抽象代数

Contents

Part I

笔记

Chapter 0

预备知识

Chapter	Summary
0.1	数论基础

0.1 数论基础

定理 0.1.1 (CRT 中国剩余定理). 对两两互质的 $m_1, m_2, \cdots, m_n$ ，下述同余方程组有解，且在模 $M = m_1 m_2 \cdots m_n$ 的意义下解唯一.

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv a_n (\mathrm{mod}\, m_n) \end{cases}$$

证明 设 $M_i = \dfrac{M}{m_i}, 1 \leq i \leq n$ ，于是 $(m_i, M_i) = 1$ ，则存在 t_i 使得

$$t_i M_i \equiv 1 (\mathrm{mod}\, m_i)$$

令

$$x = \sum_{t=1}^{n} a_i t_i M_i$$

则方程组的解为 $\bar{x}$ （在模 M 下）.

定理 0.1.2 (Euler 定理). 若 $(a, m) = 1$ ，则 $a^{\varphi(m)} = 1 (\mathrm{mod}\, m)$.

证明 因为 $U(m)$ 是有限交换群，且 $a \in U(m)$ ，设

$$U(m) = \{e, a, a_1, a_2, \cdots a_n\}$$

定义

$$G = \{ae, a^2, aa_1, aa_2, \cdots, aa_n\}$$

则对任意 $aa_i, aa_j \in G$ ，若 $a_i \neq a_j$ ，则 $aa_i \neq aa_j$ ，因此 $|G| \geq |U(m)|$ ，又因为 $G \subset U(m)$ ，因此 $G = U(m)$ ，于是两个集合全部元素乘积相等，就得到

$$a^{|U(m)|} = 1(\mathrm{mod}\, m)$$

因为 $|U(m)| = \varphi(m)$ ，证毕.

命题 0.1.1. 质因数分解 $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ ，则

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Chapter 1

群环域

Chapter	Summary
1.1	运算法则：运算的定义、单位元和逆元、负元等定义，以及等价关系和商集的定义.
1.2	群环域定义：给出了群环域的定义，以及全变换群、对称群等特殊且常见的群.
1.3	整数模 n 的剩余类环：定义剩余类环，以及其单位群（乘法群）.

1.1 运算法则

Section	Summary
1.1.1	运算
1.1.2	元
1.1.3	商集

1.1.1 运算

定义 1.1.1 (二元运算)**. 代数运算**是一个 $A \times B \to C$ 的映射，若 $A = B = C$ ，也称为 A 上的代数运算.

命题 1.1.1 (广义结合律)**.** 若 A 上的运算有结合律，则有广义结合律.

证明过程应当不是重点，具体见课本 p4-5

1.1.2 元

定义 1.1.2 (单位元，逆元，零元，负元). $e \in A$ 称为**单位元**，若 $ae = ea = a, \forall a \in A$.

A 有单位元 e ，对 $a \in A$ ，若存在 $b \in A$ 使得 $ab = ba = e$ ，称 b 为 a 的**逆元**.

设 A 上的运算记为加法 $+$ ，若 A 有单位元，则记为 0 并称为**零元**. 若 $a \in A$ 可逆，则 a 的唯一逆元记为 $-a$ ，称为 a 的**负元**.

命题 1.1.2 (元的性质). 若 A 有单位元，则单位元唯一.

若 A 运算**有结合律**，则可逆元素的逆元唯一.

1.1.3 商集

定义 1.1.3 (商集). A 在等价关系 R 下的所有等价类构成的集合称为 A 关于 R 的**商集**，记为 $A\backslash R$.

若 A 上有运算 $\cdot$ ，在商集 $A\backslash R$ 上定义运算 $\circ$

$$\overline{a} \circ \overline{b} = \overline{a \cdot b}$$

则 $\circ$ **是否是** $A\backslash R$ **上的运算**？据此我们提出相容的概念：

定义 1.1.4 (相容). 假设 $\circ$ 是 $A\backslash R$ 上的运算，则运算结果唯一，也就是等价类的代表的选取不影响运算结果，即

$$\overline{a_1} = \overline{a_2} \ \ \overline{b_1} = \overline{b_2}, \qquad \overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}$$

容易验证这个必要条件也是充分的，即满足上述条件的 $\circ$ 是 $A\backslash R$ 上的运算.

上述条件称为 $\circ$ 和等价关系 R **相容**. 也称 $\circ$ 是 A **上的运算** $\cdot$ **诱导出的商集** $A\backslash R$ **上的运算**.

1.2 群环域定义

Section	Summary
1.2.1	群的定义
1.2.2	环、域的定义

1.2.1 群的定义

定义 1.2.1 (幺半群和群). **半群**是一个有满足结合律的运算的非空集合；进一步，若半群有单位元，称为**幺半群**.

每个元素都有逆元的幺半群称为**群**.

例 1.2.1. $\mathrm{GL}_n(F)$ 为域 F 上所有 n 阶可逆矩阵构成的集合，运算为矩阵乘法，称为 F 上的 n 级**一般线性群**.

$\mathrm{SL}_n(F)$ 为数域 F 上所有行列式为 1 的 n 阶矩阵构成的集合，运算为矩阵乘法，称为 F 上的 n 级**特殊线性群**.

定义 1.2.2 (单位群). S 为幺半群，$U(S)$ 表示 S 中所有可逆元构成的集合，容易验证 $U(S)$ **在** S **的运算下构成群**.

半群 S 中的可逆元也称为 S 的**单位**，故称 $U(S)$ 为**幺半群** S 的**单位群**.

定义 1.2.3 (全变换群). T_M 表示集合 M 上的全体变换构成的集合，运算为映射乘法，则 T_M 为一个幺半群，单位元为 id_M .

该幺半群上的单位群记为 S_M ，称为 M 的**全变换群**，即全体可逆变换（双射）构成的集合.

特别地，若 M 有限，不妨设 $M = \{1, 2, \cdots, n\} := [n]$ ，将 $[n] \to [n]$ 的双射称为**置换**，所有 n 元置换在置换乘法下构成的群 $S_{[n]}$ 称为 n **元对称群**，简记为 S_n .

1.2.2 环、域的定义

定义 1.2.4 (环). 对加法做成交换群，对乘法做成幺半群，且乘法对加法左右分配的 R 称为**环**.

环的乘法单位元称为**环的单位元**，记为 1 ，加法的零元称为**环的零元**，记为 0 .

对乘法，R 的可逆元也称为 R 的**单位**. 幺半群 $(R, \cdot)$ 的单位群称为**环** R **的单位群**，记为 $U(R)$.

定义 1.2.5 (除环和域). **除环**（或**体**）是含有至少 2 个元素且每个非零元都可逆的环.

R 为环，$a \neq 0$ ，若存在 $b \neq 0$ 使得 $ab = 0$ ，称 a 是 R 的一个**左零因子**，同理有**右零因子**. 二者统称为 R 的**零因子**.

零因子一定不可逆，因此除环没有零因子.

交换的除环称为**域**

定义 1.2.6 (整环). **整环**是至少含有 2 个元素且没有零因子的交换环.

1.3 整数模 n 的剩余类环

定义 1.3.1. 在 $\mathbb{Z}$ 定义等价关系 $\sim$

$$a \sim b \iff n \mid a-b$$

该等价关系的商集

$$\mathbb{Z}_n := \mathbb{Z}/\sim = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

且对 $\overline{a_1} = \overline{a_2}, \overline{b_1} = \overline{b_2}$ ，有

$$\overline{a_1 + b_1} = \overline{a_2 + b_2} \quad \overline{a_1 b_1} = \overline{a_2 b_2}$$

因此 $\mathbb{Z}$ 上的加法和乘法诱导了商集 $\mathbb{Z}_n$ 上的运算，且是相容的，即

$$\overline{a} + \overline{b} = \overline{a+b} \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

容易验证 $\mathbb{Z}_n$ 在这样的加法和乘法下构成交换环，称为**整数模 n 的剩余类环**，其单位群也称为**整数模 n 的乘法群**，记为 $U(n)$.

上述环和群都是交换的.

命题 1.3.1. 环 $\mathbb{Z}_n$ 为域当且仅当 n 为素数.

Chapter 2

群的基本性质和作用

Chapter	Summary
2.1	对称群和交错群：讨论多元对称群和图形的对称群.
2.2	子群和同态：给出子群的定义和充要条件. 定义同态.
2.3	循环群：循环群的定义和性质.
2.4	群在集合上的作用
2.5	陪集、指数、Lagrange 定理
2.6	轨道长度和类方程
2.7	正规子群与商群
2.8	同态基本定理

2.1 对称群和交错群

Section	Summary
2.1.1	置换的分解与型、共轭：置换可以分解为对换和不相交轮换乘积，并提出型的概念，以及两个置换型相同当且仅当共轭.
2.1 2	图形的对称群：给出图形对称群的结构.

2.1.1 置换的分解与型

定理 2.1.1 (对换分解). 任意置换可以写成对换的乘积. 置换写成对换的方式不唯一，但是对换的个数的奇偶性固定，和置换的奇偶性相同.

定义 2.1.1 (交错群). 所有 n 元偶置换组成的集合 A_n 对置换乘法构成群. 称为 n 元**交错群**.

命题 2.1.1. 不相交的轮换可以交换.

定理 2.1.2 (置换的分解). 任意置换可以分解成不相交的轮换乘积，若不计轮换因子的顺序，则分解式唯一.

定义 2.1.2 (共轭变换). G 是群，则 $a, b \in G$ 称为**共轭**的，若存在 $c \in G$ 使得

$$b = cac^{-1}$$

也称 cac^{-1} 为用 c 对 a 做共轭变换.

定义 2.1.3 (置换的型). 把置换写成不相交轮换的乘积，其中长度为 i 的轮换出现 λ_i 次，则记**置换的型**为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$.

对 S_n 中的置换，显然

$$\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n$$

把正整数 n 写成递降正整数和的表示

$$n = r_1 + r_2 + \cdots + r_k \quad r_1 \geq r_2 \geq \cdots \geq r_k \geq 1$$

称为 n 的一个分拆，n 的所有分拆的个数称为 n 的分拆数，记为 $p(n)$.

显然 n 元置换的型和 n 的分拆一一对应，因此 S_n 中置换的型的个数为 $p(n)$.

下面考虑两个共轭的置换的型的关系.

定理 2.1.3 (共轭置换相同型). 两个置换共轭当且仅当它们的型相同.

证明 对 $\rho, \sigma \in S_n$ ，有

$$\rho\sigma\rho^{-1} = \begin{pmatrix} \rho(1) & \rho(2) & \cdots & \rho(n) \\ \rho(\sigma(1)) & \rho(\sigma(2)) & \cdots & \rho(\sigma(n)) \end{pmatrix}$$

特别地，有

$$\rho(a_1a_2\cdots a_k)\rho^{-1} = (\rho(a_1)\rho(a_2)\cdots\rho(a_k))$$

即 $k-$ 轮换的共轭还是 $k-$ 轮换.

设 $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ ，其中 σ_i 是互不相交的轮换，则

$$\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1})\cdots(\rho\sigma_k\rho^{-1})$$

仍是不相交的轮换的乘积. 因此共轭置换同型.

反之，若 $\sigma,\tau\in S_n$ 的型相同，记轮换分解式为

$$\sigma=(a_1\cdots a_{k_1})(a_{k_1+1}\cdots a_{k_1+k_2})\cdots(a_{k_1+\cdots+k_{s-1}+1}\cdots a_{k_1+\cdots+k_{s-1}+k_s})$$
$$\tau=(b_1\cdots b_{k_1})(b_{k_1+1}\cdots b_{k_1+k_2})\cdots(b_{k_1+\cdots+k_{s-1}+1}\cdots b_{k_1+\cdots+k_{s-1}+k_s})$$

其中 $n=k_1+k_2+\cdots+k_s$ ，令 $\rho(a_i)=b_i$ ，则 $\rho\sigma\rho^{-1}=\tau$ ，因此同型置换共轭.

命题 2.1.2 (同型置换个数)**.** 在 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换个数为

$$\frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_n!1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}}$$

证明 考虑 $\lambda_1+\lambda_2+\cdots+\lambda_n$ 个小括号，使得其中 λ_i 个小括号放入 i 个元素，此时每个放置对应一个型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换.

而不相交轮换的乘积可交换，因此有 $\lambda_i!$ 种不同放置方式得到相同的置换.

最后，每个 $i-$ 轮换的第一个元素不固定，但前后次序固定，因此每个 $i-$ 轮换有 i 中不同放置方法得到相同的轮换，有 λ_i 个这样的轮换.

2.1.2 图形的对称群

在 $\mathbb{R}^3$ 内保持图形 S 不变的空间运动，即 $\mathbb{R}^3$ 上的旋转变换，在映射乘法下构成一个群，称为**图形 S 的对称群**.

这里讨论平面上正多边形的对称群.

定义 2.1.4. P 是正 n 边形，记 P 的对称群为 D_n .

用 $[n]$ 表示 P 的顶点，则考虑置换

$$\sigma_i(a)=a+i(\mathrm{mod}\,n)\quad \tau_i=-a+i(\mathrm{mod}\,n)\quad \sigma_i,\tau_i\in D_n$$

几何意义上，σ_i 相当于 P **绕中心沿逆时针方向旋转** $\dfrac{2i\pi}{n}$ ，而 τ_i 相当于 P **以直线 L_i 为轴作反射**，其中当 $i=2t+1$ 时，L_i 是 O 和边 $\{t,t+1\}$ 中点的连线；当 $i=2t$ 时，L_i 是 O 和顶点 t 的连线.

下面考虑任意 $\pi\in D_n$ ，定义 P 上的等价关系：$a\sim b\iff\{a,b\}$ 是 P 的一条边，因为 D_n 的置换保持边不变，因此 $1\sim 2\implies\pi(1)\sim\pi(2)$ ，于是

$$\pi(1)=i,\pi(2)=i+1(\mathrm{mod}\,n)\ \pi(2)=i-1(\mathrm{mod}\,n)$$

若 $\pi(2)=i+1$，则由 $2\sim 3$ 继续归纳得到 $\pi(a)=a+i-1(\mathrm{mod}\, n)$，即 $\pi=\sigma_{i-1}$. 同理，若 $\pi(2)=i-1$，可以得到 $\pi=\tau_{i+1}$，于是

$$D_n=\{\sigma_i,\tau_i : i=1,2,\cdots,n\}$$

显然 σ_i,τ_i 都两两不同，因此 D_n 是一个 $2n$ 阶群，包含 n 个旋转和 n 个反射. 此群称为**二面体群**.

注意这里 τ_i 的反射轴按照最开始没有经过任何变换的图形来定义，也就是反射轴不随着图形移动. 同理，σ_i 的旋转也是不根据反射改变方向，即在纸面上画图的时候总是逆时针旋转.

容易验证 $\tau_i^2=e$，且

$$\sigma_i=\sigma_1^i,\quad \sigma_i^{-1}=\sigma_{n-i},\quad \sigma_i\tau_j=\tau_{i+j}$$

记 $r=\sigma_1, s=\tau_1$，则

$$r^n=e,\quad s^2=e,\quad rs=sr^{-1}$$

于是

$$D_n=\{r^is^j : i=1,2,\cdots,n; j=0,1\}$$

即在 D_n 有

$$r^ks=sr^{-k}$$

2.2 子群与同态

Section	Summary
2.2.1	子群性质和陈述：子群的定义和判断子群的充要条件.
2.2.2	同态：同态和同构的定义. 同台的性质以及自同态环、自同构群和二者之间的关系.

2.2.1 子群性质和陈述

定理 2.2.1 (子群充要条件). G 是群，$\emptyset\neq H\subset G$，则下列陈述等价

1. $H\leq G$
2. $ab\in H,\forall a,b\in H$ 且 $h^{-1}\in H,\forall h\in H$

3. $ab^{-1} \in H, \forall a, b \in H$

子群的交依然是子群.

定义 2.2.1 (生成子群和循环群). $S \subset G$ ，则 G 存在包含 S 的子群，如 G 本身，则 G 所有包含 S 的子群的交依然是包含 S 的子群，且是其中最小的一个，称为 G 的**由 S 生成的子群**，记为 $\langle S \rangle$ ，也称 S 是群 G 的一个**生成集**.

设 S 是 G 的一个非空**子集**，则 G 的包含 S 的子群是存在的，例如 G 本身. 此时 G 的所有包含 S 的子群的交仍然是包含 S 的子群，且是其中最小的一个. 称这个子群为 G 的**由 S 生成的子群**，并记为 $\langle S \rangle$.

特别地，若 S 是有限集，则称 $\langle S \rangle$ 为 G 的**有限生成子群**.

进一步，若 $G = \langle S \rangle$ ，则称群 G 由子集 S **生成**，也称 S 是群 G 的一个生成集. [1]

G 为群，若存在 $a \in G$ 使得 $G = \langle a \rangle$ ，称 G 为**循环群**，a 为循环群的一个**生成元**.

定义 2.2.2 (集合乘积和逆). G 是一个群，K, L 为 G 非空子集，定义

$$KL = \{ab : a \in K, b \in L\} \quad K^{-1} = \{a^{-1} : a \in K\}$$

分别称为 K 和 L 的**集合乘积**，K 的**逆**.

命题 2.2.1 (子集充要条件). G 为群，$H \subset G$ 且非空，则 $H \leq G$ 当且仅当 $H^2 = H, H^{-1} = H$.（这里的 H^2 应该是两个不同元素相乘，而不是相同元素的平方）.

2.2.2 同态

定义 2.2.3 (群同态). G_1, G_2 为群，若映射 $\sigma : G_1 \to G_2$ 保持运算，称为 $G_1 \to G_2$ 的**同态映射**，简称**同态**.

双射同态称为**同构映射**，简称**同构**.

若 G_1, G_2 之间存在同构映射，称二者同构，记为 $G_1 \cong G_2$.

定义 2.2.4 (自同构群). G 为群，$\mathrm{Aut}(G)$ 表示 G 的所有自同构构成的集合，是 G 上全变换群 S_G 的一个非空子集，容易证明 $\mathrm{Aut}(G) \leq S_G$ ，称为 G 的**自同构群**.

定义 2.2.5 (自同态环). G 为交换群，运算记为 $+$ ，$\mathrm{End}(G)$ 表示 G 的全体自同态构成的集合，对 $\varphi, \psi \in \mathrm{End}(G)$ ，定义

$$(\varphi + \psi)(g) = \varphi(g) + \psi(g) \quad (\varphi\psi)(g) = \varphi(\psi(g)) \quad \forall g \in G$$

[1] 注意这里 S 是一个子集，而不要求是子群.

容易验证 End(G) 对上面的运算构成环，称为**交换群 G 的自同态环**.

环 End(G) 的单位群就是交换群 G 的自同构群 Aut(G) .

定理 2.2.2 (同态性质)**.** $\sigma : G \to G'$ 为同态，则

1. $\sigma(g^{-1}) = \sigma(g)^{-1}, \sigma(e) = e'$ ，其中 e, e' 为 G, G' 的单位元
2. 若 $H \leq G$ ，则 $\sigma(H) \leq G'$
3. 若 $H' \leq \sigma(G)$ ，则 $\sigma^{-1}(H) \leq G$

$\sigma^{-1}(e')$ 称为**同态 σ 的核**，记为 $\operatorname{Ker}\sigma$.

命题 2.2.2. $\sigma : G \to G'$ 为同态，则 σ 为单射当且仅当 $\operatorname{Ker}\sigma = \{e\}$.

定理 2.2.3 (挖补定理)**.** 群 $G \cap H' = \emptyset, H \leq G, H \cong H'$ ，则存在 G' 使得 $H' \leq G', G \cong G'$.

证明 $\eta : H \to H'$ 为同构，令 $G' = (G \backslash H) \cup H'$ ，定义

$$\varphi : G \to G' \quad \varphi(a) = \begin{cases} a & a \in G \backslash H \\ \eta(a) & a \in H \end{cases}$$

因为 $G \cap H' = \emptyset$ ，则 φ 是双射.

对 $\forall a', b' \in G'$ ，存在唯一的 $a, b \in G$ 使得 $\varphi(a) = a', \varphi(b) = b'$ ，定义

$$a' \odot b' = \varphi(ab)$$

则 $\odot$ 是 G' 上运算，且 G' 在该运算下构成群，于是

$$\varphi(ab) = \varphi(a) \odot \varphi(b)$$

即 φ 是同态，于是 $G \cong G'$.

设 H' 的运算为 $\circ$ ，对 $\forall g', h' \in H'$ ，存在唯一的 g, h 使得 $\eta(g) = g', \eta(h) = h'$ ，于是

$$g' \circ h' = \eta(gh) = \varphi(gh) = \varphi(g) \odot \varphi(h) = \eta(g) \odot \eta(h) = g' \odot h'$$

即 H' 运算和限制在 H' 上的 G' 的运算是一样的，因此 $H' \leq G'$.

形象上看，上述定理就是把 G 的子群 H 挖出来，再把与 H 同构的群 H' 补进去，这样可把 H' 看成是 G 的子群.

实际上这种看法也是很自然的，如同我们习惯上把整数看成是分母为 1 的有理数，把实数看成是虚部为 0 的复数一样.

2.3 循环群

Section	Summary
2.3.1	元素的阶：定义元素的阶，以及元素阶和群的阶的因数关系. 计算元素的幂的阶. 讨论循环群的元素的阶及其个数.
2.3.2	循环群的子群：以循环群阶任意因子为阶的子群存在且唯一
2.3.3	有限循环和交换：对有限交换群，方次数等于阶当且仅当群是循环群.
2.3 4	有限循环的自同构：有限循环群的自同构群和剩余类环的单位群同构.

2.3.1 元素的阶

定理 2.3.1 (判断循环群有限与否). $G=\langle a\rangle$ 为循环群，若 a 任意不同幂不相等，则 G 无限；否则，存在 a 的正整数次幂为单位元，且 G 为有限群，进一步，设 n 为满足 $a^n=e$ 的最小正整数，则 $a^n=e$.

定义 2.3.1 (生成元的阶). G 为一个群，$a\in G$ ，称 a 生成的循环子群 $\langle a\rangle$ 的阶为 a 的阶，记为 $o(a)$.

当不存在 n 使得 $a^n=e$ 时，称 a 为**无限阶元素**，记 $o(a)=\infty$.

若 $\sigma:G_1\to G_2$ 为同构，则 $a^n=e\iff\sigma(a)^n=e$ ，记 $o(a)=o(\sigma(a))$.

命题 2.3.1 (阶的因子性). $a\in G$ ，则 $a^k=e\iff o(a)\mid k$.

推论 2.3.1. G 是 n 阶交换群，则 $o(a)\mid n$.

证明 设 $G=\{a_1,a_2,\cdots,a_n\}$ ，则

$$aG=\{aa_1,aa_2,\cdots,aa_n\}\subset G$$

且 $aa_i\neq aa_j\iff a_i\neq a_j$ ，因此 $aG=G$ ，于是

$$a^na_1a_2\cdots a_n=a_1a_2\cdots a_n\implies a^n=e$$

该推论的结论对非交换群成立，但是证明过程对非交换群不成立. 对非交换群的情况，可以如下证明：

定理 2.3.2 (Lagrange 定理). G 是群，则 $|H|\mid|G|,\forall H\leq G$.

证明 定义

$$gH = \{gh : h \in H\} \quad g \in G$$

显然 $gh_1 \neq gh_2 \iff h_1 \neq h_2$，因此 $|gH| = |H|$.

对 $g_1 \neq g_2$，假设存在 $h \in H$ 使得 $g_1 h = g_2 h$，则消去 h 得到 $g_1 = g_2$，矛盾，因此

$$g_1 H \cap g_2 H = \emptyset \quad \forall g_1, g_2 \in G, g_1 \neq g_2$$

因此 G 被每一个 $g \in G$ 划分为不相交的左陪集，每个左陪集的阶都是 $|gH| = |H|$，记 G 关于 H 的左陪集个数为 $[G : H]$，得到

$$|G| = [G : H] \cdot |H|$$

证毕.

则 $o(a) = |\langle a \rangle|$，其中 $\langle a \rangle$ 是 G 的子群，因此 $o(a) \mid |G| = n$，证毕.

命题 2.3.2. G 为有限交换群，则

$$\prod_{g \in G} g = \prod_{a \in G, o(a)=2} a$$

证明 若 $o(a) \geq 3$，则 $a \neq a^{-1}$，于是所有 $o(a) \geq 3$ 在元素在 $\prod_{g \in G} g$ 中和自身的逆抵消.

定理 2.3.3 (幂的阶). G 为群，$a \in G, k \in \mathbb{N}_+$，则

$$o(a^k) = \frac{o(a)}{\gcd(o(a), k)}$$

证明 记 $d = \gcd(o(a), k)$，且 $o(a) = n_1 d, k = k_1 d$，则 $\gcd(n_1, k_1) = 1$，因为

$$(a^k)^{n_1} = (a^{k_1 d})^{n_1} = (a^n)^{k_1} = e$$

于是 $o(a^k) \mid n_1$，又因为

$$a^{k o(a^k)} = (a^k)^{o(a^k)} = e$$

因此 $o(a) \mid k o(a^k)$，即 $n_1 \mid k_1 o(a^k)$，又因为 $\gcd(n_1, k_1) = 1$，于是 $n_1 \mid o(a^k)$，因此 $o(a^k) = n_1$，证毕.

命题 2.3.3 (循环群元素的阶). G 为 n 阶循环群，则 G 中元素的阶为 n 的因子，进一步，对 n 的任意正因子 d，G 中阶为 d 的元素有 $\varphi(d)$ 个.

证明 $G=\langle g\rangle$，对任意 $a\in G$，则 $a=g^k$，于是 $a^n=g^{kn}=(g^n)^k=e$，因此 $o(a)\mid n$.

若 $o(a)=d$，其中 $a=g^k, 0\leq k\leq n-1$，则

$$o(a)=o(g^k)=\frac{o(g)}{\gcd(o(g),k)}=\frac{n}{\gcd(n,k)}=d$$

则 $\gcd(n,k)=\dfrac{n}{d}\implies \gcd\left(d,\dfrac{kd}{n}\right)=1$，现在考虑这样的 k 有多少个.

设 $n=md$，则 $\gcd\left(d,\dfrac{k}{m}\right)=1$，对任意 t 满足 $0<t<d,(t,d)=1$，令 $k=tm$，有

$$k\leq (d-1)m<n,\quad \left(d,\frac{k}{m}\right)=(d,t)=1$$

因此每个 t 对应一个 k，于是 k 的个数有 $\varphi(d)$ 个，证毕.

把循环群 G 的元素按照阶来划分，就得到

$$\sum_{d|n}\varphi(d)=n$$

定理 2.3.4 (阶互素交换元素积的阶). G 是群，$a,b\in G, ab=ba, (o(a),o(b))=1$，则 $o(ab)=o(a)o(b)$.

证明 不妨设 $o(a)=m,o(b)=n,o(ab)=s$，因为 $(ab)^{mn}=e$，于是 $s\mid mn$，又因为

$$a^{sn}=a^{sn}b^{sn}=(ab)^{sn}=e$$

于是 $m\mid sn$，又因为 $(m,n)=1$，得到 $m\mid s$，类似地有 $n\mid s$，于是 $mn\mid s$，即 $s=mn$.

命题 2.3.4 (无限循环群同构整数加法群). 任意无限循环群 G 和整数加法群 $\mathbb{Z}$ 同构.

证明 容易验证 $\sigma:\mathbb{Z}\to G, k\mapsto a^k$ 是一个同构，这里 $G=\langle a\rangle$.

命题 2.3.5 (有限循环群同构). 两个有限阶循环群同构当且仅当它们阶相等.

2.3.2 循环群的子群

定理 2.3.5 (循环群子群). 循环群的子群依然是循环群.

定理 2.3.6. $G=\langle a\rangle$ 为 n 阶循环群，则 G 的子群的阶都是 n 的因子，进一步，对 n 的任意正因子 d，阶为 d 的子群存在且唯一.

证明 设 $H \leq G$，则存在 $0 \leq s \leq n-1$ 使得 $H = \langle a^s \rangle$，因此

$$|H| = o(a^s) = \frac{n}{\gcd(n,s)}$$

为 n 的因子.

对 n 的正因子 d，有 G 的 d 阶子群 $\langle a^{n/d} \rangle$. 设 $H = \langle a^s \rangle$ 为 G 的 d 阶子群，则 $o(a^s) = d$，即

$$a^{sd} = (a^s)^d = e \implies n \mid sd \implies s = \frac{n}{d}t, t \in \mathbb{Z}$$

于是

$$a^s = (a^{n/d})^t \implies a^s \in \langle a^{n/d} \rangle \implies H \subset \langle a^{n/d} \rangle$$

又 $|H| = |\langle a^{n/d} \rangle| = d \implies H = \langle a^{n/d} \rangle$，因此唯一.

于是对 $G = \langle a \rangle, |G| = n$，其所有子群构成的集合为

$$\mathscr{G} = \{\langle a^d \rangle : d \mid n, d > 0\}$$

2.3.3 循环和交换

已知循环群是交换群，那么何时交换群为循环群？这里我们讨论有限循环群的情况.

定义 2.3.2 (方次数). G 为群，对 $\forall a \in G$ 都有 $a^t = e$ 的最小正整数 t 称为 G 的**方次数**，记为 $\exp(G)$.

如果 G 是有限交换群，由 2.3.1 得到 $a^{|G|} = e, \forall a \in G$，于是对有限交换群，有

$$\exp(G) \leq |G|$$

引理 2.3.1. G 为有限交换群，g 为最大阶元素，则 $\exp(G) = o(g)$.

证明 设

$$o(g) = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, o(h) = p_1^{f_1} p_2^{f_2} \cdots p_s^{f_s}$$

其中 p_i 是互不相等的素数，$e_i \geq 0, f_i \geq 0$，则只需证 $f_i \leq e_i, 1 \leq i \leq s$.

假设存在 $f_i > e_i$，不妨设 $i = 1$，令

$$g_1 = g^{p_1^{e_1}} \quad h_1 = h^{p_2^{f_2} \cdots p_s^{f_s}}$$

则

$$o(g_1) = \frac{o(g)}{p_1^{e_1}} = p_2^{e_2} \cdots p_s^{e_s}$$

类似地 $o(h_1)=p_1^{f_1}$ ，因为 g_1,h_1 可交换，且 $(o(g_1),o(h_1))=1$ ，于是

$$o(g_1h_1)=p_1^{f_1}p_2^{e_2}\cdots p_s^{e_s}>o(g)$$

矛盾.

下面给出有限交换群循环的充要条件

定理 2.3.7. G 有限交换，则 G 循环 $\iff \exp(G)=|G|$.

证明 循环群生成元的阶等于群的阶，必要性显然；

若 $\exp(G)=|G|$ ，由引理，此时存在 g 使得 $o(g)=\exp(G)=|G|$ ，则 $\langle g\rangle$ 是 G 的子群，且阶为 $|G|$ ，因此 $G=\langle g\rangle$.

定理 2.3.8. G 是有限交换群，则 G 是循环群 $\iff$ 对任意 $m\in\mathbb{N}_+$ ，方程 $x^m=e$ 在 G 中解个数不超过 m .

证明

1. 充分性：设 $m=\exp(G)$ ，则 G 的每个元素都是 $x^m=e$ 的解，因为 $|G|\leq m=\exp(G)$ ，又 $\exp(G)\leq|G|$ 得到 $\exp(G)=|G|$ ，因此 G 是循环群.

2. 必要性：$G=\langle g\rangle,|G|=n$ ，对任意 $m\in\mathbb{N}_+$

   $$H=\{x\in G:x^m=e\}$$

   容易验证 $H\leq G$ ，于是 H 为循环群，不妨设 $H=\langle g^s\rangle$ ，其中 $s\mid n$ ，则

   $$|H|=o(g^s)=\frac{n}{s}$$

   由 H 的定义

   $$(g^s)^m=g^{sm}=e\implies n\mid sm\implies \frac{n}{s}\leq m$$

   因此 $x^m=e$ 在 G 中解的个数不超过 m .

推论 2.3.2. 域的乘法群的有限子群是循环群.

证明 域 F 上的 m 次多项式 x^m-1 在 F 中解的个数不超过 m ，证毕.

定义 2.3.3. 若 $U(n)$ 为循环群，称模 n 有原根，循环群 $U(n)$ 的生成元称为模 n 的**原根**.

2.3.4 有限循环的自同构

定理 2.3.9. $G=\langle a\rangle$ 为 n 阶循环群，则 $\mathrm{Aut}(G)\cong U(n)$.

证明 对 $\overline{r}\in U(n), 0\leq r\leq n-1$ ，且 $\gcd(r,n)=1$ ，定义 $\alpha_r: G\to G$

$$\alpha_r(a^k)=a^{kr}\quad 0\leq k\leq n-1$$

容易验证 $\alpha_r\in\mathrm{Aut}(G)$.

取 $\alpha\in\mathrm{Aut}(G)$ ，设 $\alpha(a)=a^r, 0\leq r\leq n-1$ ，因为 $o(a)=n$ ，也是

$$o(a^r)=o(\alpha(a))=o(a)=n$$

从而 $\gcd(r,n)=1$ ，于是 $\overline{r}\in U(n)$ ，由 α 保持运算得到对 $\forall a^k\in G$

$$\alpha(a^k)=\alpha(a)^k=a^{kr}\quad 0\leq k\leq n-1$$

于是 $\alpha=\alpha_r$ ，即

$$\mathrm{Aut}(G)=\{\alpha_r:\overline{r}\in U(n)\}$$

则 $T: U(n)\to\mathrm{Aut}(G), \overline{r}\mapsto\alpha_r$ 为同构.

2.4 群在集合上的作用

Section	Summary
2.4.1	群作用和群同态：群作用的定义，以及群作用存在的充要条件.
2.4.2	Cayley 定理：任意群和一个变换群同构.
2.4.3	群作用轨道：定义群作用的轨道，即群作用下的等价类

2.4.1 群作用和群同态

全变换群的子群都称为**变换群**.

定义 2.4.1 (群作用). G 是群，M 是非空集合，若有映射

$$\rho: G\times M\to M\quad (g,m)\mapsto\rho(g,m)=g\circ m$$

满足对 $\forall m\in M, \forall g_1,g_2\in G$

1. $e \circ m = m$ ，其中 e 是 G 单位元

2. $g_1 \circ (g_2 \circ m) = (g_1 g_2) \circ m$

则称**群 G 作用在集合 M 上**，这个映射 ρ 也称为一个**群作用**.

定理 2.4.1. 群 G 在 M 上有群作用的充要条件是 $G \to S_M$ 存在群同态.

证明

1. 必要性：设 $\rho : G \times M \to M$ 是一个群作用，对 $\forall g \in G$ 定义一个 M 上的变换

$$T(g) : M \to M \quad T(g)(m) = g \circ m \quad \forall m \in M$$

则 $(T(g)T(g^{-1}))(m) = m$ ，即 $T(g)T(g^{-1}) = \mathrm{id}_M$ ，同理 $T(g^{-1})T(g) = \mathrm{id}_M$ ，于是 $T(g)$ 为 M 上的可逆变换，即 $T(g) \in S_M$ ，定义映射 $T : G \to S_M$ 为

$$g \mapsto T(g) \quad \forall g \in G$$

则 $\forall g_1, g_2 \in G, m \in M$ 有

$$T(g_1 g_2)(m) = (T(g_1)T(g_2))(m)$$

即 $T(g_1 g_2) = T(g_1)T(g_2)$ ，因此 T 为 $G \to S_M$ 的同态.

