

抽象代数

■ 抽象代数

▼ 第零章 杂题和小结论

▼ 0.0 其他

- 0.0.1 定义-命题 (半直积)
- 0.0.2 定义-命题 11.10.3 (半直积的内在版本)

▼ 0.1 群

- 0.1.1 令 S 是整数加群 \mathbb{Z}^+ 的子群, 则 S 或为平凡子群 $\{0\}$, 或是有形式 Z_a , 其中 a 为 S 中最小正整数。
- 0.1.2 Any group can be expressed as a union of cyclic subgroups.
- 0.1.3 A group G has only finitely many subgroups $\Leftrightarrow G$ is finite.
- 0.1.4 There does not exist a group with exactly two elements of order 2
- 0.1.5 Abel单群一定为素数阶循环群
- 0.1.6
- 0.1.7 (1) $|GL_n(F_p)| = \prod_{k=0}^{n-1} (p^n - p^k)$, $|SL_n(\mathbb{F}_p)| = \frac{|GL_n(\mathbb{F}_p)|}{p-1}$; (2) 求 $GL_n(F_p)$ 的 sylow-p子群, 并确定sylow—p子群的个数
- (2) G 有 4 阶子群吗? 如果有, 它是正规子群吗?
- 0.1.9 Showing that a p-group has a normal subgroup for each divisor of its order
- 0.1.10 n 为素数时, S_n 中n阶元一定是n-轮换。当n为一般整数时不一定成立

▼ 0.2 环

- 0.2.1 n 阶实方阵全体对于通常的矩阵加法和乘法形成含幺环, 叫做 n 阶实方阵环, 表示成 $M_n(R)$. 零元素为 n 阶零方阵,幺元素为 n 阶单位方阵 I_n . 类似可定义有理矩阵环 $M_n(Q)$, 复矩阵环 $M_n(C)$ 等. 当 $n \geq 2$ 时, 易知它们均不是交换环.

更一般地, 对于任意环 R , 我们仍旧像通常那样定义元素属于 R 的两个 n 阶方阵的加法和乘法, 可以直接验证全体这种 n 阶方阵形成环, 叫做环 R 上的 n 阶方阵环, 表示成 $M_n(R)$. 如果环 R 有幺元素 1_R , 则环 $M_n(R)$ 也有幺元素 $I_n = \begin{pmatrix} 1_R & & \\ & \ddots & \\ & & 1_R \end{pmatrix}$. 进而, 如果 R 是交换环, 我们可以定义方阵 $A = (a_{ij}) \in M_n(R)$ 的行列式 $\det A = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$. 基于环 R 的乘法交换性, 我们可以看出 $\det A$ 仍具有行列式通常那些性质, 例如:

$$\begin{aligned} (1) (\det A)(\det B) &= \det(AB); \\ (2) A(\text{adj}A) &= (\text{adj}A)A = (\det A) \cdot I_n. \end{aligned}$$

其中 $\text{adj}A$ 表示 A 的伴随方阵, 即 $\text{adj}A = (A_{ji})$, 而 A_{ij} 是 A 中元素 a_{ij} 的代数余子式. 上面 (1) 式表明, 当 R 为含幺交换环时, 行列式映射

$$\det : M_n(R) \rightarrow R, \quad A \mapsto \det A$$

是乘法半群的同态 (并且易知这是满同态). 因此若 A 是环 $M_n(R)$ 中的单位, 则 $\det A$ 也是环 R 中的单位. 反之, 如果 $\det A \in U(R)$, 则由上面的 (2) 式可知 $(\det A)^{-1} \text{adj}A$ 是 A 的逆元素, 即 $A \in U(M_n(R))$. 这就完全决定了矩阵环 $M_n(R)$ 的单位群 (其中 R 为含幺交换环):

$$U(M_n(R)) = \{A \in M_n(R) \mid \det A \in U(R)\}$$

. 乘法群 $U(M_n(R))$ 叫做含幺交换环 R 上的 n 次一般线性群, 表示成 $GL(n, R)$. 例如 $GL(n, \mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$, 而对任意域 F , $GL(n, F) = \{A \in M_n(F) \mid \det A \neq 0\}$.

