抽象代数

Contents

Part I

笔记

Chapter 0

预备知识

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.

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

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

$$t_i M_i \equiv 1 (\bmod m_i)$$

令

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

则方程组的解为 $\overline{x}$ （在模 M 下）。

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

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

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

因为 $|U(m)|=\varphi(m)$ ，证毕。

Chapter 1

群环域

1. 运算法则
2. 群环域定义
3. 整数模 n 的剩余类环

1.1 运算法则

- 运算
- 元
- 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**?

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

- 群的定义
- 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

2.1 对称群和交错群

- 置换的分解与型、共轭
- 图形的对称群

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 词，则称**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

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

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

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

若 $\pi(2)=i+1$ ，则由 $2\sim 3$ 继续归纳得到 $\pi(a)=a+i-1(\operatorname{mod} n)$ ，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

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

即在 D_n 有

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

2.2 子群与同态

- 子群性质和陈述
- 同态

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**.

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 $H^2=H, H^{-1}=H$.

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

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

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

环 $\mathrm{End}(G)$ 的单位群就是交换群 G 的自同构群 $\mathrm{Aut}(G)$.

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 $\mathrm{Ker}\,\sigma$.

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

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

- 元素的阶
- 循环群的子群
- 有限循环和交换
- 有限循环的自同构

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 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

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

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 $g_1h=g_2h$ ，则消去 h 得到 $g_1=g_2$ ，矛盾，因此

$$g_1H\cap g_2H=\emptyset\quad \forall g_1,g_2\in G,g_1\neq g_2$$

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 $\prod\limits_{g\in G}g$ 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 $o(a)=n_1d, k=k_1d$ ，则 $\gcd(n_1,k_1)=1$ ，因为

$$(a^k)^{n_1}=(a^{k_1d})^{n_1}=(a^n)^{k_1}=e$$

于是 $o(a^k)\mid n_1$ ，又因为

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

因此 $o(a)\mid ko(a^k)$ ，即 $n_1\mid k_1o(a^k)$ ，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 $a=g^k, 0\le k\le n-1$ ，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

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

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

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

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

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

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

$$o(g_1 h_1) = p_1^{f_1} p_2^{e_2} \cdots p_s^{e_s} > o(g)$$

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

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

容易验证 $\alpha_r\in\mathrm{Aut}(G)$ 。

取 $\alpha\in\mathrm{Aut}(G)$ ，设 $\alpha(a)=a^r,0\le r\le n-1$ ，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 $\forall a^k\in G$

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

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

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. $g_1\circ(g_2\circ m)=(g_1g_2)\circ m$

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 $G\to M$ 的全变换群 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

$$T(g_1g_2)(m)=(T(g_1)T(g_2))(m)$$

即 $T(g_1g_2)=T(g_1)T(g_2)$ ，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。

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 $\rho: G\times G\to G$ ，其中对 $\forall a,g\in G$

$$\rho(g,a)=gag^{-1}$$

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

$$I_g(a_1a_2) = I_g(a_1)I_g(a_2)$$

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 的所有内自同构左乘做成的集合，容易验证

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

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

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

定义 2.5.1 (陪集). $H \le G$ ，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. $H \le G$ ，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

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

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 $[G:H]$.

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 $HK=G$.

2.6 轨道长度和类方程

- 群作用的轨道长度
- 群作用的轨道个数

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 $\sum\limits_{g \in G} |\psi(g)|$ 。

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。

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

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

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 $\frac{n+3}{2}$ 个共轭类，其中只有一个共轭类包含一个元素，即 C_e ；有 $\frac{n-1}{2}$ 个共轭类包含 2 个元素，分别为 $C_{r^j}, j = 1, 2, \cdots, \frac{n-1}{2}$ ；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 $\frac{n}{2} + 3$ 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 $\frac{n}{2} - 1$ 个共轭类包含 2 个元素，分别为 $C_{r^j}, j = 1, 2, \cdots, \frac{n}{2} - 1$ ；有 2 个共轭类包含 $\frac{n}{2}$ 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

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。

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。

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 $(i_1 i_2 i_3) \in N$ ，则对任意 $(j_1 j_2 j_3)$ ，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

$$\rho(i_1 i_2 i_3)\rho^{-1} = (j_1 j_2 j_3) \in N$$

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

$$\delta(i_1 i_2 i_3)\delta^{-1} = (ij)\rho(i_1 i_2 i_3)\rho^{-1}(ij)^{-1} = (j_1 j_2 j_3) \in N$$

证毕。

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 $\operatorname{rank}(M) \leq \operatorname{rank}(N)$ ，当 $\operatorname{rank}(M) < \operatorname{rank}(N)$ 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 $\displaystyle\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} j^m$

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 $\begin{pmatrix} n \\ k \end{pmatrix}$ 中情况，由容斥原理，此时 $\bigcup\limits_{b\in B} T_b$ 的元素个数为

$$\sum_{k=1}^{n}(-1)^{k-1}\begin{pmatrix} n \\ k \end{pmatrix}(n-k)^m$$

于是满射的个数为

$$n^m-\sum_{k=1}^{n}(-1)^{k-1}\begin{pmatrix} n \\ k \end{pmatrix}(n-k)^m=\sum_{k=0}^{n}(-1)^{k}\begin{pmatrix} n \\ k \end{pmatrix}(n-k)^m$$

