抽象代数学

有限域上不可约多项式

$\mathbb{F}_q$ q阶有限域 其中 $q=p^e$，$e\geq 1\in\mathbb{N}$，p 素数 也记作 $\mathbb{F}_q=GF(p^e)$.

$\mathbb{E}=\overline{\mathbb{F}_q}$ 代数闭包

Frobenius 自同构：$\mathbb{E}\xrightarrow{F}\mathbb{E}$ $\quad F(\alpha)=\alpha^q$

性质(1) $\forall n\geq 1\in\mathbb{N}$，$\mathbb{F}_{q^n}=\{x\in\mathbb{E}\mid F^n(x)=x\}$

(2) 设 $f(x)\in\mathbb{F}_q[x]$，$\alpha\in\mathbb{E}$ 是 $f(x)$ 的一个根，则 $F(\alpha)=\alpha^q$，$F^2(\alpha)=\alpha^{q^2}$，$\cdots$ 均是 $f(x)=0$ 的根.

证明：(1) F 是一个域自同构（过去讲义证明过）

$$\mathbb{F}_{q^n}=\{\alpha\in\mathbb{E}\mid\alpha\text{ 是 }x^{q^n}-x=0\text{ 的根}\}=\{\alpha\in\mathbb{E}\mid F^n(\alpha)=\alpha\}$$

(2) 设 $f(x)=\sum_{i=0}^{n}c_ix^i$ $\quad c_i\in\mathbb{F}_q$ $\quad f(\alpha)=0$

$$F(f(x))=\sum_{i=0}^{n}c_iF(x^i)\Rightarrow F(f(\alpha))=f(F(\alpha))=0$$

命题 设 $\alpha\in\mathbb{E}=\overline{\mathbb{F}_q}$，且 $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=n$，则 α 在 $\mathbb{F}_q[x]$ 中极小多项式 $P_\alpha(x)$ 在 $\mathbb{E}[x]$ 中形式为：

$$P_\alpha(x)=(x-\alpha)(x-F(\alpha))\cdots(x-F^{n-1}(\alpha))$$

证明：因为 $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=n$，$\alpha^{q^n}=\alpha$ 即 $F^n(\alpha)=\alpha$.

由性质(2)，α 的 F-轨道元均是 $P_\alpha(x)$ 的根.

设$\{\alpha, F(\alpha), \cdots, F^m(\alpha)\}$是F-轨道中不同元素，$F^{m+1}(\alpha)=\alpha$.

则$(x-\alpha)\cdots(x-F^m(\alpha))=g(x)$在F作用下不变$\Rightarrow g(x)\in\mathbb{F}_q[x]$

$\Rightarrow m=n-1$

例1 $f(x)=x^3+x^2+1\in\mathbb{Z}_2[x]$ $f(x)$不可约

考虑 $\dfrac{\mathbb{Z}_2[x]}{(f(x))}=\mathbb{Z}_2(\alpha)$ $\alpha=x+(f(x))$是$f(x)$的一个根.

验证：

$f(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$

例2. $f(x)=x^3+2x+1\in\mathbb{Z}_3[x]$ $f(x)$不可约

设$f(r)=0\Rightarrow f(x)=(x-r)(x-\underset{F(r)}{\underset{\parallel}{r^3}})(x-\underset{F^2(r)}{\underset{\parallel}{r^9}})$

验证：

$r^3=r+2$, $r^9=r+1$

推论 设$f(x)\in\mathbb{F}_q[x]$是n次不可约多项式. 则$f(x)$在$\mathbb{F}_{q^n}$中分裂，$\mathbb{F}_{q^n}\simeq\dfrac{\mathbb{F}_q[x]}{(f(x))}$

定理 $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$是一个$n$阶循环群，F是一个生成元

证明：~~令$\mathbb{F}_q$~~ 显然$\langle F\rangle$是$Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$的$n$阶循环子群. ($F^n=id$). 因为$\mathbb{F}_{q^n}^\times$是一个循环群，设$\alpha$是一个生成元.