注: 这里 $U(R)$ 表示环 R 的乘法逆元的集合 (单位群)

■ 域

▼ 第一章 群

▼ §1 群的典型例子: 循环群, 二面体群, 矩阵群, 对称群

- 7. 设 m 是正整数, 在 $0, 1, 2, \dots, m-1$ 中, 与 m 互素的整数的个数记作 $\varphi(m)$, 称它为 Euler (欧拉) 函数. 证明: Z_m 的单位群 Z_m^* 的阶等于 $\varphi(m)$.
- 12. 设 $\sigma = (i_1, i_2, \dots, i_r)$, 则对于任意 $\tau \in S_n$, 有

$$\tau \sigma \tau^{-1} = (\tau(i_1), \tau(i_2), \dots, \tau(i_r))$$

▼ §2 子群, 陪集, Lagrange 定理, 循环群的子群

- 2. 设 H, K 都是群 G 的子群, 令 $HK \stackrel{\text{def}}{=} \{hk \mid h \in H, k \in K\}$. 则 HK 为子群当且仅当 $HK = KH$.
- 5. (1) $S_n = \langle (12), (23), \dots, (n-1\ n) \rangle$; (2) $S_n = \langle (12), (12\ \dots\ n) \rangle$.
- 6. 当 $n \geq 3$ 时, (1) A_n 由 3-轮换生成; (2) $A_n = \langle (123), (124), \dots, (12n) \rangle$.
- 9. 如果群 G 的阶为偶数, 则 G 必有 2 阶元素.
- 10. 证明 Euler 定理: 设 n 是正整数, 如果整数 a 与 n 互素, 则

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

其中 $\varphi(n)$ 是 Euler 函数。

- 13. 写出 A_4 的所有子群，并证明 A_4 没有 6 阶子群。
- 14. 设 H, K 是群 G 的有限子群，则 $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$

▼ §3 群的同构，群的直积

- 1. 实数加群 \mathbb{R} 与正实数乘法群 \mathbb{R}^* 同构。
- 8. 证明: $\mathbb{Z}_3 \times \mathbb{V} \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, 其中 \mathbb{V} 是 Klein 群。
- 10. $D_{12}, D_4 \times \mathbb{Z}_3, A_4 \times \mathbb{Z}_2$ 这三个 24 阶非交换群中, 有同构的吗?
- 11. $D_{2n} \cong D_n \times \mathbb{Z}_2$ when n is odd.
- 12. $O_n \cong SO_n \times \{I, -I\}$ when n is odd

▼ §4 群的同态，正规子群，商群，可解群

- 3. 设 F 是一个域, σ 是 $GL_n(F)$ 到 F^* 的一个映射: $\sigma(A) = |A|, \forall A \in GL_n(F)$. 则 $GL_n(F)/SL_n(F) \cong F^*$.
- 10. $D'_n = \langle \sigma^2 \rangle$ (where $D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = I, \tau\sigma\tau = \sigma^{-1} \rangle$)
- 12. $S'_n = A_n, n \geq 3$.
- 13. $A'_n = A_n, n \geq 5$
- 14. 写出 S_4 的导群列, 由此看出, S_4 是可解群。
- 17. A_n is simple group, $n \geq 5$
- 15. 如果置换群 G 含有奇置换, 则 G 必有指数为 2 的子群。
- 16. 设 σ 是群 G 到群 G' 的一个满同态, 记 $K = \text{Ker } \sigma$. 设 $H' \triangleleft G'$, 令 $\sigma^{-1}(H') \stackrel{\text{def}}{=} \{g \in G \mid \sigma(g) \in H'\}$. 证明: (1) $\sigma^{-1}(H') \triangleleft G$, 且 $\sigma^{-1}(H') \supseteq K$; (2) $H' \mapsto \sigma^{-1}(H')$ 是 G' 的子群集合到 G 的包含 K 的子群集合的一个双射。

▼ §5 群在集合上的作用，群的自同构，轨道-稳定子定理

- 4. 设 F 是一个域, $GL_n(F)$ 的中心为 $\{kI_n \mid k \in \mathbb{Z}\}$.
- 5. $GL_2(C)$ 的每一个元素

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

引起了扩充复平面 $C \cup \{\infty\}$ 上的一个变换:

$$z \mapsto \frac{az + b}{cz + d},$$

称它为 Möbius (默比乌斯) 变换。证明: (1) 所有 Möbius 变换组成的集合 G 对于变换的乘法成一个群, 称它为 Möbius 群; (2) $GL_2(C)/Z(GL_2(C)) \cong G$.

