抽象代数大作业

Author
李云艾
2023 年 5 月

Contents

1 hw1：18 阶群分类

Proposition 1.1. 18 阶群在同构意义下仅有五种.

Proof. **1.Abel 群**

$18 = 2 * 3^2 = (2 * 3) * 3$ 故 18 阶 Abel 群为 $\mathbb{Z}_{18}$ 和 $\mathbb{Z}_6 \oplus \mathbb{Z}_3$

2. 非 Abel 群

二面体群 D_9 显然为一 18 阶群

又由于 18 阶非 Abel 群 Sylow3 子群 H 指数为 2，个数为 1，为一正规子群。不妨设二阶元为 c，$H = \langle a, b\rangle$，则 ab 均为三阶元。故由正规性，可设 $cac^{-1} = a^i b^j$ $cbc^{-1} = a^s b^t$

$$a = c^2 ac^{-2} = ca^i b^j c^{-1} = \left(a^i b^j\right)^i \left(a^s b^t\right)^j = a^{i^2+sj} b^{ij+tj}$$

故

$$i^2 + sj \equiv 1, \quad j(i+t) \equiv 0 \pmod 3$$

同理

$$t^2 + sj \equiv 1, \quad s(i+t) \equiv 0 \pmod 3$$

接下来根据 i，s，t，j 的值进行讨论。易得根据 a,b 地位的等价性，s=0 可转换为 j=0 的情况，故仅分以下三类进行讨论：

1）当 j=s=0，此时有 $i^2 \equiv 1 \equiv t^2 (\mathrm{mod} 3)$，(i, t)=(2,1) 或（1，2）此时有（a，b 了可对换，不影响结果）$cac^{-1} = a, \quad cbc^{-1} = b^2$

(i, t)=(2,2)，则得到 $cac^{-1} = a^2, \quad cbc^{-1} = b^2$

2) 当 $s \neq 0, j = 0$ 时，$i + t \equiv 0, i^2 \equiv 1 \equiv t^2 (\mathrm{mod} 3)$. 于是

(i, t)=(1,2), 或 (2,1).

设 (i, t)=(1,2)，则有 $cab^s c^{-1} = a\left(a^s b^2\right)^s = a^{s^2+1} b^{2s} = a^2 b^{2s} = (ab^s)^2$

将 ab^s 记成 b．则与 1）中第一种群同构. 类似的 (i, t)=(2,1) 时有相同结果

3）设 $s \neq 0,\ j \neq 0$．若 j=1，则 $i + t \equiv 0,\ i^2 + s \equiv 1 \equiv t^2 + s (\mathrm{mod} 3)$．若 $(i, t) \neq (0, 0)$，则 (i, t)=(1,2) 或 (2,1)．于是 $i^2 \equiv 1 \equiv t^2$, 从而 s=0，矛盾! 因此 i=t=0．此时 s=1，即 $cac^{-1} = b, \quad cbc^{-1} = a$，此时与 1) 中第一种情况相同.j=2 时，i=t=0, 经验证也相同。

因此，非 Abel 非二面体群的十八阶群仅有两种结构, 并且他们确实是群，可以分别写成：

$T = \mathbb{Z}_3 \times D_3$ **以及** $S_3 \times S_3$ **中由 a=((123), 1), b=(1,(123)), c=((12),(12)) 生成的子群.**

综上，十八阶群可能有以下五种结构：

$\mathbb{Z}_{18}, \quad \mathbb{Z}_6 \oplus \mathbb{Z}_3$,

$D_9 = \langle a, b \mid a^9 = 1 = b^2, ba = a^8 b\rangle$,

$\mathbb{Z}_3 \times D_3 = \langle a, b, c \mid a^3 = b^3 = c^2 = 1, ba = ab, ca = ac, cb = b^2 c\rangle$,

$S = \langle a, b, c \mid a^3 = b^3 = c^2 = 1, ba = ab, ca = a^2 c, cb = b^2 c\rangle$.

