近世代数之十四

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 单位根
2. 分圆域

单位根

1. 单位根$w \in k$满足$w^n = 1_k$。
2. 单位根的阶$\mathrm{ord}(w) = d$: 最小的正整数d使得$w^d = 1$。此时，称z为d次**本原单位根**。
3. 设有d次本原单位根。则$\mathrm{char}(k) \nmid d$。

引理

设单位根$w \in k$满足$\mathrm{ord}(w) = d$。则$w^n = 1_k$当且仅当$n|d$。

单位根的群

事实：若存在d次本原单位根w。

则$\{1, w, \cdots, w^{d-1}\} = \mathrm{Root}_k(x^d - 1)$，为$k^\times$的$d$阶子群。

这是**唯一可能**的d阶子群。

定理

设k为（可能无限的）域，且$H \subseteq k^\times$为d阶子群。则存在d次本原单位根w，且$H = \{1, w, \cdots, w^{d-1}\}$.

特别地，有限域的单位群$\mathbb{F}_{p^n}^\times$是循环群。

复单位根

设$n \geq 2$，考虑$\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$。

则$\mathrm{Root}_{\mathbb{C}}(x^n - 1) = \{1, \zeta, \cdots, \zeta^{n-1}\}$。

$$x^n - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1}).$$

引理

复n次本原单位根的全体恰为$\{\zeta^d \mid 1 \leq d < n, \gcd(d,n) = 1\}$，恰有$\phi(n)$个。

分圆域

定义

分圆域$\mathbb{Q}(\zeta)$，等于$x^n - 1 \in \mathbb{Q}[x]$的分裂域。

注意：$\mathbb{Q}(\zeta_2) = \mathbb{Q}$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$

分圆多项式

定义

n次分圆多项式

$$\Phi_n(x) = \prod_{n\text{次本原单位根}w} (x-w) = \prod_{\{1\le d<n|\gcd(d,n)=1\}} (x-\zeta^d)$$

故，$\deg\Phi_n(x) = \phi(n)$。

分圆多项式的计算

补充定义$\Phi_1(x) = x - 1$.

引理

$x^n - 1 = \prod_{d|n} \Phi_d(x)$。于是，$\Phi_n(x) \in \mathbb{Z}[x]$.

例子

$\Phi_2(x) = (x+1)$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$,

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$

不可约性

定理 (Gauss 1801/Kronecker 1854)

分圆多项式$\Phi_n(x) \in \mathbb{Z}[x]$不可约。

从而，

定理

以下断言成立：

1. $\dim_{\mathbb{Q}} \mathbb{Q}(\zeta_n) = \phi(n)$
2. 存在群同构$\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq U(\mathbb{Z}_n)$，满足$\sigma \mapsto \bar{k}$，其中$\sigma(\zeta) = \zeta^k$.

证明

例子 (特殊情况)

设p为素数。证明：$f(x)=1+x+\cdots+x^{p-1}=\frac{x^p-1}{x-1}$不可约。

考虑$g(x)=f(x+1)$，利用关于p的*Eisenstein*判别法。

例子 (一般情况)

考虑n次本原单位根w的最小多项式$f(x)$，设$p\nmid n$为素数。

断言$f(w^p)=0$。归纳，我们有$f(w^{p_1p_2\cdots p_t})=0$。

为了证断言，w^p的最小多项式为$g(x)\in\mathbb{Z}[x]$。

故，$f(x)\cdot g(x)|\Phi_n(x)$，但$f(x)|g(x^p)$。

模p方法： $\mathbb{Z}[x]\mapsto\mathbb{F}_p[x]$，但$x^n-\bar{1}\in\mathbb{F}_p[x]$无重根。

Kronecker-Weber 定理

定理 (Kronecker 1853-Weber 1886)

设$K/\mathbb{Q}$为某个多项式的分裂域且$\mathrm{Aut}(K/\mathbb{Q})$为*Abel*群。则存在$n$以及子域$L \subseteq \mathbb{Q}(\zeta_n)$使得$K \simeq L$。

注：任何有限Abel群G，存在合适的n使得$U(\mathbb{Z}_n) \twoheadrightarrow G$。