2. 充分性：根据上面证明，若 $T : G \to S_M$ 为群同态，定义映射 $\rho : G \times M \to M$

$$\rho(g, m) = g \circ m = T(g)(m)$$

容易验证 ρ 就是群作用.

因为如上的等价性，我们称群 G 到集合 M 的全变换群 S_M 的一个群同态为一个群作用.

2.4.2 Cayley 定理

定理 2.4.2 (Cayley 定理)**.** 任意群同构一个变换群.

证明 对群 G ，考虑 G 在自身的左乘作用 $L_G : G \times G \to G$ ，其中

$$L_G(g, a) = g \circ a = ga \quad \forall g, a \in G$$

该群作用导出群同态 $T : G \to S_G$ ，其中 $T(g)(a) = ga, \forall a, g \in G$.

对任意 $g_1, g_2 \in G$ 若 $T(g_1) = T(g_2)$，则 $g_1 = g_2$，因此 T 是单同态，所以 $G \cong T(G)$，且 $T(G) \leq S_G$，因此 G 和 S_G 的一个子群同构，于是同构于一个变换群.

特别地，若 $|G| = n$，则 $S_G = S_n$，由上述定理，任意 n 阶群同构 S_n 的一个子群. 把对称群的子群称为**置换群**，因此每个有限群同构于一个置换群.

例 2.4.1 (内自同构群). G 是一个群，考虑自身上的**共轭作用** $\rho : G \times G \to G$：

$$\rho(g, a) = gag^{-1} \quad \forall a, g \in G$$

该作用对应的同态记为 $T : g \mapsto I_g$，对 $g \in G$，其中 $I_g \in S_G$ 定义为

$$I_g(a) = gag^{-1}$$

对任意 $a_1, a_2 \in G$ 有

$$I_g(a_1 a_2) = I_g(a_1) I_g(a_2)$$

因此 I_g 是 G 的一自同构，称 I_g 为 g 对应的 G 的**内自同构**，用 $\mathrm{Inn}(G)$ 表示 G 的所有内自同构做成的集合，容易验证

$$I_g I_h = I_{gh} \quad I_g^{-1} = I_{g^{-1}}$$

因此 $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$，称 $\mathrm{Inn}(G)$ 为 G 的**内自同构群**.

2.4.3 群作用轨道

定义 2.4.2 (群作用轨道). 设 G 作用在集合 M 上，定义 M 上的关系 R

$$xRy \iff \exists g \in G, y = g \circ x$$

则 R 是等价关系，在这个等价关系下，对 $x \in M$，其等价类

$$\overline{x} = \{y \in M : \exists g \in G, y = g \circ x\} = \{g \circ x : g \in G\}$$

称 $\overline{x}$ 为 x 在 G 作用下的**轨道**，简称过 x 的轨道，记为 O_x.

定理 2.4.3 (轨道的性质). G 作用在 M 上，通过等价类的性质得到：

1. $O_y = O_x \iff y \in O_x$
2. O_x, O_y 相等或不相交

3. 在每条轨道上各取一个元素组成 M 的一个子集 I，称为 M 的轨道代表元集，则

$$M = \bigcup_{x \in I} O_x$$

且其中 O_x 各不相交，即群作用的轨道集合是 M 的一个划分.

定义 2.4.3. G 作用在 M 上，若这个作用只有一个轨道，则称 G 在 M 上的作用**传递**.

2.5 陪集、指数、Lagrange 定理

Section	Summary
2.5.1	陪集：陪集定义，以及陪集本质是群作用的轨道，因此具有轨道的性质，进而得到 Lagrange 定理，并提出指数的概念，以及一些指数的计算性质.
2.5.2	商集：商集的定义，即子群的所有陪集构成的集合.

2.5.1 陪集

定义 2.5.1 (陪集). $H \leq G$，则 H 在 G 上有左乘和右乘作用，对 $x \in G$，左乘作用过 x 的轨道为

$$O_x = \{hx : h \in H\} := Hx$$

称为 H 在 G 中的一个**右陪集**，同理定义左陪集.

陪集是群作用轨道，因此有轨道的性质.

定理 2.5.1. $H \leq G$，则

1. $xH = yH \iff y \in xH \iff x^{-1}y \in H \vee y^{-1}x \in H$
2. xH, yH 相等或不相交
3. 在 G 的每个左陪集中任取一个元素组成 G 的一个子集 I，称为 G 的**左陪集代表**，则

$$G = \bigcup_{x \in I} xH$$

其中 xH 各不相交.

把

$$G = \bigcup_{x \in I} xH = \bigcup_{y \in J} Hy$$

称为 G 的**左（右）陪集分解**.

显然 $h \mapsto xh$ 是 $H \to xH$ 的双射，这就得到了我们前面的 Lagrange 定理.

定义 2.5.2 (指数)**.** 因为

$$(xH)^{-1} = \{(xh)^{-1} : h \in H\} = Hx^{-1}$$

因此若 I 是 G 关于 H 的左陪集代表元集，则 I^{-1} 就是右陪集代表元集，因此 H 在 G 的左右陪集个数相等，这个个数称为 H 在 G 的**指数**. 记为 $[G : H]$.

推论 2.5.1 (Lagrange 定理推论)**.** 1. 素数阶群是循环群

2. 4 阶群是交换群

证明

1. $|G| = p$ 为素数，任取 $g \in G, g \neq e$ ，则 $o(g) \mid p, o(g) \neq 1$ ，于是 $o(g) = p$ ，因此 $|\langle g \rangle| = p$ ，即 $G = \langle g \rangle$.

2. $|G| = 4$ ，对 $\forall g \in G, g \neq e$ ，有 $o(g) \mid 4, o(g) \neq 1$ ，于是 $o(g) = 2, 4$.

   若 $a \in G, o(a) = 4$ ，则 $G = \langle a \rangle$ 为循环群，显然交换. 否则，对 $\forall x \in G, x^2 = e$ ，即 $x^{-1} = x$ ，则

   $$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

命题 2.5.1 (指数性质)**.** 1. $K \leq H \leq G$ ，则

$$[G : K] = [G : H][H : K]$$

2. H, K 为 G 的有限子群，则

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

3. H, K 为 G 有限子群，则

$$[G : H \cap K] \leq [G : H][G : K]$$

证明

1. 分解

$$G=\bigcup_{x\in I}xH\quad H=\bigcup_{y\in J}yK$$

则

$$G=\bigcup_{(x,y)\in I\times J}xyK$$

下证上述是不交并. 对 $(x,y),(x',y')\in I\times J$ ，若 $xyK=x'y'K$ ，则

$$xH\cap x'H=\emptyset\implies x=x'$$

于是 $yK=y'K\implies y=y'$ ，证毕.

2. 设 $H\cap K=L$ ，分解

$$HK=\bigcup_{x\in I}xL\cdot\bigcup_{y\in J}Ly=\bigcup_{(x,y)\in I\times J}=xLy$$

因此 $|HK|=|I||J||L|$. 若 $xLy\cap x'Ly'\neq\emptyset$ ，则存在 $a,b\in L$ 使得

$$xay=x'by'\implies (x')^{-1}xa=by'y^{-1}\in H\cap K=L$$

于是 $(x')^{-1}x,y'y^{-1}\in L$ ，从而

$$xL=x'L\quad Ly=Ly'\implies x=x',y=y'$$

显然 $\forall x\in I,y\in J$ 有 $|xLy|=|L|$ ，又 $|H|=|I||L|,|K|=|J||L|$ ，代入即证.

3. 等价于

$$|H\cap K||G|\geq|H||K|$$

因为 $|HK|\leq|G|$ ，由上面一个结论即证，且等号成立当且仅当 $|G|=|HK|$ ，即当且仅当 $HK=G$.

2.5.2 商集

定义 2.5.3 (商集). $H\leq G$ ，H 所有左陪集构成的集合称为 G **关于子群** H **的左商集**，记为 $(G/H)_l$ ，同理有右商集 $(G/H)_r$. 显然两个集合的基数都是 $[G:H]$.

2.6 轨道长度和类方程

Section	Summary
2.6.1	群作用的轨道长度：定义稳定化子. 轨道长度等于稳定化子的指数.
2.6.2	群作用的轨道个数：计算群作用的轨道个数.
2.6.3	共轭类：群在自身共轭的作用的轨道称为共轭类，其稳定化子称为中心化子. 通过共轭类分解得到有限群的类方程.

2.6.1 群作用的轨道长度

定义 2.6.1. G 作用在集合 M 上，对 $x \in M$ ，定义

$$G_x = \{g \in G : g \circ x = x\}$$

容易验证 $G_x \leq G$ ，称为 G 作用下 x 的**稳定化子**或**稳定子群**.

定理 2.6.1. G 作用在集合 M 上，则过 x 的轨道 O_x 的长度（集合 O_x 的基数）等于 G_x 在 G 中的指数.

证明 定义

$$\phi : O_x \to (G \backslash G_x) \quad \phi(g \circ x) = gG_x$$

容易验证 ϕ 是双射，证毕.

从证明可以知道，若

$$O_x = (x_1, x_2, \cdots, x_k, \cdots)$$

且 $x_i = g_i \circ x$ ，则

$$\{g_1, g_2, \cdots, g_k, \cdots\}$$

为 G_x 在 G 中左陪集的代表元集.

由上述定理直接得到下面的推论：

推论 2.6.1. 有限群 G 作用在集合 M 上，则每个轨道的长度都有限，且为 $|G|$ 的因子.

推论 2.6.2. G 传递地作用在集合 M 上，则

$$|M| = [G : G_x]$$

其中 x 是 M 任意一个元素.

定义 2.6.2 (共轭子群). G 为群，$H \leq G$，则对 $\forall g \in G$，$gHg^{-1} \leq G$，称为与 H 共轭的 G 的子群，也称为 H 的**共轭子群**.

命题 2.6.1. 群作用的同一个轨道的两个元素的稳定化子共轭.

例 2.6.1. G 为群，Δ 为 G 所有子群构成的集合，考虑 G 在 Δ 上的共轭作用. 即

$$g \circ H = gHg^{-1} \quad \forall g \in G, H \in \Delta$$

对 $H \in \Delta$，H 的轨道就是 H 的全部共轭子群的集合，在这个作用下 H 的稳定化子

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

称为 H 关于 G 的**正规化子**. 由上述定理 H 的共轭子群个数为

$$|O_H| = [G : N_G(H)]$$

2.6.2 群作用的轨道个数

定理 2.6.2 (Burnside 引理). 有限群 G 作用在集合 M 上，对 $g \in G$，用

$$\psi(g) = \{x \in M : g \circ x = x\}$$

表示被 g 固定的 M 中元素构成的集合，则 G 作用的轨道个数为

$$\frac{1}{|G|} \sum_{g \in G} |\psi(g)|$$

证明 用两种方式计算 (g, x) 的个数，其中 x 被 g 固定.

一方面这样的有序对个数有 $\sum_{g \in G} |\psi(g)|$.

另一方面，对 $x \in M$，有 $|G_x|$ 个 $g \in G$ 固定 x，因此这样的有序对个数 $\sum_{x \in M} |G_x|$.

因为 $|G_x| = |G|/|O_x|$，因此

$$\sum_{g \in G} |\psi(g)| = \sum_{x \in M} |G_x| = |G| \sum_{x \in M} \frac{1}{|O_x|}$$

且 G 作用的轨道为 M 的划分，且 $\sum_{y \in O_x} \frac{1}{|O_y|} = 1$，证毕.

2.6.3 共轭类

考虑群 G 在自身的共轭作用，此作用的轨道称为 G 的**共轭类**，含元素 x 的共轭类记为 G_x ，即

$$G_x = \{gxg^{-1} : g \in G\}$$

x 在 G 共轭作用下的稳定化子称为 x 在 G 中的**中心化子**，记为 $C_G(x)$ ，即

$$C_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

由前面定理

$$|C_x| = [G : C_G(x)]$$

令

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G : gx = xg, \forall x \in G\}$$

称 $Z(G)$ 为 G 的中心，即与 G 中所有元素都交换的 G 的元素组成的集合.

例 2.6.2 (二面体群的所有共轭类). n 为奇数时，D_n 有 $\dfrac{n+3}{2}$ 个共轭类，其中只有一个共轭类包含一个元素，即 C_e ；有 $\dfrac{n-1}{2}$ 个共轭类包含 2 个元素，分别为 $C_{r^j}, j = 1, 2, \cdots, \dfrac{n-1}{2}$ ；有一个共轭类包含 n 个元素，即 C_s . 此时 $Z(D_n) = \{e\}$.

n 为偶数时，D_n 有 $\dfrac{n}{2} + 3$ 个共轭类，其中有 2 个共轭类包含一个元素，分别为 $C_e, C_{r^{n/2}}$ ；有 $\dfrac{n}{2} - 1$ 个共轭类包含 2 个元素，分别为 $C_{r^j}, j = 1, 2, \cdots, \dfrac{n}{2} - 1$ ；有 2 个共轭类包含 $\dfrac{n}{2}$ 个元素，分别为 C_s, C_{rs} . 此时 $Z(D_n) = \{e, r^{n/2}\}$.

G 为有限群，且 G 全部互不相同的共轭类为 $C_{x_1}, \cdots, C_{x_n}$ ，由群作用的集合分解为轨道的不交并得到

$$G = \bigcup_{i=1}^{n} C_{x_i}$$

计算两端集合元素个数得到

$$|G| = \sum_{i=1}^{n} |C_{x_i}| = \sum_{i=1}^{n} [G : C_G(x_i)]$$

称为有限群 G 的**类方程**，进一步，设 G 的元素个数大于 1 的共轭类为 $C_{y_1}, \cdots, C_{y_m}$ ，因为 $Z(G)$ 中每个元素构成恰含一个元素的共轭类，于是

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(y_i)]$$

定义 2.6.3. p 是素数，称有限群 G 为 $p-$ 群，若 $|G| = p^n, n \in \mathbb{N}$.

命题 2.6.2. G 为 $p-$ 群，则 $p \mid |Z(G)|$ ，从而 $Z(G) \neq \{e\}$.

证明 若 G 每个共轭类都含有一个元素，则 $Z(G) = G$ ，结论成立. 否则考虑 G 的类方程

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(y_i)]$$

显然 $C_G(y_i) \neq G$ ，又因为 $|G|$ 为 p 的幂，则 $[G : C_G(y_i)]$ 也是 p 的幂，且不等于 1 ，于是

$$p \mid [G : C_G(y_i)] \quad \forall 1 \leq i \leq m$$

又 $p \mid |G|$ ，于是 $p \mid |Z(G)|$ ，且 $z \in Z(G)$ ，得到 $Z(G) \neq e$.

2.7 正规子群与商群

Section	Summary
2.7.1	正规子群：正规子群的定义和等价条件.
2.7.2	商群：商群的定义和 G/Z 定理.
2.7.3	单群：单群的定义和性质.

2.7.1 正规子群

定义 2.7.1. $H \leq G$ ，若对 $\forall h \in H, g \in G$ 都有 $ghg^{-1} \in H$ ，称 H 是 G 的**正规子群**，记为 $H \trianglelefteq G$.

命题 2.7.1. $H \leq G$ ，则下列陈述等价

1. $H \trianglelefteq G$
2. $g^{-1}hg \in H, \forall h \in H, g \in G$
3. $gH = Hg, \forall g \in G$
4. $gHg^{-1} = H, \forall g \in G$
5. $g^{-1}Hg = H, \forall g \in G$

命题 2.7.2. 1. $\sigma : G \to H$ 为群同态，则 $\operatorname{Ker}\sigma \trianglelefteq G$.

2. $H \leq Z(G)$ ，则 $H \trianglelefteq G$ ，特别地 $Z(G) \trianglelefteq G$.

由定义，若 h 属于某个正规子群，则其共轭元素都属于这个正规子群，因此一个群的正规子群是**一些共轭类的并**. 反之，若群的一些共轭类的并构成子群，则必为正规子群.

2.7.2 商群

定义 2.7.2 (商群)**.** 若 $H \trianglelefteq G$ ，则 H 任意左陪集也是右陪集，此时简称为 H 的**陪集**. H 在 G 的所有陪集的集合记为 G/H ，称为 G 关于 H 的**商集**.

在商集 G/H 上 G 的运算诱导如下的运算

$$(g_1H)(g_2H) = (g_1g_2)H$$

即陪集的运算就是陪集代表元诱导出的运算，容易验证 G/H 在这个运算下构成一个群.

H 在上下文清楚时，gH 常被记为 $\overline{g}$ ，商群 G/H 常记为 $\overline{G}$.

定理 2.7.1 (G/Z 定理)**.** 若 $G/Z(G)$ 为循环群，则 G 交换.

若 G 交换，则 $Z(G) = G \implies G/Z(G) = \{\overline{e}\}$ ，因此上述定理告诉我们若 $G/Z(G)$ 循环，则它是平凡的单位元群.

推论 2.7.1. p 为素数，则 p^2 阶群交换.

2.7.3 单群

定义 2.7.3. 至少有两个元素且只有平凡的正规子群的群称为**单群**.

若一个群有非平凡的正规子群，则可以作出非平凡的商群. 单群做不出非平凡的商群，因此是基本的群.

一个基本的问题是，能不能找到所有的单群？

定理 2.7.2. 交换单群一定是素数阶循环群.

非交换单群的情况复杂得多，有限单群可以分为下面几类

1. 素数阶循环群
2. $n \geq 5$ 的交错群 A_n
3. Lie 型单群，共 16 族

4. 26 个散在单群

阶数最大的散在单群称为**魔群**

这里我们介绍 $n \geq 5$ 的 A_n .

定理 2.7.3. $n \geq 5$ 时 A_n 是单群

证明 取 A_n 的一个不等于 $\{(1)\}$ 的正规子群 N ，则需要证明 $N = A_n$.

先证明 A_n 可以被 3– 轮换生成. 重点在

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

然后就只需证 N 包含所有 3– 轮换.

先证明 N 一定有 3– 轮换，考虑 N 的不动元最多的非恒等置换 τ ，证明 τ 一定是 3– 轮换，即不动元个数 $n-3$.

然后，若 $(i_1i_2i_3) \in N$ ，则对任意 $(j_1j_2j_3)$ ，定义

$$\rho(i_t) = j_t \quad t = 1, 2, 3$$

且 ρ 把 i_1, i_2, i_3 外的元素映到 j_1, j_2, j_3 外的元素，若 $\rho \in A_n$ ，则

$$\rho(i_1i_2i_3)\rho^{-1} = (j_1j_2j_3) \in N$$

否则 $\rho \notin A_n$ ，因为 $n \geq 5$ ，则存在 j_1, j_2, j_3 以外的 i, j 使得 $\delta = (ji)\rho$ ，则 $\delta \in A_n$ ，且

$$\delta(i_1i_2i_3)\delta^{-1} = (ij)\rho(i_1i_2i_3)\rho^{-1}(ij)^{-1} = (j_1j_2j_3) \in N$$

证毕.

2.8 同态基本定理

Section	Summary
2.8.1	第一同构定理
2.8.2	第二、三同构定理

2.8.1 第一同构定理

$N \trianglelefteq G$，则有商群 $\overline{G} = G/N$，其元素为陪集 $gN = \overline{g}, g \in G$，在 $\overline{G}$ 中的运算为

$$\overline{g_1} \cdot \overline{g_2} = \overline{g_1 g_2}$$

定义映射 $\eta : G \to \overline{G}, \eta(g) = \overline{g}$，则容易验证 η 是一个满同态，称为 $G \to \overline{G}$ 的**自然同态**或**典范同态**.

容易验证 $\operatorname{Ker}\eta = N$，从而每个**正规子群一定是同态核**. 上一节开头证明了**同态核是正规子群**，因此本质上二者相同.

又注意到 $\eta(G) = G/N$，即商群一定是同态像. 因此自然地考虑同态像是否一定也是商群：

定理 2.8.1 (同态基本定理). $\pi : G \to G_1$ 是同态，则

$$G/\operatorname{Ker}\pi \cong \pi(G)$$

证明 记 $K = \operatorname{Ker}\pi$，则 $K \trianglelefteq G$，于是有商群 G/K，定义

$$\pi_1 : G/K \to \pi(G) \quad gK \mapsto \pi(g)$$

先证明 π_1 良定义：对 $\forall g, h \in G$，若 $gK = hK$，则 $h \in gK$，于是存在 $k \in K$ 使得 $h = gk$，则

$$\pi(h) = \pi(gk) = \pi(g)\pi(k) = \pi(g)e' = \pi(g)$$

其中 e' 为 G_1 单位元. 于是 π_1 是良定义的映射.

显然 π_1 是满射. 对 $a, b \in G$，若 $\pi_1(aK) = \pi_1(bK)$，则 $\pi(a) = \pi(b)$，于是

$$\pi(a^{-1}b) = \pi(a^{-1})\pi(b) = \pi(a)^{-1}\pi(b) = e'$$

从而 $a^{-1}b \in \operatorname{Ker}\pi = K \implies aK = bK$，因此 π_1 是双射.

任取 $g_1K, g_2K \in G/K$，则

$$\pi_1(g_1Kg_2K) = \pi_1(g_1g_2K) = \pi(g_1g_2) = \pi(g_1)\pi(g_2) = \pi_1(g_1K)\pi_1(g_2K)$$

即 π_1 是同态，综上 π_1 是同构，证毕.

推论 2.8.1. G 为有限群，$\pi : G \to G_1$ 为群同态，则 $\operatorname{Ker}\pi, \pi(G)$ 都是有限群，且

$$|G| = |\operatorname{Ker}\pi| \cdot |\pi(G)|$$

推论 2.8.2. V,U 为域 K 上线性空间，$\varphi: V \to U$ 为线性映射，则

$$V/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\varphi$$

即**线性映射基本定理**.

定理 2.8.2 (N/C 定理)**.** $H \leq G$ ，则 $N_G(H)/C_G(H)$ 同构 $\mathrm{Aut}(H)$ 的一个子群.

证明 因为 $C_G(S) \trianglelefteq N_G(S)$ ，且二者都是 G 的子群. 设 $H \leq G$ ，则对 $\forall g \in N_G(H)$ 和 $h \in H$ 有 $ghg^{-1} \in H$ ，定义

$$\sigma(g): H \to H \quad \sigma(g)(h) = ghg^{-1}, h \in H$$

容易验证 $\sigma(g)$ 是 H 的自同构，且

$$\sigma: N_G(H) \to \mathrm{Aut}(H) \quad g \mapsto \sigma(g)$$

是群同态，同态核

$$\begin{aligned}\mathrm{Ker}\,\sigma &= \{g \in N_G(H) : ghg^{-1} = h, \forall h \in H\} \\ &= C_{N_G(H)}(H) = C_G(H) \cap N_G(H) = C_G(H)\end{aligned}$$

于是由同态基本定理

$$N_G(H)/C_G(H) \cong \sigma(N_G(H)) \leq \mathrm{Aut}(H)$$

证毕.

命题 2.8.1. G 是有限群，p 是 $|G|$ 最小素因子，且 N 是 G 指数为 p 的子群，则 $N \trianglelefteq G$.

证明 设 $|G| = n \geq 2, n = pn'$ ，则 $|N| = n'$ ，记

$$P = (G/N)_l = \{g_iN : g_i \in G\}$$

为 G 关于 N 的左商集. 容易验证

$$g \circ (g_iN) = gg_iN$$

是 G 在集合 P 上的一个群作用. 于是有群同态 $\varphi: G \to S_p$. 又因为 $g \in \mathrm{Ker}\,\varphi$ 当且仅当 $gaN = aN, \forall a \in G$ ，于是

$$\mathrm{Ker}\,\varphi = \bigcap_{a \in G} aNa^{-1}$$

是 N 的一个子群，于是 $|\mathrm{Ker}\,\varphi| \mid |N|$ ，于是

$$p = \frac{|G|}{|N|} \mid \frac{|G|}{|\mathrm{Ker}\,\varphi|} = |\varphi(G)|$$

因为 $\varphi(G) \leq S_p$ ，于是 $|\varphi(G)| \mid p!$ ，又因为 $p^2 \not| p!$ ，于是 $p^2 \not| |\varphi(G)|$ ，进一步，对素数 $r > p$ ， $r \not| p!$ ，因此 $r \not| |\varphi(G)|$ ，于是 $|\varphi(G)| = p$ ，于是 $|\mathrm{Ker}\,\varphi| = n'$. 而 $\mathrm{Ker}\,\varphi \leq N$ 且 $|N| = n'$ ，因此 $\mathrm{Ker}\,\varphi = N$. 由于同态核一定是正规子群，因此 $N \trianglelefteq G$.

同态基本定理也称**第一同构定理**. 下面再给出两个同构定理

2.8.2 第二、三同构定理

定理 2.8.3 (第二同构定理). $N \trianglelefteq G, H \leq G$ ，则 $H \cap N \trianglelefteq H, N \trianglelefteq NH \leq G$ ，且

$$NH/N \cong H/H \cap N$$

[2]

证明 因为 $N \trianglelefteq G$ ，故

$$NH = \bigcup_{h \in H} Nh = \bigcup_{h \in H} hN = HN$$

于是 $NH \leq G$. 由 $N \trianglelefteq G$ 且 $N \leq NH$ ，则 $N \trianglelefteq NH$ ，定义

$$\varphi : H \to NH/N \quad h \mapsto \overline{h} = hN$$

容易验证 φ 是满同态，且

$$\mathrm{Ker}\,\varphi = \{h \in H : hN = N\} = H \cap N$$

于是 $H \cap N \trianglelefteq H$ ，由同态基本定理

$$NH/N \cong H/H \cap N$$

定理 2.8.4 (第三同构定理). $N \trianglelefteq G, M \trianglelefteq G$ ，且 $N \leq M$ ，则

$$G/M \cong (G/N)(M/N)$$

[2]在定理条件下 $|NH||H \cap N| = |N||H|$ ，进一步第二同构定理中 N, H 的条件可以放弱为 $N, H \leq G$ 且 $H \leq N_G(N)$.

证明 定义

$$\varphi : G/N \to G/M \quad gN \mapsto gM$$

若对 $g_1, g_2 \in G$，有 $g_1N = g_2N$，则 $g_1^{-1}g_2 \in N$，又 $N \leq M$，则 $g_1^{-1}g_2 \in M$，从而 $g_1M = g_2M$. 因此 φ 是映射，容易验证还是满同态，且

$$\operatorname{Ker}\varphi = \{gN : gM = M\} = \{gN : g \in M\} = M/N$$

于是由同态基本定理

$$G/M \cong (G/N)(M/N)$$

第三同构定理可以推广为如下形式，证明类似

定理 2.8.5 (第三同构定理). $\eta : G \to H$ 为群同态，若 $M \trianglelefteq G, M \supset \operatorname{Ker}\eta$，则 $\eta(M) \trianglelefteq \eta(G)$，且

$$G/M \cong \eta(G)/\eta(M)$$

[3]

定理 2.8.6 (对应定理). $N \trianglelefteq G$，记 $\mathcal{M}$ 为 G 中包含 N 的所有子群的集合，而 $\overline{\mathcal{M}}$ 为 $\overline{G} = G/N$ 的所有子群的集合，即

$$\mathcal{M} = \{M : N \leq M \leq G\} \quad \overline{\mathcal{M}} = \{\overline{M} : \overline{M} \leq \overline{G} = G/N\}$$

则 $\pi : \mathcal{M} \to \mathcal{M}, M \mapsto \overline{M} = M/N$ 为双射，且有以下性质：对 $M_1, M_2, M \in \mathcal{M}$

1. $M_1 \leq M_2 \iff \overline{M_1} \leq \overline{M_2}$
2. $M_1 \leq M_2 \implies [M_2 : M_1] = [\overline{M_2} : \overline{M_1}]$
3. $\overline{\langle M_1, M_2\rangle} = \langle \overline{M_1}, \overline{M_2}\rangle$
4. $\overline{M_1 \cap M_2} = \overline{M_1} \cap \overline{M_2}$
5. $M \trianglelefteq G \iff \overline{M} \trianglelefteq \overline{G}$，且有 $G/M \cong \overline{G}/\overline{M}$

证明 这里证明 π 是双射：因为 $N \trianglelefteq G$，于是对 $N \leq M \leq G$ 有 $N \trianglelefteq M$. 于是 $\overline{M} = M/N \leq G/N$，因此 π 是 $\mathscr{M} \to \overline{\mathscr{M}}$ 的映射. 反之，对 $\overline{M} \in \overline{\mathscr{M}}$，定义

$$\lambda(\overline{M}) = \{g \in G : \overline{g} \in \overline{M}\}$$

[3] $N \trianglelefteq G$，则有 $\overline{G} = G/N$，取 $\eta : G \to G/N$ 为自然同态，则 $\eta(G) = G/N$，且 $\operatorname{Ker}\eta = N$，对 $M \trianglelefteq G$，且 $N \leq M$，有 $\eta(M) = M/N$，由此可以得到第三同构定理的第一个形式.

因为对任意 $g \in N$ 有 $\overline{g} = \overline{e} \in \overline{M}$ ，由定义 $g \in \lambda(\overline{M})$ ，于是 $\lambda(\overline{M}) \supset N$.

对任意 $g, h \in \lambda(\overline{M})$ ，即 $\overline{g}, \overline{h} \in \overline{M}$ ，因为 $\overline{M}$ 是群，于是 $\overline{gh} = \overline{g}\overline{h} \in \overline{M}$ ，即 $gh \in \lambda(\overline{M})$.

又因为 $\overline{g^{-1}} = \overline{g}^{-1} \in \overline{M}$ ，于是 $g^{-1} \in \lambda(\overline{M})$ ，因此 $\lambda(M) \leq G$ ，于是 $\lambda(M) \in \mathscr{M}$.

于是 λ 是 $\overline{\mathscr{M}} \to \mathscr{M}$ 的映射，为了证明 π 是双射，只需要检查对任意 $M \in \mathscr{M}, \overline{M} \in \overline{\mathscr{M}}$ ，有

$$\lambda\pi(M) = M \quad \pi\lambda(\overline{M}) = \overline{M}$$

即可. 这是显然的，因此 π 是双射.

(1) $\sim$ (5) 的证明见习题 2.8

Chapter 3

群的结构

Chapter 4

群的结构

Chapter	Summary
3.1	群的直积：
3.2	Sylow 定理：
3.3	有限交换群的结构：
3.4	可解群：
3.5	Jordan-Holder 定理：

4.1 群的直积

Section	Summary
3.1.1	直积的定义和性质：直积的定义；直积阶的计算；直积保持子群和正规子群；交换直积同构.
3.1.2	直积的子群分解：直积的子群可以写成子群的直积的充要条件是阶互素.
3.1.3	内直积：给出内直积的定义，并给出群可以写成内直积的充分条件.
3.1.4	半直积：介绍群的同构作用，给出半直积的定义，并联系内直积，给出可以分解成共轭作用的半直积的充分条件.

群扩张是通过已知群来构造更大的群，本节我们给出两种群扩张的方法：直积和半直积.

4.1.1 直积的定义和性质

定义 4.1.1. G_1, G_2 为群，二者作为集合的乘积

$$G = G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

在运算

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

下构成群，称为 G_1, G_2 的直积，记为 $G = G_1 \times G_2$.

命题 4.1.1. 直积有下列性质：

1. 若 G_1, G_2 都是交换群，则 $G_1 \times G_2$ 也是交换群.
2. 若 G_1, G_2 都是有限群，则 $|G_1 \times G_2| = |G_1||G_2|$.
3. 若 $H_1 \leq G_1, H_2 \leq G_2$ ，则 $H_1 \times H_2 \leq G_1 \times G_2$.
4. 若 $H_1 \trianglelefteq G_1, H_2 \trianglelefteq G_2$ ，则 $H_1 \times H_2 \trianglelefteq G_1 \times G_2$.
5. $G_1 \times G_2 \cong G_2 \times G_1$.
6. G_1, G_2 分别同构 $G_1 \times G_2$ 的正规子群 $G_1 \times \{e_2\}, \{e_1\} \times G_2$ ，因此也可以说 G_1, G_2 是 $G_1 \times G_2$ 的正规子群.

定理 4.1.1. 若 m, n 互素，则 m 阶循环群和 n 阶循环群的直积为 mn 阶循环群.

若 m, n 不互素，此时直积 $G_1 \times G_2$ 不再是循环群. 一般地，设 $G = G_1 \times G_2, g_1 \in G_1, g_2 \in G_2$ ，则

$$o(g_1, g_2) = \mathrm{lcm}(o(g_1), o(g_2))$$

推论 4.1.1 (中国剩余定理)**.** 0.1.1

4.1.2 直积的子群分解

我们前面已经知道直积的性质之一是若 $H_1 \leq G_1, H_2 \leq G_2$ ，则 $H_1 \times H_2 \leq G_1 \times G_2$. 反过来，是不是 $G_1 \times G_2$ 的子群都可以写成子群的直积？

结论一般是不成立的，如下面的反例

例 4.1.1. p 为素数，G_1, G_2 都是 p 阶循环群，则 $G_1 \times G_2$ 有 $p^2 - 1$ 个 p 阶元素，由于每个 p 阶群友 $p-1$ 个 p 阶元素，于是 $G_1 \times G_2$ 的 p 阶子群个数为

$$\frac{p^2-1}{p-1} = p+1$$

而 G_1, G_2 的子群的直积只有四种可能，其中只有 $\{e\} \times G_2, G_1 \times \{e\}$ 是 $G_1 \times G_2$ 的 p 阶子群，比较一下得到 $G_1 \times G_2$ 剩下的 $p-1 \geq 1$ 个 p 阶子群都不是 G_1 和 G_2 的子群的直积.

但是我们可以证明，当 G_1, G_2 的阶互素的时候，结论成立.

定理 4.1.2. 有限群 G_1, G_2 的阶互素，则 $G_1 \times G_2$ 的子群都可以写成 G_1, G_2 子群的直积.

证明 设 $K \leq G_1 \times G_2$，定义两个满同态

$$p_1(a,b) = a \quad p_2(a,b) = b$$

令 $H_1 = p_1(K), H_2 = p_2(K)$，则 $H_1 \leq G_1, H_2 \leq G_2$.

对 $(a,b) \in K$，由定义 $a \in H_1, b \in H_2$，于是 $K \subset H_1 \times H_2$.

对 $a \in H_1$，由定义，存在 $c \in G_2$ 使得 $(a,c) \in K$. 设 $m = o(a), n = o(c)$，则 m, n 互素，于是由 CRT，存在 r 满足

$$r \equiv 1 (\mathrm{mod}\, m) \quad r \equiv 0 (\mathrm{mod}\, n)$$

因此

$$a^r = a^1 = a \quad c^r = c^0 = e_2$$

于是

$$(a, e_2) = (a,c)^r \in K$$

同理对 $\forall b \in H_2, (e_1, b) \in K$，于是

$$(a,b) = (a,e_2)(e_1,b) = \in K \quad \forall (a,b) \in H_1 \times H_2$$

于是 $H_1 \times H_2 \leq K$，证毕.