- 6. 设 G 是一个群, 证明: 如果 $G/Z(G)$ 是循环群, 则 G 是 Abel 群。
- 7. 分别求 D_{2m-1}, D_{2m} 的中心, 其中 $m \geq 2$.
- 8. 求 S_n 的中心, 其中 $n \geq 3$.
- 14. Determine all conjugacy classes of D_{2m-1} and D_{2m} , where $m \geq 2$.
- 15. 设 σ 的不相交的轮换分解式 (包含所有的 1-轮换) 为

$$\sigma = (a_1 a_2 \dots a_{l_1})(b_1 b_2 \dots b_{l_2}) \dots (q_1 q_2 \dots q_{l_r})$$

其中 $l_1 \geq l_2 \geq \dots \geq l_r$, 且 $l_1 + l_2 + \dots + l_r = n$ 。则我们把有序数组 (l_1, l_2, \dots, l_r) 称为置换 σ 的型 (type), 也称为 n 的一个分拆 (partition)。证明: (1) σ_1 与 σ_2 在 S_n 中共轭当且仅当 σ_1 与 σ_2 同型; (2) S_n 中共轭类的个数等于 n 的分拆的个数。

- 16. 求 S_4 的共轭类的个数, 以及每个共轭类的代表和元素数目。
- 17. 求 A_4 的共轭类的个数, 以及每个共轭类的代表和元素数目。
- 18. 设 σ 是一个 n -轮换。求 σ 的共轭类的元素数目, 以及 $C_{S_n}(\sigma)$ 的阶。
- 19. 求 O_2 的所有共轭类。
- 20. 群 G 的子群 H 为正规子群当且仅当 H 是 G 的一些共轭类的并集。
- 21. (1) 求 S_5 的共轭类的个数, 以及每个共轭类的代表和元素数目; (2) 证明: S_5 只有三个正规子群, 即 $\{1\}, A_5, S_5$ 。
- 22. 设 G 为 p -群, $N \triangleleft G$, 且 $|N| = p$. 证明: $N \subseteq Z(G)$.
- 23. 设 G 是一个群, G 的所有子群组成的集合记作 Ω . 令 $G \times \Omega \rightarrow \Omega : (a, H) \mapsto aHa^{-1}$. 容易看出这给出了群 G 在 Ω 上的一个作用。 H 的轨道 $G(H)$ 是由 H 的所有共轭子群组成的。 H 的稳定子群 $G_H = \{g \in G \mid gHg^{-1} = H\}$ 称为 H 在 G 中的正规化子 (normalizer), 记作 $N_G(H)$ 。显然, $H \triangleleft N_G(H)$ 。证明: 如果 G 为有限群, $H < G$, 则 H 的共轭子群的个数等于 $[G : N_G(H)]$.
- 24. 设 H 是有限群 G 的一个非平凡子群, 则 $G \neq \bigcup_{g \in G} gHg^{-1}$.
- 25. 设 G 为一个 $2k$ 阶群, k 为奇数, 证明: G 必有指数为 2 的子群。
- 26. Let H be a subgroup of the group G , then the kernel of the left multiplication action of G on the left coset set $(G/H)_l$ is equal to $\bigcap_{x \in G} xHx^{-1}$.
- 27. 设 G 为一个有限群, $H < G$, 且 $[G : H] = n > 1$. 证明: G 或者有一个指数整除 $n!$ 的非平凡正规子群, 或者 G 同构于 S_n 的一个子群。
- 32. 设群 G 与群 H 分别作用在集合 Ω 和 W 上. 令

$$(g, h) \circ (x, y) \stackrel{\text{def}}{=} (g \circ x, h \circ y),$$

易证明这给出了群 $G \times H$ 在集合 $\Omega \times W$ 上的一个作用, 称它是乘积作用 (product action)。 $\Omega \times W$ 里的元素 (x, y) 的轨道 $(G \times H)(x, y) = G(x) \times H(y)$, (x, y) 的稳定子群 $(G \times H)_{(x,y)} = G_{(x)} \times H_{(y)}$ 。-->