□

2 hw2：Wedderburn 定理证明

Theorem 2.1. 有限除环是域. 即不存在有限的非交换除环

Proof. 先证：对于任何除环 D，其中乘法群的中心 C(D) 构成 D 的子环：

中心是乘法群的子群，故我们仅需作如下验证：

对于任何 x,y, 属于 C(D), 与 D 中任意 z

$$(x-y)z = xz - yz = zx - zy = z(x-y)$$

故 C(D) 是一交换子环，故为域

令 $q := |C(D)|$, 易得 q 大于等于 2，因为任意子环必含零元和幺元

又由于 $C(D) = \bigcap_{x\in D} C_D(x)$, 故 D，$C_D(x)$ 均可看作 C(D) 上的有限维线性空间，故 $|C_D(x)| = q^{n_x}$,$|D| = q^n$, 即欲证 D 是交换的仅需证 n=1

令 $D^* := D - \{0\}$, 考虑其中共轭类，则有

$$|D^*| = |Z(D^*)| + \sum_x [D^* : C_{D^*}(x)]$$

故

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{n_x} - 1}$$

接下来的证明需要用到以下定理：

[Zsigmondy] 对于互素的 a，b，且 a>b, 则对任意 n（除去 n 等于 1，2，6 时的某些特殊情况），存在素数 p，p 整除 $a^n - b^n$, 但对任意 0<k<n,p 不整除 $a^k - b^k$

则除去上述定理中的特殊情况，存在 p 整除 $q^n - 1$ 和 $\frac{q^n-1}{q^{n_x}-1}$，对于 k<n, 不整除 $q^k - 1$, 而上述关于共轭类等式成立需 p 整除 q-1，故此时 n 只能等于 1.

现讨论 Zsigmondy 定理不成立的特殊情况：

1.n=2，此时 D 在 C(D) 上的向量空间是二维的，但易得此时的任意元素可写成 a+bk，a，b 均属于中心，则此时 D 是交换的，D=C(D), 与 n=2 矛盾

2.n=6，q=2，代入原等式易得无整数解，故不成立。

综上，n=1，D 是域。

□

以下补充对 Zsigmondy 定理的简要证明。关于此定理，Zsigmondy (1892), Birkhoff and Vandiver (1904), Dickson (1905), Artin (1955), Hering (1974) 和 Lüneburg (1981) 等均给出过他们的证明, 他们的证明中均涉及到了分圆多项式 $a^n - b^n = \prod_{d\,n} \Phi_d a, b$。(章老师上传的资料中在讲本原根的时候有对此做过介绍，故此处略去相关介绍,)

Theorem 2.2. 对于互素的 a，b，且 a>b, 则对任意 n（除去 n 等于 1，2，6 时的某些特殊情况），存在素数 p，p 整除 $a^n - b^n$, 但对任意 0<k<n,p 不整除 $a^k - b^k$

证明用到以下引理：

(1) $\exists x \in Z$ 满足 $(\Phi_a(x), \Phi_b(x)) > 1$, 则 $\frac{a}{b}$ 是一个素数的幂.

(2) 整数 a, n>1, $\Phi_n(a)$ 的全体素因子都是 n 的因子, 则 $\Phi_n(a)$ 是素数或 n=2 .

(3) 整数 a, n>1, p 是 n 的素因子, $n = p^k r$,$(p, r) = 1$, $b = a^{p^{k-1}}$, 则 $\Phi_n(a) > (b^{p-2}(b-1))^{\varphi(r)}$(证明略)

Proof. 主定理（Zsigmondy）的证明：

n=2 时, $(2^s-1)^2 = 2^{s+1}\left(2^{s-1}-1\right)$,$(2^s-1) = 2\left(s^{s-1}-1\right)$, n>2 时, 若 a^n-1 的每个素因子 p , 都存在 0<j<n s.t. $p \mid a^j-1$, 则对于 $\Phi_n(a)$ 的每个素因子 p, $\exists 0 < j < n$s.t. $p \mid \Phi_j(a)$, 由 (1) 知 $p \mid n$, 故由推论 4, $\Phi_n(a) = p$, 故 p>2 . 令 $n = p^k r$,(p, r)=1 , , 由推论 5 得 $p = \Phi_n(a) > (b^{p-2}(n-1))^{\varphi(n)}$, 故 $p > b^{p-2} > 2^{p-2}$, 显然只能有 p=3 . 故 $a^{3^{k-1}} = b = 2$, 故 a=2, k=1, r=1,2 故 n=3,6 , 又 n=3 时, $2^n-1 = 7$ 不是 $2^j = 1$,0<j<3 的因子, 故只能有 n=6, $2^6-1 = 3^2 \times 7$, $3\,|2^2-1, 7|\,2^3-1$

综上所述, 只有 n=2, $a = 2^s-1$, s>1 和 n=6, a=2 不满足.

$\square$