4.1.3 内直积

我们先考虑如下问题：若 H, K 是 G 的子群，在什么条件下有

$$G \cong H \times K$$

定理 4.1.3. 设 G 为群，$H, K \leq G$ ，且满足：

1. $G = HK$
2. $H \cap K = \{e\}$
3. H 中每个元素和 K 中每个元素可交换

则 $G \cong H \times K$.[1]

证明 定义映射 $\sigma : H \times K \to G, \sigma(h, k) = hk$.

由 (1) ，σ 是满射.

若 $\sigma(h_1, k_1) = \sigma(h_2, k_2)$ ，则 $h_1k_1 = h_2k_2$ ，即

$$h_2h_1^{-1} = k_2k_1^{-1} \in H \cap K$$

由 (2) ，$h_1 = h_2, k_1 = k_2$ ，即 σ 是单射.

最后

$$\begin{aligned}\sigma((h_1, k_1)(h_2, k_2)) &= \sigma(h_1h_2, k_1k_2) = (h_1h_2)(k_1k_2) \\ &= (h_1k_1)(h_2k_2) = \sigma(h_1, k_1)\sigma(h_2, k_2)\end{aligned}$$

于是 σ 是群同构，证毕.

由上面的定理，我们引出内直积的定义：

定义 4.1.2. H, K 是 G 的子群且 $G \cong H \times K$ ，则称 G 为子群 H, K 的**内直积**，习惯上也记为 $G = H \times K$.

下面给出上面充要条件的一个应用：

例 4.1.2. p 为素数，G 为 p^2 阶群，则 G 一定是交换群，且是循环群或者两个 p 阶循环群的直积.

若 G 中存在 p^2 阶元素，则 G 是循环群，证毕.

[1]根据证明过程，这里 (1), (2) 保证 G 和 $H \times K$ 一一对应，(1), (3) 保障 H, K 都是 G 的正规子群，因此如果把 (3) 换成 $H, K \trianglelefteq G$ ，命题也成立.

若 G 中不存在 p^2 阶元素，即非单位元的阶均为 p . 由 2.6.2 ，可以取非单位元 $a \in Z(G)$ 和非单位元 $b \in G\backslash\langle a\rangle$ ，此时 $b \notin \langle a\rangle$ 且 $\langle a\rangle, \langle b\rangle$ 都是 p 阶群，因此

$$\langle a\rangle \cap \langle b\rangle = \{e\}$$

从而

$$|\langle a\rangle\langle b\rangle| = \frac{|\langle a\rangle||\langle b\rangle|}{|\langle a\rangle \cap \langle b\rangle|} = p^2$$

因此 $G = \langle a\rangle\langle b\rangle$ ，又 a, b 可交换（$a \in Z(G)$ ）所以 $\langle a\rangle, \langle b\rangle$ 的每个元素可交换，从而

$$G \cong \langle a\rangle \times \langle b\rangle$$

是两个循环群的直积，是交换群.

例 4.1.3. $\gcd(s, t) = 1$ ，则

$$U(st) \cong U(s) \times U(t)$$

[2] 下面我们用 $\mathbb{Z}_m$ 表示 m 阶循环群. Gauss 证明了 $U(2) \cong \{1\}, U(4) \cong \mathbb{Z}_2$ ，当 $m \geq 3$ 时

$$U(2^m) \cong Z_2 \cong \mathbb{Z}_{2^{m-2}}$$

而对任意奇素数 p 和任意正整数 m 有

$$U(p^m) \cong \mathbb{Z}_{\varphi(p^m)} \quad \varphi(p^m) = p^m - p^{m-1}$$

于是对任意正整数，$U(n)$ 可以分解为循环群的直积，即给出了 $U(n)$ 的结构，由此也可以得到 $U(n)$ 为循环群当且仅当 $n = 1, 2, 4, p^m, 2p^m$ ，其中 p 是奇素数，m 是正整数.

4.1.4 半直积

在介绍半直积之前，我们先介绍**同构作用**.

在群作用的部分，我们已经说明了群 G 在集合 M 上的作用即 G 到 S_M 的同态. 设 H 是群，熟知 $\mathrm{Aut}(H) \leq S_H$.

[2] 对任意 $x \in U(st)$

$$x \mapsto (x(\mathrm{mod}\, s), x(\mathrm{mod}\, t))$$

是 $U(st) \to U(s) \times U(t)$ 的同构映射.

更进一步，对 n 素因子分解 $n = p_1^{e_1} \cdots p_k^{e_k}$ ，则

$$U(n) \cong U(p_1^{e_1}) \times \cdots \times U(p_k^{e_k})$$

定义 4.1.3. 设 H, K 是两个群，称群同态 $\varphi : K \to \mathrm{Aut}(H)$ 为 K 在 H 上的**同构作用**.

下面给出几个群在群上的同构作用的例子：

例 4.1.4. 1. 对任意 $y \in K$，定义 $\varphi(y) = \mathrm{id}_H$，即 H 的恒等自同构，显然 $\varphi : K \to \mathrm{Aut}(H)$ 为群同态，称为**平凡同构作用**.

2. 设 F 为域，对 $t \in F^*$，定义 $\varphi_t : F \to F$ 为 $\varphi_t(x) = tx$，容易验证 φ_t 是 F 的加法群的自同构. 定义 $\varphi : F^* \to \mathrm{Aut}(F)$ 为 $\varphi(t) = \varphi_t$，则 φ 是群同态，就得到 F 的乘法群 F^* 在 F 加法群上的同构作用.

3. 设 $H \trianglelefteq G, K \leq K$，对任意 $y \in K$，定义 $\varphi_y : H \to H$ 为 $\varphi_y(x) = yxy^{-1}$，则 $\varphi : y \mapsto \varphi_y$ 是 $K \to \mathrm{Aut}(H)$ 的群同态，因此 φ 是 K 在 H 上的同构作用，称为 K 在 H 上的**共轭作用**.

4. 对任意群 H，设 $K \leq \mathrm{Aut}(H)$，则包含映射 $i : K \to \mathrm{Aut}(H)$ 是 K 在 H 上的一个同构作用，这里 i 定义为 $i(y) = y, \forall y \in K$.

设 H, K 是两个群，φ 是 K 在 H 上的同构作用，并对任意 $y \in K$ 记

$$\varphi_y = \varphi(y) \in \mathrm{Aut}(H)$$

在 $H \times K$ 上定义运算：

$$(x, y)(u, v) = (x\varphi_y(u), yv) \quad (x, y), (u, v) \in H \times K$$

则 $H \times K$ 在该运算下构成群.

定义 4.1.4. 设 H, K 是两个群，φ 是 K 在 H 上的同构作用，$H \times K$ 在上述运算下构成的群称为 H, K （关于同构作用 φ ）的**半直积**，记为 $H \rtimes_\varphi K$.

若 φ 是 K 在 H 上的平凡同构作用，则 $H \rtimes_\varphi K$ 即 $H \times K$. 否则，则 $H \rtimes_\varphi K$ 是非交换群，这是因为 φ 非平凡，则存在 $y \in K, x \in H$ 使得 $\varphi_y(x) \neq x$，从而

$$(x, e_K)(e_H, y) = (x, y) \neq (\varphi_y(x), y) = (e_H, y)(x, e_K)$$

下面通过几个例子来熟悉半直积：

例 4.1.5. $H = \langle x \rangle$ 为 n 阶循环群，$K = \langle a \rangle$ 为 2 阶循环群，定义 K 在 H 上的同构作用为

$$\varphi_a : x \mapsto x^{-1}$$

则半直积 $H \rtimes_\varphi K = D_n$，即二面体群.

例 4.1.6. $H=\mathbb{Z}_3$ 为 3 阶循环群，$\mathrm{Aut}(\mathbb{Z}_3)\cong U(3)$ 为 2 阶群，其非单位元为负自同构

$$\theta: x\mapsto -x$$

设 $K=\mathbb{Z}_4$ ，其生成元为 1 ，从 $\mathbb{Z}_4$ 出发的群同态 φ 被 $\varphi(1)=\varphi_1$ 唯一确定，定义

$$\varphi:\mathbb{Z}_4\to \mathrm{Aut}(\mathbb{Z}_3)$$

为 $\varphi_1=\theta$ ，即 $\varphi_0=\varphi_1^0,\varphi_2=\varphi_1^2$ 为恒等自同构，而 $\varphi_1,\varphi_3=\varphi_1^3$ 为负自同构 θ . 由此得到的半直积 $\mathbb{Z}_3\rtimes_\varphi\mathbb{Z}_4$ 为 12 阶非交换群，其中的运算为

$$(x,n)(y,m)=(x+(-1)^n y,n+m)$$

这样我们已经得到了三个互补同构的 12 阶非交换群：$A_4,D_6,\mathbb{Z}_3\rtimes_\varphi\mathbb{Z}_4$ （A_4 没有 6 阶元，而 D_6 有，且 A_4,D_6 都没有 4 阶元，而 $\mathbb{Z}_3\rtimes_\varphi\mathbb{Z}_4$ 有）

类似直积的定义性质和定理 4.1.3 ，我们有

定理 4.1.4. 设 G 为群，$H,K\leq G$ ，且满足：

1. $G=HK$
2. $H\cap K=\{e\}$
3. $H\trianglelefteq G$

则 $G\cong H\rtimes_\varphi K$ ，其中 φ 是 K 在 H 上的共轭作用，即 $\varphi_y(x)=yxy^{-1}$. [3]

证明 同样定义映射 $\sigma: H\rtimes_\varphi K\to G,\sigma(h,k)=hk$ ，类似由 $(1),(2)$ 得到 σ 为双射，进一步，验证 σ 保持运算，于是 σ 为同构.

例 4.1.7. 当 $n\geq 3$ 时，由上述定理得到 $S_n=A_n\rtimes\langle(12)\rangle$.

4.2 Sylow 定理

Section	Summary

[3]设 G 为群，H,K 为 G 的两个子群且满足该定理的条件，我们也称 G 为 H,K 的半直积，记为 $H\rtimes K$.

3.2.1 Sylow 第一定理：群阶的任意素因子幂阶子群存在。推论得到 Cauchy 定理，并引出 Sylow $p-$ 子群的概念。

3.2.2 Sylow 第二定理：Sylow $p-$ 子群和 $p-$ 子群的关系、Sylow $p-$ 子群之间的关系。

3.2.3 Sylow 第三定理：Sylow $p-$ 子群的个数。

3.2.4 Sylow 定理的应用：分析阶和素数相关的群的结构。

3.2.5 素数阶群的结构：进一步分析素数阶群的结构。

在本节开始之前，我们先介绍一些定义和引理：

p 是素数，n 是正整数，且 $n = p^r m$ ，其中 $p \not| m$ ，则 p^r 称为 n 的 p **部分**，也称 n 的 $p-$adic 阶为 r 。[4]

引理 4.2.1. $n = p^r m$ ，其中 p 是素数，则对任意 $0 \leq k \leq r$ ，$C_{p^k}^n$ 的 p 部分为 p^{r-k} .

证明可以见课本 P91，证明本身本节要介绍的结论关系不大。

4.2.1 Sylow 第一定理

定理 4.2.1. 群 G 的阶为 $n = p^r m$ ，这里 p^r 是 n 的 $p-$ 部分，则对 $0 \leq k \leq r$ ，G 有 p^k 阶子群。

证明 设 Ω 是 G 的所有 p^k 元子集构成的集合，考虑 G 在 Ω 上的左乘作用

$$(g, A) \mapsto gA \quad g \in G, A \in \Omega$$

其所有不同的轨道为 $O_{A_i}, 1 \leq i \leq t$ ，则

$$|\Omega| = \bigcup_{i=1}^{t} |O_{A_i}|$$

由上述引理得到

$$p^{r-k+1} \not| |\Omega| = C_{p^k}^n$$

因此至少有一条轨道 O_{A_j} 满足 $p^{r-k+1} \not| |O_{A_j}|$ ，下证 A_j 的稳定化子 G_{A_j} 就是 G 的 p^k 阶子群。

因为

$$|G| = |O_{A_j}| \cdot |G_{A_j}|$$

[4]下面我们提到 $p-$ 部分的时候默认 p 是素数。

其中 $|G|$ 的 p 部分为 p^r ，且 $|O_{A_j}|$ 的 p 部分至多为 p^{r-k} ，因此 $|G_{A_j}|$ 的 p 部分至少为 p^k ，则 $|G_{A_j}| \geq p^k$.

取 $a \in A_j$ ，对任意 $g \in G_{A_j}$ ，由 $gA_j = A_j \implies ga \in A_j$ ，因此右陪集

$$G_{A_j}a = \{ga : g \in G_{A_j}\} \subset A_j$$

于是

$$|G_{A_j}| = |G_{A_j} \cdot a| \leq |A_j| = p^k$$

综上 $|G_{A_j}| = p^k$ ，证毕。

通过 Sylow 第一定理，我们可以得到推论：

推论 4.2.1 (Cauchy 定理). 群 G 的阶为 $n = p^r m, r \geq 1, p^r$ 为 n 的 $p-$ 部分，则 G 中有 p 阶元素。

且由 Sylow 第一定理，我们知道 p^r 阶子群存在，称其为 G 的 **Sylow $p-$ 子群**.

4.2.2 Sylow 第二定理

下面我们考虑不同的 Sylow $p-$ 子群之间的关系，即 Sylow 第二定理：

定理 4.2.2 (Sylow 第二定理). p 为素数，G 是有限群，$K \leq G$ 且 $p \mid |K|$. 设 P 是 G 的一个 Sylow $p-$ 子群，则存在 P 的某个共轭子群 $P' = aPa^{-1}$ 使得 $P' \cap K$ 是 K 的一个 Sylow $p-$ 子群，其中 $a \in G$.

证明 考虑 K 在 G 关于 P 的左商集

$$X = (G/P)_l = \{aP : a \in G\}$$

上的左乘作用，即

$$g \circ (aP) = (ga)P \quad g \in K, aP \in X$$

因为 $|X| = [G : P]$ ，且 P 是 G 的 Sylow $p-$ 子群，因此 $p \not| |X|$ ，故存在 $x = aP$ 使得包含 x 的轨道 O_x 满足 $p \not| |O_x|$ 。在此左乘作用下 x 的稳定子群

$$K_x = aPa^{-1} \cap K$$

是 $P' = aPa^{-1}$ 的子群，因此 $|K_x|$ 为 p 的幂，再由

$$|O_x| \cdot |K_x| = |K|$$

和 $p \not| |O_x|$ 得到 $|K_x|$ 恰为 $|K|$ 的 p 部分，因此 K_x 是 K 的 Sylow $p-$ 子群。

注意到：由于共轭子群的阶相同，因此 G 的 Sylow $p-$ 子群的共轭子群依然是 Sylow $p-$ 子群。

从 Sylow 第二定理可以得到推论：

推论 4.2.2. p 为有限群 G 的阶的素因子，则：

1. G 的任意 $p-$ 子群一定是 G 的某个 Sylow $p-$ 子群的子群。
2. G 的任意两个 Sylow $p-$ 子群共轭，从而 G 的 Sylow $p-$ 子群正规当且仅当 G 的 Sylow $p-$ 子群只有一个。

证明 设 K 是 G 的 $p-$ 子群，则 K 的 Sylow $p-$ 子群是其自身，于是存在 G 的 Sylow $p-$ 子群 P' 使得 $P' \cap K = K$ ，于是 $K \leq P'$ ，即 (1) .

特别地，若 K 也是 G 的 Sylow $p-$ 子群，由 $|K| = |P'|$ 得到 $K = P' = aPa^{-1}$ ，即 (2) .

4.2.3 Sylow 第三定理

下面我们考虑 Sylow $p-$ 子群的个数，即 Sylow 第三定理：

定理 4.2.3 (Sylow 第三定理). 设 $|G| = p^r m$ ，其中 p^r 是 $|G|$ 的 p 部分，且 $r \geq 1$ 。记 n_p 为 G 的 Sylow $p-$ 子群的个数，则

$$n_p \mid m \quad n_p \equiv 1 (\mathrm{mod}\, p)$$

证明 设 P 是 G 的一个 Sylow $p-$ 子群，由第二定理的推论，G 的所有 Sylow $p-$ 子群构成集合

$$X = \{aPa^{-1} : a \in G\}$$

考虑 P 在集合 X 上的共轭作用，即

$$g \circ (aPa^{-1}) = (ga)P(ga)^{-1} \quad g \in P, aPa^{-1} \in X$$

该作用的每个轨道长度都是 $|P|$ 的因此，从而是 p 的幂。

该作用下包含 P 的轨道为 $\{P\}$ 。反之，设 $\{P_i\}$ 是只有一个元素的轨道，由于对任意的 $g \in P$ 都有

$$gP_ig^{-1} = P_i$$

因此 $P \leq N_G(P_i)$，因此 P 也是 $N_G(P_i)$ 的一个 Sylow $p-$ 子群，又 P_i 是 $N_G(P_i)$ 的正规 Sylow $p-$ 子群，因此 $N_G(P_i)$ 的 Sylow $p-$ 子群唯一，从而 $P_i = P$，因此只存在一个轨道只包含一个元素，其余轨道长度都是 p 的倍数，则

$$n_p \equiv 1 (\mathrm{mod}\, p)$$

进一步，P 的共轭子群的个数 $[G : N_G(P)]$，因此

$$n_p \mid |G| = p^r m$$

又因为 n_p, p 互素，于是 $n_p \mid m$.

4.2.4 Sylow 定理应用

下面给出一些 Sylow 定理的应用例子：

命题 4.2.1. p, q 是素数，则 pq, p^2q 阶群不是单群。[5]

证明 若 $p = q$，则由 4.1.2，p^2 阶群是交换群，阶不是素数，因此不是单群。若 p^3 阶群为交换群，则显然不是单群。对非交换的 p^3 阶群，由 2.6.2，中心为非平凡正规子群，从而也不是单群。

下面设 $p \neq q$，设 $|G| = pq$，不妨设 $q > p$，则由 Sylow 第三定理得到 $n_q = 1$，于是 G 的 Sylow $q-$ 子群是 G 的非平凡正规子群，G 不是单群。

设 $|G| = p^2q$。若 $p > q$，同样得到 $n_p = 1$，从而 G 不是单群。若 $p < q$，则 $n_q = 1$ 或 p^2。若 $n_q = p^2$，则 G 有 p^2 个 q 阶群，此时 G 中 q 阶元素个数为 $p^2(q-1)$，从而其它阶元素有 p^2 个，此时 $n_p = 1$，则 G 的 Sylow $p-$ 子群为其非平凡正规子群，因此 G 不是单群。

综上，证毕。

命题 4.2.2. p 为奇素数，则 $2p$ 阶群为循环群或二面体群。

证明 设 $|G| = 2p$，其 Sylow $p-$ 子群 P 是正规循环群，记 $P = \langle a \rangle$，又 $|G| = 2p$，由 Cauchy 定理得到 G 中有 2 阶元素 b，显然 $b \notin \langle a \rangle$，所以

$$\langle a \rangle \cap \langle b \rangle = \{e\}$$

[5] 设 p 是素数，有限群 G 是 $p-$ 群，若 $|G| = p$，则 G 为交换单群。设 $|G| = p^m, m \geq 2$，若 G 交换，则 G 不是单群；若 G 非交换，则 $Z(G)$ 为 G 的非平凡正规子群，从而 G 不是单群，这样得到：有限 $p-$ 群是单群当且仅当 G 的阶为 p .

若 G 的阶有两个不同的素因子，则著名的 Burnside 定理告诉我们 G 不是单群。

比较群的阶可得

$$G = \langle a \rangle \langle b \rangle$$

由于 $\langle a \rangle \trianglelefteq G$ ，故 $bab^{-1} = a^r$ ，其中 $0 \leq r < p$ ，由 $b^2 = e$ 得到

$$a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

因此 $r^2 \equiv 1 (\mathrm{mod}\, p)$ ，即 $r \equiv \pm 1 (\mathrm{mod}\, p)$ 。若 $r \equiv 1$ ，则 $ab = ba$ ，此时 $G = \langle a \rangle \times \langle b \rangle$ ，即 G 为循环群 $\mathbb{Z}_{2p}$ 。若 $r \equiv -1$ ，则 $bab^{-1} = a^{-1}$ ，此时

$$G = \langle a, b : a^p = b^2 = e, bab^{-1} = a^{-1} \rangle$$

为二面体群 D_p .

定理 4.2.4. 阶数最小的有限非交换单群同构于交错群 A_5 .

证明 分两个步骤证明：先证明若有限群阶小于 60 ，则不是非交换单群。然后证明若 G 是 60 阶单群，则 $G \cong A_5$.

1. 由 4.2.1 处的注释，素数幂次阶群都不是非交换单群。且该命题告诉我们 pq, p^2q 阶群不是单群（$p \neq q$ 都是素数）。若 m 为奇数，因为指数为 2 的群都是正规子群，因此 $2m$ 阶群不是单群。综上，只需要考虑 $n = |G| = 24, 36, 40, 48, 56$ 的情形。

   (a) $n = 24 = 2^3 \cdot 3$ ，则 $n_2 = 1, 3$ 。若 $n_2 = 3$ ，则 G 在其三个 Sylow 2− 子群集合上的共轭作用诱导了群同态

   $$\rho : G \to S_3$$

   显然 ρ 不是单射。若 $\mathrm{Ker}\rho = G$ ，则对 $\forall g \in G$ 和 G 的一个 Sylow 2− 子群 P 有 $gPg^{-1} = P$ ，与 Sylow 2− 子群不唯一矛盾，因此 $\mathrm{Ker}\,\rho \neq G, \{e\}$ ，是 G 的非平凡正规子群，因此 G 不是单群。同理可证 $n = 48$ 的情形。

   (b) $n = 36 = 2^2 \cdot 3^2$ ，则 $n_3 = 1, 4$ 。若 $n_3 = 4$ ，则 G 在这四个 G 的 Sylow 3− 子群上的共轭作用诱导了群同态 $\rho : G \to S_4$ ，和 (a) 同理 $\mathrm{Ker}\,\rho$ 是 G 的非平凡的正规子群，因此 G 不是单群。

   (c) $n = 40 = 2^3 \cdot 5$ ，则 $n_5 = 1$ 不是单群。

   (d) $n = 56 = 2^3 \cdot 7$ ，则 $n_7 = 1, 8$ 。若 $n_7 = 8$ ，则 G 中 7 阶元素个数为 $8(7-1) = 48$ ，则其它阶元素只有 8 个，从而 $n_2 = 1$ ，G 不是单群。

2. 再证明若 G 是 60 阶单群，则 $G \cong A_5$.

   若 $H \leq G, [G:H] = m$ ，则 G 在 H 的左陪集集合上的左乘作用诱导非平凡同态

   $$\rho : G \to S_m$$

   若 $m \leq 4$ ，则 ρ 不是单射，从而 Kerρ 是 G 的非平凡正规子群，与 G 是单群矛盾。因此 G 没有指数 $2 \leq m \leq 4$ 的子群。

   下面证明一定存在指数为 5 的子群。：因为是单群，Sylow 子群不唯一，考虑 G 的 Sylow $2-$ 子群，则 $n_2 = 3, 5, 15$. 若 $n_2 = 3$ ，则 G 的一个 Sylow $2-$ 子群的正规化子为指数为 3 的子群，矛盾。若 $n_2 = 5$ ，此时 H 为 G 的一个 Sylow $2-$ 子群的正规化子，阶数为 5 。若 $n_2 = 15$ ，则进一步 $n_3 = 10, n_5 = 6$ ，此时 G 中 3 阶元素有 $10(3-1)$ 个，5 阶元素 $6(5-1)$ 个。若 G 的任意两个 Sylow $2-$ 子群的交只含单位元，则 G 中 $2, 4$ 阶元素 $15(4-1)$ 个，合起来超过 60 ，因此存在 G 的两个 Sylow $2-$ 子群 P_1, P_2 使得 $P_1 \cap P_2 \neq \{e\}$. 由于 P_1, P_2 都是 4 阶群，容易得到

   $$|P_1 \cap P_2| = 2 \quad P_1 \cap P_2 = \{e, x\}$$

   令 $H = \langle P_1, P_2 \rangle$ 因为 P_1, P_2 均为交换群，x 和 P_1, P_2 每个元素都交换，于是 $\langle x \rangle \trianglelefteq H$ ，由 G 为单群得到 $H \neq G$ ，由

   $$4 \mid |H| \mid 60$$

   和 $|H| > 4$ 得到 $|H| = 12, 20$ ，且 G 没有指数为 3 的子群，因此 $|H| = 12$ ，即 G 的指数为 5 的子群。因此 G 一定存在指数为 5 的子群 H 。

   考察 G 在 H 的左陪集集合上的左乘作用诱导的非平凡同态 $\rho : G \to S_5$ ，则 Ker$\rho = \{e\}$ ，即 ρ 是单同态，因此 $G \cong M \leq S_5$. 由于 $[S_5 : M] = 2$ ，于是 $M \trianglelefteq S_5$ ，从而 $M \cap A_5 \trianglelefteq A_5$ ，进一步有 $M \cap A_5 \neq \{e\}$ ，否则

   $$|MA_5| = \frac{|M||A_5|}{|M \cap A_5|} = 60^2 > |S_5|$$

   得到矛盾。因为 A_5 是单群，于是 $M \cap A_5 = A_5$. 从而 $A_5 \subset M$ ，由 $|M| = |A_5|$ 得到 $M = A_5$ ，因此 $G \cong A_5$.

4.2.5 素数阶群的结构

设 p 是素数， 4.1.2 确定了所有的 p^2 阶群。若 p, q 是不相同的素数，不妨设 $p < q$ ，则 pq 阶群都有哪些？前面的命题给出了 $p = 2$ 的情形，得到 $2q$ 阶群是循环群或者二面体群。下面我们继续考察这个问题。

例 4.2.1. 对任意素数 $p < q$，若 $p \not| (q-1)$，则 pq 阶群只有一个，即 pq 阶循环群；若 $p \mid (q-1)$，则有 2 个 pq 阶群，其一为循环群，另一同构非交换群

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in H, b \in \mathbb{Z}_q \right\}$$

其中 H 是 $\mathbb{Z}_q^*$ 的唯一 p 阶子群（因为 $p \mid (q-1)$ ）。

例 4.2.2. 设 $n = 255$，因为 $\varphi(255) = 128$，由 $\gcd(255, \varphi(255)) = 1$ 得到 255 阶群一定循环，下面给出一个简洁证明：

设 G 为 255 阶群，容易得到 Sylow 17− 阶子群唯一，设为 H，则 H 是 17 阶循环群且 $H \trianglelefteq G$.

对 H 使用 N/C 定理，此时 $N_G(H) = G$，则 $G/C_G(H)$ 同构 $\mathrm{Aut}(H)$ 的一个子群，因此

$$|G/C_G(H)| \mid 255 \quad |G/C_G(H)| \mid 16$$

于是 $|G/C_G(H)| = 1$，因此 $C_G(H) = G$，于是 $H \leq Z(G)$，由第三同构定理得到

$$G/Z(G) \cong (G/H)/(Z(G)/H)$$

从而

$$|G/Z(G)| \mid |G/H| = 15$$

于是 $|G/Z(G)| = 1, 3, 5, 15$ 。由上一个例子的结论，$G/Z(G)$ 是循环群，由 G/Z 定理得到 G 交换。

由于交换群任意子群都正规，因此 G 的 Sylow 3−, 5− 子群都是正规子群，从而唯一。设二者分别为 K, L，容易验证 $G = KLH$ 且

$$K \cap LH = L \cap KH = H \cap KL = \{e\}$$

于是 $G \cong K \times L \times H$，注意到 K, L, H 是阶数互素的循环群，因此 G 是循环群。

4.3 有限交换群的结构

Section	Summary

3.3.1 有限交换群分解 Sylow 子群直积：证明任意有限交换群是它所有 Sylow 子群的直积。

3.3.2 有限交换 p- 群分解循环子群直积：证明有限交换 $p-$ 群 A 可以分解为循环子群的直积，且参与直积的子群个数和子群的阶由 A 唯一确定，提出了初等因子的概念，给出获得互补同构的同阶有限交换群的方法。

3.3.3 有限交换群结构定理：在初等因子基础上提出不变因子的概念，提出有限交换群结构定理

4.3.1 有限交换群分解 Sylow 子群直积

一般地，任意有限交换群可以分解为循环群的直积，且分解是唯一的。

设 G 是 n 阶交换群，标准分解式 $n = p_1^{e_1} \cdots p_s^{e_s}$ 。因为 G 是交换群，每个子群都正规，因此 Sylow 子群唯一，设 P_i 为 G 的 Sylow p_i- 子群，记

$$\tilde{P}_i = P_1 \cdots P_{i-1} P_{i+1} \cdots P_s$$

由交换性得到 $P_1 \cdots P_s$ 和 $\tilde{P}_i$ 都是 G 的子群，又 $|P_i \cap \tilde{P}_i| = 1$ ，对 s 归纳可以得到

$$|\tilde{P}_i| = \frac{n}{p_i^{e_i}} \quad |P_1 P_2 \cdots P_s| = n$$

因此

$$G \cong P_1 \times P_2 \times \cdots P_s$$

即任意有限交换群是 Sylow 子群的直积。根据习题 3.1 的第 1 题，为了找到群 G 的结构，只需要讨论有限交换 $p-$ 群即可。

4.3.2 有限交换 p- 群分解循环子群直积

下面的一个引理和两个定理，我们将证明有限交换 $p-$ 群可以分解成循环子群的直积。

引理 4.3.1. A 是有限交换 $p-$ 群，则 A 循环当且仅当 A 只有一个 p 阶子群。

证明 必要性显然。下证充分性：设 A 只有一个 p 阶子群 P ，对 $|A|$ 归纳。考虑 A 上的自同态

$$\eta : a \mapsto a^p$$

则 $P \leq \mathrm{Ker}\eta$ 。反之对 $\forall b \in \mathrm{Ker}\eta, b \neq e$ ，则 $o(b) = p$ ，从而 $\langle b \rangle$ 是 A 的 p 阶子群，于是 $\langle b \rangle = P$ ，即 $b \in P$ ，于是 $\mathrm{Ker}\eta \leq P$ 。因此 $\mathrm{Ker}\eta = P$ ，由同态基本定理得到

$$A/P \cong \eta(A)$$

若 $\eta(A)=\{e\}$，则 $A=P$ 为循环群。若 $\eta(A)\neq\{e\}$，则 $\eta(A)$ 中有 p 阶元素，类似地可以得到 $P\leq\eta(A)$，显然

$$|\eta(A)|=\frac{|A|}{p}<|A|$$

由归纳假设，$\eta(A)$ 循环，设 $\eta(A)=\langle g\rangle$，再设 a 是 η 下 g 的一个原像，即 $\eta(a)=a^p=g$，于是

$$\frac{|A|}{p}=|\eta(A)|=o(g)=\frac{o(a)}{p}\implies o(a)=|A|$$

于是 $A=\langle a\rangle$ 为循环群。

定理 4.3.1. 设 A 是有限交换 $p-$ 群，a 是 A 中一个最高阶元素，则存在 $B\leq A$ 使得 $A\cong\langle a\rangle\times B$.

证明 对 $|A|$ 做归纳。记 $o(a)=p^r$，若 $o(a)=|A|$，则 $A=\langle a\rangle$，令 $B=\{e\}$ 即可。

若 A 非循环，由引理，A 的 p 阶子群不唯一，取一个不含于 $\langle a\rangle$ 的 p 阶子群 P，设

$$\overline{A}=A/P$$

注意到

$$o(aP)\mid o(a)$$

且若 $o(aP)<o(a)$，可以得到 $(aP)^{p^{r-1}}=P$，因此 $a^{p^{r-1}}\in P$，从而 $P=\langle a^{p^{r-1}}\rangle\leq\langle a\rangle$，和 P 的选取矛盾，因此 $o(aP)=o(a)$，于是 aP 是 $\overline{A}$ 中最高阶元素，由归纳假设，存在 $\overline{B}\leq\overline{A}$ 使得

$$\overline{A}\cong\langle aP\rangle\times\overline{B}$$

由对应定理，存在 $B\leq A$ 使得 $B\geq P$ 且 $\overline{B}=B/P$，由上式得到 $A=\langle a\rangle B$。进一步，由 $\langle aP\rangle\cap\overline{B}=\{P\}$ 得到 $\langle a\rangle\cap B\leq P$。又 $P\not\leq\langle a\rangle$，于是 $\langle a\rangle\cap B=\{e\}$，从而

$$A\cong\langle a\rangle\times B$$

定理 4.3.2. 有限交换 $p-$ 群 A 可以分解为它的循环子群的直积，即存在 $a_1,\cdots,a_t\in A$ 使得

$$A\cong\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_t\rangle$$

且直积因子个数 t 和它们的阶 $p^{m_1},\cdots,p^{m_t}$ 由 A 唯一确定。

证明 先证明可分解性。不妨设 $A\neq\{e\}$，其中元素阶的最大值为 p^{m_1}，其中 $m_1\geq1$，选取一个 p^{m_1} 阶元素 a_1。由上一个定理得到 $B_1\leq A$ 使得 $A\cong\langle a_1\rangle\times B_1$。

若 $B_1 = \{e\}$，则 $A \cong \langle a_1 \rangle$。否则，设 B_1 元素最大阶 p^{m_2}，其中 $m_2 \geq 1$，则 $m_1 \geq m_2$。选取 B_1 中一个 p^{m_2} 阶元素 a_2，则由上一个定理得到 $B_2 \leq B_1$，使得 $B_1 \cong \langle a_2 \rangle \times B_2$，由习题 3.1 第 1 题得到

$$A \cong \langle a_1 \rangle \times \langle a_2 \rangle \times B_2$$

继续这个过程，就得到

$$A \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_t \rangle$$

再证明唯一性：对 $|A|$ 归纳，若 $|A| = p$，则 A 循环，分解唯一性显然。设 $|A| > p$，考虑自同态

$$\eta : a \mapsto a^p$$

容易验证若

$$A \cong \langle a_1 \rangle \times \cdots \times \langle a_t \rangle$$

其中 a_i 的阶为 p^{m_i}，则

$$\mathrm{Ker}\eta \cong \langle a_1^{p^{m_1-1}} \rangle \times \cdots \times \langle a_t^{p^{m_t-1}} \rangle \quad \eta(A) \cong \langle a_1^p \rangle \times \cdots \times \langle a_t^p \rangle$$

于是 $|\mathrm{Ker}\eta| = p^t$ 是 A 唯一确定的子群 $\mathrm{Ker}\eta$ 的阶，由此得到 t 的不变性。对 η 的像，利用归纳假设得到 $a_1^p, \cdots, a_t^p$ 的阶 $p^{m_1-1}, \cdots, p^{m_t-1}$ 被 $\eta(A)$ 唯一确定，从而也被 A 唯一确定，因此 $p^{m_1}, \cdots, p^{m_t}$ 被群 A 唯一确定。

任意有限交换群是它所有 Sylow 子群的直积，而每个 Sylow 子群又是循环群的直积，由此我们得到下面这个有限交换群的结构定理。用 $\mathbb{Z}_m$ 表示 m 阶循环群。

定理 4.3.3. G 为 n 阶交换群，素因数分解 $n = p_1^{e_1} \cdots p_s^{e_s}$，其中 $p_1, \cdots, p_s$ 为互不相同的素数，则

$$G \cong \mathop{\times}_{i=1}^{s} (\mathbb{Z}_{p_i^{l_{i1}}} \times \mathbb{Z}_{p_i^{l_{i2}}} \times \cdots \times \mathbb{Z}_{p_i^{l_{ik_i}}})$$

其中 l_{ij} 为正整数且满足对 $1 \leq i \leq s$ 有

$$l_{i1} \geq l_{i2} \geq \cdots \geq l_{ik_i} \quad \sum_{j=1}^{k_i} l_{ij} = e_i$$

多重集合

$$\{p_1^{l_{11}}, p_1^{l_{12}}, \cdots, p_1^{l_{1k_1}}, \cdots, p_s^{l_{s1}}, p_s^{l_{s2}}, \cdots, p_s^{l_{sk_s}}\}$$

由群 G 唯一确定，称其中的元素为 G 的**初等因子**。

推论 4.3.1. 有限交换去被它的初等因子唯一确定，即两个 n 阶交换群同构当且仅当它们的初等因子相同。

对每个 $1 \leq i \leq s$ ，因为

$$l_{i1} \geq l_{i2} \geq \cdots \geq l_{ik_i} \quad \sum_{j=1}^{k_i} l_{ij} = e_i$$

所以 $(l_{i1}, \cdots, l_{ik_i})$ 恰为 e_i 的一个分拆，因此有序组 $(l_{i1}, \cdots, l_{ik_i})$ 个数为 e_i 的分拆数 $p(e_i)$ ，于是互不同构的 $n = p_1^{e_1} \cdots p_s^{e_s}$ 阶交换群个数为

$$p(e_1)p(e_2)\cdots p(e_s)$$

例 4.3.1. 由于 $3969 = 7^2 \cdot 3^4$ ，而分拆数 $p(2) = 2, p(4) = 5$ ，于是互补同构的 3969 阶交换群个数为 10 . 一般地，设 $p \neq q$ 为素数，则互补同构的 p^2q^4 阶交换群个数为 10 .