▼ §6 Sylow 定理

- 1. 证明不存在阶为 148 的单群。
- 2. 证明不存在阶为 36 的单群。
- 3. 证明不存在阶为 56 的单群。
- 4. 证明不存在阶为 30 的单群。
- 5. 证明 6 阶群或者是循环群, 或者同构于 S_3 。
- 6. 决定 10 阶群的类型。
- 7. 决定 15 阶群的类型。
- 8. 决定 35 阶群的类型。
- 9. 决定 21 阶群的类型。
- 10. 设 p, q 都是素数, 且 $p < q$ 。决定 pq 阶群的类型。
- 11. 设 p, q 是不同的素数。证明 p^2q 阶群必包含一个正规的 Sylow 子群。
- 12. 设群 G 的阶为 p^3 , 其中 p 是素数。证明: 如果 G 是非交换群, 则 $|Z(G)| = p$, 且 $Z(G) = G'$ 。
- 13. 设 p 是素数。计算 S_p 中 Sylow p -子群的个数。由此证明 Wilson 定理:

$$(p-1)! \equiv -1 \pmod{p}.$$

- 14. 设 G 为一个有限群, $N \triangleleft G$, P 是 N 的一个 Sylow p -子群。证明: $G = N \cdot N_G(P)$ 。
- 15. 证明: 如果有限群 G 有一个循环的 Sylow 2-子群, 则 G 有一个指数为 2 的子群。

▼ §7 有限 Abel 群的结构

- 1. 决定 12 阶 Abel 群的互不同构的类型。
- 2. 决定 108 阶 Abel 群的互不同构的类型。
- 3. 决定 360 阶 Abel 群的互不同构的类型。
- 4. 决定 144 阶 Abel 群的互不同构的类型。
- 5. 决定 216 阶 Abel 群的互不同构的类型。
- 6. 求下列群的初等因子: (1) $Z_{16} \times Z_{15} \times Z_{20}$; (2) $Z_9 \times Z_{45}$; (3) $Z_4 \times Z_{14} \times Z_{16}$ 。
- 7. 设 G 是 100 阶 Abel 群。(1) 证明 G 必含有 10 阶元; (2) G 的初等因子应当怎样才能使 G 不含大于 10 的元素?
- 8. 证明: 如果有限 Abel 群的阶没有平方因子, 则它必为循环群。
- 9. 证明: 一个 Abel p -群如果恰好有 $p-1$ 个 p 阶元, 则它一定是循环群。
- 10. 设 V 是域 Z_2 上的 n 维线性空间, 决定 V 的加法群的结构, 写出它的初等因子, 它是不是初等 Abel 2-群?
- 11. 设 V 是域 Z_p 上的 n 维线性空间, p 是素数。 V 的加法群是不是初等 Abel p -群?