$\forall\sigma\in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$，$\sigma$完全由$\sigma(\alpha)$决定，设$\alpha$在$\mathbb{F}_q$上极小多项式为$P_\alpha(x)$，则$\deg P_\alpha(x)=n=[\mathbb{F}_{q^n}:\mathbb{F}_q]$，$\mathbb{F}_{q^n}\cong\dfrac{\mathbb{F}_q[x]}{(P_\alpha(x))}$

$\sigma(\alpha)$ 仍是 $P_\alpha(x)$ 的根. 因此 $\sigma(\alpha)=F^i(\alpha)$

若 $F^i(\alpha)=F^j(\alpha)$ $(i<j)$ 则 $\alpha=F^{j-i}(\alpha)=\alpha^{q^{j-i}}$, 但 α 是 $\mathbb{F}_{q^n}^\times$ 的生成元, $n|j-i$

由之前讨论

$$\{\alpha, F(\alpha), \cdots, F^{n-1}(\alpha)\} \longleftrightarrow \{f(x)=(x-\alpha)(x-F(\alpha))\cdots(x-F^{n-1}(\alpha)) \mid f(x)\ n\text{次不可约}\in\mathbb{F}_q[x]\}$$

定理 $f(x)=x^{q^n}-x\in\mathbb{F}_q[x]$ 是次数整除 n 的全体首一不可约多项式乘积.

证明: 设 $g(x)\in\mathbb{F}_q[x]$ 不可约, $\deg g(x)=m$.

~~$g(x)\mid x^{q^n}-x$~~ 设 $g(x)$ 在 $\mathbb{F}_q$ 上分裂域为 $\mathbb{L}\cong\frac{\mathbb{F}_q[x]}{(g(x))}=\mathbb{F}_{q^m}$

$f(x)$ 在 $\mathbb{F}_q$ 上分裂域为 $\mathbb{F}_{q^n}$

$g(x)\mid f(x)\Longleftrightarrow\mathbb{F}_{q^m}\subseteq\mathbb{F}_{q^n}\Longleftrightarrow m\mid n$

~~反之, 若 $m\mid n$,~~

考虑 $x^n-1\in\mathbb{Q}[x]$，它在 $\mathbb{C}$ 中有 n 个根：$1,w,w^2,\cdots,w^{n-1}$

其中 $w=e^{i\frac{2\pi}{n}}$，$\mathbb{Q}(w)$ 是 x^n-1 在 $\mathbb{Q}$ 上的分裂域，称为

$\mathbb{Q}$ 的 ~~是~~ 第 n 个分圆扩张（the n-th cyclotomic extension of $\mathbb{Q}$）

x^n-1 在 $\mathbb{Q}[x]$ 中不可约因子称为分圆多项式（cyclotomic polynomial），考虑 w 生成的 n 阶循环群（关于乘法），w^k

$1\le k\le n$ 是生成元 $\Longleftrightarrow (n,k)=1$，若 $\langle w^k\rangle=\langle w\rangle$，$w^k$ 称为

本原单位根（n 阶）共有 $\phi(n)$ 个 n 次本原单位根.

定义 给定正整数 n，令 $w_1,w_2,\cdots,w_{\phi(n)}$ 是全部 n 次本原单位根，第 n 个分圆多项式（$\mathbb{Q}$ 上）是

$$\Phi_n(x)=(x-w_1)(x-w_2)\cdots(x-w_{\phi(n)})\text{（首一多项式）}$$

定理1 设 $n>0\in\mathbb{N}$，$\Phi_n(x)$ 是一个整系数多项式

证明：需要如下定理.

定理2 $x^n-1=\prod_{d|n}\Phi_d(x)$ 这里 $n>0\in\mathbb{N}$，$d\in\mathbb{N},d>0$

证明：$x^n-1=0$ 的全部零点 $\{1,w,\cdots,w^{n-1}\}$ $\langle w\rangle$ 是一个阶为 n 的循环群. 对 $1\le j\le n-1$，$o(w^j)|n$ 令 $o(w^j)=d$.

则 w^j 是 $x^d-1=0$ 的根，且是本原根 $\Rightarrow\Phi_d(x)$ 包含因子 $(x-w^j)$

另一方面，若 $x-\alpha\,|\,\Phi_d(x)$，$d|n$. 则 $\alpha^d=1\Rightarrow\alpha^n=1$ 即 $x-\alpha\,|\,x^n-1$

最后，设 $d_1 \neq d_2$，$d_1, d_2 \mid n$，则 $\Phi_{d_1}(x)$ 和 $\Phi_{d_2}(x)$ 无公共零点

否则设 $x-\alpha \mid \Phi_{d_1}(x)$，$x-\alpha \mid \Phi_{d_2}(x)$，$\Rightarrow \alpha^{d_1}=\alpha^{d_2}=1$。

令 $d=(d_1, d_2)$ $d_1 \neq d_2 \Rightarrow d<d_1$ 或 $d<d_2$ 但 $\alpha^{d}=1$，设 $d_1<d_2$

则 α 不能是 $\Phi_{d_2}(x)$ 的本原根.