4.3.3 有限交换群结构定理

设 $k = \max\{k_1, \cdots, k_s\}$ ，令

$$\begin{aligned} d_k &= p_1^{l_{11}} \cdots p_s^{l_{s1}} \\ d_{k-1} &= p_1^{l_{12}} \cdots p_s^{l_{s2}} \\ &\cdots \\ d_1 &= p_1^{l_{1k}} \cdots p_s^{l_{sk}} \end{aligned}$$

其中约定若 $j > k$ ，则 $l_{ij} = 0$ 。由于 $p_1^{l_{1j_1}}, \cdots, p_s^{l_{sj_s}}$ 两两互素，故

$$\mathbb{Z}_{p_1^{l_{1j_1}}} \times \mathbb{Z}_{p_2^{l_{2j_2}}} \times \cdots \times \mathbb{Z}_{p_s^{l_{sj_s}}} \cong \mathbb{Z}_{p_1^{l_{1j_1}} p_2^{l_{2j_2}} \cdots p_s^{l_{sj_s}}}$$

由此得到下面这个有限交换群的结构定理：

定理 4.3.4 (有限交换群结构定理)**.** G 为 n 阶交换群，则

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}$$

其中 $d_i \geq 2$ 为正整数，且 $d_j \mid d_{j+1}, d_1 d_2 \cdots d_n = n$ 。多重集合

$$\{d_1, \cdots, d_k\}$$

由 G 唯一确定，其中的元素称为 G 的**不变因子**。

推论 4.3.2. 有限交换群被它的不变因子唯一确定，即 n 阶交换群同构当且仅当不变因子相同。

例 4.3.2. $1500 = 2^2 \cdot 3 \cdot 5^3$ ，其中 $p(2) = 2, p(1) = 1, p(3) = 3$ ，故互补同构的 1500 阶交换群有 6 个。进一步，初等因子有如下可能

$$\{2^2, 3, 5^3\}, \{2, 2, 3, 5^3\}, \{2^2, 3, 5^2, 5\}, \{2, 2, 3, 5^2, 5\}, \{2^2, 3, 5, 5, 5\}, \{2, 2, 3, 5, 5, 5\}$$

于是得到互不同构的 6 个 1500 阶交换群。

上一章将 8 阶非交换群进行了分类，为二面体群 D_4 或四元数群 Q ，又 $8 = 2^3$ ，于是 8 阶交换群的初等因子有如下可能

$$\{2^3\}, \{2^2, 2\}, \{2, 2, 2\}$$

则互不同构得 8 阶交换群有 3 个，分别为 $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ 。于是我们就证明了如下定理：

定理 4.3.5. 8 阶群一共有 5 个，其中有上述三个交换群，和两个非交换群 D_4, Q .

4.4 可解群

Section	Summary
3.4.1	换位子：换位子的定义及其性质，以及换位子的代数理解，即群交换当且仅当换位子只有单位元，并求特殊群 S_n 的换位子。
3.4.2	导群：通过换位子引出换位子群，即导群的概念，指出导群是非交换性的一种度量。讨论了 S_n, D_n 的换位子群。
3.4.2	可解群：介绍了 n 级导群的定义，提出可解群的概念，并给出和同态、正规子群和商群相关的一些命题。
3.4.3	可解的充要条件：给出了可解的充要条件，即存在可解群列。

4.4.1 换位子

定义 4.4.1. 设 G 为群，$a, b \in G$ ，令 $[a, b] = aba^{-1}b^{-1}$ ，称为 a, b 的**换位子**。

显然 a, b 可交换当且仅当 $[a, b] = e$. 对 $a, b, c \in G$ 和任意群同态 $\sigma : G \to H$ 有

$$[a, b]^{-1} = [b, a] \quad c[a, b]c^{-1} = [cac^{-1}, cbc^{-1}] \quad \sigma([a, b]) = [\sigma(a), \sigma(b)]$$

即换位子的逆、共轭和同态像还是换位子。但是换位子的乘积不一定是换位子，因此所有换位子不一定构成子群。

显然交换群的换位子只有单位元。对非交换群，判断元素是否为换位子是一个困难的问题。

例 4.4.1. 考虑 $S_n, n \geq 3$ ，符号函数 $\mathrm{sgn} : S_n \to \{\pm 1\}$ 是群同态，且 $\{\pm 1\}$ 是交换群，于是

$$\mathrm{sgn}([\sigma, \tau]) = 1$$

因此 S_n 中的换位子一定是偶置换。

令 $\sigma = (123), \tau = (12)$ ，则

$$[\sigma, \tau] = (132)$$

即 3– 轮换 (132) 为换位子。又 3– 轮换彼此共轭，因此 S_n 中的 3– 轮换都是换位子。

4.4.2 导群

定义 4.4.2. 群 G 的所有换位子生成的子群称为 G 的**换位子群**，或者**导群**，记为 $[G, G]$ 或 $G^{(1)}$ ，即

$$G^{(1)} = \langle aba^{-1}b^{-1} : a, b \in G \rangle$$

显然 G 交换当且仅当 $G^{(1)} = \{e\}$ ，因此某种意义上 $G^{(1)}$ 是 G 的非交换性的一种度量，$G^{(1)}$ 越大，G 离交换性越远。又因为换位子的共轭还是换位子，因此 $G^{(1)} \trianglelefteq G$.

下面我们看两个例子，分别讨论了 S_n, D_n 的导群。

例 4.4.2. 对 $n \geq 3$ ，由于 A_n 可以由 3– 轮换生成，而 3– 轮换都是换位子，于是 $A_n \leq S_n^{(1)}$ ，又每个换位子都是偶置换，所以 $S_n^{(1)} \leq A_n$ ，因此 $S_n^{(1)} = A_n$.

例 4.4.3. 设正整数 $n \geq 3$ ，考虑二面体群 D_n

$$D_n = \{r^i s^j : i = 0, \cdots, n-1; j = 0, 1\} \quad r^n = s^2 = e, rs = sr^{-1}$$

对 $a, b \in D_n$ ，若 a, b 都是旋转，则 a, b 可交换，即 $[a, b] = e$ 。若 a, b 分别为旋转和反射，则 $b^{-1} = b$ ，于是

$$[a, b] = r^i r^j s r^{-i} r^j s = r^{2i}$$

若 a, b 分别为反射和旋转，则 $a^{-1} = a$ ，同理得到 $[a, b] = r^{-2i}$ 。若 a, b 都是反射，则

$$[a, b] = (a, b)^2 = r^{2(i-j)}$$

综上 D_n 的换位子都是 r^2 的幂，又因为对任意 i 有 $r^{2i} = [r^i, s]$ ，因此 r^2 的任意幂都是换位子，因此

$$D_n^{(1)} = \langle r^2 \rangle$$

容易看出 n 为奇数时 $\langle r^2 \rangle = \langle r \rangle$ ，当 n 为偶数时 $\langle r^2 \rangle$ 是 $\langle r \rangle$ 指数为 2 的子群。

4.4.3 可解群

下面我们讨论同态像什么时候交换：

命题 4.4.1. $\sigma : G \to H$ 为群同态，则 $\sigma(G)$ 交换当且仅当 $G^{(1)} \leq \mathrm{Ker}\sigma$.

证明 记 $K = \mathrm{Ker}\sigma$，则 $\sigma(G) \cong G/K$ 交换当且仅当对 $\forall a, b \in G$，$[aK, bK] = [a, b]K = K$，即 $[a, b] \in K$，等价于 $G^{(1)} \leq K$.

特别地，设 $N \trianglelefteq G$，考虑自然同态 $\pi : G \to G/N$，容易得到推论：

推论 4.4.1. 设 $N \trianglelefteq G$，则 G/N 是交换群当且仅当 $G^{(1)} \leq N$，特别地，$G/G^{(1)}$ 交换。

递归地定义 G 的 n **级导群**如下：$G^0 = G, G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$.

定义 4.4.3. 若存在某个正整数 n 使得 $G^{(n)} = \{e\}$，则称 G 为**可解群**。[6]

下面我们考虑 n 级导群的同态像：

命题 4.4.2. $\sigma : G \to H$ 为群同态，则 $\sigma(G)^{(n)} = \sigma(G^{(n)})$.

证明 对 n 归纳。因为 $\sigma([a, b]) = [\sigma(a), \sigma(b)]$，因此 $\sigma(G)^{(1)} = \sigma(G^{(1)})$，即命题对 $n = 1$ 成立。对 $n \geq 2$，设命题对 $n - 1$ 成立，即 $\sigma(G)^{(n-1)} = \sigma(G^{(n-1)})$，则

$$\sigma(G)^{(n)} = (\sigma(G)^{n-1})^{(1)} = \sigma(G^{(n-1)})^{(1)} = \sigma((G^{(n-1)})^{(1)}) = \sigma(G^{(n)})$$

定理 4.4.1. 可解群的子群和商群依然是可解群。

证明 若 G 可解，则存在 n 使得 $G^{(n)} = \{e\}$。对任意 $H \leq G$ 有 $H^{(n)} \leq G^{(n)}$，因此 $H^{(n)} = \{e\}$，即 H 可解。

对 $N \trianglelefteq G$，记自然同态 $\pi : G \to G/N$，则

$$\pi(G)^{(n)} = \pi(G^{(n)}) = \pi(\{e\}) = \{\overline{e}\}$$

因此 $G/N = \pi(G)$ 可解。

定理 4.4.2. 设 $N \trianglelefteq G$，若 $N, G/N$ 均可解，则 G 可解。

证明 由于 G/N 可解，故存在正整数 n 使得

$$(G/N)^{(n)} = \{\overline{e}\}$$

[6] 显然交换群都是可解群。设 G 是非交换单群，由于 $G^{(1)} \trianglelefteq G$，因此 $G^{(1)} = G$，于是 $G^{(n)} = G$，因此非交换单群都不是可解群。

利用自然同态 $\pi : G \to G/N$ 得到

$$(G/N)^{(n)} = \pi(G)^{(n)} = \pi(G^{(n)})$$

即 $\pi(G^{(n)}) = \{\overline{e}\}$ ，因此

$$G^{(n)} \subset \mathrm{Ker}\pi = N$$

又 N 可解，于是 $N^{(m)} = \{e\}$ ，于是

$$G^{(n+m)} = (G^{(n)})^{(m)} \subset N^{(m)} = \{e\}$$

因此 G 可解。

推论 4.4.2. 有限 $p-$ 群可解。

证明 设 $|G| = p^n$ ，对 n 归纳：当 $n = 1$ ，G 是循环群，可解。

设 $n > 1$ 且结论对 $< n$ 成立，令 $N = Z(G)$ ，则 $N \trianglelefteq G$ 。若 $N = G$ ，则 G 为交换群，结论成立。否则，因为 $N \neq \{e\}$ ，设 $|N| = p^m$ ，则 $1 \leq m < n$ ，此时 $|G/N| = p^{n-m}$ ，由归纳假设 $N, G/N$ 都可解，证毕。

4.4.4 可解的充要条件

定理 4.4.3. G 为群，则 G 是可解群的充要条件是存在 G 的子群列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{e\}$$

使得对任意 $0 \leq i \leq s-1$ ，G_i/G_{i+1} 都是交换群。

证明 必要性：设 G 可解，则存在正整数 s 使得 $G^{(s)} = \{e\}$ ，取 $G_i = G^{(i)}$ 即可。

充分性：用归纳法证明：$G^{(i)} \leq G_i, 1 \leq i \leq s$ 。因为 G/G_1 为交换群，所以 $G^{(1)} \leq G_1$ ，即 $i = 1$ 时结论正确。现在设 $G^{(i)} \leq G_i$ ，因为 G_i/G_{i+1} 是交换群，于是 $G_i^{(1)} \leq G_{i+1}$ ，而由归纳假设 $G^{(i)} \leq G_i$ ，因此

$$G^{(i+1)} = (G^{(i)})^{(1)} \leq G_i^{(1)} \leq G_{i+1}$$

于是 $G^{(s)} \leq G_s = \{e\}$ ，证毕。

定义 4.4.4. 称对任意 $0 \leq i \leq s-1$ ，G_i/G_{i+1} 都是交换群的 G 的子群列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{e\}$$

为 G 的一个**可解群列**。

结合上一个定理，即 G 可解当且仅当 G 有可解群列。

例 4.4.4. 考察 S_n ，S_2 是交换群，因此可解。S_3 有一个可解群列

$$S_3 \trianglerighteq A_3 \trianglerighteq \{(1)\}$$

因此 S_3 可解，类似得到 S_4 有可解群列

$$S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq \{(1)\}$$

于是 S_4 为可解群。但对 $n \geq 5$ ，因为 $S_n^{(1)} = A_n$ ，其中 A_n 是非交换单群，即 $A_n^{(1)} = A_n$ ，因此 $S_n^{(m)} = A_n, m \geq 2$ ，于是 S_n 不可解。

Part II

课本习题

Chapter 1

群环域

1.1 习题 1.1

题目 1.1.1. 判断下列论断是否正确，若正确，给出证明，否则举出反例：

1. $\mathbb{R} \to \mathbb{R}^+, y \mapsto y^2$ 是一个映射
2. 在 $\mathbb{R}$ 中 $xRy \iff |x-y| \leq 3$ 是一个等价关系
3. 在 $\mathbb{Z}$ 中 $mRn \iff {}_2 \mid m-n$ 不是一个等价关系
4. 在 $\mathbb{C}^{n\times n}$ 中 $MRN \iff \exists P, Q \in \mathbb{C}^{n\times n}, s.t.\, M = PNQ$ 是等价关系
5. 非空集合上的关系可以同时是等价和偏序

证明

1. $0 \in \mathbb{R}$ 在 $\mathbb{R}^+$ 中没有像，错误
2. 显然 $1R4, 4R7$ 但是 $1R7$ 不成立，不满足传递性，错误
3. $1R2, 2R3$ 但是 $1R3$ 不成立，不满足传递性，正确
4. 若 MRN ，则 $\text{rank}(M) \leq \text{rank}(N)$ ，当 $\text{rank}(M) < \text{rank}(N)$ 时 NRM 不成立，不满足对称性，错误
5. 对 $A = \{a\}$ ，则 A 上的等价关系同时偏序，正确

题目 1.1.2. 证明

1. f 有左逆当且仅当 f 单射，f 有右逆当且仅当 f 满射

2. 若 f 有左逆 g 和右逆 h ，则 $g=h$

证明

1. 假设 $f:A\to B$ 是单射，定义 $B\to A$ 的对应关系 $g:f(x)\to x$ ，因为 f 单，因此 g 是映射，此时 $gf=\mathrm{id}_A$ ；假设 f 有左逆 g ，且存在 $x_1,x_2\in A$ 使得 $f(x_1)=f(x_2),x_1\neq x_2$ ，则

$$g(f(x_1))=g(f(x_2))\implies x_1=x_2$$

矛盾，因此 f 是单射.

假设 $f:A\to B$ 是满射，定义 $B\to A$ 的对应关系 h 使得 $f(h(y))=y$ ，则因为 f 满，于是 h 是映射；假设 f 有右逆 h ，且存在 $y\in B$ 使得 $f(x)\neq y,\forall x\in A$ ，又 $f(h(y))=y,h(y)\in A$ ，矛盾，因此 f 是满射.

2. 此时 f 单且满，于是 f 是双射，且

$$f(h(y))=y\quad\forall y\in B$$
$$g(f(x))=x\quad\forall x\in A$$

则

$$f(h(f(x)))=f(x)\implies h(f(x))=x\quad\forall x\in A$$

因此 $g=h$ ，证毕.

题目 1.1.3. 设 A,B 是有限集合，$|A|=m,|B|=n$ ，证明

1. $f:A\to B$ 个数为 n^m
2. 若 $f:A\to B$ 为单射，则 $m\leq n$ ，进一步，若 $m\leq n$ ，则 $A\to B$ 单射个数为 $\dfrac{n!}{(n-m)!}$
3. 若 $f:A\to B$ 为满射，则 $m\geq n$ ，进一步，若 $m\geq n$ ，则 $A\to B$ 满射个数为 $\sum\limits_{j=0}^{n}(-1)^{n-j}\binom{n}{j}j^m$
4. 设 $m=n$ ，则 $A\to B$ 的单射或满射都是双射

证明

1. 乘法原理，显然

2. 乘法原理，显然

3. 对 $b \in B$ ，定义 T_b 是所有使得 $b \notin f(A)$ 的映射 f 组成的集合，考虑含 k 个 B 元素的子集，使得 $f(A)$ 不包含这 k 个元素的映射个数为 $(n-k)^m$ ，在 B 中挑选 k 个元素有 $\binom{n}{k}$ 中情况，由容斥原理，此时 $\bigcup_{b\in B} T_b$ 的元素个数为

$$\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)^m$$

于是满射的个数为

$$n^m-\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)^m=\sum_{k=0}^{n}(-1)^{k}\binom{n}{k}(n-k)^m$$

令 $j=n-k$ ，则上式即

$$\sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j}j^m$$

证毕

4. A, B 有限，显然

题目 1.1.4. 在 $\mathbb{Z}$ 中考虑等价关系

$$m\sim_1 n \iff 6\mid m-n \quad m\sim_2 n \iff 2\mid m-n$$

1. 描述 $\sim_1$ 诱导的 $\mathbb{Z}$ 的划分 $\mathbb{Z}_6$ 和 $\sim_2$ 诱导的 $\mathbb{Z}$ 的划分 $\mathbb{Z}_2$

2. 以上划分中是否存在一个比另一个更细

证明

1. 记集合 $A_i=\{6k+i, k\in\mathbb{Z}\}, 0\le i\le_5$ ，则 $\mathbb{Z}_6=\{A_0, A_2, \cdots, A_5\}$ ；记集合 $B_j=\{2k+j, k\in\mathbb{Z}\}, j=0,1$ ，则 $\mathbb{Z}_2=\{B_0, B_1\}$

2. 因为 $B_0=A_0\cup A_2\cup A_4, B_1=A_1\cup A_3\cup A_5$ ，因此 $\mathbb{Z}_6$ 比 $\mathbb{Z}_2$ 更细

题目 1.1.5. 判断下列集合上的运算是否满足结合律或交换律

1. $\mathbb{Z}$ 上 $a*b=a-b$

2. $\mathbb{Z}^+$ 上 $a*b=2^{ab}$

3. $\mathbb{C}^{2\times 2}$ 上 $M * N = MN - NM$

证明

1. 不满足结合律，不满足交换律

2. 不满足结合律，满足交换律

3. 不满足结合律，不满足交换律

题目 1.1.6. 设 $A = \mathbb{Q}\backslash\{-1\}$ ，即不等于 -1 的所有有理数构成的集合，对与 $a, b \in A$ ，定义 $\circ$ 为

$$a \circ b = a + b + ab$$

证明 $\circ$ 是 A 上的运算，且满足交换律和结合律. 进一步判断 A 中是否有单位元？A 中元素是否有逆元？在有逆元时求出元素 $a \in A$ 的逆元

证明 对任意的 $a, b \in A$ ，若 $a \circ b = -1$ ，则 $(a+1)(b+1) = 0$ ，得到 $a = -1$ 或 $b = -1$ ，矛盾，因此 $a \circ b \in A$ ，显然对确定的 a, b ，$a + b + ab$ 是唯一确定的，因此 $\circ$ 是 $A \to A$ 的映射，是 A 上的运算.

显然 $\forall a, b \in A$ ，$a \circ b = a + b + ab = b \circ a$ ，满足交换律. 且 $\forall a, b, c \in A$

$$\begin{aligned}(a \circ b) \circ c &= (a + b + ab) \circ c \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a \circ (b \circ c)\end{aligned}$$

满足结合律.

若存在 $e \in A$ 使得 $\forall a \in A$ 有 $a \circ e = a + e + ae = a$ ，则 $e(a+1) = 0$ ，即 $e = 0$. 因此 A 中有单位元 e . 假设 $a \in A$ 存在逆元，记为 $a^{-1} \in A$ ，则

$$a \circ a^{-1} = a + a^{-1} + aa^{-1} = e = 0$$

解得 $a^{-1} = -\dfrac{a}{a+1}$ ，在 $a \in A$ 时 a^{-1} 总存在.

题目 1.1.7. 考虑 $\mathbb{Q}$ 上的等价关系：

$$u \sim v \iff u - v \in \mathbb{Z}$$

证明 $\mathbb{Q}$ 上的加法与等价关系 $\sim$ 相容.

证明 对任意 $u \in \mathbb{Q}$，记 u 所代表的等价类为 $\bar{u}$，即 $\bar{u} = \{v : u - v \in \mathbb{Z}\}$. 要证明等价类的加法和等价类的代表选取无关，即

$$若\overline{u_1} = \overline{u_2}, \overline{v_1} = \overline{v_2}, 则\overline{u_1 + v_1} = \overline{u_2 + v_2}$$

记 $u = u_1 - u_2, v = v_1 - v_2$，则 $u, v \in \mathbb{Z}$，于是

$$\overline{u_1 + v_1} = \overline{u_2 + v_2 + u + v} = \overline{u_2 + v_2}$$

证毕.

1.2 习题 1.2

题目 1.2.1. S 为幺半群，$a, b \in S$，若 ab 可逆，是否有 a, b 均可逆？

证明 令 S 是所有线性映射构成的集合，运算是映射乘法，则

$$a : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x \quad b : \mathbb{R} \to \mathbb{R}^2 : t \mapsto (t, 0)$$

则 $ab : \mathbb{R} \to \mathbb{R} : t \mapsto t$ 是双射，可逆，而此时 a 不是双射，不可逆.

题目 1.2.2. 设 S 为幺半群，$a_1, \cdots, a_m \in S$ 且两两可交换，证明 $a_1 a_2 \cdots a_m$ 可逆当且仅当 $a_1, \cdots, a_m$ 均可逆.

证明 S 为幺半群，其上运算有结合律. 因此若 $a_1, a_2 \cdots, a_m$ 均可逆，记 S 的单位元为 e，a_i 的逆元为 a_i^{-1}，则

$$(a_1 a_2 \cdots a_m)(a_m^{-1} a_{m-1}^{-1} \cdots a_1^{-1}) = e$$

于是 $a_m^{-1} a_{m-1}^{-1} \cdots a_1^{-1} \in S$ 是 $a_1 a_2 \cdots a_m$ 的逆元.

若 $a_1 a_2 \cdots a_m$ 可逆，设其逆元为 b，即 $a_1 \cdots a_m b = b a_1 \cdots a_m = e$，因为 a_i 两两可交换，得到

$$a_2 a_3 \cdots a_m (a_1 b) = (b a_1) a_2 a_3 \cdots a_m = e$$

于是

$$\begin{aligned} b a_1 \cdots a_m (a_1 b) &= e(a_1 b) = a_1 b \\ &= (b a_1)(a_2 \cdots a_m a_1 b) \\ &= b a_1 \end{aligned}$$

于是 $b a_1 = a_1 b$，即 a_1, b 可交换. 同理得到，$a_i, b (1 \le i \le m)$ 可交换，于是

$$a_1 (a_2 \cdots a_m b) = (a_2 \cdots a_m b) a_1 = e$$

则 a_1 可逆，逆元为 $a_2 \cdots a_m b$，同理可得 $a_i (1 \le i \le m)$ 可逆，证毕.

题目 1.2.3. 设 A 是一个非空集合，其上有一个运算，$e_l \in A$ ，若对任意 $a \in A$ ，均有 $e_l a = a$ ，则称 e_l 为 A 的一个左单位元，同理定义右单位元. 对 $a \in A$ ，若存在 $b \in A$ 使得 $ba = e_l$ ，则称 b 为 a 的一个左逆元，同理定义右逆元.

1. 若 A 中运算满足结合律，存在左单位元，且 A 中每个元素都有左逆元，证明 A 是一个群.

2. 若 A 中运算满足结合律，存在右单位元，且 A 中每个元素都有右逆元，证明 A 是一个群.

证明

1. 先证明左单位元同时也是右单位元，从而证明 A 存在单位元：对 $\forall a \in A$

   $$(e_l a)e_l = ae_l \quad e_l(ae_l) = e_l a$$

   又因为 A 中运算满足结合律，于是 $ae_l = e_l a = a$ ，因此 e_l 是 A 的单位元. 把 e_l 记为 e .

   下证 e 是唯一的：假设存在 $e' \in A$ 使得 $\forall a \in A$ 满足 $ae' = e'a = a$ ，则

   $$ee' = e' = e$$

   因此 e 唯一.

   下证 A 的左逆元也都是右逆元，即 A 的每个元素都有逆元. $\forall a \in A$ ，记 a 的左逆元为 a^{-1} ，即 $a^{-1}a = e$ ，则

   $$a(a^{-1}a) = ae = a = (aa^{-1})a$$

   则 aa^{-1} 是 a 的单位元，于是 $aa^{-1} = e$ ，因此 a^{-1} 也是 a 的右逆元. 证毕

2. 左右对称，同理

题目 1.2.4. G 为一个半群，且对任意 $a, b \in G$ ，方程 $ax = b, xa = b$ 都在 G 中有解，证明 G 是一个群.

证明 令 $a = b$ ，则 $ax = a, xa = a$ 对 $\forall a \in G$ 有解，于是 G 有单位元 e .

令 $b = e$ ，则 $ax = e, xa = e$ 对 $\forall a \in G$ 有解，于是 G 的元素都可逆.

题目 1.2.5. 设 G 是一个群，$a, b \in G$ ，如果 $aba^{-1} = b^r$ ，其中 r 是一个整数，证明对任意正整数 i 有 $a^i b a^{-i} = b^{r^i}$.

证明 当 $i=2$ 时，因为 $aba^{-1}=b^r$ ，因此 $ab=b^ra$ ，于是

$$\begin{aligned} ab^ra^{-1}&=(ab)b^{r-1}a^{-1}=b^rab^{r-1}a^{-1}=b^r(ab)b^{r-2}a^{-1}\\ &=b^{2r}ab^{r-2}a^{-1}=\cdots=b^{r(r-1)}ab^{r-(r-1)}a^{-1}=b^{r^2}\end{aligned}$$

于是 $a^2ba^{-2}=a(ab)a^{-2}=ab^ra^{-1}=b^{r^2}$. 假设 $a^iba^{-i}=b^{r^i}$ 成立，则 $a^ib=b^{r^i}a^i$ ，于是

$$\begin{aligned} a^{i+1}ba^{-(i+1)}&=a^i(ab)a^{-(i+1)}=a^i(b^ra)a^{-(i+1)}=a^ib^ra^{-i}\\ &=(a^ib)b^{r-1}a^{-i}=b^{r^i}a^ib^{r-1}a^{-i}=b^{r^i}(a^ib)b^{r-2}a^{-i}\\ &=b^{2r^i}a^ib^{r-2}a^{-i}=\cdots=b^{(r-1)r^i}a^iba^{-i}\\ &=b^{(r-1)r^i}b^{r^i}a^ia^{-i}=b^{r^{i+1}}\end{aligned}$$

由数学归纳法，证毕.

题目 1.2.6. 设 G 是一个群，若 $\forall a,b\in G$ 都有 $(ab)^2=a^2b^2$ ，证明 G 为交换群.

证明 因为 G 是群，存在消去律，于是

$$(ab)^2=a^2b^2\implies ab=ba$$

题目 1.2.7. $n\geq 3$ ，在 n 元对称群 S_n 中找两个元素 σ,r 使得 $\sigma\tau\neq\tau\sigma$.

证明 令 $\sigma=(123),\tau=(12)$ ，则 $\sigma\tau=(13),\tau\sigma=(23)$.

1.3 习题 1.3

题目 1.3.1. R 为交换环，对 $\forall a,b\in\mathbb{R}$ ，定义

$$a\oplus b=a+b-1\quad a\odot b=a+b-ab$$

证明 R 在 $\oplus,\odot$ 下构成交换环.

证明 因为 $a+b=b+a$ ，因此 $a\oplus b=b\oplus a$ ，于是 R 对 $\oplus$ 做成交换群；又因为

$$\begin{aligned}(a\odot b)\odot c&=(a+b-ab)\odot c\\ &=a+b-ac+c-ac-bc+abc\\ &=a+(b+c-bc)-a(b+c-bc)\\ &=a\odot(b\odot c)\end{aligned}$$

且 $a \odot e = e \odot a = a$ ，于是 R 对 $\odot$ 做成幺半群. 且

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c - 1) \\ &= a + b + c - 1 - ab - ac + a \\ &= a + b - ab + a + c - ac - 1 \\ &= (a + b - ab) \oplus (a + c - ac) \\ &= (a \odot b) \oplus (a \odot c) \\ (a \oplus b) \odot c &= (a + b - 1) \odot c \\ &= a + b + c - 1 - ac - bc + c \\ &= c + a - ac + c + b - bc - 1 \\ &= (c + a - ac) \oplus (c + b - bc) \\ &= (c \odot a) \oplus (c \odot b) \end{aligned}$$

因此乘法对加法左右分配.

题目 1.3.2. 设 R 为环，定义 $a - b = a + (-b)$ ，证明：对 $\forall a, b, c \in R$ ，有

1. $-(a + b) = (-a) + (-b) = -a - b$ ；
2. $-(a - b) = (-a) + b$ ；
3. $-(ab) = (-a)b = a(-b)$ ；
4. $(-a)(-b) = ab$ ；
5. $a(b - c) = ab - ac$.

证明

1. $(-a) + (-b) + a + b = 0 \implies (-a) + (-b) = -(a + b)$ ，证毕.
2. $(-a) + b + (a - b) = (-a) + b + a + (-b) = 0 \implies (-a) + b = -(a - b)$ ，证毕.
3. $(-a)b + ab = [(-a) + a]b = 0, a(-b) + ab = a[b + (-b)] = 0$ ，证毕.
4. $(-a)(-b) - ab = (-a)(-b) + (-ab) = (-a)[(-b) + b] = 0$ ，证毕
5. $a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$ ，证毕.

题目 1.3.3. 设 R 为环，$a,b\in R$ ，且 a,b 可交换，证明二项式定理：对任意正整数 n

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

证明 当 $n=2$ 时，有

$$(a+b)^2=(a+b)(a+b)=a^2+2ab+b^2$$

假设

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

则

$$\begin{aligned}(a+b)^{n+1}&=\sum_{k=0}^{n}\binom{n}{k}(a^{n-k}b^{k+1}+a^{n-k+1}b^k)\\&=\left(\sum_{k=0}^{n-1}\binom{n}{k}a^{n-k}b^{k+1}+b^{n+1}\right)+\left(\sum_{k=0}^{n-1}\binom{n}{k+1}a^{n-k}b^{k+1}+a^{n+1}\right)\\&=a^{n+1}+\sum_{k=0}^{n-1}\binom{n+1}{k+1}a^{n-k}b^{k+1}+b^{n+1}\\&=\sum_{k=0}^{n+1}\binom{n+1}{k}a^{n-k+1}b^k\end{aligned}$$

由数学归纳法，证毕.

题目 1.3.4. 给一个没有乘法消去律的环的例子

证明 所有 n 阶矩阵在矩阵加法、矩阵乘法下构成的环.

题目 1.3.5. 证明整环有消去律.

证明 在整环 R 上，当 $a\neq 0$ ，对 $ab=ac$ ，若 $b\neq c$ ，则 $b-c\neq 0$ ，于是

$$a(b-c)=0$$

因为整环没有零因子，矛盾，因此 $b=c$ ，证毕.

题目 1.3.6. R 为环，$a\in R,a\neq 0$ ，且存在 $b\in\mathbb{R},b\neq 0$ 使得 $aba=0$ ，证明 a 是 R 的一个左零因子或右零因子.

证明 若 $ba=0$，则 a 是右零因子，否则，$a(ba)=0$，则 a 是一个左零因子.

题目 1.3.7. R 为有限环，$a,b\in\mathbb{R}$ 且 $ab=1$，证明 $ba=1$.

证明 考虑变换 $f:R\to R\quad x\mapsto ax$，则对任意 $t\in R$，有 $t=f(bt)$，因此 f 是满射，又因为 R 有限，于是 f 是双射，记 f^{-1} 为 f 的逆映射. 因为

$$f(xr)=a(xr)=(ax)r=f(x)r\quad x,r\in R$$

则对任意 $y=f(x),r\in R$

$$f^{-1}(yr)=f^{-1}(f(x)r)=f^{-1}(f(xr))=xr=f^{-1}(f(x))r=f^{-1}(y)r$$

令 $y=1$，得到 $f^{-1}(x)=f^{-1}(1)x=cx$，则

$$cf(1)=f^{-1}(f(1))=1$$

又因为 $f(1)=a$，于是 $ca=1$，则

$$b=1\cdot b=(ca)b=c(ab)=c$$

于是 $b=c$，因此 $ba=1$.

题目 1.3.8. R 为环，$a,b\in R$ 且 $ab=1$ 但 $ba\neq 1$，证明存在无穷多个 $x\in R$ 满足 $ax=1$.

证明 令 $t=1-ba\neq 0$，则

$$at=a(1-ba)=a-(ab)a=0$$

因为 $t\neq 0$，因此 $b+mt\neq b+nt,m\neq n$，此时对任意的 $n\in\mathbb{N}_+$，有

$$a(b+nt)=ab+nat=1$$

证毕.

题目 1.3.9. R 为环，$a\in R$，若存在 $n\in\mathbb{N}_+$ 使得 $a^n=0$，称 a 为**幂零元**，证明若 a 为幂零元，则 $1-a$ 可逆.