▼ §8 自由群, 群的表现

- 1. 把下列由字母表 $X = \{x, y, z\}$ 形成的字化简成既约字: (1) $w_1 = x^{-1}y^4y^{-1}y^{-3}zz^{-2}y^{-1}z^{-1}$; (2) $w_2 = z^{-2}y^3x^{-2}x^{-2}yx^2z^{-3}z^3$; (3) $w_3 = z_3^2yxx^{-1}xz^{-1}y^2z^{-1}y^{-1}$ 。
- 2. w_1, w_2, w_3 同第 1 题, 求 $w_1w_2w_3$ 。
- 3. 在 3-辫群 B_3 中, 求 b_1^2, b_2^2, b_1b_2 , 其中 b_1, b_2 是初等辫子 (见 §8 的图 1-10)。
- 4. 在 3-辫群 B_3 中, 分别写出 b_1^2, b_2^2, b_1b_2 产生的 S_3 中的置换。
- 5. 找出 B_3 中的两个不同的辫子, 它们都产生置换 (132)。
- 6. 在 4-辫群 B_4 中, 求 b_1b_3, b_3b_1 和 $b_3b_1b_3^{-1}$, 其中 b_1, b_3 都是初等辫子 (见 §8 的图 1-14)。从所画的图看, b_1b_3 与 b_3b_1 相等吗?
- 7. 设 G 和 G' 是两个群, x_1, x_2, \dots, x_n 称为一个字, 其中每个 x_i 属于无交并 $G \cup G'$ (即, 把 G 的元素与 G' 的元素看成不同的元素形成的并集, 注意即使 $G = G'$, 在求无交并 $G \cup G'$ 时, 也需要把前一个集合 G 与后一个集合 G' 的元素看成不同的元素)。称一个字是既约的, 如果 x_i 与 x_{i+1} 不在同一个群里 ($1 \leq i < n$), 并且 x_i 不是 G 或 G' 的单位元 ($1 \leq i \leq n$)。可证明每一个字能化简成唯一的既约字 (类似于本节定理 1 的证法)。两个既约字 w_1 与 w_2 相乘就是在 w_1 后面接着写 w_2 , 然后把它化简成既约字。所有既约字连同字空间的集合对于上述乘法成一个群, 称它为 G 与 G' 的自由积 (free product), 记作 $G * G'$ 。证明: $Z * Z \cong F_2$, 其中 F_2 代表由 2 个元素生成的自由群。

▼ 第二章 环

▼ §1 环的类型和性质, 理想

- 2. 有限整环是域。
- 4. 设 R 是有单位元的环, 则 R 的每一个非平凡的理想都不能含有单位元。
- 5. 域 F 没有非平凡的理想。
- 6. 设 R 是一个有单位元的交换环, 如果 R 没有非平凡的理想, 则 R 是一个域。
- 10. 设 D 是一个除环, 证明 $M_n(D)$ 是单环。

▼ 第三章 域扩张及其自同构

0.0 其他

0.0.1 定义-命题(半直积)

设 H 和 N 为群, $\varphi : H \rightarrow \text{Aut}(N)$ 为群同态; 记 $h \in H$ 对 φ 的像为 $\varphi_h : N \rightarrow N$ 。在积集 $N \times H$ 上定义二元运算

$$(n, h)(n', h') := (n\varphi_h(n'), hh').$$

这给出群结构, 称为 H 和 N 相对于 φ 的半直积, 记为 $N \rtimes_{\varphi} H$ 。它满足

$$1_{N \rtimes H} = (1_N, 1_H), \quad (n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1}).$$

群 N 和 H 分别通过 $n \mapsto (n, 1_H)$ 和 $h \mapsto (1_N, h)$ 嵌入为 $N \rtimes H$ 的子群。进一步, $N \triangleleft N \rtimes_{\varphi} H$; 事实上,

$$(1_N, h)(n, 1_H)(1_N, h)^{-1} = (\varphi_h(n), 1_H).$$

先说明定义的动机: 我们的思路是将 H 和 N 嵌入一个更大的群 G , 使得 $N \triangleleft G$ 而且 G 的所有元素都能唯一地表为 nh , 其中 $n \in N$ 而 $h \in H$ 。熟悉的写法

$$nh \cdot n'h' = \underbrace{n h n' h^{-1}}_{\in N} h h'$$

表明只要能对所有 h 和 n' 描述 $Ad_h(n') = hn'h^{-1}$, 则 G 的乘法便唯一从 N 和 H 的乘法确定。定义中的 φ_h 正是此处的 $Ad_h \in \text{Aut}(N)$ 。关于公允和逆元的描述也都可以按此理解。

严格论证将反其道而行, 从 N, H 和 φ 构造这般的群 G , 而自然的思路是在积集 $N \times H$ 上建群。

严格证明

首先是乘法结合律:

$$((n, h)(n', h'))(n'', h'') = (n\varphi_h(n'), hh')(n'', h'') = (n\varphi_h(n')\varphi_{hh'}(n'')), hh'h'',$$

$$(n, h)((n', h')(n'', h'')) = (n, h)(n'\varphi_{h'}(n'')), h'h'') = (n\varphi_h(n'\varphi_{h'}(n'')), hh'h'').$$