例 $x^6-1=\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$

$\Phi_1(x)=x-1$，$\Phi_2(x)=x+1$，$\Phi_3(x)=x^2+x+1$

$\Phi_6(x)=x^2-x+1$ 设 $\{1, w, w^2, \cdots, w^5\}$ 是 x^6-1 的根 则 $\Phi_3(x)=(x-w^2)(x-w^4)$（注 $x^3-1=0$ 的根和 x^6-1 的根的关系）.

回到定理1的证明：

$n=1$ ✓ 假设 $g(x)=\prod\limits_{\substack{d\mid n \\ d<n}} \Phi_d(x)$ 有整系数. 由定理2，

$x^n-1=\Phi_n(x)g(x)$. $\Rightarrow \Phi_n(x) \in \mathbb{Q}[x]$（比较两边系数）

但 x^n-1 和 $g(x)$ 均为首一多项式 $\Rightarrow \Phi_n(x) \in \mathbb{Z}[x]$

例 使用定理1, 2，可以递归求出 $\Phi_n(x)$

$n=p$ 素数 $\Phi_p(x)\Phi_1(x)=x^p-1 \Rightarrow \Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$

一般地，$\Phi_n(x)=(x^n-1)\Big/\prod\limits_{\substack{d\mid n \\ d<n}} \Phi_d(x)$.

例如 $x^{10}-1=\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x) \Rightarrow$

$\Phi_{10}(x)=x^4-x^3+x^2-x+1$.

定理3. $\Phi_n(x)$ 是 $\mathbb{Z}[x]$ 中不可约多项式.

证明：设 $f(x)\in\mathbb{Z}[x]$ 是 $\Phi_n(x)$ 的一个首一不可约因子. 因为 $\Phi_n(x)$ 无重根. 只需证明：$\Phi_n(x)$ 的零点是 $f(x)$ 的零点.

设 $x^n-1=f(x)g(x)$, $g(x)\in\mathbb{Z}[x]$. 设 w 是一个 n 次本原根, 且 $f(w)=0$. 则 $f(x)$ 是 w 在 $\mathbb{Q}$ 上极小多项式. 若 p 素数, 且 $(p,n)=1$, 则 w^p 也是 n 次本原根. $0=(w^p)^n-1=f(w^p)g(w^p)$

若 $f(w^p)\neq 0$, 则 $g(w^p)=0 \Rightarrow w$ 是 $g(x^p)=0$ 的一个零点

$\Rightarrow f(x)\mid g(x^p)$ (在 $\mathbb{Q}[x]$ 中) 但是 $f(x), g(x^p)$ 均首一

$\Rightarrow f(x)\mid g(x^p)$ 在 $\mathbb{Z}[x]$ 中. $g(x^p)=f(x)h(x)$, $h(x)\in\mathbb{Z}[x]$

令 $\bar{g}(x)$, $\bar{f}(x)$, $\bar{h}(x)$ 是它们在 $\mathbb{Z}_p[x]$ 中像; $\mathbb{Z}[x]\longrightarrow\mathbb{Z}_p[x]$

$\Rightarrow \bar{g}(x^p)=\bar{f}(x)\bar{h}(x)$ 即 $(\bar{g}(x))^p=\bar{f}(x)\bar{h}(x)$, 但是 $\mathbb{Z}_p[x]$ 是唯一分解整区. 存在不可约多项式 $m(x)\mid\bar{f}(x)$, $m(x)\mid\bar{g}(x)$, $m(x)\in\mathbb{Z}_p[x]$, 从而 $m(x)^2\mid x^n-1$ (在 $\mathbb{Z}_p[x]$ 中), 这展示 x^n-1 在 $\mathbb{Z}_p$ 的某扩域上有重根. $(x^n-1)'=nx^{n-1}$, $p\nmid n$

$\Rightarrow (nx^{n-1}, x^n-1)=1$ 矛盾! 因此, $f(w^p)=0$

我们已证明：若 β 是 n 次本原根, 且 $f(\beta)=0$. 则对于任何和 n 互素素数 p, $f(\beta^p)=0$. 因为 $\Phi_n(x)$ 的任一零点形如 w^k, $1\le k<n$, $(k,n)=1$. 令 $k=p_1p_2\cdots p_t$, p_i 素数.