证明 因为

$$(1-a)(1+a+\cdots+a^{n-1})=(1+a+\cdots+a^{n-1})(1-a)=1-a^n=0$$

于是 $(1-a)^{-1}=1+a+\cdots+a^{n-1}$.

题目 1.3.10. R 为环，$a,b\in R$ ，设 $1-ab$ 可逆，证明 $1-ba$ 也可逆，求出 $(1-ba)^{-1}$.

证明 注意到

$$\begin{aligned}&(1-ba)[1+b(1-ab)^{-1}a]\\=&1-ba+(1-ba)b(1-ab)^{-1}a\\=&1-ba+(b-bab)(1-ab)^{-1}a\\=&1-ba+b(1-ab)(1-ab)^{-1}a\\=&1-ba+ba=1\end{aligned}$$

$$\begin{aligned}&[1+b(1-ab)^{-1}a](1-ba)\\=&1-ba+b(1-ab)^{-1}a(1-ba)\\=&1-ba+b(1-ab)^{-1}(a-aba)\\=&1-ba+b(1-ab)^{-1}(1-ab)a\\=&1-ba+ba=1\end{aligned}$$

因此 $(1-ba)^{-1}=1+b(1-ab)^{-1}a$.

题目 1.3.11. 证明有限整环是域

证明 即证明有限整环 R 的每个非零元都可逆. 考虑 R 上的变换

$$\varphi_a:R\to R\quad x\mapsto ax\quad a\neq 0,x\in R$$

若 $\varphi_a(x)=\varphi_a(y)$ ，则 $a(x-y)=0$ ，因为 R 是整环，于是 $x-y=0$ ，即 φ_a 是单射，因为 R 有限，于是 φ 是满射，则存在 x 使得 $\varphi(x)=ax=1$ ，因为 R 是交换环，于是 $xa=1$ ，即 $x=a^{-1}$ ，对任意 $a\neq 0$ 都存在逆，证毕.

题目 1.3.12. 设 R 为除环，$a,b\in R$ 且 $ab\neq 0,1$ ，证明华罗庚等式

$$a-(a^{-1}+(b^{-1}-a)^{-1})^{-1}=aba$$

证明 即证

$$a-aba=(a^{-1}+(b^{-1}-a)^{-1})^{-1}$$

即证

$$(a-aba)(a^{-1}+(b^{-1}-a)^{-1})=1$$

展开得到

$$1-ab+a(b^{-1}-a)^{-1}-aba(b^{-1}-a)^{-1}=1$$

即证

$$a(b^{-1}-a)^{-1}=ab+aba(b^{-1}-a)^{-1}$$

两边同时左乘 a^{-1} ，即证

$$(b^{-1}-a)^{-1}=b+ba(b^{-1}-a)^{-1}$$

两边同时右乘 $b^{-1}-a$ ，即证

$$1=b(b^{-1}-a)+ba$$

展开显然成立，证毕.

题目 1.3.13. R 为一个无零因子环，$e\in R$ 满足对所有 $a\in R$ 有 $ea=a$ ，证明 e 为 R 的单位元.

证明 对 $a\neq 0$ ，有 $(e-1)a=0$ ，因为 R 无零因子，于是 $e-1=0$ ，证毕.

题目 1.3.14. D 是整环，在 D 中解方程 $x^2=1$.

解 因为 $x^2=1$ ，则

$$x^2-1=x^2-x+x-1=x(x-1)+(x-1)=(x+1)(x-1)=0$$

因为 D 没有零因子，于是 $x+1=0$ 或 $x-1=0$ ，即 $x=1$ 或 $x=-1$.

题目 1.3.15. 设 R 为环，若 $u\in R$ 存在右逆元但不唯一，证明 u 有无穷多个右逆元.

证明 假设 $v_1,v_2\in R$ 是 u 的两个相异的右逆元，即 $uv_1=uv_2=e,v_1\neq v_2$. 若 $v_1u=e$ ，则

$$v_1uv_2=ev_2=v_2=v_1(uv_2)=v_1$$

矛盾，因此 $v_1u\neq e$.

令 $w_k=(e-v_1u)u^k+v_1$ ，则 $uw_k=(u-uv_1u)u^k+uv_1=e$ ，于是 $w_k(k\in\mathbb{N}^*)$ 是 u 的右逆，若存在 $m,n\in\mathbb{N}^*,m>n$ 使得 $w_m=w_n$ ，则

$$(e-v_1u)u^m=(e-v_1u)u^n$$

两边同时右乘 v_1^m ，得到

$$(e-v_1u)u^mv_1^m=(1-v_1u)u^nv_1^m$$

其中 $u^mv_1^m=u^{m-1}(uv_1)v_1^{m-1}=\cdots=e,u^nv_1^m=v_1^{m-n}$ ，于是

$$e-v_1u=(e-v_1u)v_1v_1^{m-n-1}=(v_1-v_1uv_1)v_1^{m-n-1}=0$$

则 $v_1u=e$ ，矛盾，因此 $\{w_k\}_{k\in\mathbb{N}^*}$ 两两不等，于是有无穷多个 u 的右逆，证毕.

1.4 习题 1.4

题目 1.4.1. 证明在 p 元域 $\mathbb{Z}_p$ 中有

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

其中 $a, b \in \mathbb{Z}_p$ ，k 为任意正整数.

证明 当 p 是素数时，对 $\forall k \in \mathbb{Z}(1 \leq k \leq p-1)$ ，有 $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ ，显然 $k!, (p-k)!$ 的因子都小于 p ，于是 $\binom{p}{k}$ 是 p 的倍数. $\mathbb{Z}_p$ 是域，则 p 是素数. 当 $k=1$ 时，$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k$ ，因此 $(a+b)^p = a^p + b^p$.

假设 $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ ，则

$$(a+b)^{p^{k+1}} = (a^{p^k} + b^{p^k})^p = (a^{p^k})^p + (b^{p^k})^p$$

由数学归纳法，证毕.

题目 1.4.2. 给出一个有限非交换群 G 使得 $a^4 = e, \forall a \in G$.

解 考虑四元数群 $\{\pm 1, \pm i, \pm j, \pm k\}$.

题目 1.4.3. 求出方程 $x^2 - 1 = 0$ 在 $\mathbb{Z}_{360}$ 的全部解.

证明 即 $x^2 \equiv 1 (\mathrm{mod}\, 360)$ ，得到

$$\begin{cases} x^2 \equiv 1 (\mathrm{mod}\, 8) \\ x^2 \equiv 1 (\mathrm{mod}\, 9) \\ x^2 \equiv 1 (\mathrm{mod}\, 5) \end{cases} \Longrightarrow \begin{cases} x \equiv 1, 3, 5, 7 (\mathrm{mod}\, 8) \\ x \equiv 1, 8 (\mathrm{mod}\, 9) \\ x \equiv 1, 4 (\mathrm{mod}\, 5) \end{cases}$$

用 CRT 得到总共 16 个解

$$\{\overline{1}, \overline{19}, \overline{71}, \overline{89}, \overline{91}, \overline{109}, \overline{161}, \overline{179}, \overline{181}, \overline{199}, \overline{251}, \overline{269}, \overline{271}, \overline{289}, \overline{341}, \overline{359}\}$$

题目 1.4.4. 证明群 $U(3^5)$ 中一定有一个元素 g 使得 $U(3^5)$ 中每个元素都是 g 的幂. 这个结论对 $U(2^5)$ 是否正确？

证明 下面证明结论：$U(n)$ 是循环群，当且仅当 $n=2,4,p^r,2p^r$ ，其中 p 是奇素数，r 是正整数.

$n=2,4$ 显然.

先证明一个引理

引理 1.4.1. $a,b\in G$ ，且 $ab=ba$ ，设 $o(a)=m,o(b)=n$ ，若 $(m,n)=1$ ，则 $|ab|=mn$.

证明 不妨设 $o(ab)=s$ ，又因为 $(ab)^{mn}=e$ ，于是 $s\mid mn$ ，又因为 $a^{sn}=a^{sn}b^{sn}=(ab)^{sn}=e$ ，于是 $m\mid sn$ ，又因为 $(m,n)=1$ ，得到 $m\mid s$ ，类似地有 $n\mid s$ ，于是 $mn\mid s$ ，即 $s=mn$.

下面给出几个命题

命题 1.4.1. 有限交换群 G 存在元素 a 使得所有元素的阶都是 $o(a)$ 的因数.

证明 设 a 是 G 中阶最大的元素，假设存在 b 使得 $o(b)\mid o(a)$ ，则存在一个素数 p 使得

$$p^k\mid o(b)\quad p^k\not| o(a)$$

于是令

$$o(a)=s_1p^{k'}\quad o(b)=t_1p^k\quad 0\le k'<k,(s_1,p)=1$$

则

$$o(a^{p^{k'}})=\frac{o(a)}{(o(a),p^{k'})}=s_1\quad o(b^{t_1})=\frac{o(b)}{(o(b),t_1)}=p^k$$

因为 $(s_1,p^k)=1$ ，于是由引理得到 $o(a^{p^{k'}}b^{t_1})=p^ks_1>p^{k'}s_1=s=o(a)$ ，与 $o(a)$ 是最大阶矛盾.

命题 1.4.2. G 是有限交换群，若对 $\forall m\in\mathbb{N}_+$ ，方程 $x^m=e$ 至多有 m 个根，则 G 是循环群.

证明 此时存在 $a\in G$ 使得任意元素的阶是 $o(a)$ 因数，设 $o(a)=n$ ，则 $x^n=e,\forall x\in G$ ，由题，得到 $|G|\le n$ ，又因为 $\langle a\rangle\subset G$ ，于是 $|G|\ge n$ ，于是 $|G|=|\langle a\rangle|=n\implies G=\langle a\rangle$ ，证毕.

因为 $\mathbb{Z}_p$ 是域，在域上的多项式的根个数不超过次数，因此对任意 $m\in\mathbb{N}_+$ ，方程 $x^m=e$ 至多有 n 个根，则在 $U(p)$ 上亦然，因此 $U(p)$ 是循环群.

下面证明引理

引理 1.4.2. G 是有限交换群，$|G|=n$ ，则 $a^n=1,\forall a\in G$.

证明 设 $G=\{a_1,a_2,\cdots,e\}$，令 $\overline{G}=\{a_1^2,a_1a_2,\cdots,a_1e\}$，若

$$a_1a_i=a_1a_j \implies a_i=a_j$$

因此 $|\overline{G}|=n$，又因为 $\overline{G}\subset G$，于是 $G=\overline{G}$，则两个集合的所有元素乘积相等，即

$$a_1a_2\cdots e=a_1a_2\cdots e\cdot a_1^n \implies a_1^n=1$$

证毕.

直接推论可以得到 Euler 定理 $\overline{a}^{\varphi(m)}=\overline{1},\forall\overline{a}\in U(m)$.

引理 1.4.3. 若存在 $\overline{a}^{\varphi(p)}\neq 1,\overline{a}\in U(p^2)$，则 $\overline{a}^{\varphi(p^{r-1})}\neq 1,\overline{a}\in U(p^r),\forall r\geq 2$.

证明 假设 $r-1$ 时结论成立，即

$$\overline{a}^{\varphi(p^{r-2})}\neq 1,\overline{a}\in U(p^{r-1})$$

由 Euler 定理，此时 $a^{\varphi(p^{r-2})}\equiv 1(\mathrm{mod}\,p^{r-2})$，记 $a^{\varphi(p^{r-2})}=1+kp^{r-2}$，其中 $p\mid k$，则

$$a^{\varphi(p^{r-1})}=(a^{\varphi(p^{r-2})})^p=(1+kp^{r-2})^p\equiv 1+kp^{r-1}\neq 1(\mathrm{mod}\,p^r)$$

当 $r=2$ 结论显然，证毕.

下证 $U(p^r)$ 是循环群. 因为已知 $U(p)$ 是循环群，取生成元 a 讨论

1. 若 $\overline{a}^{\varphi(p)}\neq 1(\overline{a}\in U(p^2))$，则 $\overline{a}^{\varphi(p^{r-1})}\neq\overline{1}(\overline{a}\in U(p^r),r\geq 2)$，设 $\overline{a}$ 在 $U(p^r)$ 的阶为 s，则

   $$\overline{a}^s=\overline{1}(\overline{a}\in U(p^r)) \implies \overline{a}^s=\overline{1}(\overline{a}\in U(p))$$

   于是 $\varphi(p)\mid s$，由 Euler 定理 $\overline{a}^{\varphi(p^r)}=\overline{1}(\overline{a}\in U(p^r))$，从而 $s\mid\varphi(p^r)$，于是

   $$s=p^t(p-1)\quad 0\leq t\leq r-1$$

   假设 $t<r-1$，则 $s\mid\varphi(p^{r-1})$，则 $\overline{a}^{\varphi(p^{r-1})}=\overline{1}(\overline{a}\in U(p^r))$，矛盾，因此 $t=r-1$，进而 $s=\varphi(p^r)$，即 $\overline{a}$ 和 $U(p^r)$ 的阶相等，进而 $\overline{a}$ 是 $U(p^r)$ 的生成元，证毕.

2. 若 $\overline{a}^{\varphi(p)}=1(\overline{a}\in U(p^2))$，取 $b=a+p$，则 $\overline{a}=\overline{b}$，且因为 $(a,p)=1$，进而 $(a^{p-1},p)=1$，于是

   $$\overline{b}^{\varphi(p)}=\overline{a+p}^{\varphi(p)}=\overline{1}+(p-1)pa^{p-2}\neq\overline{1}\quad U(p^2)$$

   因此转化为第一种情况.

下证 $U(2p^r)$ 是循环群，已知 $U(p^r)$ 是循环群，取 $U(p^r)$ 的生成元 $\overline{a}$ 讨论

1. 若 a 是奇数，则 $(a,2p^r)=1$ ，从而 $\overline{a}\in U(2p^r)$ ，设 $o(\overline{a})=s(U(2p^r))$ ，则

$$\overline{a}^s=\overline{1}(U(2p^r))\implies \overline{a}^s=\overline{1}(U(p^r))$$

因为 $\overline{a}$ 是 $U(p^r)$ 的生成元，于是 $\varphi(p^r)\mid s$ ；又因为 $\overline{a}^{\varphi(2p^r)}=1(U(2p^r))$ ，得到 $s\mid\varphi(2p^r)$ ，因为 $\varphi(p^r)=\varphi(2p^r)$ ，于是 $s=\varphi(2p^r)$ ，即 $\overline{a}$ 和 $U(2p^r)$ 的阶相等，进而 $\overline{a}$ 是 $U(2p^r)$ 的生成元，证毕.

2. 若 a 是偶数，取 $b=a+p^r$ ，则 b 是奇数且 $\overline{b}$ 是 $U(p^r)$ 生成元，转化为第一种情况.

下证必要性，若 $U(m)$ 是循环群，设 $\overline{a}$ 是 $U(m)$ 的一个生成元，此时 $\overline{a}^{\varphi(m)}=\overline{1}(U(m))$ ，取 m 的唯一分解

$$m=\prod_{i=1}^{s}p_i^{n_i}$$

则

$$\overline{a}^{\varphi(p_i^{n_i})}=\overline{1}(U(p_i^{n_i}))$$

令 $n=[\varphi(p_1^{n_1}),\varphi(p_2^{n_2}),\cdots,\varphi(p_s^{n_s})]$ ，则 $\overline{a}^n=\overline{1}(U(p_i^{n_i})),\forall 1\le i\le s$ ，于是 $\overline{a}^n=\overline{1}(U(m))$ ，因此 $\varphi(m)\mid n$ ，从而 $\varphi(m)\le n$ ，又因为

$$\varphi(m)=\prod_{i=1}^{s}\varphi(p_i^{n_i})\ge[\varphi(p_1^{n_1}),\varphi(p_2^{n_2}),\cdots,\varphi(p_s^{n_s})]=n$$

于是 $n=\varphi(m)$ ，即 $\varphi(p_i^{n_i})$ 两两互素.

假设 m 存在两种不同的奇素数因数 p_i,p_j ，则

$$\varphi(p_i^{n_i})=p_i^{n_i-1}(p_i-1),\varphi(p_j^{n_j})=p_j^{n_j-1}(p_j-1)$$

都是偶数，矛盾，于是 $m=2^lp^r$ ，其中 p 是奇素数.

若 $r\ge 1$ ，则 $\varphi(p^r)$ 是偶数，且 $\varphi(2^l)=2^{l-1}$ ，则 $l\le 1$ ，此时 $m=p^r,2p^r$.

若 $r=0$ ，则 $m=2^l$ ，此时 $|U(m)|=\varphi(2^l)=2^{l-1}$ ，当 $l\ge 2$ 时是偶数，设此时循环群

$$U(m)=\{e,g,g^2,\cdots g^{2^{l-1}-1}\}$$

若存在 $g^k\in U(m),0\le k\le 2^{l-1}-1$ 使得 $o(g^k)=2$ ，则 $k^2=2^{l-1}\implies k=2^{l-2}$ ，即 $U(m)$ 中阶为 2 的元素唯一. 考虑

$$x^2\equiv 1(\mathrm{mod}\,2^l)$$

等价于 $2^l \mid (x-1)(x+1)$ ，因为对奇数 x ，有 $(x-1,x+1)=(x+1,2)=2$ ，因此 $x-1,x+1$ 中有一个是 2^{l-1} 的倍数，即方程的解为

$$x \equiv 1(\mathrm{mod}\, 2^{l-1}) \quad x \equiv -1(\mathrm{mod}\, 2^{l-1})$$

即当 $l \geq 3$ 时，$U(m)$ 中阶为 2 的元素至少有两个，显然 $U(m)$ 不是循环群，因此 $l=1,2$.

综上，证毕

题目 1.4.5. 在 $\mathbb{Z}_{29}$ 中计算 $\overline{28^{60}}$.

证明 因为在 $\mathbb{Z}_{29}$ 中

$$\overline{28} = \overline{-1}$$

因此

$$\overline{28^{60}} = \overline{(-1)^{60}} = 1$$

Chapter 2

群的基本性质和作用

2.1 习题 2.1

题目 2.1.1. 设 $n \geq 3$，$\sigma \in S_n$ 且 $\sigma \neq \mathrm{id}_{[n]}$，证明存在 $\tau \in S_n$ 使得 $\sigma\tau \neq \tau\sigma$.

证明 假设 $\forall \tau \in S_n, \tau\sigma = \sigma\tau$，任取 $i \neq j$，则对 $\tau = (ij)$，有

$$\sigma(\tau(i)) = \tau(\sigma(i))$$

其中 $\sigma(\tau(i)) = \sigma(j)$，假设 $\sigma(i) \neq i, j$，则 $\tau(\sigma(i)) = \sigma(i)$，于是 $\sigma(i) = \sigma(j)$，矛盾，因此

$$\sigma(i) = j \quad \text{or} \quad \sigma(j) = i$$

假设 $\sigma(i) = j$，则同理可以得到 $\sigma(j) = i$，于是 σ 将 i, j 对换.

因为 $n \geq 3$，此时取 $k \neq i, j$，令 $\tau = (jk)$，则同理得到 σ 将 j, k 对换，或 σ 下 j, k 保持不变，二者都与 σ 将 i, j 对换矛盾，因此 σ 保持 i, j 保持不变. 因为 i, j 的任意性，σ 保持所有任意两个元素不变，于是 $\sigma = \mathrm{id}_{[n]}$，矛盾，证毕.

题目 2.1.2. 设 $n \geq 3, \sigma = (12\cdots n)$，计算 σ^k，进一步地，对 $\tau \in S_n$，若 τ, σ 可交换，证明 τ 为 σ 的幂.

证明 $\sigma^k(i) = i + k - n \cdot \left[\dfrac{i+k-1}{n}\right]$.

设 $\tau(i) = n$

1. 若 $i = n$，则 $\tau\sigma(n) = \tau(1) = \sigma\tau(n) = \sigma(n) = 1$，即

$$\tau(1) = 1, \tau(n) = n$$

此时对任意 $j \neq 1, j \neq n$ ，有 $\sigma(j) = j+1, \tau(j) \neq n$ ，于是

$$\tau\sigma(j) = \tau(j+1) = \sigma\tau(j) = \tau(j) + 1$$

归纳得到 $\tau = \sigma^n = e$.

2. 若 $i \neq n$ ，则

$$\tau\sigma(i) = \tau(i+1) = \sigma\tau(i) = 1$$

对 $i+2 \leq k \leq n$ ，有

$$\begin{aligned} \tau(k) &= \tau\sigma(k-1) \\ &= \sigma\tau(k-1) \\ &= \tau(k-1) + 1 \end{aligned}$$

于是得到

$$\tau : \begin{matrix} i & i+1 & i+2 & \cdots & n \\ n & 1 & 2 & \cdots & n-i \end{matrix}$$

此时 $\tau(1) = \tau\sigma(n) = \sigma\tau(n) = \tau(n) + 1 = n - i + 1$ ，同理得到当 $2 \leq k \leq i-1$ 时

$$\begin{aligned} \tau(k) &= \tau\sigma(k-1) \\ &= \sigma\tau(k-1) \\ &= \tau(k-1) + 1 \end{aligned}$$

于是

$$\tau : \begin{matrix} 1 & 2 & \cdots & i & i+1 & i+2 & \cdots & n \\ n-i+1 & n-i+2 & \cdots & n & 1 & 2 & \cdots & n-i \end{matrix}$$

即 $\tau = \sigma^{n-i}$ ，证毕.

题目 2.1.3. 证明如果一个置换是不相交的等长度的轮换的乘积，那么该置换一定可以写为一个轮换的方幂.

证明 对 $\sigma = C_1 C_2 \cdots C_t$ ，其中 $C_j (1 \leq j \leq t)$ 是长度为 m 的轮换，记

$$C_j = (x_{j,1}, x_{j,2}, \cdots, x_{j,m})$$

以 C_j 为列向量，把 $[tm]$ 的所有元素排成矩阵

$$\begin{pmatrix} x_{1,1} & x_{2,1} & \cdots & x_{t,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{t,2} \\ \vdots & \vdots & & \vdots \\ x_{1,m} & x_{2,m} & \cdots & x_{t,m} \end{pmatrix}$$

按行的方向排列所有元素，得到长度为 tm 的轮换

$$\Gamma = (x_{1,1}, x_{2,1}, \cdots, x_{t,1}, x_{1,2}, \cdots, x_{t,2}, \cdots, x_{1,m}, \cdots, x_{t,m})$$

则

$$\Gamma(x_{j,i}) = \begin{cases} x_{j+1,i} & j < t \\ x_{1,i+1} & j = t \end{cases}$$

即 Γ 让矩阵的元素保持行不变，移动到下一列，若已经是最后一列，则移动到下一行的同一列，于是 Γ^t 将元素保持列不变，移动到下一行，即 $i+1$ 在模 m 的意义上

$$\Gamma^t(x_{j,i}) = x_{j,i+1}$$

这正是 C_j 的作用叠加，因此

$$\Gamma^t = C_1 C_2 \cdots C_t$$

证毕.

题目 2.1.4. 把 S_9 中元素 $(147)(789)(39)(942)(356)$ 写成不相交轮换的乘积.

解 计算得到

$$(147)(789)(39)(942)(356) = (142356)(789)$$

题目 2.1.5. 找出 S_8 中与 $\sigma = (123)(45) \in S_8$ 交换的所有元素.

解 因为不相交的轮换可交换，因此下列集合中的元素都与 σ 可交换：

$$\{(123)^a(45)^b\tau : a \in \{0,1,2\}, b \in \{0,1\}, \tau \in S_{\{6,7,8\}}\}$$

共有 36 个.

下证上面列出的就是全部和 σ 可交换的元素.

对满足 $\sigma\tau = \tau\sigma$ 的置换 τ ，假设 $\tau(a) = b, a \in \{1,2,3\}, b \in \{4,5\}$ ，由对称性，不妨设 $\tau(1) = 4$ ，则

$$\tau(2) = \tau(\sigma(1)) = \sigma(\tau(1)) = \sigma(4) = 5$$

$$\tau(3) = \tau(\sigma(2)) = \sigma(\tau(2)) = \sigma(5) = 4$$

$$\tau(1) = \tau(\sigma(3)) = \sigma(\tau(3)) = \sigma(4) = 5$$

与 $\tau(1) = 4$ 矛盾，因此对 $a \in \{1,2,3\}, \tau(a) \notin \{4,5\}$.

假设 $\tau(a) \in \{6,7,8\}, a \in \{1,2,3\}$ ，不妨设 $\tau(1) = 6$ ，则

$$tau(2) = \tau(\sigma(1)) = \sigma(\tau(1)) = \sigma(6) = 6$$

矛盾，因此对 $a \in \{1,2,3\}, \tau(a) \notin \{6,7,8\}$.

于是 $\{\tau(1),\tau(2),\tau(3)\} = \{1,2,3\}$. 于是 τ 的分解式含有 $(123)^a, a \in \{0,1,2\}$.

同理可以得到 $\{\tau(4),\tau(5)\} = \{4,5\}$ ，于是 τ 的分解式含有 $(45)^b, b \in \{0,1\}$. 又因为不相交的轮换交换，因此 $S_{\{6,7,8\}}$ 的任意置换都和 σ 可交换. 证毕.

题目 2.1.6. 设 p 为素数，$\sigma \in S_p$ 不是恒等变换，若 σ^p 为恒等变换，证明 σ 是一个 $p-$ 轮换.

证明 设 $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ ，其中 σ_i 是不相交的轮换，则因为不相交轮换可交换，得到

$$\sigma^p = \sigma_1^p\sigma_2^p\cdots\sigma_k^p = \mathrm{id}_{[p]}$$

则 $\sigma_i^p = \mathrm{id}_{[p]}$.

考虑轮换 $\tau = (a_1a_2\cdots a_m)$ ，则

$$\tau^k(a_i) = a_t \quad t = i + k - \left[\frac{i+k}{m}\right]$$

于是对 σ_i^p 有 $p = ka_i$ ，其中 a_i 是 σ_i 的长度，又因为 p 是质数，因此 $k = p$ 或 $a_i = p$ ，证毕.

题目 2.1.7. 给出交错群 A_5 中置换的型，求 A_5 中与 (12345) 共轭的所有元素，并证明 A_5 中型为 1^12^2 的置换彼此共轭.

证明 A_5 中所有置换的型为

$$5^1 \quad 1^23^1 \quad 1^12^2 \quad 1^5$$

(12345) 的型为 5^1 ，因为在 S_5 中与 (12345) 共轭的充要条件是型为 5^1 ，因此在 A_5 中 $\tau \in A_5$ 与 (12345) 共轭的必要条件是型为 5^1 ，即 τ 是一个 $5-$ 轮换. 且存在 $\sigma \in A_5$ 使得 $\sigma(12345)\sigma^{-1} = \tau$.

任取 $\sigma \in A_5$ ，则

$$\sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))$$

因为 $\sigma \in A_5$ 是一个偶置换，因此 $\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5)$ 是一个偶序列，反过来，对任意一个偶序列 $\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5)$ ，存在一个偶置换 $\sigma \in A_5$ 使得

$$\sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))$$

因此在 A_5 中和 (12345) 共轭的元素为形式上 12345 排列为偶序列的所有 $5-$ 轮换.

同理任取 $\sigma \in A_5$ ，对型为 $1^1 2^2$ 的置换 $(ab)(cd)$ 有

$$\sigma(ab)(cd)\sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))$$

于是对任意两个型为 $1^1 2^2$ 的置换 $(ab)(cd), (mn)(pq)$

1. 若 $\{a,b,c,d\} = \{m,n,p,q\}$ ，则不妨设 $a = m$ ，假设 $b = n$ ，则两个置换相等，因此共轭；否则，不妨设 $b = p$ ，则 $\{c,d\} = \{n,q\}$ ，不妨设 $d = q, c = n$ ，则考虑一个偶置换 $\sigma \in A_5$

   $$\sigma = (acb)$$

   得到

   $$\sigma(ab)(cd)\sigma^{-1} = (ca)(bd)$$

   因此两置换共轭

2. 若 $\{a,b,c,d\} \neq \{m,n,p,q\}$ ，不妨设

   $$\{a,b,c\} = \{m,n,p\} \quad d \neq q$$

   于是 $c \in \{m,n,p\}$ ，假设 $c \neq p$ ，则不妨设 $c = n$ ，则 $m \in \{a,b\}$ ，不妨设 $m = b$ ，则此时 $(mn)(pq) = (bc)(aq)$ ，考虑 $\sigma = (dcbaq) \in A_5$ ，则

   $$\sigma(ab)(cd)\sigma^{-1} = (qa)(bc) = (mn)(pq)$$

   因此两个置换共轭. 若 $c = p$ ，则 $(ab) = (mn)$ ，考虑 $\sigma = (cqd) \in A_5$ ，则

   $$\sigma(ab)(cd)\sigma^{-1} = (ab)(qc) = (mn)(cq)$$

   因此两个置换共轭.

综上，证毕.

题目 2.1.8. 交错群 A_n 中两个型相同的置换是否一定在 A_n 中共轭？

证明 不一定，如 A_4 中的两个型相同的置换 $a = (123), b = (132)$ ，容易得到此时

$$ab = ba = \mathrm{id}_{[4]} \implies b = a^{-1}$$

假设存在 $c \in A_4$ 使得 $cac^{-1} = b = a^{-1}$ ，则

$$aca = c$$

其中

$$c[1,2,3,4] = [c(1), c(2), c(3), c(4)]$$

$$aca[1,2,3,4] = ac[2,3,1,4] = a[c(2), c(3), c(1), c(4)]$$

于是 $a(c(4)) = c(4) \implies c(4) = 4$ ，且

$$[ac(2), ac(3), ac(1)] = [c(1), c(2), c(3)]$$

假设 $c(2) = 1$ ，则 $c(1) = ac(2) = a(1) = 2$ ， $c(3) = ac(1) = a(2) = 3$ ，此时

$$c = (12) \notin A_4$$

假设 $c(2) = 2$ ，则 $c = (13) \notin A_4$ ，假设 $c(2) = 3$ ，同理得到 $c = (23) \notin A_4$ ，因此这样的 c 不存在，即 a, b 不共轭，证毕.

题目 2.1.9. 求正四面体和正十二棱锥的对称群.

解 正四面体对称群为 A_4 （不包括镜面反射）或 S_4 （包括镜面反射）

正十二棱锥对称群为 $\langle\sigma\rangle$ （不包括镜面反射）或 $\{\sigma^s\tau^l : s = 0, 1, \cdots, 11; l = 0, 1\}$ （包括镜面反射）其中 σ 为绕中轴线逆时针旋转 $\dfrac{\pi}{6}$ ， τ 为以 OA_1A_7 平面镜面反射.

题目 2.1.10. 在二面体群 D_4 找 3 个元素 a, b, c 满足 $ab = bc$ 但 $a \neq c$.

解 $D_4 = \{\sigma^s\tau^t : s = 0, 1, 2, 3; t = 0, 1\}$ ，则

$$\sigma(\sigma\tau) = \sigma^2\tau \neq (\sigma\tau)\sigma = \tau$$

题目 2.1.11. 在二面体群 D_4 中找 3 个元素 a, b, c 满足 $ab = bc, a \neq c$.

解 设

$$D_4 = \{r^i s^j : i = 0, 1, 2, 3, j = 0, 1\}$$

其中

$$r^4 = e \quad s^2 = e \quad rs = sr^{-1}$$

则令

$$a = rs \quad b = r \quad c = r^3 s$$

得到

$$ab = rsr = s = r(r^3 s) = bc$$

且 $a \neq c$.

2.2 习题 2.2

题目 2.2.1. $H \subset G$ 非空，在 G 中定义关系 $\sim$

$$a \sim b \iff ab^{-1} \in H$$

证明 $\sim$ 是 G 上的等价关系当且仅当 $H \leq G$.

证明

1. 充分性：若 $H \leq G$ ，则 $e \in H$ ，于是 $a \sim a$ ，满足反身性；且

   $$ab^{-1} \in H \implies (ab^{-1})^{-1} = ba^{-1} \in H$$

   满足对称性；最后

   $$ab^{-1} \in H, bc^{-1} \in H \implies (ab^{-1})(bc^{-1}) = ac^{-1} \in H$$

   满足传递性，证毕.

2. 必要性：若 $\sim$ 是 G 上的等价关系，则 $e = aa^{-1} \in H$ ；对任意 $a \in H$ 有

   $$ae^{-1} \in H \implies a \sim e \implies e \sim a \implies ea^{-1} = a^{-1} \in H$$

   于是对任意 $a \in H, b^{-1} \in H$ ，有

   $$a \sim e, b^{-1} \sim e \implies a \sim b^{-1} \implies ab \in H$$

   证毕.

题目 2.2.2. 考虑整数加法群 $\mathbb{Z}$ ，设 $H \leq \mathbb{Z}$

1. 证明：若 $m, n \in H$ ，则 $\gcd(m, n) \in H$

2. 证明存在整数 $m \in \mathbb{Z}$ 使得 $H = m\mathbb{Z}$

3. 设 $m_1, m_2, \cdots, m_k$ 为两两不同的 k 个非零整数，证明

   $$m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap \cdots \cap m_k\mathbb{Z} = \operatorname{lcm}(m_1, m_2, \cdots, m_k)\mathbb{Z}$$

4. 任取无穷多个两两不同的整数 $\{m_k\}_{k\in\mathbb{N}}$ ，利用 (3) 结论证明

   $$\bigcap_{k\in\mathbb{N}} m_k\mathbb{Z} = \{0\}$$

证明

1. 由 Bezout 定理，存在 $a,b\in\mathbb{Z}$ 使得 $am+bn=\gcd(m,n)\in\mathbb{Z}$，证毕.

2. $H\leq\mathbb{Z}$，则单位元 $0\in H$，若 $H=\{0\}$，则 $m=0$，否则，设 a 为 $H_+=\{h\in H:h>0\}$ 中的最小元素，对任意 $b\in H_+$，有带余除法 $b=na+r,0\leq r<a$，则 $r=b-na\in H$，若 $r\neq 0$，则 $r<a,r\in H_+$，与 a 是 H_+ 中最小元素矛盾，因此对任意 $b\in H_+$ 有 $a\mid b$，又 $a\mathbb{Z}\subset H$，因此 $H=a\mathbb{Z}$.

3. 记要证的等式两边的集合分别为 A,B，则

$$\begin{aligned} a\in A &\iff m_i\mid a,\quad \forall 1\leq i\leq k\\ &\iff \operatorname{lcm}(m_1,m_2,\cdots,m_k)\mid a\\ &\iff a\in B \end{aligned}$$

   证毕.

4. 假设存在 $a\neq 0,a\in\bigcap\limits_{k\in\mathbb{N}}m_k\mathbb{Z}$，不妨设 $a>0$，则

$$\bigcap_{k\in\mathbb{N}}m_k\mathbb{Z}\subset a\mathbb{Z}\cap(a+1)\mathbb{Z}\implies a\in a\mathbb{Z}\cap(a+1)\mathbb{Z}\implies a^2+a\mid a$$

   矛盾.

题目 2.2.3. 设 $n\geq 3$，在对称群 S_n 中令 $\sigma=(12\cdots n),\tau=(12)$，证明 $S_n=\langle\sigma,\tau\rangle$.