问题化为证 $\varphi_h(n')\varphi_{hh'}(n'') = \varphi_h(n'\varphi_{h'}(n''))$; 因为 φ_h 是同态, 目标进一步化为 $\varphi_{hh'} = \varphi_h\varphi_{h'}$, 然而 $\varphi : H \rightarrow \text{Aut}(N)$ 也是同态, 故结合律得证。

公允 $(1_N, 1_H)$ 的性质容易归结为 $\varphi_{1_H} = \text{id}_N$ 和 $\varphi_h(1_N) = 1_N$ 。至于逆元的性质, 我们有

$$\begin{aligned} (n, h)(\varphi_{h^{-1}}(n^{-1}), h^{-1}) &= (n\varphi_h(\varphi_{h^{-1}}(n^{-1})), hh^{-1}) \\ &= (nn^{-1}, hh^{-1}) = (1_N, 1_H), \\ (\varphi_{h^{-1}}(n^{-1}), h^{-1})(n, h) &= (\varphi_{h^{-1}}(n^{-1})\varphi_{h^{-1}}(n), h^{-1}h) \\ &= (\varphi_{h^{-1}}(n^{-1}n), h^{-1}h) = (1_N, 1_H). \end{aligned}$$

最后, 嵌入 $H \hookrightarrow N \rtimes_{\varphi} H$ 和 $N \hookrightarrow N \rtimes_{\varphi} H$ 的同态性质是毫无困难的。按此计算

$$(1_N, h)(n, 1_H)(1_N, h)^{-1} = (\varphi_h(n), h)(1_N, h^{-1}) = (\varphi_h(n), 1_H);$$

此处用到了 $\varphi_h(1_N) = 1_N$ 。

注:

如果取 $\varphi : H \rightarrow \text{Aut}(N)$ 为平凡同态, 亦即 $\forall h, \varphi_h = \text{id}_N$, 则 $N \rtimes H$ 便化为直积 $N \times H$ 。

留意到若将 N 和 H 等同于 $N \rtimes_{\varphi} H$ 的子群, 则它们的交为平凡子群, 而且 $N \rtimes_{\varphi} H = NH$; 这蕴涵 $N \rtimes_{\varphi} H$ 都能唯一地写成 nh 的形式。

example: 验证 $(n, h) \mapsto h$ 给出满同态 $N \rtimes_{\varphi} H \rightarrow H$, 而且它诱导同构 $(N \rtimes_{\varphi} H)/N \cong H$ 。

0.0.2 定义-命题 11.10.3 (半直积的内在版本)

设 H 和 N 为群 G 的子群, 满足下述条件

$$N \triangleleft G, \quad G = NH, \quad N \cap H = \{1\}.$$

考虑由 $\text{Ad}_h(n) = hn h^{-1}$ 给出的同态 $\text{Ad} : H \rightarrow \text{Aut}(N)$, 则有群同构

$$\begin{aligned}\Phi : N \rtimes_{\text{Ad}} H &\xrightarrow{\sim} G \\ (n, h) &\mapsto nh.\end{aligned}$$

此时也称 G 是子群 H 和正规子群 N 的半直积, 合理地记为 $G = N \rtimes H$ 。

证明 验证 Φ 是群同态: $(n, h)(n', h') = (n \text{Ad}_h(n'), hh')$ 被映为 $n \text{Ad}_h(n')hh'$, 然后后者即 $nhn'h^{-1}hh' = (nh)(n'h')$ 。

条件 $G = NH$ 相当于说 Φ 满。最后证明 Φ 单: 若 $\Phi(n, h) = 1$, 则 $n = h^{-1} \in N \cap H = \{1\}$ 。因此 Φ 是同构。

example: S_n 是 A_n 与 $\langle (12) \rangle$ 的半直积

0.1 群

0.1.1 令 S 是整数加群 \mathbb{Z}^+ 的子群, 则 S 或为平凡子群 $\{0\}$, 或是有形式 Z_a , 其中 a 为 S 中最小正整数。

