha \Rightarrow Frob_p|_{\mathbb{F}_p} = id$.

$\therefore Frob_p \in Aut(\mathbb{F}_q/\mathbb{F}_p)$.

$\forall \alpha \in \mathbb{F}_q$. $Frob_p^n(\alpha) = \alpha^{p^n} \underset{\text{命题2}}{=} \alpha \Rightarrow Frob_p^n = id$.

另一方面. 设 $Frob_p^m = id$, 其中 $1 \le m \le n$, 则 $\{\alpha \in \mathbb{F}_q \mid \alpha^{p^m} - \alpha = 0\} = \mathbb{F}_q$

$\Rightarrow p^n = |\{\alpha \in \mathbb{F}_q \mid \alpha^{p^m} - \alpha = 0\}| \le p^m \Rightarrow n \le m \Rightarrow n = m$.

$\therefore |\langle Frob_p \rangle| = n$.

§5.1 推论3 $\Rightarrow |Aut(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p] = n$

$\therefore Aut(\mathbb{F}_q/\mathbb{F}_p) = \langle Frob_p \rangle$

3) $U(F)$ 为 $U(\mathbb{F}_q)$ 的子群. 拉格朗日定理 $\Rightarrow |U(F)| \mid |U(\mathbb{F}_q)|$.

$\because |U(F)| = p^d - 1$, $|U(\mathbb{F}_q)| = p^n - 1$ $\therefore p^d - 1 \mid p^n - 1 \Rightarrow d \mid n$

设 $d \mid n \Rightarrow p^d - 1 \mid p^n - 1 \Rightarrow X^{p^d-1} - 1 \mid X^{p^n-1} - 1 \Rightarrow X^{p^d} - X \mid X^{p^n} - X$.

令 $F = \{\alpha \in \mathbb{F}_q \mid \alpha^{p^d} - \alpha = 0\}$.

$\because \mathbb{F}_q$ 为 $X^{p^n} - X$ 在 $\mathbb{F}_p$ 上的分裂域 $\therefore X^{p^d} - X$ 在 $\mathbb{F}_q$ 中有 p^d 个根.

$\therefore |F| = p^d$ 前面断言 $\Rightarrow F$ 为域

若 $F \subseteq \mathbb{F}_q$ 为子域且 $|F| = p^d$ 则由命题2 $\Rightarrow \alpha^{p^d} - \alpha = 0$ $\forall \alpha \in F$

i.e $F = \{\alpha \in F \mid \alpha^{p^d} - \alpha = 0\} = \{\alpha \in \mathbb{F}_q \mid \alpha^{p^d} - \alpha = 0\} = F$. □

注：由定理2及 BA II P13 定理3知：

$$\{\mathbb{F}_q\text{的子域}\} \xleftrightarrow{\text{双射}} \{d \mid d|n\} \xleftrightarrow{\text{双射}} \{\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)\text{的子群}\}$$

定理3：设 $q=p^n$，$m>0$. 则

1) $\mathbb{F}_q[X]$ 中存在 m 次不可约多项式

2) 设 $f\in\mathbb{F}_q[X]\setminus\mathbb{F}_q$ 不可约，则 $\mathbb{F}_q[X]/\langle f\rangle$ 为 f 在 $\mathbb{F}_q$ 上的分裂域.

证：1) 由定理1，$\exists\, K/\mathbb{F}_q$ s.t. $[K:\mathbb{F}_q]=m$. 设 $U(K)=\langle\theta\rangle$，$f_\theta$ 为 θ 在 $\mathbb{F}_q$ 上的极小多项式，则 f_θ 不可约. $\because K=\mathbb{F}_q(\theta)$ $\therefore m=[K:\mathbb{F}_q]=\deg f_\theta$.

2) 记 $K=\mathbb{F}_q[X]/\langle f\rangle$，$m=\deg f$. 则 $|K|=q^m$. 设 θ 为 f 在 K 中一根，则 $K=\mathbb{F}_q(\theta)$.