则 $w, w^{p_1}, (w^{p_1})^{p_2}, \cdots, w^{(p_1\cdots p_{t-1})p_t}=w^k$ 均是 $f(x)$ 的零点

$\Rightarrow \Phi_n(x)$ 所有零点属于 $f(x)$ 的零点

例. $x^6-1\in\mathbb{Z}_2[x]$

在 $\mathbb{Z}[x]$ 中, $x^6-1=(x-1)(x+1)(x^2+x+1)(x^2-x+1)$

$\Rightarrow \mathbb{Z}_2[x]$ 中 $\quad x^6-1=(x+1)^2(x^2+x+1)^2$

$\Rightarrow x^2+x+1$ 在 $\mathbb{Z}_2[x]$ 不可约(无零点)

定理 设 w 是第 n 次本原单位根. 则 $Gal(\mathbb{Q}(w)/\mathbb{Q})\simeq U_n$

证明: w 在 $\mathbb{Q}$ 上极小多项式为 $\cancel{\mathbb{Q}(w)}$ $\Phi_n(x)$, $\forall\sigma\in Gal(\mathbb{Q}(w)/\mathbb{Q})$

$\sigma(w)$ 也是 $\Phi_n(x)$ 的根, 即 $\sigma(w)$ 也是 n 次本原单位根, 则 $\exists j$

$$\sigma(w)=w^j \qquad (j,n)=1,\quad 0\leq j<n$$

反之, 若 $(a,n)=1$, 定义 $\sigma(w)=w^a$ 诱导了一个自同构 $\tilde{\sigma}$ $\in Gal(\mathbb{Q}(w)/\mathbb{Q})$. 这建立一个群同构

$$\begin{aligned} U_n &\longrightarrow Gal(\mathbb{Q}(w)/\mathbb{Q}) \\ j &\longmapsto \sigma_j : w\longmapsto w^j \end{aligned}$$

注: $\Phi_n(x)\in\mathbb{Z}[x]$ 不可约, 但可能存在素数 p, 在 $\mathbb{Z}_p[x]$ 中, 它可约. 例如: 设 p 素数, $(m,p)=1$, $e\geq 1$, 在 $\mathbb{Z}_p[x]$ 中, 有

$$\Phi_{p^e m}(x)=(\Phi_m(x))^{(p-1)(p^{e-1})} \qquad \text{注意 } \varphi(p^e)=p^{e-1}(p-1).$$

(见 garrett 的 abstract algebra)

应用：正n边形能否通过直尺、圆规作图得到?

设$\mathbb{F}$是一个域，取$\mathbb{F}\subseteq\mathbb{R}$，$\mathbb{F}$中的元素出发，使用直尺(无刻度)和圆规，且知道单位长度，作图得到长度$\alpha\in\mathbb{R}$

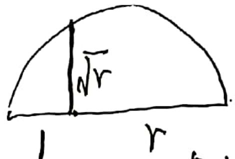
则α称为可构的(constructible)

性质：若$\alpha, \beta\neq 0$是可构的，则$\alpha+\beta, \alpha-\beta, \alpha\cdot\beta, \alpha/\beta$可构.

$\Rightarrow$ 可构数全体是包含$\mathbb{Q}$的$\mathbb{R}$的子域.

给定$\mathbb{F}$，产生新的可构数(点)的方式只有：$\mathbb{F}$中的圆交直线 $\Rightarrow \sqrt{\alpha}, \alpha\in\mathbb{F}$.

例 $r\in\mathbb{F}$



$\Rightarrow \mathbb{F}\subseteq\mathbb{F}(\sqrt{\alpha})=\mathbb{F}_1 \quad [\mathbb{F}_1:\mathbb{F}]=\begin{cases}1 & \sqrt{\alpha}\in\mathbb{F}\\ 2 & \sqrt{\alpha}\notin\mathbb{F}\end{cases}$

性质：若c是可构的，则$[\mathbb{Q}(c):\mathbb{Q}]=2^k \quad \exists k\geq 0\in\mathbb{N}$

例如 $\sqrt[3]{2}$ 是不可构的

$\cos 20^\circ$是不可构的，因为它是$8x^3-6x-1=0$的根

$\Rightarrow [\mathbb{Q}(\cos 20^\circ):\mathbb{Q}]=3 \Rightarrow 60^\circ$不能只通过尺规三等分.