证明: 令 S 是 \mathbb{Z} 的一个子群, 则 $0 \in S$ 。如果 0 是 S 中唯一的元素, 则 S 为平凡子群。因而对这一情形结论成立。否则, S 包含异于 0 的整数 n , 且要么 n 是正数, 要么 $-n$ 是正数。由子群的第三个性质知: $-n \in S$ 。故 S 含有正整数。我们必须证明 $S = Z_a$, 其中 a 为 S 中最小正整数。

首先证明 Z_a 是 S 的子集, 换句话说, $ka \in S$ 对于任意整数 k 成立。如果 k 是正整数, 则 $ka = a + a + \cdots + a$ (k 项)。由于 $a \in S$, 由子群的封闭性和归纳法知 $ka \in S$ 。子群中元素的逆元仍属于 S , 因此 $-ka \in S$ 。最后, $0a = 0 \in S$ 。

其次, 证明 S 是 Za 的子集, 即 S 中任意元素 n 是 a 的整数倍。用带余除法, 记 $n = qa + r$, 其中 q, r 都是整数且余数 r 的取值范围为 $0 \leq r < a$ 。由于 $Za \subseteq S$, 故 $qa \in S$, 当然 $n \in S$ 。因为 S 是子群, 故也有 $r = n - qa \in S$ 。现在, 根据我们的选取, a 为 S 中最小正整数, 而余数 r 满足 $0 \leq r < a$ 。因此, 属于 S 的唯一余数是 0 。所以, $r = 0$ 且 n 是 a 的整数倍数 qa 。

0.1.2 Any group can be expressed as a union of cyclic subgroups.

This follows directly from set inclusion: every element $g \in G$ belongs to the cyclic subgroup $\langle g \rangle$, so $G = \bigcup_{g \in G} \langle g \rangle$.

0.1.3 A group G has only finitely many subgroups $\Leftrightarrow G$ is finite.

Assume G has finitely many subgroups. We only need to prove: an infinite group G must have infinitely many subgroups.

First, suppose G is not cyclic. By [the previous problem](#), $G = \bigcup_{g \in G} \langle g \rangle$, and there must exist some $\langle g_0 \rangle$ that is an infinite cyclic group. Thus, without loss of generality, we may assume G is the cyclic group $\langle g_0 \rangle$, which has infinitely many subgroups: $\langle g_0 \rangle, \langle g_0^2 \rangle, \langle g_0^3 \rangle, \dots$

Next, if G is finite, the conclusion is obvious by [the previous problem](#).

□

0.1.4 There does not exist a group with exactly two elements of order 2

Suppose, for contradiction, that G is a group with exactly two distinct elements of order 2, say a and b .

Case 1: $ab = ba$.

Then ab is distinct from a , b , and e , and $(ab)^2 = a^2b^2 = e$, so ab has order 2. This contradicts the assumption that G has only two elements of order 2.

Case 2: $ab \neq ba$.

Consider aba . Since $a \neq b$, aba is distinct from a , b , and e . Moreover, $(aba)^2 = ab(a^2)ba = abba = e$, so aba has order 2, again yielding a contradiction.

Thus, no such group G can exist.

□

0.1.5 Abel单群一定为素数阶循环群

熟知Abel群的子群一定为正规子群。又因 G 是单群，其正规子群仅有 $\{e\}$ 和 G 本身。于是任取非单位元 $g \in G, g \neq e$, 构造子群 $\langle g \rangle$, 由于 $\langle g \rangle \neq \{e\}$, 故 $\langle g \rangle = G$ 。

断言 $|G| = n$ 为素数 若不然, 存在 $a, b > 1$ 使得 $n = ab$, 循环群 G 必存在一个 a 阶子群 (例如由 g^b 生成的子群 $\langle g^b \rangle$) , 这与 G 无非平凡子群矛盾。

□

0.1.6

0.1.7 (1) $|GL_n(F_p)| = \prod_{k=0}^{n-1} (p^n - p^k)$, $|SL_n(\mathbb{F}_p)| = \frac{|GL_n(\mathbb{F}_p)|}{p-1}$; (2) 求 $GL_n(F_p)$ 的 sylow-p子群, 并确定sylow-p子群的个数