命题2 $\Rightarrow \theta^{q^m}-\theta=0 \Rightarrow f\mid X^{q^m}-X$ $\because K$ 为 $X^{q^m}-X$ 在 $\mathbb{F}_p$ 上的分裂域

$\therefore f=\lambda(X-\theta)(X-\alpha_2)\cdots(X-\alpha_m)$，$\lambda\in\mathbb{F}_q$，$\alpha_2,\cdots\alpha_m\in K$

又 $\because K=\mathbb{F}_q(\theta)=\mathbb{F}_q(\theta,\alpha_2,\cdots\alpha_m)$ $\therefore K$ 为 f 在 $\mathbb{F}_q$ 上的分裂域 □

记 $\Psi_d(q):=|\{\mathbb{F}_q[X]\text{中}d\text{次不可约多项式}\}|$

显然 $\Psi_d(q)<+\infty$. 问题：$\Psi_d(q)=?$

Mobius反演公式：

$$\mu(n)=\begin{cases}1, & n=1\\ (-1)^k & n=p_1\cdots p_k,\ p_i\text{为互异素数}\\ 0 & d^2\mid n,\ d>1\end{cases}$$

称为Mobius函数.

性质：1) 若 $\gcd(m,n)=1$ 则 $\mu(mn)=\mu(m)\mu(n)$（乘性函数）

2) 设 $n=p_1^{m_1}\cdots p_r^{m_r}$，$\underline{n}=p_1\cdots p_r$ p_i 为互异素数

则 $$\sum_{d\mid n}\mu(d)=\sum_{d\mid \underline{n}}\mu(d)$$

3) $$\sum_{d\mid n}\mu(d)=\begin{cases}1 & n=1\\ 0 & n>1\end{cases}$$

注意到在 $\underline{n}=p_1\cdots p_r$ 中有 s 个素因子的因子个数为 $\binom{r}{s}$

从而 $$\sum_{d\mid \underline{n}}\mu(d)=\sum_{s=0}^{r}\binom{r}{s}(-1)^s=(1-1)^r=0.$$

4) $$\sum_{d\mid n\mid m}\mu\left(\frac{m}{n}\right)=\begin{cases}1 & d=m\\ 0 & d\mid m\text{且}d<m\end{cases}$$

4) $\sum_{d|n|m} \mu(\frac{m}{n}) = \begin{cases} 1 & \\ 0 & d|m \text{ 且 } d<m \end{cases}$

令 $m=ds$, $n=dt$ 则 $\sum_{d|n|m} \mu(\frac{m}{n}) = \sum_{t|s} \mu(\frac{s}{t}) = \begin{cases} 1 & s=1 \ (d=m) \\ 0 & s>1 \ (d<m) \end{cases}$

设 $(A,+)$ 为交换群，$f, g: \mathbb{Z}_{\geq 0} \to A$ 为两个函数(映射)

若 $f(n) = \sum_{d|n} g(d)$ 则 $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$ (Mobius反演公式)

$$\sum_{n|m} \mu(\tfrac{m}{n}) f(n) = \sum_{n|m} \mu(\tfrac{m}{n}) \sum_{d|n} g(d) = \sum_{n|m} \sum_{d|n} \mu(\tfrac{m}{n}) g(d)$$

$$= \sum_{d|m} \sum_{d|n|m} \mu(\tfrac{m}{n}) g(d) = \sum_{d|m} g(d) \sum_{d|n|m} \mu(\tfrac{m}{n}) = g(m)$$

乘法版本：$(A,\cdot)$ 为交换群. $f, g: \mathbb{Z}_{\geq 0} \to A$ 为两函数.

若 $f(n) = \prod_{d|n} g(d)$ 则 $g(n) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}$

例：1) 欧拉函数：$\varphi(n) = \left| U(\mathbb{Z}/n\mathbb{Z}) \right| = \prod_{i=1}^{r} p_i^{m_i-1}(p_i-1)$, $n = \prod_{i=1}^{r} p_i^{m_i}$

$$n = \sum_{d|n} \varphi(d) \Rightarrow \varphi(n) = \sum_{d|n} \mu(\tfrac{n}{d}) d = \sum_{d|n} \mu(d) \tfrac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}$$

$n = p_1 \cdots p_r$

$$= n \sum_{d|n} \frac{\mu(d)}{d} = n\left(1 - \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1\leq i<j\leq r} \frac{1}{p_i p_j} - \cdots\right)$$

$$= n\left(1-\tfrac{1}{p_1}\right)\cdots\left(1-\tfrac{1}{p_r}\right)$$

2) 分圆多项式：$n>0$, $\zeta \in \mathbb{C}$ 称为 n-次本原根若 $\zeta^n = 1$ 且 $\zeta^i \neq 1$ $\forall 1 \leq i < n$.

