近世代数之十六

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 循环群

1. 设$X \subseteq G$。记(X)为包含X的最小子群，称为由X生成的子群。
2. 问：(X)中有哪些元素？
3. 若$(X) = G$，则称X为G的**生成元集**.

循环群

定义

群G称为**循环群**，若存在$a \in G$满足$(a) = G$。此时，称a为G的**生成元**。

例子

1. $\mathbb{Z}$, 生成元为1或者-1
2. $\mathbb{Z}_n$
3. μ_n

循环群的结构

命题

设G为循环群。则G同构于$\mathbb{Z}$ 或$\mathbb{Z}_n$。

命题

设G为循环群，生成元为g。

1. 若$|G| = \infty$。则G恰有两个生成元，且子群恰为$\{1_G\}, (g^d)$, 任何$d \geq 1$；每个子群均为循环群，均同构于$\mathbb{Z}$, 也同构于G.
2. 若$|G| = n < \infty$。则恰有$\phi(n)$个生成元$\{g^k, \gcd(k, n) = 1\}$，对于每个$d|n$，存在唯一的子群H_d，满足$|H_d| = d$。

注：$n = \sum_{d|n} \phi(d)$, 因为$\phi(d)$恰为d阶元的个数。

命题

n阶群G为循环群当且仅当存在n阶元。特别地，p阶群一定为循环群。

注：这是第一个按阶数的群分类定理！

例：群同构$\mu_3 \times \mu_2 \simeq \mu_6$.

循环群的刻画(续)

定理

设$|G| = n < \infty$。则G为循环群$\Longleftrightarrow$ 任何$d|n$，至多存在唯一的d阶子群。

hint：考虑d阶元的个数！

域单位群的子群

定理

设k为域，$G \leq k^\times$为有限子群。则G为循环群。

例子

考虑有限域$E/\mathbb{F}_p$。则$E^\times$为循环群，特别地，$E/\mathbb{F}_p$为域的单扩张！