令 $j=n-k$ ，则上式即

$$\sum_{j=0}^{n}(-1)^{n-j}\begin{pmatrix} n \\ j \end{pmatrix}j^m$$

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 $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)!}$ ，显然 $k!, (p-k)!$ 的因子都小于 p ，于是 $\begin{pmatrix} p \\ k \end{pmatrix}$ 是 p 的倍数。$\mathbb{Z}_p$ 是域，则 p 是素数。当 $k=1$ 时，$(a+b)^p = \displaystyle\sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} a^{p-k} b^k$ ，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 $x^2 \equiv 1 (\bmod 360)$ ，得到

$$\begin{cases} x^2 \equiv 1(\bmod 8) \\ x^2 \equiv 1(\bmod 9) \\ x^2 \equiv 1(\bmod 5) \end{cases} \implies \begin{cases} x \equiv 1,3,5,7(\bmod 8) \\ x \equiv 1,8(\bmod 9) \\ x \equiv 1,4(\bmod 5) \end{cases}$$

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 $a^{\varphi(p^{r-2})}\equiv 1(\bmod p^{r-2})$ ，记 $a^{\varphi(p^{r-2})}=1+kp^{r-2}$ ，其中 $p\mid k$ ，则

$$a^{\varphi(p^{r-1})}=(a^{\varphi(p^{r-2})})^p=(1+kp^{r-2})^p\equiv 1+kp^{r-1}\neq 1(\bmod p^r)$$

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 $m = 2^l p^r$ ，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

$$x^2 \equiv 1 \pmod{2^l}$$

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

$$x \equiv 1(\operatorname{mod} 2^{l-1}) \quad x \equiv -1(\operatorname{mod} 2^{l-1})$$

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

$$\sigma(\sigma\tau)=\sigma^2\tau\neq(\sigma\tau)\sigma=\tau$$

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 $a \neq 0, a \in \bigcap_{k\in\mathbb{N}} m_k\mathbb{Z}$ ，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

$$\begin{array}{ccccccccc}
 & 1 & 2 & \cdots & k+1 & k+2 & \cdots & n-1 & n \\
\sigma^{-k} & n-k+1 & n-k+2 & \cdots & 1 & 2 & \cdots & n-k-1 & n-k \\
\tau\sigma^{-k} & n-k+1 & n-k+2 & \cdots & 2 & 1 & \cdots & n-k-1 & n-k \\
\sigma^k\tau\sigma^{-k} & 1 & 2 & \cdots & k+2 & k+1 & \cdots & n-1 & n
\end{array}$$

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 $|\mathrm{det}A| = 1$.

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

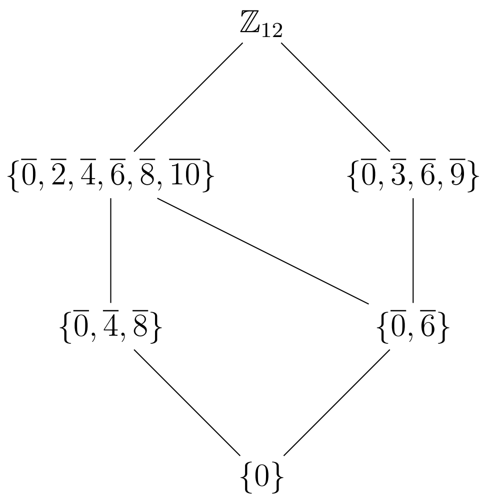
$$f^2 = g^3 = e, \quad gf = fg^{-1} = fg^2, \quad g^2 f = fg$$

因此 $H \cong S_3$.

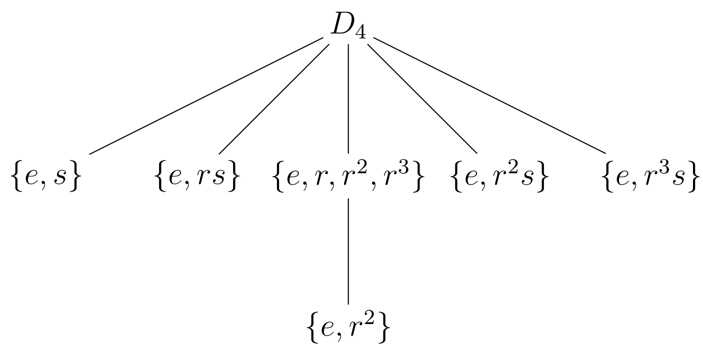
题目 2.2.7. 对有限群 G ，其子群图画法为：图的点是 G 的子群，任给两个不同子群 H, K ，存在连接 H, K 的线段当且仅当 $H < K$ 且不存在其它子群 L 使得 $H < L < K$ ，通常把 H 放在较低的位置。

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，$H \leq G, K = \mathrm{Ker}\,\sigma$ ，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
$1^3 2$	2
$1^2 3$	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.