$\Gamma_n = \mathbb{Q}(\zeta)$ 称为分圆域 (ζ: n-次本原根) $\quad \Phi_n(X) = \prod_{\zeta \in \mathbb{C}\ n\text{次本原根}} (X-\zeta)$.

ζ 为 n 次本原根 则 $\langle \zeta \rangle$ (乘法群) $= \{1, \zeta, \cdots \zeta^{n-1}\} = \{\alpha \in \mathbb{C} \mid \alpha^n - 1 = 0\}$

且 $\psi: \mathbb{Z}/n\mathbb{Z} \to \langle \zeta \rangle$ 为群同构 $\quad P_n := \{n\text{次本原单根}\}$

$i+n\mathbb{Z} \to \zeta^i$

$$i+n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z}) \iff \exists\, j \in \{1, \cdots n-1\} \text{ s.t. } ij \equiv 1 \bmod n$$

$$\iff \zeta^{ij} = \zeta \iff \zeta^i \in P_n$$

$\therefore \varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})| = |P_n|$.

另外：$\zeta^i \in P_d \Rightarrow d|n$. $\therefore \{1, \zeta, \cdots \zeta^{n-1}\} = \bigcup_{d|n} P_d$

$\therefore X^n - 1 = \prod_{d|n} \Phi_d(X)$ （利用归纳法可证 $\Phi_d(X) \in \mathbb{Z}[X]$）

Mobius反演公式 $\Rightarrow \Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$

例：$\Phi_1(X) = X - 1$. $\Phi_2(X) = \frac{(X^2-1)}{(X-1)} = X + 1$.

$\Phi_4(X) = \frac{(X^4-1)}{(X^2-1)} = X^2 + 1$

3) 命题3：设 $q = p^n$, $f \in \mathbb{F}_q[X] \setminus \mathbb{F}_q$ 不可约, $d = \deg f$ 则

1) $f | X^{q^d} - X$ 2) $\forall m > 0$, $f | X^{q^m} - X \Leftrightarrow d | m$.

证：1) $|\mathbb{F}_q[X]/\langle f \rangle| = q^d$. 设 θ 为 f 在 $\mathbb{F}_q[X]/\langle f \rangle$ 中的根，则 $\theta^{q^d} - \theta = 0$

$\therefore f | X^{q^d} - X$

2) ($\Rightarrow$) 设 $K/\mathbb{F}_q$ 为域扩张 s.t. $[K : \mathbb{F}_q] = m$. 则 K 为 $X^{q^m} - X$ 在 $\mathbb{F}_p$ 上的分裂域 从而为 $X^{q^m} - X$ 在 $\mathbb{F}_q$ 上的分裂域，设 θ 为 f 在 K 中的根

则 $[\mathbb{F}_q(\theta) : \mathbb{F}_q] = \deg f = d$, $\therefore |\mathbb{F}_q(\theta)| = q^d$

$\because |K| = q^m$ 且 $\mathbb{F}_q(\theta)$ 为 K 的子域 由定理2：$d | m$.

($\Leftarrow$) 由1) $f | X^{q^d} - X$ 又 $X^{q^d} - X | X^{q^m} - X \Rightarrow f | X^{q^m} - X$. □

$S_n(q) := \{\mathbb{F}_q[X]$ 中的 n-次不可约多项式$\}$

$f \in S_n(q) \xrightarrow{\text{命题3}} f | X^{q^n} - X$

命题2 $\Rightarrow \mathbb{F}_q[X]/\langle f \rangle$ 为 $X^{q^n} - X$ 在 $\mathbb{F}_p$ 上的分裂域

$\forall \alpha \in \mathbb{F}_q[X]/\langle f \rangle$, 设 f_α 为 α 在 $\mathbb{F}_q$ 上的极小多项式，则 $f_\alpha | X^{q^n} - X$

$\therefore X^{q^n} - X = \prod_{d|n} \prod_{f \in S_d(q)} f$

$\therefore q^n = \sum_{d|n} d \cdot \psi_d(q) \Rightarrow n\psi_n(q) = \sum_{d|n} \mu(\frac{n}{d}) q^d$

$\therefore \psi_n(q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$