证明 显然 $\langle\sigma,\tau\rangle\leq S_n$.

因为任意 S_n 中的置换都可以写成不相交的轮换的乘积，任意轮换又可以分解为对换的乘积，任意对换又可以分解为相邻对换的乘积，因此只需证 σ,τ 可以生成任意相邻对换即可.

考虑 $\sigma^k\tau\sigma^{-k}$，则

	1	2	$\cdots$	$k+1$	$k+2$	$\cdots$	$n-1$	n
σ^{-k}	$n-k+1$	$n-k+2$	$\cdots$	1	2	$\cdots$	$n-k-1$	$n-k$
$\tau\sigma^{-k}$	$n-k+1$	$n-k+2$	$\cdots$	2	1	$\cdots$	$n-k-1$	$n-k$
$\sigma^k\tau\sigma^{-k}$	1	2	$\cdots$	$k+2$	$k+1$	$\cdots$	$n-1$	n

即 $(k+1,k+2)=\sigma^k\tau\sigma^{-k}$，因此任意相邻对换可以被 τ,σ 生成，于是 $S_n\leq\langle\sigma,\tau\rangle$，证毕.

题目 2.2.4. 证明：若 n 为大于 2 的偶数，则 $A_n = \langle (123), (23\cdots n) \rangle$ ；若 n 为大于 2 的奇数，则 $A_n = \langle (123), (12\cdots n) \rangle$.

证明

题目 2.2.5. 考虑 2 阶整系数方阵的集合 $\mathbb{Z}^{2\times 2}$ ，其上运算为矩阵乘法.

1. 证明 $A \in \mathbb{Z}^{2\times 2}$ 可逆当且仅当 $|\det A| = 1$.
2. 记所有满足 $|\det A| = 1$ 的整系数 2 阶方阵构成的集合为 $\mathrm{GL}_2(\mathbb{Z})$ ，证明 $\mathrm{GL}_2(\mathbb{Z})$ 关于矩阵乘法构成群，且该群可以由
$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$
生成.

证明

1. 当 $|\det A| = 1$ 时，即
$$|\det A| = \left| \begin{vmatrix} a & b \\ c & d \end{vmatrix} \right| = |ad - bc| = 1$$
当 $ad - bc = 1$ 时，令
$$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \implies AB = BA = I$$
对 $bc - ad = 1$ 同理.

当 A 可逆时，设
$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad B = \begin{bmatrix} x & y & w \end{bmatrix} \quad AB = BA = I$$
解得
$$\begin{cases} x = -d/(bc - ad) \\ y = b/(bc - ad) \\ z = c/(bc - ad) \\ w = -a/(bc - ad) \end{cases}$$
因为 $x, y, z, w \in \mathbb{Z}$ ，于是
$$yz - xw = \frac{1}{bc - ad} \in \mathbb{Z}$$
于是 $bc - ad = \pm 1$ ，即 $|\det A| = 1$ ，证毕.

2. 因为 $|\det I| = 1$，因此 $I \in \mathrm{GL}_2(\mathbb{Z})$，且 $\forall A \in \mathrm{GL}_2(\mathbb{Z})$，都有 $AI = IA = A$，于是 I 是 $\mathrm{GL}_2(\mathbb{Z})$ 的单位元.

   由上一小问结论，此时 $\forall A \in \mathrm{GL}_2(\mathbb{Z}), A^{-1} \in \mathrm{GL}_2(\mathbb{Z})$.

   对 $\forall A, B \in \mathrm{GL}_2(\mathbb{Z})$，因为 $|AB| = |A||B| = 1$，因此 $AB \in \mathrm{GL}_2(\mathbb{Z})$，又因为矩阵乘法满足结合律，因此 $\mathrm{GL}_2(\mathbb{Z})$ 关于矩阵乘法构成一个群.

   记

$$U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, L = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

   则

$$U^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}, R^k = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}, L^k = \begin{bmatrix} 1 & 0 \\ 0 & (-1)^k \end{bmatrix} \quad k \in \mathbb{Z}$$

   左乘 U^k 表示把矩阵的第二行的 k 倍加到第一行，左乘 $\mathbb{R}^k$ 表示把矩阵第一行的 k 被加到第二行，又因为 $|\det A| = 1$，设

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

   则 $|ad - bc| = 1$，由 Bezout 定理，$(a, c) = 1$，于是由 Euclid 算法，A 在交替左乘 U, R 的整数次之后可以使得

$$P \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

   其中 $P = U^{k_1} R^{t_1} \cdots U^{k_n} R^{l_n}$，此时

$$PA = \begin{bmatrix} 1 & b' \\ 0 & d' \end{bmatrix}$$

   因为左乘 U^k, R^k 行列式不变，于是 $\det PA = \pm 1 \implies d' = \pm 1$.

   若 $d' = 1$，此时 $U^{-b'} PA = I$，若 $d' = -1$，此时 $LU^{b'} PA = I$，于是

$$A = P^{-1} U^{-b'} L^{-1}$$

   证毕.

题目 2.2.6. 已知定义在 $\mathbb{R} \cup \{\infty\}$ 上的函数

$$f(x) = \frac{1}{x}, \quad g(x) = \frac{x-1}{x}$$

考虑这两个函数生成的 $\mathbb{R} \cup \{\infty\}$ 的全变换群 $S_{\mathbb{R} \cup \{\infty\}}$ 的子群 H，其中运算是函数复合，证明 $H \cong S_3$.

证明 注意到

$$f^2 = g^3 = \mathrm{id}_{\mathbb{R}\cup\{\infty\}}$$

$S_3 = \{e, (12), (13), (23), (123), (132)\}$ ，令 $\sigma = (12), \tau = (123)$ ，则

$$\sigma^2 = \tau^3 = e, \quad \tau\sigma = \sigma\tau^{-1} = \sigma\tau^2, \quad \tau^2\sigma = \sigma\tau$$

设 $\varphi(f) = \sigma, \varphi(g) = \tau$ ，因为

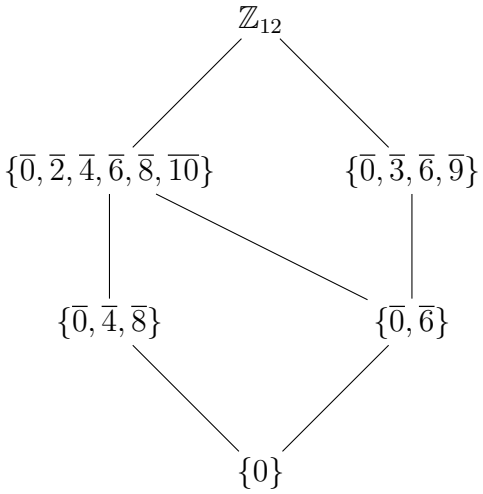
$$f^2 = g^3 = e, \quad gf = fg^{-1} = fg^2, \quad g^2f = fg$$

因此 $H \cong S_3$.

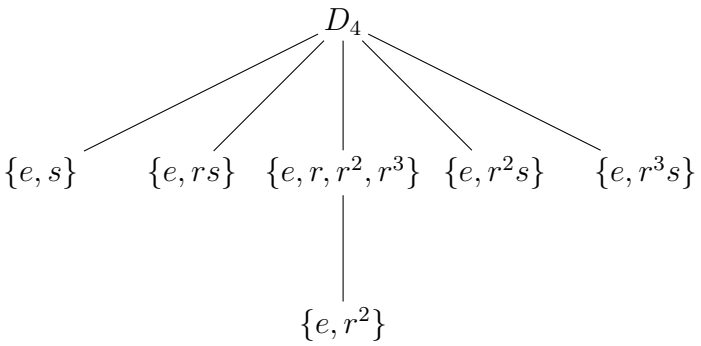
题目 2.2.7. 对有限群 G ，其子群图画法为：图的点是 G 的子群，任给两个不同子群 H, K ，存在连接 H, K 的线段当且仅当 $H < K$ 且不存在其它子群 L 使得 $H < L < K$ ，通常把 H 放在较低的位置.

画出 $\mathbb{Z}_{12}, D_4$ 的子群图.

解 $\mathbb{Z}_{12}$ 的子群图



D_4 的子群图



题目 2.2.8. 设 G 是群，$K, L \leq G$ ，证明 $KL \leq G$ 当且仅当 $KL = LK$.

证明

1. 若 $KL = LK$ ，设 e 为 G 的单位元，因为 $K, L \leq G$ ，因此 $e \in K, e \in L$ ，于是 $e \in KL$ ，即 KL 有单位元.

   对任意 $k_1l_1 \in KL, k_2l_2 \in KL$ ，因为 $KL = LK$ ，因此为 $l_1k_2 \in LK$ ，存在 $k_3l_3 \in KL$ 使得

   $$l_1k_2 = k_3l_3$$

   于是

   $$(k_1l_1)(k_2l_2) = k_1(l_1k_2)l_2 = (k_1k_3)(l_3l_2) \in KL$$

   即 KL 对 G 的运算封闭.

   对任意 $kl \in KL$ ，因为 $KL = LK$ ，因此对 $l^{-1}k^{-1} \in LK$ ，存在 $k'l' \in KL$ 使得

   $$(kl)^{-1} = l^{-1}k^{-1} = k'l' \in KL$$

   因此 KL 的元素都存在逆，综上，$KL \leq G$.

2. 若 $KL \leq G$ ，$\forall lk \in LK, l \in L, k \in K$ ，因为 $K \leq G, L \leq G$ ，于是 $k^{-1}l^{-1} \in KL$ ，又因为 $KL \leq G$ ，于是 $(k^{-1}l^{-1})^{-1} = lk \in KL$ ，因此 $LK \subset KL$.

   对 $\forall kl \in KL$,因为 $KL \leq G$,于是 $(kl)^{-1} = l^{-1}k^{-1} \in KL$,于是存在 $k' \in K, l' \in L$ 使得

   $$k'l' = l^{-1}k^{-1} \implies l'^{-1}k'^{-1} = kl \in lk$$

   因此 $KL \subset LK$ ，综上，证毕.

题目 2.2.9. 证明：$\sigma : G \to G'$ 为同态，则

1. $\sigma(e) = e'$
2. $\sigma(g^{-1}) = \sigma(g)^{-1}, \forall g \in G$
3. $\sigma(H) \leq G', \forall H \leq G$
4. $\sigma^{-1}(H') \leq G, \forall H' \leq \sigma(G)$

证明

1. 对任意 $g \in G$

$$\sigma(g) = \sigma(eg) = \sigma(e)\sigma(g) = \sigma(ge) = \sigma(g)\sigma(e)$$

因此 $\sigma(e) = e'$

2. 对任意 $g \in G$

$$\sigma(e) = \sigma(gg^{-1}) = \sigma(g)\sigma(g^{-1}) = \sigma(g^{-1}g) = \sigma(g^{-1})\sigma(g) = e'$$

因此 $\sigma(g^{-1}) = \sigma(g)^{-1}$

3. 对任意 $\sigma(a), \sigma(b) \in \sigma(H)$

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)\sigma(b)^{-1} \in \sigma(H)$$

证毕

4. 对任意 $\sigma^{-1}(a), \sigma^{-1}(b) \in \sigma(H')$

$$\sigma^{-1}(ab^{-1}) = \sigma^{-1}(a)\sigma^{-1}(b)^{-1} \in \sigma^{-1}(H)$$

证毕.

题目 2.2.10. 确定对称群 S_n 到 2 阶群 μ_2 的所有同态.

解 不妨记 $\mu_2 = \{1, -1\}$，其中 1 是单位元，显然 μ_2 只有平凡子群.

对同态 $\varphi : S_n \to \mu_2$，若 $\varphi(S_n) = \{1\}$，则 φ 平凡地把所有 S_n 中的置换映射为 1 .

若 $\varphi(S_n) = \{1, -1\}$，记 $A_n = \operatorname{Ker}\varphi, B_n = S_n \backslash \operatorname{Ker}\varphi$，则此时存在 $\sigma \in S_n$ 使得 $\varphi(\sigma) = -1$，将 σ 分解成对换 $t_1, \cdots, t_m$ 的乘积，得到

$$\varphi(\sigma) = \varphi(t_1) \cdots \varphi(t_m) = -1$$

则 $t_1, \cdots, t_m$ 中至少一个的像为 -1，不妨设 $\varphi(t_1) = -1$.

因为 S_n 中型相同的置换共轭，因此任意对换 t 都和 t_1 共轭，即存在 $\pi \in S_n$ 使得 $t = \pi t_1 \pi^{-1}$，于是

$$\varphi(t) = \varphi(\pi)\varphi(t_1)\varphi(\pi^{-1})$$

因为 φ 是同态，因此 $\varphi(\pi^{-1}) = \varphi(\pi)^{-1}$，于是 $\varphi(t) = \varphi(t_1)$，因此任意对换 $t \in S_n$ 都有 $\varphi(t) = -1$.

任意置换可以在排除顺序的条件下唯一分解成对换的乘积，因此得到

$$\operatorname{Ker}\varphi = A_n \quad \varphi^{-1}(-1) = S_n \backslash A_n$$

其中 A_n 是 S_n 中所有偶置换构成的集合.

题目 2.2.11. 证明 S_4 的子群 $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ 与 μ_4 不同构.

证明 不妨设 $\mu_4 = \{1, i, -1, -i\}$ ，注意到 $V_4 \backslash \{(1)\}$ 中的元素都是 2 阶，而 $i, -i$ 是 4 阶元素，证毕.

题目 2.2.12. 设 G 为群，G 上的变换 σ 定义为 $\sigma(a) = a^{-1}, \forall a \in G$ ，证明 σ 是 G 的自同构当且仅当 G 是交换群.

证明

1. 充分性：若 G 交换，此时 $\sigma(e) = e$ ，且对任意 $a, b \in G$ 有

$$\sigma(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \sigma(a)\sigma(b)$$

   因此 σ 是 G 的自同态，显然 σ 是双射，证毕.

2. 必要性：假设 G 不交换，则存在 $a, b \in G$ 使得 $ab \neq ba$ ，则

$$\sigma(a^{-1}b^{-1}) = (a^{-1}b^{-1})^{-1} = ba \neq ab = \sigma(a^{-1})\sigma(b^{-1})$$

   与 σ 同态矛盾，证毕.

题目 2.2.13. 求有理数加法群的自同构群.

解 设 $f : \mathbb{Q} \to \mathbb{Q}$ 是同构，则 $f(x + y) = f(x) + f(y), \forall x, y \in \mathbb{Q}$. 于是

$$f(0) = 0 \quad f(-x) = -f(x) \quad \forall x \in \mathbb{Q}$$

于是对任意 $m \in \mathbb{Z}$ 有

$$f(mx) = mf(x) \quad \forall x \in \mathbb{Q}$$

令 $y = \dfrac{x}{m}$ ，则

$$f(my) = f(x) = mf(y) = mf\left(\frac{x}{m}\right) \implies f\left(\frac{x}{m}\right) = \frac{1}{m}f(x), \forall x \in \mathbb{Q}, m \in \mathbb{Z}$$

于是

$$f(tx) = tf(x) \quad \forall t \in \mathbb{Q}, x \in \mathbb{Q}$$

因此 $\mathrm{Aut}(\mathbb{Q}, +) = \{f : f(x) = cx, c \in \mathbb{Q}\}$.

题目 2.2.14. 证明实数加群与正实数乘法群同构.

证明 实数在加法下构成的群记为 $\mathbb{R}$，正实数在乘法下构成的群记为 $\mathbb{R}^+$，则定义 $\sigma:\mathbb{R}\to\mathbb{R}^+$

$$\sigma(a)=e^a\quad a\in\mathbb{R}$$

容易验证这是一个映射，且满足

$$\sigma(0)=1\quad \sigma(a+b)=\sigma(a)\sigma(b)\quad \forall a,b\in\mathbb{R}$$

证毕.

题目 2.2.15. 设 $\sigma:G\to G'$ 为群同态，$H\leq G, K=\operatorname{Ker}\sigma$，证明 $\sigma^{-1}(\sigma(H))=HK$ 且 $HK\leq G$.

证明 对 $\forall g\in\sigma^{-1}(\sigma(H))$，则 $\sigma(g)\in\sigma(H)$，于是存在 $h\in H$ 使得 $\sigma(g)=\sigma(h)$，于是

$$\sigma(h^{-1}g)=\sigma(h^{-1})\sigma(g)=\sigma(h^{-1})\sigma(h)=e$$

因此 $h^{-1}g\in K$，于是 $g=h(h^{-1}g)\in HK$，因此 $\sigma^{-1}(\sigma(H))\subset HK$.

对 $\forall hk\in HK$，则 $\sigma(hk)=\sigma(h)\sigma(k)=\sigma(h)\in\sigma(H)$，于是 $hk^{-1}\in\sigma^{-1}(\sigma(H))$，因此 $HK\subset\sigma^{-1}(\sigma(H))$，因此 $\sigma^{-1}(\sigma(H))=HK$.

设 G,G' 的单位元分别为 e,e'，因为 $H\leq G, K=\operatorname{Ker}\sigma$，则 $e\in H, e\in K$，于是 $e\in HK$.

对 $\forall hk\in HK$，则 $\sigma(k^{-1}h^{-1})=\sigma(h^{-1})\in\sigma(H)$，于是 $k^{-1}h^{-1}\in\sigma^{-1}(\sigma(H))=HK$.

对 $\forall h_1k_1\in HK, h_2k_2\in HK$，则 $\sigma(h_1k_1h_2k_2)=\sigma(h_1h_2)\in\sigma(H)$，于是 $h_1k_1h_2k_2\in\sigma^{-1}(\sigma(H))=HK$，综上，$HK\leq G$.

2.3 习题 2.3

题目 2.3.1. 群 S_5 中元素的阶有哪几种？S_{10} 中元素的阶最大是多少？

解 把 S_5 按照型分类，则

1^5	1
1^32	2
1^23	3
14	4
12^2	2
23	6
5	5

因此全部的阶为 $1,2,3,4,5,6$.

同理尝试得到 S_{10} 的最大阶为 30 .

题目 2.3.2. 证明不存在恰有两个 2 阶元素的群.

证明 假设群 G 存在 $a \neq b$ 使得 $a^2 = b^2 = e$ ，且 $a, b \neq e$ ，记 $r = ab$ ，显然 $ab \neq e$ ，于是 $o(r) \geq 2$ ，考虑 G 的子群 $H = \langle a, b \rangle$ ，因为

$$r^n = e, \quad a^2 = b^2 = e, \quad ara = r^{-1}$$

于是 H 的元素可以写成两类

$$\{r^k a : 0 \leq k \leq n-1\} \quad \{r^k : 0 \leq k \leq n-1\}$$

其中 $(r^k a)^2 = r^k a r^k a = r^k r^{-k} = e$ ，若存在 $r^i a = r^j a$ ，则 $r^{i-j} = e$ ，得到 $i = j$ ，又因为当 n 为偶数时，$(r^{n/2})^2 = e$ ，因此 H 中总是至少有三个阶为 2 的元素，且 $H \subset G$ ，矛盾.

题目 2.3.3. 1. 求出加法群 $\mathbb{Z}_{12}$ 的所有生成元，并确定它的自同态集合 $\mathrm{End}(\mathbb{Z}_{12})$

2. 证明对 $\forall m, , n \in \mathbb{N}_+$ 存在 $\mathbb{Z}_m \to \mathbb{Z}_n$ 的满同态当且仅当 $n \mid m$

证明

1. 生成元即和 12 互素的数，为 $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$.

   下面考虑 $\mathbb{Z}_{12}$ 的任意一个自同态 φ ，显然

   $$\varphi(\overline{0}) = \overline{0} \quad \varphi(\overline{6}) = \overline{6}$$

   又因为若 $a + b = 0$ ，则

   $$\varphi(a) + \varphi(b) = \varphi(a + b) = \overline{0}$$

   因此 φ 在 $\{(1,11), (2,10), (3,9), (4,8), (5,7)\}$ 上是一个置换.

   且 φ 必须把生成元换到生成元. 若 $\varphi(1) = 11$ ，则容易得到

   $$\varphi(x) = 12 - x$$

   若 $\varphi(1) = 1$ ，容易得到 $\varphi(x) = \mathrm{id}_{\mathbb{Z}_{12}}$. 因此自同态集合是 $\{\varphi_0, \mathrm{id}_{\mathbb{Z}_2}\}$ ，其中

   $$\varphi_0(x) = 12 - x$$

2. 若 $n \mid m$ ，不妨设 $m = nk$ ，分别记

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\} \quad \mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

则定义对应关系：

$$\varphi : \mathbb{Z}_m \to \mathbb{Z}_n \quad p \to p - \left[\frac{p}{n}\right] n$$

其中 $\left[\dfrac{p}{n}\right]$ 是不超过 $\dfrac{p}{n}$ 的最大整数. 容易验证

$$\varphi(p+m) = \varphi(p+kn) = \varphi(p)$$

因此这是一个良定义的映射. 且

$$\varphi(p+q) = p+q - \left[\frac{p+q}{n}\right] n = p - \left[\frac{p}{n}\right] n + q - \left[\frac{q}{n}\right] n = \varphi(p) + \varphi(q)$$

在 $\mathbb{Z}_n$ 上显然成立（因为 $n \mid \left[\dfrac{p+q}{n}\right] n - \left[\dfrac{q}{n}\right] n$ ）于是这是一个满同态.

若存在满同态 $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$ ，则此时 $\varphi(\mathbb{Z}_m) = \mathbb{Z}_n$ ，由同态基本定理

$$\mathbb{Z}_m / \operatorname{Ker}\varphi \cong \mathbb{Z}_n \implies \frac{m}{|\operatorname{Ker}\varphi|} = n$$

证毕.

题目 2.3.4. 证明：若 $\exp(G) = 2$ ，则 G 为交换群.

证明 此时 $\forall g \in G, g^2 = e \implies g = g^{-1}$ ，则对任意 $a, b \in G$ 有

$$(ab)^2 = e \implies abab = e \implies ba = a^{-1}b^{-1} = ab$$

证毕.

题目 2.3.5. 证明偶数阶有限群必存在二阶元素.

证明 假设群 G 不存在二阶元素，则

$$g \neq g^{-1} \quad \forall g \in G, g \neq e$$

于是所有不为 e 的元素可以分别二元组 $\{(g_1, g_1^{-1}), (g_2, g_2^{-1}), \cdots\}$ ，此时 $|G|$ 显然是奇数，矛盾，证毕.

题目 2.3.6. G 为群，$a, b \in G$ ，证明 $o(ab) = o(ba)$.

证明 若 $(ab)^k = e$，则 $a((ba)^{k-1}b) = e$，于是

$$(ba)^{k-1}ba = (ba)^k = e$$

同理若 $(ba)^m = e$，则 $(ab)^m = e$，证毕.

题目 2.3.7. 在群 $\mathrm{GL}_2(\mathbb{Q})$ 中令

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

计算 $o(A), o(B), o(AB)$.

解 计算得到

$$o(A) = 3 \quad o(B) = 3 \quad o(AB) = +\infty$$

题目 2.3.8. G 是交换群，证明 G 中所有有限阶元素构成 G 的一个子群.

证明 记 G' 是 G 中所有有限阶元素构成的集合. 若 G 是有限群，则 $G' = G$，结论显然.

对 $\forall a, b \in G'$，设 $o(a) = m, o(b) = n$，则 $(ab)^{mn} = a^m b^n = e$，证毕.

题目 2.3.9. 设 G 只有有限个子群，证明 G 是有限群.

证明 假设 G 是无限群，若 G 中存在无限阶的元素 g，则

$$G_n = \{e, g^n, g^{2n}, \cdots\}$$

是 G 的一个子群，显然这样的子群有无穷多个，矛盾，因此 G 的所有元素都是有限阶元素. 任取 $a \in G, a \neq e$，则 $G_1 = \{e, a, \cdots, a^{o(a)-1}\}$ 是一个 G 的子群. 在 $G - G_1$ 中任选 b，则 $G_2 = \{e, b, \cdots, b^{o(b)-1}\}$ 是 G 的一个子群，因为 G 是无限群，因此这样的子群有无穷多个，矛盾，因此 G 是有限群. [1]

题目 2.3.10. 证明 A_4 没有 6 阶子群.

[1] 所有元素的阶都有限的群也可以是无限群，如

$$G = \{e^{2i\pi\theta} : \theta \in \mathbb{Q}\}$$

对乘法构成群，显然是无限群，且每个元素的阶都有限.

证明 下证 6 阶群只有两种结构：6 阶循环群或和 $S_3 \cong D_3$ 同构.

若 6 阶群 H 不是循环群，此时 H 的非单位元元素的阶为 2 或 3 . 假设 H 不存在 3 阶元素，若 $H = \langle e, a, b\rangle, a \neq b$ ，则

$$H = \{e, a, b, ab\}$$

其中 $(ab)^2 = e \implies ab = ba$ ，此时 H 是 4 阶元素，因此存在 $c \in H$ ，其中 c 和上述 4 个元素都相等，此时

$$H = \{e, a, b, c, ab, ac, bc\}$$

与 H 是 6 阶群矛盾，因此 H 中存在 3 阶元素. 容易验证此时只有 D_3 同构才能构成群.

显然 A_4 不是循环群. 考虑 A_4 中的二阶元素

$$(12)(34) \quad (13)(24) \quad (14)(23)$$

任意两个不同元素相乘得到另一个，而对 D_3 的二阶元素

$$s \quad rs \quad r^2 s$$

其中任意两个不同元素相乘得到一个三阶元素，因此 A_4 也不存在和 D_3 同构的子群，证毕.

题目 2.3.11. g 是群 G 中的 rs 阶元素，其中 $\gcd(r, s) = 1$ ，证明存在 $a, b \in G$ 使得 $g = ab, o(a) = r, o(b) = s$ ，且 a, b 都是 g 的幂.

证明 由 Bezout 定理，存在整数 m, n 使得

$$mr + ns = 1$$

令 $a = g^{ns}, b = g^{mr}$ ，显然 $g = ab$.

若 $\gcd(n, r) = p > 1$ ，则 $p \mid 1$ 矛盾，因此 $\gcd(n, r) = \gcd(m, s) = 1$ ，于是

$$o(a) = o(g^{ns}) = \frac{o(g)}{\gcd(o(g), ns)} = \frac{rs}{\gcd(rs, ns)} = r$$

同理 $o(b) = s$ ，证毕.

题目 2.3.12. $\sigma \in S_n$ ，σ 的阶为素数 p ，证明 σ 是若干个互不相交的长为 p 的轮换之积.

证明 因为 σ 可以不计顺序唯一分解为不相交轮换的乘积，设

$$\sigma = \tau_1\tau_2\cdots\tau_m$$

其中 τ_i 是不相交的轮换，则又因为不相交的轮换可交换，于是

$$e = \sigma^p = \tau_1^p\tau_2^p\cdots\tau_m^p$$

其中 τ_i^p 是不相交轮换的乘积，因为 e 的唯一分解是 e ，于是 $\tau_i^p = e$ ，又因为 p 是素数，因此 $o(\tau_i) = p$ ，证毕.

题目 2.3.13. G 为群，$g \in G$ ，正整数 $k, o(g)$ 互素，证明 $x^k = g$ 在 $\langle g\rangle$ 中恰有一个解.

证明 因为 $k, o(g)$ 互素，则存在整数 m, n 使得

$$mk + no(g) = 1$$

则令 $x = g^m$ ，得到 $x^k = g^{mk} = g$. 假设 (m_0, n_0) 是上述方程的一组解，则显然

$$\{(m, n) : m = m_0 + to(g), n = n_0 - tk, t \in \mathbb{Z}\}$$

于是 $\{m : m = m_0 + to(g), t \in \mathbb{Z}\}$ 中有且仅有一个在 $[0, o(g)]$ 区间内，即题目要求的唯一解.

题目 2.3.14. 证明有理数加法群的任意有限生成子群都是循环群.

证明 任取一个 $(\mathbb{Q}, +)$ 的有限生成子群

$$S = \left\langle \frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots, \frac{p_n}{q_n} \right\rangle \quad \gcd(p_i, q_i) = 1$$

记 $d = \mathrm{lcm}(q_1, q_2, \cdots, q_n)$ ，则存在 k_i 使得

$$\frac{p_i}{q_i} = \frac{p_i k_i}{d}$$

记 $p_i k_i = t_i$ ，则 $\dfrac{p_i}{q_i} = \dfrac{t_i}{d}$. 于是

$$S = \sum_{i=1}^{n} z_i \frac{t_i}{d} = \frac{1}{d}\sum_{i=1}^{n} z_i t_i \quad z_i \in \mathbb{Z}$$

令 $g = \gcd(t_1, t_2, \cdots, t_n)$ ，由 Bezout 定理，存在整数 a_i 使得

$$a_1 t_1 + a_2 t_2 + \cdots + a_n t_n = g$$

于是

$$\frac{g}{d}=\sum_{i=1}^{n}a_i\frac{t_i}{d}\in S$$

又因为对任意 $\sum_{i=1}^{n}z_it_i$ ，显然它都是 g 的倍数，因此任意 S 的元素都是 $\frac{g}{d}$ 的倍数，于是

$$S=\left\langle\frac{g}{d}\right\rangle$$

证毕.

题目 2.3.15. 设 G 是有限生成的交换群，若 G 的每个生成元的阶都有限，证明 G 是有限群.

证明 设 $G=\langle a_1,a_2,\cdots,a_n\rangle$ ，其中 $o(a_i)=m_i\in\mathbb{Z}$. 因为 G 是交换群，则对任意 $g\in G$ ，有

$$g=a_1^{b_1}a_2^{b_2}\cdots a_n^{b_n}\quad b_i\leq m_i$$

因此 G 是有限群，证毕.

题目 2.3.16. 设 $H\leq G,g\in G$ ，若 $o(g)=n,g^m\in H$ 且 $\gcd(n,m)=1$ ，证明 $g\in H$.

证明 由 Bezout 定理存在整数 p,q 使得

$$pn+qm=1$$

则 $(g^m)^q=g\in H$ ，证毕.

题目 2.3.17. 设 p 为奇素数，m 为正整数，证明 $U(p^m)$ 为循环群，若 $p=2$ ，结论是否正确？

证明

题目 2.3.18. 设 G 为 n 阶循环群，m 为正整数，求 $x^m=e$ 在 G 中解的个数.

解 设 $G=\langle g\rangle,x=g^t,0\leq t<n$ ，即求

$$n\mid tm\quad 0\leq t<n$$

的解的个数. 记 $d=\gcd(n,m)$ ，则 $m=m'd,n=n'd$ ，其中 $\gcd(m',n')=1$ ，于是

$$n\mid tm\iff n'\mid tm'\iff n'\mid t$$

则

$$k=0,n',\cdots,(d-1)n'$$

共有 d 个，因此解的个数为 $\gcd(n,m)$.

题目 2.3.19. 设 G 为循环群，分别就 G 无限或有限的情形给出 G 的自同态环. （由此也可以得到 G 的自同构群）

解 自同态环是针对加法交换群考虑的.

当 G 是无限群时，设 $G = \langle 0, g, 2g, \cdots \rangle$. 此时 G 的自同态由生成元的像完全决定，于是对任意 $m \in \mathbb{Z}$

$$\varphi(mg) = m\varphi(g) = m(kg) = (km)g$$

因此自同态环

$$\mathrm{End}(G) \cong \mathbb{Z}$$

自同构群 $\mathrm{Aut}(G)$ 即 $\mathrm{End}(G)$ 的单位群，于是

$$\mathrm{Aut}(G) \cong \{\pm 1\}$$

当 G 是有限群时，设 $G \cong \mathbb{Z}/n\mathbb{Z}$ ，同样取生成元 g 且 $ng = 0$ ，任意同态 φ 由

$$\varphi(g) = ag \quad 0 \leq a \leq n-1$$

决定，容易得到自同态环

$$\mathrm{End}(G) \cong \mathbb{Z}/n\mathbb{Z}$$

因此自同构群

$$\mathrm{Aut}(G) \cong U(n) = (\mathbb{Z}/n\mathbb{Z})^{\times}$$

题目 2.3.20. 求二面体群 D_4 的自同构群.

解 二面体群

$$D_4 = \{r^i s^j : i = 0, 1, 2, 3; j = 0, 1\}$$

其中

$$r^4 = e \quad s^2 = e \quad rs = sr^{-1}$$

其中 r, r^3 是 4 阶元素，r^2, rs, r^2s, r^3s 是 2 阶元素. 显然同构保持元素的阶，因此

$$\{\varphi(r), \varphi(r^3)\} = \{r, r^3\}$$

若 $\varphi(r) = r, \varphi(r^3) = r^3$ ，则 $\varphi(r^2) = r^2$. 因为 $\varphi(s)$ 决定 φ ，讨论得到

$$\varphi_1(s) = s \quad \varphi_2(s) = rs \quad \varphi_3(s) = r^2s \quad \varphi_4(s) = r^3s$$

都是自同构.

若 $\varphi(r)=r^3,\varphi(r^3)=r$ ，则 $\varphi(r^2)=r^2$ ，此时

$$\varphi_5(s)=s \quad \varphi_6(s)=rs \quad \varphi_7(s)=r^2s \quad \varphi_8(s)=r^3s$$

也都是自同构，令

$$\psi: D_4\to \mathrm{Aut}(D_4) \quad r^is^j\to \varphi_{i+4j} \quad i=0,1,2,3; j=0,1$$

容易验证这是一个同构，因此

$$\mathrm{Aut}(D_4)\cong D_4$$

题目 2.3.21. 举例说明不同构的群可以有同构的自同构群.

解 考虑循环群 C_3,C_4 的自同构群. 因为循环群的同构必须把生成元对应到生成元，于是

$$\mathrm{Aut}(C_3)=\{\varphi(g)=g,\varphi(g)=g^2\} \quad \mathrm{Aut}(C_4)=\{\varphi(g)=g,\varphi(g)=g^3\}$$

二者都同构 C_2 .

题目 2.3.22. 设 G 是群，对任意正整数 k ，定义 $G^k=\{g^k:g\in G\}$ ，证明：

1. 若 G 交换，则 $G^k\leq G$.
2. G 是循环群当且仅当 G 的任意子群都是某个 G^k .

证明

1. 任取 $a^k,b^k\in G^k,a,b\in G$ ，则因为 G 交换，得到

   $$a^kb^k=(ab)^k\in G^k$$

   证毕.

2. 充分性：若 G 的任意子群都是某个 G^k ，则存在 n 使得 $G^n=\{e\}\leq G$ ，于是 G 的元素的阶不超过 n 且是 n 的因子. 设 $g\in G$ 是最大阶元素，假设 $o(g)=r<n$ ，

   必要性：若 G 是循环群，设生成元为 g ，则对任意 $H\leq G$ ，记 H 中正数幂次最小的元素为 g^k ，则 $\langle g^k\rangle\leq H$. 假设存在 $g^t\in H$ 使得 $k\not| t$ ，则由带余除法

   $$t=kq+r \quad 0<r<k$$

   于是

   $$g^t\cdot g^{-kq}=g^r\in H$$

   与 k 是正数幂次最小的元素矛盾，因此 $H\leq\langle g^k\rangle$ ，证毕.

2.4 习题 2.4

题目 2.4.1. 设 X 是所有实函数构成的集合，对任意 $a \in \mathbb{R}^*, f(x) \in X$ ，证明

$$a \circ f(x) = f(ax)$$

给出实数域的乘法群 $\mathbb{R}^*$ 在集合 X 上的作用.