正n边形能被尺规作图 $\Longleftrightarrow \cos\frac{2\pi}{n}$ 是可构的 $\Longleftrightarrow [\mathbb{Q}(\cos\frac{2\pi}{n}):\mathbb{Q}]$
$=2^k \ \exists k\in\mathbb{N}$

观察：$\mathbb{Q}\subseteq\mathbb{Q}(\cos\frac{2\pi}{n})\subseteq\mathbb{Q}(\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n})=\mathbb{Q}(\omega)$

定理（Gauss）一个正 n 边形能通过直尺和~~规~~圆规构造

$\Longleftrightarrow n=2^k p_1 p_2 \cdots p_t$，其中 $k\geq 0$，$p_1,\cdots,p_t$ 互异素数，且 $p_i=2^{m_i}+1$

$i=1,\cdots,t$，$m_i\in\mathbb{N}$.

证明："$\Rightarrow$" $[\mathbb{Q}(\cos\frac{2\pi}{n}):\mathbb{Q}]=[\mathbb{Q}(\omega):\mathbb{Q}]/[\mathbb{Q}(\omega):\mathbb{Q}(\cos\frac{2\pi}{n})]$

$=|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|/|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\cos\frac{2\pi}{n}))|$

已知 $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})\simeq U_n \quad |U_n|=\varphi(n)$

$\forall \sigma\in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \quad \sigma(\omega)=\omega^j, \quad (j,n)=1$.

即 $\sigma(\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n})=\cos\frac{2\pi j}{n}+i\sin\frac{2\pi j}{n}$

$\sigma\in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\cos\frac{2\pi}{n}))\Longleftrightarrow j=1$ 或 $n-1$

即 $|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\cos\frac{2\pi}{n}))|=2$

$\Rightarrow [\mathbb{Q}(\cos\frac{2\pi}{n}):\mathbb{Q}]=\frac{\varphi(n)}{2}$

设 $n=2^k p_1^{n_1} p_2^{n_2}\cdots p_t^{n_t} \quad k\geq 0, \quad \varphi(n)=2^{k-1}p_1^{n_1-1}(p_1-1)\cdots p_t^{n_t-1}(p_t-1)$

正 n 边形能尺规作图得到 $\Rightarrow [\mathbb{Q}(\cos\frac{2\pi}{n}):\mathbb{Q}]=2^l \ \exists l$

$\Rightarrow n_1=\cdots=n_t=1$，$p_i-1$ 是 2 的幂

"$\Longleftarrow$" n 形如 $2^k p_1\cdots p_t$ 且 $p_i=2^{m_i}+1$，则 $\varphi(n)=2^l \ \exists l$.

$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})\simeq U_n$ 是 Abelian，阶为 2^l.

由群论，有限 Abelian 群结构，存在子群链

$H_0 \subset H_1 \subset \cdots \subset H_t = Gal(\mathbb{Q}(w)/\mathbb{Q})$

其中 $H_0 = \{id\}$，$[H_{i+1} : H_i] = 2$

由Galois基本对应定理，存在中间域链

$$\underset{\mathbb{E}_0}{\overset{\|}{\mathbb{Q}(w)}} \supseteq \underset{\mathbb{E}_1}{\overset{\|}{\mathbb{Q}(\cos\frac{2\pi}{n})}} \supseteq \mathbb{E}_2 \supseteq \cdots \supseteq \mathbb{E}_t = \mathbb{Q}$$

$[\mathbb{E}_i : \mathbb{E}_{i+1}] = 2$ 　固定 $\mathbb{E}_i$，$\exists \beta_i$，$\mathbb{E}_{i+1} = \mathbb{E}_i(\beta_i)$ β_i 在 $\mathbb{E}_i[x]$

中极小多项式为 $x^2 + b_i x + c_i$，$b_i, c_i \in \mathbb{E}_i$，即

$$\mathbb{E}_{i+1} = \mathbb{E}_i(\sqrt{b_i^2 - 4c_i})$$

若 $\mathbb{E}_i$ 中元素可构 $\Rightarrow \sqrt{b_i^2 - 4c_i}$ 可构 $\Rightarrow \mathbb{E}_{i+1}$ 中元素可构

$\Rightarrow \cdots \Rightarrow \mathbb{Q}(\cos\frac{2\pi}{n})$ 中元素可构 $\Rightarrow \cos\frac{2\pi}{n}$ 可构.