证明 乘法群 $\mathbb{R}^*$ 的单位元是 1 ，对任意 $f(x) \in X$ 有

$$1 \circ f(x) = f(x)$$

对任意 $a, b \in \mathbb{R}^*$ ，有

$$a \circ (b \circ f(x)) = a \circ f(bx) = f(abx) = ab \circ f(x)$$

证毕.

题目 2.4.2. 设 $\mathscr{H}$ 为上半复平面 $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ ，对 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ 和 $z \in \mathscr{H}$ ，令

$$\gamma \circ z = \frac{az + b}{cz + d}$$

证明这是群 $\mathrm{SL}_2(\mathbb{R})$ 在集合 $\mathscr{H}$ 上的一个作用，并求该作用的轨道个数.

证明 $\mathrm{SL}_2(\mathbb{R})$ 的单位元是 E ，则对 $\forall z \in \mathscr{H}$ 有 $E \circ z = z$. 对任意 $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{R})$ ，有

$$\begin{aligned} \gamma_1 \circ (\gamma_2 \circ z) &= \gamma_1 \circ \frac{a_2 z + b_2}{c_2 z + d_2} \\ &= \frac{a_1 \cdot \dfrac{a_2 z + b_2}{c_2 z + d_2} + b_1}{c_1 \cdot \dfrac{a_2 z + b_2}{c_2 z + d_2} + d_1} \\ &= \frac{(a_1 a_2 + b_1 c_2) z + (a_1 b_2 + b_1 d_2)}{(a_2 c_1 + c_2 d_1) z + (b_2 c_1 + d_1 d_2)} \\ &= \gamma_1 \gamma_2 \circ z \end{aligned}$$

证毕.

对任意 $x + iy \in \mathscr{H}$ ，因为

$$\gamma = \begin{bmatrix} \sqrt{y} & \dfrac{x}{\sqrt{y}} \\ 0 & \dfrac{1}{\sqrt{y}} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R}) \quad \gamma \circ i = x + iy$$

于是 $z \in O_i, \forall z \in \mathscr{H}$ ，因此 $\mathscr{H}$ 只有一个轨道.

题目 2.4.3. 设 G 为群，证明 G 在自身的共轭作用传递当且仅当 $G=\{e\}$.

证明 充分性显然.

若 G 在自身的共轭作用传递，则任取 $a,b\in G$ ，存在 $g\in G$ 使得

$$b=gag^{-1}$$

令 $a=e$ ，则任取 $b\in G$ 有 $b=gag^{-1}=e$ ，证毕.

题目 2.4.4. 设

$$V=\left\{I=\begin{bmatrix}1&0\\0&1\end{bmatrix},A=\begin{bmatrix}1&0\\0&-1\end{bmatrix},B=\begin{bmatrix}-1&0\\0&1\end{bmatrix},C=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\right\}$$

证明 $V\leq \mathrm{GL}_2(\mathbb{R})$ ，令

$$M=\{(1,0),(1,1),(0,1),(-1,1),(-1,0),(-1,-1),(0,-1),(1,-1)\}$$

是 $\mathbb{R}^2$ 的子集，对任意 $g\in V,\alpha\in M$ ，定义 $\rho(g,\alpha)=\alpha g^T$ ，证明 ρ 是一个群作用，并求该作用下的轨道.

证明 V 的单位元为 I ，对任意 $\alpha\in M$ 有 $\rho(I,\alpha)=\alpha I=\alpha$. 对任意 $X,Y\in V,\alpha\in M$ ，有

$$X\circ(Y\circ\alpha)=X\circ(\alpha Y^T)=\alpha Y^TX^T=\alpha(XY)^T=XY\circ\alpha$$

证毕.

注意到 I,A,B,C 的作用分别是不变、改变第二个分量正负、改变第一个分量正负、改变两个分量正负. 因此共有三个轨道

$$O_1=\{(1,1),(1,-1),(-1,1),(-1,-1)\}$$
$$O_2=\{(0,1),(0,-1)\}\quad O_3=\{(1,0),(-1,0)\}$$

题目 2.4.5. 记 $\mathbb{R}^n$ 的所有 k 维子空间构成的集合为 $\mathrm{Gr}(k,n)$ ，称为 **Grassmann 流形**，对任意 $\varphi\in \mathrm{GL}_2(\mathbb{R}^n),W\in \mathrm{Gr}(k,n)$ ，定义

$$\varphi\circ W=\{\varphi(\alpha):\alpha\in W\}$$

证明这给出了群 $\mathrm{GL}_2(\mathbb{R}^n)$ 在 $\mathrm{Gr}(k,n)$ 上的一个传递作用.

证明 $\mathrm{GL}_2(\mathbb{R}^n)$ 的单位元为 E ，则 $E\circ W=\{E(\alpha):\alpha\in W\}=W$. 对任意 $\varphi_1,\varphi_2\in \mathrm{GL}_2(\mathbb{R}^n)$

$$\varphi_1\circ(\varphi_2\circ W)=\{\varphi_1(\varphi_2(\alpha)):\alpha\in W\}=\varphi_1\varphi_2\circ W$$

因此这是一个群作用，下证传递，即只有一个轨道.

任取 $\alpha, \beta \in W$ ，则 α, β 个存在一组基

$$a_1, a_2, \cdots, a_k \quad b_1, b_2, \cdots, b_k$$

各自拓展为 $\mathbb{R}^n$ 的一组基

$$\{a_1, a_2, \cdots, a_k, p_{k+1}, \cdots, p_n\} \quad \{b_1, b_2, \cdots, b_k, q_{k+1}, \cdots, , q_n\}$$

则令

$$\varphi(a_i) = b_i, i = 1, 2, \cdots, k \quad \varphi(p_j) = q_j, j = k+1, \cdots, n$$

容易验证 $\varphi(\alpha) = \beta$ ，因此该群作用传递.

题目 2.4.6. 1. 证明对任意 $\varphi \in \mathrm{Aut}(S_n)$ ，若对任意对换 $\sigma \in S_n$ 都有 $\varphi(\sigma)$ 仍为一个对换，则 $\varphi \in \mathrm{Inn}(S_n)$.

2. 证明若 $n \neq 2, 6$ ，则对任意 $\varphi \in \mathrm{Aut}(S_n)$ 和对换 $\sigma \in S_n$ 都有 $\varphi(\sigma)$ 是一个对换，并由此证明 $\mathrm{Aut}(S_n) \cong S_n$.

3. 当 $n = 2$ 或 6 时，结论 $\mathrm{Aut}(S_n) \cong S_n$ 是否成立？为什么？

证明

1. 已知两个不同的对换可交换当且仅当它们不相交. 现在考虑集合

$$A = \{(1, j) : j = 1, 2, \cdots, n\}$$

对满足条件的 φ ，则 $\varphi((1, j))$ 仍是一个对换，记

$$\tau_j = \varphi((1, j))$$

其中 φ 是自同构，因此保持可交换性. 因为对任意 $(1, i), (1, j), i \neq j$ ，二者不可交换，于是 τ_i, τ_j 也不可交换，即 τ_i, τ_j 恰有一个公共的端点. 于是

$$\tau_2, \tau_3, \cdots, \tau_n$$

给出了 $n-1$ 个二元集合，它们两两有公共点，容易验证当 $n \geq 5$ 时，这 $n-1$ 个二元集合一定有一个公共点，不妨设为 p ，于是

$$\tau_j = (p, \pi(j))$$

令 $\pi(1)=p$，则此时 $\pi\in S_n$. 于是

$$\varphi((1,j))=(\pi(1),\pi(j))$$

因为

$$(ij)=(1i)(ij)(1i)$$

于是

$$\varphi((ij))=(\pi(i)\pi(j))$$

则

$$\varphi((ij))=\pi(ij)\pi^{-1}$$

于是 $\varphi\in\mathrm{Inn}(S_n)$，证毕.

2. 对任意对换 $\sigma=(ij)$，考虑其中心化子 $C_{S_n}(\sigma)$. 若 $\varphi\in S_n$ 和 σ 交换，则

$$\varphi=\rho\cdot\pi$$

其中 ρ 关于 (ij)，保持其不变或者交换. π 是 $(3,4,\cdots,n)$ 的任意置换，于是

$$|C_{S_n}(\sigma)|=2(n-2)!$$

因为自同构保持阶和中心化子结构，于是对自同构 φ 和对换 τ 有

$$|C_{S_n}(\varphi(\tau))|=|C_{S_n}(\tau)|=2(n-2)!$$

且 $\varphi(\tau)$ 的阶为 2，于是 $\varphi(r)$ 的型为 $2^\lambda 1^{n-2\lambda}$，则

$$|C_{S_n}(\varphi(\tau))|=2^\lambda\lambda!(n-2\lambda)!$$

解方程

$$2(n-2)!=2^\lambda\lambda!(n-2\lambda)!$$

若 $k=1$，恒成立.

若 $k=2$，得到 $(n-2)(n-3)=4$，无解.

若 $k=3$，得到 $(n,k)=(6,3)$.

当 $k\geq 4$ 时

$$2(n-2)!=2^\lambda\lambda!(n-2\lambda)!\iff\frac{(n-2)!}{(n-2\lambda)!}=2^{\lambda-1}\lambda!$$

固定 λ，当 $n\geq 2\lambda$ 时左边随 n 单调递增，最小值 $(2\lambda-2)!$，容易验证此时等式无解.

综上证毕，由上一小问结论 $\mathrm{Aut}(S_n)\cong\mathrm{Inn}(S_n)\cong S_n$.

3. $n=2$ 时 $S_2 \cong C_2, \mathrm{Aut}(S_2)=\{e\}$ ，二者不同构.

   $n=6$ 时，把对换映射到三对换（三个不相交的对换的乘积）是一个 S_6 的外自同构，因此结论不成立.

2.5 习题 2.5

题目 2.5.1. 设 $\mathbb{R}^+$ 为正实数乘法群，求 $\mathbb{R}^+$ 在实数域乘法群 $\mathbb{R}^*$ 中的指数.

解 对 $a\mathbb{R}^+, a\in\mathbb{R}^*$ ，当 $a>0$ 时 $a\mathbb{R}^+=\mathbb{R}^+$ ，当 $a<0$ 时 $a\mathbb{R}^+=\{-g:g\in\mathbb{R}^+\}$ ，因此指数为 2 .

题目 2.5.2. 证明不存在恰有两个指数为 2 的子群的群.

证明 假设 $H\leq G$ 的指数为 2 ，则显然两个左陪集为

$$g_1H, g_1\in H \quad g_2H, g_2\notin H$$

两个右陪集为

$$Hg_1, g_1\in H \quad Hg_2, g_2\notin H$$

于是

$$gH=Hg$$

再证明一个引理：

引理 2.5.1 (四阶群的结构)**.** 四阶群一定是循环群或者同构于 $\mathbb{Z}_2\times\mathbb{Z}_2$.

证明 假设四阶群 G 存在 $g\in G$ 使得 $o(g)=4$ ，则 $G=\langle g\rangle$ 是循环群. 否则，所有非单位元的阶为 2 ，任取 $a,b\in G, a,b\neq e$ ，且 $a\neq b$ ，则 $ab\neq e$ ，于是 $o(ab)=e$ ，即

$$(ab)^2=abab=e \implies ab=(ab)^{-1}=ba$$

于是 $G=\{e,a,b,ab\}\cong\mathbb{Z}_2\times\mathbb{Z}_2$. 证毕

假设 H,K 是 G 的两个不同的指数为 2 的子群，则

$$gH=Hg \quad gK=Kg$$

令 $L=H\cap K$ ，则 $L\neq H, L\neq K$. 于是

$$[H:L]>1 \implies [H:L]\geq 2$$

则

$$[G:L]=[G:H][H:L]\geq 4$$

又因为

$$|HK|=\frac{|H||K|}{|H\cap L|}=\frac{|G|^2}{4|L|}\leq |G|$$

于是 $|G|\leq 4|L|$ ，于是 $[G:L]\leq 4$ ，即 $[G:L]=4$ ，且

$$[H:L]=[K:L]=2$$

此时 G/L 是 4 阶群，且 $H/L, K/L$ 都是 G/L 的二阶子群. 而四节循环群只有一个二阶子群，因此 G/L 是 Klein 四元群，有三个二阶子群，于是此时 G/L 存在另一个二阶子群 M/L ，则 M 是 G 的第三个指数为 2 的群，矛盾.

题目 2.5.3. 设 G 为群，$H,K\leq G$ ，证明 $H\cap K$ 的任意左陪集都是 H 的一个左陪集和 K 的一个左陪集的交.

证明 结论显然.

题目 2.5.4. 设 G 为群，$H,K\leq G$ 且 $[G:H],[G:K]$ 均有限，证明 $[G:H\cap K]$ 有限.

证明 因为

$$[G:H\cap K]\leq [G:H][G:K]$$

显然.

题目 2.5.5. 设 G 为群，$H,K\leq G, a,b\in G$ ，证明若 $Ha=Kb$ ，则 $H=K$.

证明 因为 $a=ea\in Ha=Kb$ ，则存在 $k\in K$ 使得 $a=kb$. 任取 $h\in H$ ，则存在 $k_1\in K$ 使得

$$ha=k_1b\implies hkb=k_1b\implies h=k_1k^{-1}\in K$$

于是 $H\leq K$ ，同理 $K\leq H$ ，证毕.

题目 2.5.6. 设 $H=\{z\in\mathbb{C}:|z|=1\}$ ，给出 H 在群 $\mathbb{C}^*$ 中的左陪集的几何解释.

解 对 $a\in\mathbb{C}^*$ ，左陪集 aH 是以 $|a|$ 为半径，以 $z=0$ 为圆心的圆.

题目 2.5.7. 设 H,K 是 G 的两个子群，对 $g\in G$ ，集合

$$HgK=\{hgk:h\in H,k\in K\}$$

称为 G 关于群 H,K 的一个双陪集，证明：

1. G 可以写成 G 关于子群 H, K 的双陪集的不交并；

2. 若 H, K 均有限，则

$$|HgK| = |H|[K : K \cap g^{-1}Hg] = |K|[H : H \cap gKg^{-1}]$$

证明

1. 在 G 上定义关系

$$aRv = b \iff \exists h \in H, k \in K, s.t.\ a = hbk$$

下证 R 是等价关系：

(a) 因为 $e \in H, e \in K$ ，因此 aRa ，有反身性

(b) 若 aRb, bRc ，则存在 $h_1, h_2 \in H, k_1, k_2 \in K$ 使得

$$a = h_1bk_1, b = h_2ck_2 \implies a = h_1h_2ck_2k_1 \implies aRc$$

有传递性

(c) 若 aRb ，则存在 $h \in H, k \in K$ 使得 $a = hbk$ ，则

$$b = h^{-1}ak^{-1} \implies bRa$$

有对称性

综上 R 是等价关系，证毕.

2. 分解

$$HgK = \bigcup_{k \in K} Hgk$$

下证

$$Hgk = Hgk' \iff k(k')^{-1} \in K \cap g^{-1}Hg$$

若 $Hgk = Hgk'$ ，则存在 $h \in H$ 使得 $hgk' = gk$ ，于是

$$g^{-1}hg = k(k')^{-1} \implies k(k')^{-1} \in K \cap g^{-1}Hg$$

若 $k(k')^{-1} \in K \cap g^{-1}Hg$ ，则 $k(k')^{-1} = g^{-1}hg$ ，得到

$$gk = hgk' \implies Hgk = Hgk'$$

因此

$$|HgK| = |H| \cdot [K : K \cap g^{-1}Hg]$$

又因为

$$[K : K \cap g^{-1}Hg] = \frac{|K|}{|K \cap g^{-1}Hg|}$$

其中

$$|K \cap g^{-1}Hg| = |g(K \cap g^{-1}Hg)g^{-1}| = |H \cap gKg^{-1}|$$

证毕.

2.6 习题 2.6

题目 2.6.1. 设 $G \leq S_n$ ，证明：

1. $G \cap A_n \leq G$
2. 若 G 中有奇置换，则 G 中奇偶置换的个数相等.

证明

1. 偶置换的复合与逆都是偶置换，结论显然.
2. 设 $\sigma \in G$ 是奇置换，则对任意 $\tau \in G \cap A_n$ ，有 $\sigma\tau$ 是奇置换，且

   $$\{\sigma\tau : \tau \in G \cap A_n\}$$

   互不相同. 因此偶置换的个数不超过奇置换的个数. 对任意的奇置换 $\pi \in G$ ，有 $\sigma\pi$ 是偶置换，且

   $$\{\sigma\pi : \pi \in G \cap (S_n \backslash A_n)\}$$

   互不相同，因此奇置换的个数不超过偶置换的个数，证毕.

题目 2.6.2. 设 n 为奇数，G 为 $2n$ 阶群，证明 G 有指数为 2 的子群.

证明 因为 $[G : H] = \dfrac{|G|}{|H|}$ ，因此只需证 G 有 n 阶子群.

考虑映射

$$f_g : G \to G \quad x \mapsto gx \quad \forall g \in G$$

则 f_g 是 G 上的置换. 在对 G 的所有元素标号的视角下，可以定义 f_g 的奇偶性. 记所有使得 f_g 是偶置换的 g 构成的集合为 G_0 . 则因为

$$f_{g_1 g_2} = f_{g_1} f_{g_2}$$

且偶置换的复合还是偶置换，且

$$(f_g)^{-1} = f_{g^{-1}}$$

得到 $G_0 \leq G$ ，其单位元是 f_e .

假设 G 中不存在二阶元素，则 $\forall g \in G, g \neq e$ 都有 $g \neq g^{-1}$ ，则 $|G| = 2k+1$ ，矛盾，因此存在 $g_0 \in G$ 且 $o(g_0) = 2$.

接下来考虑 f_{g_0} ，显然 f_{g_0} 是 $(x, g_0 x), \forall x \in G$ 之间的对换，且 $|G| = 2n$ ，其中 n 是奇数，因此 f_{f_0} 是奇数个不相交的对换的乘积，是一个奇置换，于是 $\forall g \in G_0$ ，都有 $f_{g_0 g}$ 是一个奇置换.

因此 f_g 中奇偶置换个数相同，因此

$$|G_0| = \frac{|G|}{2} = n$$

证毕.

题目 2.6.3. 设 $\sigma = (12\cdots n) \in S_n$ ，求 σ 在 S_n 中的中心化子 $C_{S_n}(\sigma)$. 进一步，设 $\sigma \in S_n$ 的型为 $1^{\lambda_1}\cdots n^{\lambda_n}$ ，求 σ 在 S_n 中的中心化子的阶以及和 σ 共轭的置换个数.

解 若 $\tau \in C_{S_n}(\sigma)$ ，则 $\tau\sigma = \sigma\tau \implies \tau\sigma^k = \sigma^k\tau$ ，于是

$$\tau(\sigma^k(1)) = \sigma^k(\tau(1)) \implies \tau(k+1) = \tau(1) + k$$

则 $\tau = \sigma^t$ ，于是

$$C_{S_n}(\sigma) = \{\sigma^0, \sigma^1, \cdots, \sigma^{n-1}\}$$

对型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换 σ ，对每个长度为 i 的轮换，有 i 种新的轮换替代，共有 λ_i 个这样的轮换，因此这里有 $\prod_{i=1}^{n} i^{\lambda_i}$ 种选择. 在同一长度的 λ_i 条轮换之间可以任意置换，这里共线 $\lambda_i!$ ，因此中心化子的阶

$$|C_{S_n}(\sigma)| = \prod_{i=1}^{n}(i^{\lambda_i}\lambda_i!)$$

群 S_n 在 S_n 上的共轭作用下，σ 的共轭类就是轨道 O_σ ，其稳定化子就是中心化子 $C_{S_n}(\sigma)$ ，于是

$$|O_\sigma| = \frac{|S_n|}{|C_{S_n}(\sigma)|} = \frac{n!}{|C_{S_n}(\sigma)|}$$

题目 2.6.4. 设群 G 作用在集合 M 上，定义

$$M_0 = \{x \in M : g \circ x = x, \forall g \in G\}$$

为作用的不动点构成的集合，证明：若 G 为 $p-$ 群，则 $|M| \equiv |M_0| (\mathrm{mod}\, p)$.

证明 设 $|G|=p^k$ ，将 M 分解为轨道的并

$$M=\bigcup_{i=1}^{r}O_{x_i}$$

则

$$|M|=\sum_{i=1}^{r}|O_{x_i}|=\sum_{i=1}^{r}\frac{|G|}{|G_{x_i}|}=p^k\sum_{i=1}^{n}\frac{1}{|G_{x_i}|}$$

若 $|O_{x_i}|=\dfrac{|G|}{|G_{x_i}|}=1$ ，则 $x_i\in M_0$. 若 $|O_{x_i}|=\dfrac{|G|}{|G_{x_i}|}\neq 1$ ，则其是 p 的倍数，因此

$$|M|\equiv|M_0|(\mathrm{mod}\,p)$$

证毕.

题目 2.6.5. 设 H 是有限群 G 的真子群，证明

$$G\neq\bigcup_{g\in G}gHg^{-1}$$

进一步，若 G 为无限群，该结论是否成立？证明或给出反例.

证明 设 H 关于 G 的正规化子为 $N_G(H)$ ，则 H 的共轭子群个数为

$$[G:N_G(H)]$$

对每个共轭子群 gHg^{-1} ，其中有 $|H|-1$ 个非单位元元素，于是

$$\left|\bigcup_{g\in G}gHg^{-1}\right|\leq[G:N_G(H)](|H|-1)+1$$

因为 $H\leq N_G(H)$ ，于是 $[G:N_G(H)]\leq[G:H]$ ，且 $H\neq G$ ，于是 $[G:H]\geq 2$ ，则

$$\left|\bigcup_{g\in G}gHg^{-1}\right|\leq[G:H](|H|-1)+1=|G|-\frac{|G|}{|H|}+1\leq|G|-1$$

因此

$$G\neq\bigcup_{g\in G}gHg^{-1}$$

考虑无限群 $G=\mathrm{GL}_n(\mathbb{C})$ ，令 B 为其中所有可逆上三角形矩阵，则 $B<G$ ，则对 $\forall g\in\mathrm{GL}_n(\mathbb{C})$ ，存在 $x\in\mathrm{GL}_n(\mathbb{C})$ 使得

$$g=xbx^{-1}\quad b\in B$$

于是

$$\mathrm{GL}_n(\mathbb{C})=\bigcup_{x\in\mathrm{GL}_n(\mathbb{C})}xBx^{-1}$$

题目 2.6.6. 写出对称群 S_5 的类方程.

解 S_5 中置换的型有

$$1^5, 2^1 1^3, 2^2 1^1, 3^1 1^2, 3^1 2^1, 4^1 1^1, 5^1$$

相同型的置换共轭，上述共轭类的阶分别为

$$1 \quad 10 \quad 15 \quad 20 \quad 20 \quad 30 \quad 24$$

2.7 习题 2.7

题目 2.7.1. 举例说明若 $H \trianglelefteq K, K \trianglelefteq G$ ，不一定有 $H \trianglelefteq G$.

解 见 2.7.4

题目 2.7.2. 设 G 为群，且 $H, K \trianglelefteq G$ ，证明 $HK \trianglelefteq G$.

证明 由题设条件，对任意 $g \in G, h \in H, k \in K$ 有

$$ghg^{-1} = h_1 \in H \quad gkg^{-1} = k_1 \in K$$

于是

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) = h_1 k_1 \in HK$$

证毕.

题目 2.7.3. 设 S 为群 G 的非空子集，令

$$C_G(S) = \{x \in G : xa = ax, \forall a \in S\} \quad N_G(S) = \{x \in G : xS = Sx\}$$

（称为 S 在 G 的中心化子和正规化子）

1. 证明 $C_G(S), N_G(S)$ 都是 G 的子群
2. 证明 $C_G(S) \trianglelefteq N_G(S)$
3. 设 $n \geq 2$ ，记 $G = \mathrm{GL}_n(\mathbb{R})$ 中上三角形矩阵构成的子群为 B ，上三角形且对角线元素全为 1 的矩阵构成的子群为 U ，证明 $N_G(U) = B, N_G(B) = B$.

证明

1. 对 $\forall x_1, x_2 \in C_G(S)$ ，则 $\forall a \in S$ 有

$$x_1x_2a = x_1ax_2 = ax_1x_2 \implies x_1x_2 \in C_G(S)$$

对 $\forall x \in C_G(S)$ ，则 $\forall a \in S$ 有

$$x^{-1}a = x^{-1}(a^{-1})^{-1} = (a^{-1}x)^{-1} = (xa^{-1})^{-1} = ax^{-1} \implies x^{-1} \in C_G(S)$$

因此 $C_G(S) \leq G$.

对 $\forall x_1, x_2 \in N_G(S)$ ，则对 $\forall a \in S$

$$x_1x_2a = x_1a'x_2 = a''x_1x_2 \in Sx_1x_2 \implies x_1x_2S \subset Sx_1x_2$$

同理有 $Sx_1x_2 \subset x_1x_2S$ ，因此 $x_1x_2 \in N_G(S)$. 对 $\forall x \in N_G(S)$ ，则 $\forall a \in S$

$$x^{-1}a = (a^{-1}x)^{-1} = (xa')^{-1} = a'^{-1}x^{-1} \in Sx^{-1} \implies x^{-1}S \subset Sx^{-1}$$

同理 $Sx^{-1} \subset x^{-1}S$ ，因此 $N_G(S) \leq G$.

2. 先证明 $C_G(S) \leq N_G(S)$ ：显然 $C_G(S) \subset N_G(S)$ ，且由 (1) 得到 $C_G(S)$ 构成群，因此 $C_G(S) \leq N_G(S)$.

对 $\forall x \in N_G(S), \forall y \in C_G(S)$ ，则 $\forall a \in G$ ，有 $x^{-1}ax \in G$ ，于是

$$yx^{-1}ax = x^{-1}axy \implies xyx^{-1}a = axyx^{-1}$$

于是 $xyx^{-1} \in C_G(S)$ ，证毕.

3. 对 $\forall b \in B, u \in U$ ，则因为上三角形矩阵相乘还是上三角形矩阵，且对角元素相乘，于是

$$bub^{-1} \in U$$

因此 $bU = Ub$ ，即 $N_G(U) = B$.

同理得到 $\forall b, b' \in B$ 有 $bb'b^{-1} \in B$ ，即 $N_G(B) = B$ ，证毕.

题目 2.7.4. 考虑二面体群

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

其中 r 为逆时针旋转 $\dfrac{\pi}{2}$ ，s 为关于一条对角线反射，记

$$V = \{e, r^2, s, sr^2\} \quad H = \{e, s\}$$

证明 $V \trianglelefteq D_4, H \trianglelefteq V$ 但 H 不是 D_4 的正规子群.

证明 因为 $rs = sr^{-1}$ ，于是对 $r \in D_4, s \in H$ 有

$$rsr^{-1} = r^2 s \notin H$$

因此 H 不是 D_4 的正规子群.

其余代入验证即证.

题目 2.7.5. 给出二面体群 D_{10} 的全部正规子群.

解 记

$$D_{10} = \{r^i s^j : 0 \leq i \leq 4; j = 0, 1\}$$

其中

$$r^5 = e \quad s^2 = e \quad rs = sr^{-1}$$

平凡地，$\{e\}, D_{10}$ 是 D_{10} 的正规子群. 其次，因为一切指数为 2 的子群都是正规子群，因此旋转子群 $R = \langle r \rangle$ 是正规子群.

下证不存在其它的正规子群. 假设存在不是上述三个的正规子群 $N \trianglelefteq D_{10}$ ，考虑 $N \cap R$. 因为 $R \cong C_5$ ，其只有平凡子群 $\{e\}, R$. 若 $N \cap R = \{e\}$ ，则 N 一定包含 $r^k s$ ，由正规性，得到

$$r(r^k s)r^{-1} = r^{k+2} s$$

因为 $\gcd(2, 5) = 1$ ，于是由上述的共轭可以得到 $s, rs, \cdots, r^4 s$ ，其中

$$(rs) \cdot (r^2 s) = r^{-1}$$

与 $N \cap R = \{e\}$ 矛盾，因此 $N \cap R = R$ ，即 $R \subset N$. 因为 $N \neq R$ ，因此 N 一定包含 $r^k s$ ，同理得到此时 N 会包含 $s, rs, \cdots, r^4 s$ ，则 $N = D_{10}$ ，矛盾.

综上，D_{10} 的全部正规子群为 $\{e\}, D_{10}, \langle r \rangle$.

题目 2.7.6. 设 G 为一个群，H 为 G 的一个阶为 m 的子群.

1. 证明：若 H 是 G 的唯一阶为 m 的子群，则 $H \trianglelefteq G$.

2. 如果 $H \trianglelefteq G$ ，H 是否为 G 的唯一阶为 m 的子群？证明或给出反例.

证明

1. 对 $\forall g \in G$ ，考虑 H 的共轭子群 gHg^{-1} ，显然 $gHg^{-1} \leq G$ ，且

$$|gHg^{-1}| = |H| = m$$

因此 $gHg^{-1} = H$ ，即 $H \trianglelefteq G$ ，证毕. [2]

[2]事实上，若 H 是唯一 m 阶子群，则 H 是特征子群，即对任意 $\varphi \in \mathrm{Aut}(G), \varphi(H) = H$.

2. 不成立，考虑 Klein 四元群 $V_4 = C_2 \times C_2 = \{e, a, b, c\}$ ，其中 $a^2 = b^2 = c^2 = e$ ，则

$$\langle a \rangle \quad \langle b \rangle \quad \langle c \rangle$$

都是 V_4 的正规子群，且都是二阶子群.

题目 2.7.7. 设有限群 G 在集合 M 上的作用传递，$N \trianglelefteq G$ ，证明 N 在 M 的同样作用下每个轨道长度均相等.

证明 任取 $x \in M$ ，在 N 作用下的轨道

$$O_x = \{n \circ x : n \in N\}$$

对 $\forall g \in G$ ，考虑 $g \circ (O_x)$ ，则

$$\begin{aligned} g \circ (O_x) &= \{g \circ (n \circ x) : n \in N\} = \{gn \circ x : n \in \mathbb{N}\} \\ &= \{(gng^{-1}g) \circ x : n \in N\} \end{aligned}$$

因为 $\{gng^{-1} : n \in N\} = N$ ，于是

$$g \circ (O_x) = N \circ (g \circ x)$$

则 g 的作用下 O_x 被映射到 $O_{g \circ x}$ ，因此在 N 的作用下

$$|O_x| = |O_{g \circ x}|$$

因此 G 在 M 上传递，因此对任意 $x' \in N$ 存在 $g \in G$ 使得 $x' = g \circ x$ ，因此在 N 的作用下每个轨道长度相等.

题目 2.7.8. 设 G 是有限群，$N \trianglelefteq G$ 且 $|N|, |G/N|$ 互素，对 $a \in G$ ，若 $o(a) \mid |N|$ ，证明 $a \in N$.

证明 设 $o(a) = m$ ，对商群运算 $(aN)^m = N$ ，于是 $o(aN) \mid m$. 又因为 G/N 是有限群，于是

$$o(aN) \mid G/N$$

假设因为 $m = o(a) \mid |N|$ ，且 $|N|, |G/N|$ 互素，于是

$$\gcd(|G/N|, m) = 1$$

于是 $o(aN) = 1$ ，因此 $aN = N$ ，即 $a \in N$. 证毕.

题目 2.7.9. 设 G 为一个群，证明 G 的任意指数有限的子群都包含一个 G 的指数有限的正规子群.

证明 对 $H \leq G$，设 $[G:H] = |G/H| = n$. 考虑 G 在陪集集合 G/H 上的左乘作用，对 $g \in G, xH \in G/H$ 定义

$$g \circ (xH) = (gx)H$$

这是一个 G/H 上的置换作用，于是得到一个群同态

$$\varphi : G \to S_{G/H} \cong S_n$$

定义

$$K := \operatorname{Ker}\varphi = \{g \in G : g \circ (xH) = xH, \forall xH \in G/H\}$$

因为 $gxH = xH \iff x^{-1}gx \in H$，对 $\forall x \in G$ 成立，于是

$$K = \bigcap_{g \in G} gHg^{-1}$$

由 2.7.2 得到同态核是正规子群，因此 K 是 G 的正规子群. 且由同态基本定理得到

$$G/K \cong \varphi(G) \subset S_n$$

即 G/K 和 S_n 的某个子群同构，因为 $|S_n| = n!$ 有限，因此其子群 $\varphi(G/H)$ 的阶有限，于是 $|G/K| = [G:K]$ 有限.

最后，因为 $K = \bigcap_{g \in G} gHg^{-1} \leq H$ 且 $K \trianglelefteq G$，因此 $K \trianglelefteq H$，证毕.

题目 2.7.10. 设 A, B, C 是群 G 的子群，且 $A \leq B$，证明：

1. $AC \cap B = A(B \cap C)$
2. 若还有 $A \cap C = B \cap C, AC = BC$，则有 $A = B$

证明

1. 对 $b \in AC \cap B$，存在 $a \in A, c \in C$ 使得 $b = ac$，则因为 $A \leq B$，于是

$$c = a^{-1}b \in B$$

则 $c \in B \cap C$，于是 $b = ac \in A(B \cap C)$，即 $AC \cap B \subset A(B \cap C)$.

对 $g \in A(B \cap C)$，存在 $a \in A, h \in B \cap C$ 使得 $g = ah$. 则 $ah \in AC$，又因为 $A \leq B$，于是 $ah \in B$，于是 $g \in AC \cap B$，即 $A(B \cap C) \subset AC \cap B$，证毕.

2. 由 (1) 的结论 $AC \cap B = A(B \cap C)$，又因为此时 $AC = BC$，因此

$$AC \cap B = A(B \cap C) = BC \cap B$$

又因为 $B \leq B$，把 (1) 中的 A 换成 B，得到

$$BC \cap B = B(B \cap C) = B$$

因此

$$B = BC \cap B = A(B \cap C)$$

由题设 $A \cap C = B \cap C$，于是

$$B = A(A \cap C) = A$$

证毕.

题目 2.7.11. 证明群的 2 阶正规子群必在群的中心里.

证明 设 H 是 G 的 2 阶正规子群，设 $H = \{e, h\}$，且 $ghg^{-1} = e \iff h = e$ 不成立，因此

$$ghg^{-1} = h \quad \forall g \in G$$

即 $gh = hg, \forall g \in G \implies h \in Z(G)$，证毕.

题目 2.7.12. 设 $n \geq 5$，证明 A_n 是 S_n 的唯一非平凡正规子群.

证明 容易证明对任意 $\sigma \in A_n, \tau \in S_n$，置换 $\tau\sigma\tau^{-1}$ 都是偶置换，且显然 $A_n \leq S_n$，因此 $A_n \trianglelefteq S_n$.

假设 $N \neq \{e\}, N \trianglelefteq S_n$，若 N 包含奇置换，则奇置换的平方是偶置换，于是存在非空集合 $M = N \cap A_n$.

任取 $m \in M, a \in A_n$，则 $m \in N \trianglelefteq S_n$，因此 $ama^{-1} \in N$，又因为 $m \in A_n$，于是 $ama^{-1} \in A_n$，因此

$$M \trianglelefteq A_n$$

因为 $n \geq 5$ 时 A_n 是单群，因此 $M = \{e\}$ 或 $M = A_n$.

若 $M = N \cap A_n = \{e\}$，则 N 不含 e 以外的偶置换，于是对任意 $\sigma \in N, \sigma \neq e$ 都有

$$\sigma^2 = e$$

若存在 $\sigma_1, \sigma_2 \in N, \sigma_1 \neq \sigma_2, \sigma_1, \sigma_2 \neq e$ ，则

$$\sigma_1\sigma_2 \in A_n \quad \sigma_1\sigma_2 \neq e$$

矛盾，因此 $N = \{e, \sigma\}$ ，又因为 $N \trianglelefteq S_n$ ，则

$$g\sigma g^{-1} = \sigma \quad \forall g \in G$$

结论在 S_n 中显然矛盾，因此 $M = N \cap A_n = A_n$ ，即 $A_n \subset N$.

假设 $N \neq A_n$ ，则存在奇置换 $\sigma \in N$ ，容易验证

$$\sigma A_n = S_n \backslash A_n$$

因此 $N = S_n$ ，证毕.

题目 2.7.13. 证明有限群 G 是二面体群的充要条件是 G 可由两个 2 阶元素生成，这里 A_4 的 4 阶子群 V_4 也看成 4 阶二面体群.

证明 对二面体群

$$D_{2n} = \{r^i s^j : i = 0, \cdots, n; j = 0, 1\}$$

其中

$$r^n = s^2 = e \quad rs = sr^{-1}$$

这里 $V_4 \cong D_2$ ，因此下面不对 V_4 给出特殊讨论.

1. 必要性：若 G 是二面体群 D_{2n} ，则

$$G = \{r^i s^j : i = 0, 1, \cdots, n-1; j = 0, 1\}$$

其中

$$r^n = s^2 = e \quad rs = sr^{-1}$$

则 $o(s) = 2$ ，且 $(rs)^2 = e \implies o(rs) = 2$ ，容易验证

$$G = \langle s, rs \rangle$$

因此 G 可由两个 2 阶元素生成，证毕.

2. 充分性：若 $G = \langle a, b \rangle$ ，其中 $o(a) = o(b) = 2$ ，令

$$s = a \quad r = ab$$

则 $rs = sr^{-1}$. 假设 $o(r) = n$ ，则

$$(ab)^n = e \implies (ab)^{n-1}ab = e \implies b = ((ab)^{n-1}a)^{-1} = a(ba)^{n-1}$$

因此对任意 $g \in \langle a, b\rangle$ ，都可以写成 $g = (ab)^k$ 或 $g = (ab)^k a$ ，因此

$$G = \{r^i s^j : i = 0, 1, \cdots, n-1; j = 0, 1\}$$

若 $o(r) = +\infty$ ，考虑

$$D_\infty = \{r^i s^j : i \in \mathbb{N}; j = 0, 1\}$$

则考虑

$$\varphi : \langle a, b\rangle \to D_\infty \quad \varphi(a) = s, \varphi(b) = ab$$

则容易验证 φ 是一个同构，证毕.

题目 2.7.14. 设 G 为一个有限群，其类方程为 $20 = 1 + 4 + 5 + 5 + 5$.

1. G 中有没有 5 阶子群？若有，是否是 G 的正规子群？

2. G 中有没有 4 阶子群？若有，是否是 G 的正规子群？

解 类方程的元素是共轭类的大小，即 G 在自身上的共轭作用的轨道的大小，又因为轨道大小等于其代表元素的稳定化子（共轭作用的稳定化子就是中心化子）的指数，且稳定化子构成子群，因此由题，G 存在大小为 $4, 5$ 的共轭类，则存在阶为 $5, 4$ 的子群（稳定化子）.

下面证明大小为 4 的共轭类中的元素 $x \in G$ 的稳定化子 $C_G(x)$ 是 G 的阶数为 5 的正规子群：因为 $|C_G(x)| = 5$ 是素数，因此 $C_G(x)$ 是循环群，又因为

$$xxx^{-1} = x \implies x \in C_G(x)$$

于是 $C_G(x) = \langle x\rangle$.

题目 2.7.15. 设 $G, G;$ 为两个群，N, N' 分别为 G, G' 的正规子群，判断一下说法是否正确，证明或给出反例：

1. 若 $G \cong G'$ 且 $N \cong N'$ ，则有 $G/N \cong G'/N'$

2. 若 $N \cong N'$ 且 $G/N \cong G'/N'$ ，则有 $G \cong G'$

3. 若 $G \cong G'$ 且 $G/N \cong G'/N'$ ，则有 $N \cong N'$

题目 2.7.16. 1. 令

$$G = G' = \mathbb{Z}_4 \times \mathbb{Z}_2 \quad N = \langle (2,0) \rangle, N' = \langle (0,1) \rangle$$

容易验证 $G \cong G', N \cong N', N \trianglelefteq G, N' \trianglelefteq G'$. 此时

$$G/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \quad G'/N' \cong \mathbb{Z}_4$$

因此结论错误.

2. 令

$$G = \mathbb{Z}_8, G' = \mathbb{Z}_4 \times \mathbb{Z}_2, N = \langle 4 \rangle, N' = \langle (0,1) \rangle$$

容易验证 $G \ncong G', N \cong N', N \trianglelefteq G, N' \trianglelefteq G'$. 而此时

$$G/N \cong \mathbb{Z}_4 \cong G'/N'$$

因此结论错误.

3. 令

$$G = G' = D_8 \quad N = \langle r \rangle, N' = \{1, r^2, s, r^2, s\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

则此时

$$D_8/N \cong \mathbb{Z}_2 \cong D_8/N'$$

而 $N \ncong N'$ ，因此结论错误.

2.8 习题 2.8

题目 2.8.1. 设群 G 恰有两个自同构，证明 G 为交换群.

证明 此时 $|\mathrm{Aut}(G)| = 2$ ，则其子群的阶 $|\mathrm{Inn}(G)| = 1$ 或 2 .

若 $|\mathrm{Inn}(G)| = 1$ ，则 G 只有 id_G 一个内自同构，即对任意 $a, g \in G$ 都有

$$gag^{-1} = a$$

因此 G 是交换群.

若 $|\mathrm{Inn}(G)| = 2$ ，我们先证明

$$\mathrm{Inn}(G) \cong \mathrm{Aut}(G)/Z(G)$$

其中 $Z(G)=\bigcap\limits_{x\in G}C_G(x)$，即 G 的中心. 我们知道

$$\mathrm{Inn}(G)=\{\varphi_g:g\in G\}\quad \varphi_g(x)=gxg^{-1}$$

现在定义

$$\Phi:G\to \mathrm{Aut}(G)\quad \Phi(g)=\varphi_g$$

显然 $\mathrm{Im}(\Phi)=\mathrm{Inn}(G)$. 下证 Φ 是群同态：对 $\forall g,h\in G,x\in G$ 有

$$\Phi(gh)(x)=\varphi_{gh}(x)=ghx(gh)^{-1}=g(hxh^{-1})g^{-1}=(\varphi_g\varphi_h)(x)$$

因此 Φ 是 $G\to \mathrm{Aut}(G)$ 的群同态. 此时

$$\mathrm{Ker}\Phi=\{g\in G:\varphi_g=\mathrm{id}_G\}=\{g\in G:gxg^{-1}=x,\forall x\in G\}=Z(G)$$

由同态基本定理证毕.

则此时商集 $\mathrm{Aut}(G)/Z(G)$ 有两个元素，我们记

$$\mathrm{Aut}(G)/Z(G)=\{Z(G),gZ(G)\}$$

则得到

$$(gZ(G))^2=g^2Z(G)=Z(G)\implies g^2\in Z(G),\forall g\in G$$

此时对 $\forall x\in G$，若 $x\notin Z(G)$，则 $xZ(G)=gZ(G)$，从而 $x=gz$，其中 $z\in Z(G)$；若 $x\in Z(G)$，则 $x=z\in Z(G)$，因此任意 $x\in G$ 都可以表示为 $x=g^az$，其中 $a=0,1$，且 z 是一个 $Z(G)$ 的元素. 任取 x,y，表示为

$$x=g^az\quad y=g^bz'$$

则

$$xy=(g^az)(g^bz')=g^{a+b}(zz')\quad yx=(g^bz')(g^az)=g^{a+b}(zz')$$

因此 G 是交换群，证毕.

题目 2.8.2. 证明阶大于 2 的有限群至少有两个自同构.

证明 假设 G 的阶 $|G|>2$. 若 G 不是交换群，则存在 $g\in G$ 使得 $g\notin Z(G)$，定义映射

$$\varphi:G\to G\quad \varphi(x)=gxg^{-1}$$

则容易验证 φ 是群同构，且因为 $g\notin Z(G)$，因此 $\varphi\neq\mathrm{id}_G$，此时 G 至少有两个自同构.

若 G 是交换群，假设 G 的元素的阶都不超过 2 ，即对任意 $g \in G, g \neq e$ 有

$$g = g^{-1}$$

设 $|G| = n$ ，此时 $G \cong (\mathbb{Z}_2)^n$ ，则其自同构群

$$\mathrm{Aut}(G) = \mathrm{GL}(n, 2)$$

显然 $|\mathrm{Aut}(G)| \geq 2$ ，此时 G 至少有两个自同构.

若 G 存在阶大于 2 的元素，定义映射

$$\varphi : G \to G \quad \varphi(g) = g^{-1}$$

则此时 $\varphi \neq \mathrm{id}_G$ ，且此时 G 是交换群，容易验证 φ 是群同构，此时 G 至少有两个自同构.

综上，证毕.

题目 2.8.3. 设 G 为群，H, K 都是 G 的正规子群，且 $H \cap K = \{e\}$ ，证明 H, K 之间元素的乘法可交换.

证明 任取 $h \in H, k \in K$ ，考虑 $hkh^{-1}k^{-1}$ ，因为 $K \trianglelefteq G$ ，因此 $hkh^{-1} \in K$ ，于是 $hkh^{-1}k^{-1} \in K$ ，同理 $hkh^{-1}k^{-1} \in H$ ，于是 $hkh^{-1}k^{-1} = e$ ，证毕.

题目 2.8.4. 设 G 为有限群，$H \leq G$ 且 $[G : H] = n > 1$ ，证明 G 必有一个指数整除 $n!$ 的非平凡正规子群或者 G 同构与 S_n 的一个子群.

证明 令 G 左乘作用在左陪集集合 $X = G/H$ 上，对 $g \in G, aH \in X$ 定义

$$g \circ (aH) = (ga)H$$

则这定义了从 G 到 X 的置换群 $\mathrm{Sym}(X) \cong S_n$ 的一个同态

$$\varphi : G \to S_n \quad g \mapsto \varphi(g) : aH \mapsto gaH$$

则

$$N = \mathrm{Ker}\varphi = \{g : gaH = aH, \forall a \in G\} = \bigcap_{a \in G} aHa^{-1}$$

显然 $N \trianglelefteq G$. 由第一同构定理

$$\varphi(G) \cong G/N$$

且 $\varphi(G)$ 是 S_n 的子群，因此

$$[G:N]=|\varphi(G)|\mid|S_n|=n!$$

若 N 是非平凡正规子群，则证毕. 否则，若 $N=\{e\}$ ，则 φ 是单同态，于是 G 同构 $\varphi(G)$ ，其中 $\varphi(G)\leq S_n$.

综上，证毕.

题目 2.8.5. 证明对应定理 2.8.6.

证明 只需要根据 π 的定义验证即可.

1. 若 $M_1\leq M_2$ ，对 $m_1N\in M_1/N$ ，则 $m_1\in M_2$ ，即 $m_1N\in M_2/N$ ，因此 $M_1/N\leq M_2/N$.

   若 $M_1/N\leq M_2/N$ ，则对任意 $m_1N\in M_1/N$ ，则 $m_1N\in M_2/N$ ，从而存在 $m_2\in M_2$ 使得 $m_1N=m_2N$ ，于是 $m_2^{-1}m_1\in N\subset M_2$ ，因此 $m_1\in M_2$ ，于是 $M_1\leq M_2$ ，证毕.

2. 定义映射

   $$\varphi:M_2/M_1\to\overline{M_2}/\overline{M_1}\quad mM_1\mapsto(mN)\overline{M_1}$$

   则 φ 是同构，因此两边陪集数量相等，证毕.

3. 因此 π 是同态，于是

   $$\pi(\langle M_1,M_2\rangle)=\langle\pi(M_1),\pi(M_2)\rangle$$

   证毕.

4. 对 $\forall m\in M_1\cap M_2$ ，有 $mN\in\overline{M_1}\cap\overline{M_2}$ ，因此 $\overline{M_1\cap M_2}\leq\overline{M_1}\cap\overline{M_2}$. 若 $\overline{g}\in\overline{M_1}\cap\overline{M_2}$ ，则

   $$g\in\pi^{-1}(\overline{M_1})\cap\pi^{-1}(\overline{M_2})=M_1\cap M_2$$

   因此 $\overline{M_1}\cap\overline{M_2}\subset\overline{M_1\cap M_2}$. 证毕.

5. 若 $M\trianglelefteq G$ ，则对任意 $mN\in\overline{M},gN\in\overline{G}$ ，得到

   $$(gN)(mN)(gN)^{-1}=(gmg^{-1})N\in\overline{M}$$

   于是 $\overline{M}\trianglelefteq\overline{G}$. 反之，若 $\overline{M}\trianglelefteq\overline{G}$ ，则对任意 $g\in G,m\in M$ ，有

   $$gmg^{-1}N=(gN)(mN)(g^{-1}N)\in\overline{M}$$

于是 $gmg^{-1} \in \pi^{-1}(\overline{M}) = M$ ，因此 $M \trianglelefteq G$.

由自然的同态合成，有商映射 $G \to \overline{G} \to \overline{G}/\overline{M}$ ，其核 $\pi^{-1}(\overline{M}) = M$ ，因此由同态基本定理

$$G/M \cong \overline{G}/\overline{M}$$

证毕.

题目 2.8.6. 设 $N \trianglelefteq G, |N| = n, [G : N] = m$ 且 m, n 互素，证明 G 的阶为 n 的正规子群一定为 N .

证明 设 $H \trianglelefteq G$ ，且 $|H| = n$ ，则

$$|NH| = \frac{|N||H|}{|N \cap H|} = \frac{n^2}{|N \cap H|}$$

又因为 $N, H \trianglelefteq G$ ，于是对任意 $n_1h_1, n_2h_2 \in NH$ ，有

$$h_1n_2h_1^{-1} = n_3 \in N \implies h_1n_2 = n_3h_1 \implies n_1h_1n_2h_2 = n_1n_3h_1h_2 \in NH$$

因此 $NH \leq G$ ，于是 $|NH| \mid |G| = mn$ ，设 $|NH| = \dfrac{mn}{t}$ ，于是

$$\frac{mn}{t} = \frac{n^2}{|N \cap H|} \implies m|M \cap H| = tn \implies n \mid m|N \cap H|$$

因为 $\gcd(m, n) = 1$ ，于是 $n \mid |N \cap H|$ ，又因为 $|N \cap H| \leq n$ ，因此 $|N \cap H| = n$ ，因此 $N = H$ ，证毕.

题目 2.8.7. 设 σ 是群 G 到交换群 H 的一个群同态，$N \leq G$ 且 $\mathrm{Ker}\sigma \subset N$ ，证明 $N \trianglelefteq G$.

证明 任取 $g \in G, n \in N$ ，则

$$\sigma(gng^{-1}) = \sigma(g)\sigma(n)\sigma(g^{-1})$$

因为 H 是交换群，因此 $\sigma(gng^{-1}) = \sigma(n)$. 因此

$$\sigma(gng^{-1}n^{-1}) = \sigma(gng^{-1})\sigma(n^{-1}) = e$$

于是 $gng^{-1}n^{-1} \in \mathrm{Ker}\sigma \subset N$ ，因此 $gng^{-1} \in N$ ，于是 $N \trianglelefteq G$ ，证毕.

题目 2.8.8. 设 G 为单群，且存在 $G \to H$ 的满同态，证明 H 为单群或者 H 为单位元群.

证明 由同态基本定理

$$G/\mathrm{Ker}\,\varphi \cong H$$

因为 G 是单群，因此 $\mathrm{Ker}\varphi = G$ 或 $\mathrm{Ker}\varphi = \{e\}$.

若 $\mathrm{Ker}\varphi = G$ ，则 $H = \{e\}$.

若 $\mathrm{Ker}\varphi = \{e\}$ ，则 φ 是单射，于是 $H \cong G$ ，因此 H 也是单群，证毕.

题目 2.8.9. 证明有限 $p-$ 群的非正规子群的个数一定是 p 的倍数.

证明 设 $\mathscr{S}$ 是有限 $p-$ 群 G 的所有非正规子群构成的集合，考虑 G 在子群上的共轭作用

$$g \circ H = gHg^{-1} \quad H \leq G$$

则 H 在共轭作用下的轨道大小

$$|O_H| = [G : N_G(H)]$$

其中 $N_G(H) = \{g \in G : gHg^{-1} = H\}$ 是 H 的正规化子，又因为 H 是 G 的正规子群当且仅当在共轭作用下的轨道 $|O_H| = 1$ ，因此对 $H \in \mathscr{S}$ ，有

$$[G : N_G(H)] \geq p \quad p \mid [G : N_G(H)]$$

将 $\mathscr{S}$ 分解为不相交的轨道的并，每个轨道的大小都是 p 的倍数，因此 $|\mathscr{S}|$ 是 p 的倍数，证毕.

题目 2.8.10. 设 G 为有限群，$\alpha \in \mathrm{Aut}(G)$ ，令 $I = \{g \in G : \alpha(g) = g^{-1}\}$ ，证明：

1. 若 $|I| > \dfrac{3}{4}|G|$ ，则 G 交换.
2. 若 $|I| = \dfrac{3}{4}|G|$ ，则 G 有一个指数为 2 的交换正规子群.

证明 先证明一个结论：对 $a \in I$ ，有 $I \cap aI = I \cap C(a)$ ，其中 $C(a) = \{g \in G : ag = ga\}$.

若 $x \in I \cap aI$ ，则 $\alpha(x) = x^{-1}$ ，且存在 $y \in I$ 使得 $x = ay$. 此时

$$\alpha(ay) = \alpha(a)\alpha(y) = (ya)^{-1} = (ay)^{-1} = \alpha(x)$$

得到 $ya = ay$ ，即 $aya = aay$ ，即 $xa = ax$ ，因此 $x \in I \cap C(a)$.

若 $x \in I \cap C(a)$ ，则 $ax = xa$ ，令 $y = a^{-1}x$ ，则

$$\alpha(y) = \alpha(a^{-1}x) = \alpha(a^{-1})\alpha(x) = ax^{-1} = x^{-1}a = y^{-1}$$

因此 $y \in I$ ，则 $x = ay \in aI$ ，于是 $x \in I \cap aI$. 证毕.

下面回到原命题

1. 当 $|I| > \frac{3}{4}|G|$ 时，对 $a \in I$ 有

$$|I \cap aI| = |I| + |aI| - |I \cup aI| = 2|I| - |I \cup aI| \geq 2|I| - |G| > \frac{1}{2}|G|$$

于是 $|I \cap C(a)| > \frac{1}{2}|G|$，即 $|C(a)| > \frac{1}{2}|G|$. 又因为 $C(a) \leq G$，因此 $|C(a)| \mid |G|$，于是得到 $|C(a)| = |G|$，即 $C(a) = G$，因为这对任意 a 成立，因此 G 是交换群.

2. 当 $|I| = \frac{3}{4}|G|$ 时，假设 G 是交换群，则 $I \leq G$，此时 $|I| \mid |G|$ 矛盾，因此 G 是非交换群. 因此 $Z(G) \neq G$，于是 $|Z(G)| \leq \frac{1}{2}|G|$.

又因为对 $a \in I$ 有

$$|C(a)| \geq |I \cap C(a)| = |I \cap aI| \geq 2|I| - |G| = \frac{1}{2}|G|$$

于是 $|C(a)| = |G|$ 或 $\frac{1}{2}|G|$.

假设对任意 $a \in I$ 都有 $|C(a)| = |G|$，则 $I \leq Z(G)$，即

$$|I| \leq |Z(G)|$$

与前面的 $|Z(G)| \leq \frac{1}{2}|G|$ 矛盾，因此存在 $a \in I$ 使得 $|C(a)| = \frac{1}{2}|G|$，此时令

$$H = C(a) \quad [G : H] = 2$$

下证 H 是交换正规子群：

先证明 H 是正规子群：对任意 $g \in G$，若 $g \in H$，则容易验证 $gH = Hg$；若 $g \notin H$，此时因此 $[G : H] = 2$，因此

$$(G/H)_l = \{H, gH\} \quad (G/H)_r = \{H, Hg\}$$

因为 $G = H \cup gH = H \cup Hg$，因此 $gH = Hg$，因此 H 是正规子群。

再证明 H 是交换群，任取 $h_1, h_2 \in H$，此时由前面的结论

$$|I \cap C(a)| \geq \frac{1}{2}|G| = |C(a)|$$

又因为 $|I \cap C(a)| \leq |C(a)|$，因此 $|I \cap H| = |H|$，于是 $H \subset I$，因此 $h_1, h_2 \in I$，则

$$\alpha(h_1h_2) = \alpha(h_1)\alpha(h_2) = h_1^{-1}h_2^{-1}$$

又因为 H 构成群，因此 $h_1h_2 \in H \subset I$，于是

$$\alpha(h_1h_2) = (h_1h_2)^{-1} = h_2^{-1}h_1^{-1}$$

于是 $h_1h_2 = h_2h_1$，证毕。

Chapter 3

群的结构

3.1 习题 3.1

题目 3.1.1. $B \cong C$，证明对 $\forall A$ 有 $A \times B \cong A \times C$. 反之是否成立？

证明 存在 $\varphi : B \to C$ 的同构. 考虑映射

$$\begin{aligned} \sigma \quad & A \times B \to A \times C \\ & (a, b) \mapsto (a, \varphi(b)) \end{aligned}$$

因为 φ 是同构，因此 σ 是双射. 又因为

$$\begin{aligned} \sigma((a_1, b_1)(a_2, b_2)) &= (a_1, \varphi(b_1))(a_2, \varphi(b_2)) \\ &= (a_1 a_2, \varphi(b_1)\varphi(b_2)) = (a_1 a_2, \varphi(b_1 b_2)) \\ &= \sigma(a_1, b_1)\sigma(a_2, b_2) \end{aligned}$$

保持群运算，证毕.

题目 3.1.2. G_1, G_2 是非单位循环群，证明：若 G_1, G_2 中至少有一个为无限循环群，则 $G_1 \times G_2$ 不是循环群.

证明 假设 $G_1 = \langle g \rangle$ 是无限循环群，$G_2 = \langle h \rangle$，若 $G_1 \times G_2$ 是循环群，则

$$G_1 \times G_2 = \langle g^k, h^m \rangle$$

因为 $(g, h) \in G_1 \times G_2$，因此 $k = m = 1$，即 $G_1 \times G_2 = \langle g, h \rangle$，显然此时 $(g, h^2) \notin G_1 \times G_2$，矛盾.

题目 3.1.3. 若 4.1.2中有限群 G_1, G_2 的阶不互素，结论如何？

解 见反例 4.1.1

题目 3.1.4. G_1, G_2 有限，$G_1 \times G_2$ 为循环群，证明 G_1, G_2 都是循环群，且阶互素.

证明 设 $G_1 \times G_2$ 的生成元为 (g_1, g_2)，则对任意 $a \in G_1$，有 $(a, e) \in G_1 \times G_2$，即

$$(a, e) = (g_1, g_2)^k = (g_1^k, g_2^k)$$

于是 $G_1 = \langle g_1 \rangle$，同理 $G_2 = \langle g_2 \rangle$.

记 $|G_1| = m, |G_2| = n$，若 $\gcd(m, n) > 1$，则 $\operatorname{lcm}(m, n) < mn$，记 $l = \operatorname{lcm}(m, n)$，则

$$(a, b)^l = (g_1^{kl}, g_2^{kl}) = (e_1, e_2)$$

即 $|G_1 \times G_2| \leq l < mn$，矛盾.

题目 3.1.5. $N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2$，证明 $N_1 \times N_2 \trianglelefteq G_1 \times G_2$，且

$$(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$$

证明 对 $\forall (n_1, n_2) \in N_1 \times N_2, (g_1, g_2) \in G_1 \times G_2$，由题目条件

$$g_1^{-1} n_1 g_1 \in N_1 \quad g_2^{-1} n_2 g_2 \in N_2$$

则

$$(g_1, g_2)^{-1}(n_1, n_2)(g_1, g_2) = (g_1^{-1} n_1 g_1, g_2^{-1} n_2 g_2) \in N_1 \times N_2$$

因此 $N_1 \times N_2 \trianglelefteq G_1 \times G_2$.

考虑映射

$$\begin{aligned} \varphi : \quad (G_1 \times G_2)/(N_1 \times N_2) &\to G_1/N_1 \times G_2/N_2 \\ (g_1, g_2)N_1 \times N_2 &\mapsto (g_1 N_1, g_2 N_2) \end{aligned}$$

显然 φ 是满射. 若 $\varphi((g_1, g_2)N_1 \times N_2) = \varphi((g_1', g_2')N_1 \times N_2))$，则

$$(g_1 N_1, g_2 N_2) = (g_1' N_1, g_2' N_2)$$

则存在 $n_1 \in N_1, n_2 \in N_2$ 使得

$$g_1 n_1 = g_1' \quad g_2 n_2 = g_2'$$

即 $(g_1, g_2)N_1 \times N_2 = (g_1', g_2')N_1 \times N_2$，因此 φ 是单射.

最后

$$\begin{aligned}&\varphi(((g_1,g_2)N_1\times N_2)((g_1',g_2')N_1\times N_2))=\varphi((g_1g_1',g_2g_2')N_1\times N_2)\\=&(g_1g_1'N_1,g_2g_2'N_2)=(g_1N_1,g_2N_2)(g_1'N_1,g_2'N_2)\\=&\varphi((g_1,g_2)N_1\times N_2)\varphi((g_1',g_2')N_1\times N_2)\end{aligned}$$

保持运算，证毕.

题目 3.1.6. $A,B\trianglelefteq G$ ，证明

$$AB/A\cap B\cong AB/A\times AB/B$$

证明 考虑

$$\begin{aligned}\varphi:\quad AB&\to AB/A\times AB/B\\g&\mapsto(gA,gB)\end{aligned}$$

则

$$\operatorname{Ker}\varphi=A\cap B$$

对任意 $a_1b_1A\in AB/A,a_2b_2B\in AB/B$ ，因为 $A\trianglelefteq G$ ，于是

$$a_1b_1A=a_1Ab_1=Ab_1=b_1A$$

且 $a_2b_2B=a_2B$ ，于是存在 $a_2b_1\in AB$ ，使得

$$\varphi(a_2b_1)=(a_2b_1A,a_2b_1B)=(a_1b_1A,a_2b_2B)$$

因此 φ 是满射，容易验证 φ 保持运算，于是由第一同构定理

$$AB/A\cap B\cong AB/A\times AB/B$$

证毕.

题目 3.1.7. $H,K,L\trianglelefteq G$ ，$G=HKL$ ，且

$$H\cap(KL)=K\cap(HL)=L\cap(HK)=\{e\}$$

证明 $G\cong H\times K\times L$.

证明 考虑

$$\begin{aligned}\varphi:H\times K\times L&\to G\\(h,k,l)&\mapsto hkl\end{aligned}$$

显然 φ 是满射. 若 $hkl=e$，则 $h=(kl)^{-1}\in H\cap(KL)\implies h=e$，同理得到 $k=l=e$，因此 φ 是单射.

又因为 H,K,L 是正规子群，于是

$$hkh^{-1}k^{-1}\in H\cap K\subset H\cap(KL)\implies hkh^{-1}k^{-1}=e$$

对 HL,KL 同理，于是 H,L,K 的元素之间可交换，则

$$\begin{aligned}\varphi((h,k,l)(h',k',l'))&=\varphi(hh',kk',ll')=hh'kk'll'\\&=hklh'k'l'\end{aligned}$$

于是 φ 保持运算，是同构，证毕.

题目 3.1.8. H,K 是有限群 G 的正规子群且 $G=HK$，且 H,K 的阶互素，证明 G 的任意子群 L 可以写成 $L=(H\cap L)(K\cap L)$.

证明 显然 $(H\cap L)(K\cap L)\subset L$，下证 $L\subset(H\cap L)(K\cap L)$.

因为 H,K 是正规子群，则

$$hkh^{-1}k^{-1}\in H\cap K$$

又因为 $|H\cap K|\mid|H|,|H\cap K|\mid|K|$，于是 $|H\cap K|=1$，则 $H\cap K=e$，即 $hk=kh$，因此 H,K 元素之间可交换.

设 $|H|=m,|K|=n$，则对 $L\subset G=HK$ 的任意元素 $l=hk$，因为且 $\gcd(m,n)=1$，于是存在 $u,v\in\mathbb{Z}$ 使得 $um+vn=1$，则

$$h=h^{um+vn}=(h^n)^v\quad l^n=h^nk^n=h^n$$

得到

$$h=(l^n)^v\in L$$

同理 $k\in L$，证毕.

题目 3.1.9. G_1,G_2 都是非单位元群，若 $G_1\times G_2$ 的任意子群都是 $H_1\times H_2$，其中 $H_i\leq G_i$，证明 G_1,G_2 的每个元素的阶都有限且对 $\forall a\in G_1,b\in G_2$，$o(a),o(b)$ 互素.

证明 假设 $a\in G_1$ 是无限阶元素，任取 $b\neq e,b\in G_2$，则 $\langle(a,b)\rangle$ 是 $G_1\times G_2$ 的子群，此时 $\langle(a,b)\rangle=H_1\times H_2$，则

$$H_1=\langle a\rangle\quad H_2=\langle b\rangle$$

显然 $H_1 \times H_2 = \{(a^i, b^j) : i, j \in \mathbb{Z}\}$ ，矛盾.

假设 $a \in G_1, b \in G_2$ 且 $\gcd(a, b) > 1$ ，令 $d = \gcd(a, b)$ ，则存在素数 p 使得 $p \mid d$. 令 $a' = a^{o(a)/p}, b' = b^{o(b)/p}$ ，则

$$o(a') = o(b') = p$$

此时 $\langle (a', b') \rangle \leq G_1 \times G_2$ ，于是存在 $H_1 \leq G_1, H_2 \leq G_2$ 使得

$$\langle (a', b') \rangle = H_1 \times H_2$$

则 $H_1 = \langle a' \rangle, H_2 = \langle b' \rangle$ ，显然

$$|\langle a', b' \rangle| = p \quad |H_1| = |H_2| = p \implies |H_1 \times H_2| = p^2$$

矛盾，证毕.

题目 3.1.10. n 是奇数，证明 $D_{2n} \cong D_n \times \mathbb{Z}_2$.

证明 因为

$$D_{2n} = \{r, s : r^{2n} = s^2 = e, srs = r^{-1}\}$$

此时 $\langle r^n \rangle$ 是阶为 2 的子群，记作 $Z = \langle r^n \rangle \cong \mathbb{Z}_2$.

令 $H = \langle r^2, s \rangle$ ，则 $o(r^2) = n$ ，且 $s(r^2)s = r^{-2} = (r^2)^{-1}$,，因此

$$H = \langle \rho, \sigma : \rho^n = \sigma^2 = 1, \sigma\rho\sigma = \rho^{-1} \rangle$$

即 $H \cong D_n$.

若 $Z \cap H \neq \{e\}$ ，则 $r^n \in Z \cap H$ ，即 $r^n \in H$. 首先 $r^n \neq e$ ，且 $r^n \neq r^{2k}$. 假设 $r^n = r^{2k}s$ ，则 $s = r^{n-2k}$ 矛盾；于是 $r^n \neq Z$ ，因此 $Z \cap H = \{e\}$.

D_{2n} 的元素为 r^i 或 $r^i s (0 \leq i < 2n)$,对每个 i 存在唯一的 $k \in \{0, \cdots, n-1\}, \varepsilon \in \{0, 1\}$ 使得

$$i \equiv 2k + n\varepsilon (\mathrm{mod}\, 2n)$$

于是

$$r^i = r^{2k}(r^n)^\varepsilon \in HZ \quad r^i s = r^{2k}(r^n)^\varepsilon s \in HZ$$

因此 $D_{2n} = HZ$ ，于是

$$D_{2n} \cong H \times Z \cong D_n \times \mathbb{Z}_2$$

题目 3.1.11. φ 是 K 在 H 上的同构作用. 若 $\{e_H\} \times K$ 是 $H \rtimes_\varphi K$ 的正规子群，证明 φ 一定是平凡同构作用且 $H \rtimes_\varphi K = H \times K$.

证明 对 $\forall(e_H,k)\in\{e_H\}\times K,(h,k')\in H\rtimes_\varphi K$ ，由条件

$$(\varphi_{k'^{-1}}(h^{-1}),k'^{-1})(e_H,k)(h,k')=(\varphi_{k'^{-1}}(h^{-1})h,k'^{-1}kk')\in\{e_H\}\times K$$

则 $\varphi_{k'^{-1}}(h^{-1})=h^{-1}$ ，于是 $\varphi(k)=\mathrm{id}_H,\forall k\in K$ ，于是 φ 是平凡同构作用. 此时 $H\rtimes_\varphi K=H\times K$ 自然成立.

题目 3.1.12. m,n 是正整数，A,B 分别为 m,n 阶循环群，则半直积 $A\rtimes B$ 在同构意义下有多少种可能？

解 记 $A=\langle a\rangle,B=\langle b\rangle$. 对任意 $\varphi:B\to\mathrm{Aut}(A)$ ，假设

$$\varphi(b)(a)=a^r\quad r\in\mathbb{Z}$$

则因为 $b^n=e_B$ ，于是 $\varphi(b^n)=\mathrm{id}_A$ ，于是

$$a^{r^n}=a\quad\forall a\in A\iff r^n\equiv1(\mathrm{mod}\,m)$$

因此

$$r\in U(m)\quad r^n\equiv1(\mathrm{mod}\,m)$$

对每个满足 $r^n\equiv1(\mathrm{mod}\,m)$ 的 r 都给出一个半直积 $A\rtimes_{\varphi_r}B$. 对 r,s ，则它们对应的 φ_r,φ_s 决定的半直积同构当且仅当存在 $k\in U(n)$ 使得 $s\equiv r^k(\mathrm{mod}\,m)$. 这是因为将 $B=\langle b\rangle$ 的生成元换成 $b'=b^k$ 时，因为 $k\in U(n)$ ，因此 b^k 依然生成 B ，此时 b' 对 A 的作用

$$b'^{-1}ab'=(b^{-1}ab)^k=a^{r^k}$$

即作用的参数从 r 变成了 r^k ，此时两个半直积是同构的.

因此不同的所有半直积类型一一对应于

$$S=\{r\in U(m):r^n\equiv1(\mathrm{mod}\,m)\}$$

的等价类，其等价关系为

$$r\sim s\iff\exists k\in U(n)\ s.t.\ s\equiv r^k(\mathrm{mod}\,m)$$