(1) 对于前者: 一个 $n \times n$ 可逆矩阵的 n 个列向量必须线性无关。第 1 列: 可以是 \mathbb{F}_p^n 中任意非零向量, 共 $p^n - 1$ 种选择。第 2 列: 不能与第 1 列共线 (即不在其张成的 1 维子空间中), 共 $p^n - p$ 种选择。第 3 列: 不能在前两列张成的 2 维子空间中, 共 $p^n - p^2$ 种选择。依此类推, 直到第 n 列。

后者可由习题1.4.3

(2)

□

0.1.8 群 G 的类方程是 $1 + 4 + 5 + 5 + 5$

(1) G 有 5 阶子群吗? 如果有, 它是正规子群吗?

证明: 设共轭类依次为 $G(x_1), G(x_2), G(x_3), G(x_4), G(x_5)$, 阶数依次为 1, 4, 5, 5, 5。由轨道稳定子定理知 $C_G(x_2)$ 阶数为 $|G|/|G(x_2)|$ 。于是 $C_G(x_2)$ 为 G 的一个 5 阶子群。断言 G 只有这一个 5 阶子群。若不然: 设 $\langle r \rangle, \langle s \rangle$ 为 G 的两个不同 5 阶子群, 则 $\langle r \rangle \cap \langle s \rangle = e$ (否则他们相同)。于是有 $r^i s^j = r^m s^n \Leftrightarrow r^{i-m} = s^{n-j} \equiv e \Leftrightarrow m = n, i = j$ (这里规定 $0 \leq i, j, m, n \leq 5$) 于是有 $|G| \geq |\{r^i s^j | 0 \leq i, j \leq 5\}| = 25$, 矛盾!

(2) G 有 4 阶子群吗? 如果有, 它是正规子群吗?

不用Sylow很目前觉得困难

0.1.9 Showing that a p-group has a normal subgroup for each divisor of its order

proof: We will use induction on n , where $|P| = p^n$. Clearly the result is true if $|P| = p^1$. Now assume the statement is true for all groups of order p^k where $k < n$.

Since P is a p -group it has nontrivial center, and $Z(P)$ is also a p -group. It follows that P has a normal subgroup of order p , say N . Form the quotient group P/N , which has order p^{n-1} , and therefore has a normal subgroup of order q for each divisor q of p^{n-1} by the induction hypothesis.

We can show that P has a normal subgroup of index $p^i, 1 \leq i \leq n$. Clearly this is true for $i = 1, n$, and $|P : N| = p^{n-1}$. Consider the canonical homomorphism $\pi : P \rightarrow P/N$, which is surjective. Then by the **Correspondence Theorem**, π and π^{-1} are inverse bijections between subgroups of P/N and subgroups of P containing N , that respect normality and index. Then since P/N (by the induction hypothesis) has a normal subgroup of index $p \leq i \leq p^{n-2}$, so does P , and the result follows.

0.1.10 n 为素数时, S_n 中 n 阶元一定是 n -轮换。当 n 为一般整数时不一定成立

hint: 任意置换 $\sigma \in S_n$ 可以唯一分解为不相交轮换的乘积: $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$, 其中 γ_i 是长度为 ℓ_i 的轮换, 且 $\ell_1 + \ell_2 + \dots + \ell_k \leq n$ 。置换的阶为: $\text{ord}(\sigma) = \text{lcm}(\ell_1, \ell_2, \dots, \ell_k)$.

0.2 环

0.2.1 n 阶实方阵全体对于通常的矩阵加法和乘法形成含幺环, 叫做 n 阶实方阵环, 表示成 $M_n(R)$. 零元素为 n 阶零方阵, 矩阵元素为 n 阶单位方阵 I_n . 类似可定义有理矩阵环 $M_n(Q)$, 复矩阵环 $M_n(C)$ 等. 当 $n \geq 2$ 时, 易知它们均不是交换环.

更一般地, 对于任意环 R , 我们仍旧像通常那样定义元素属于 R 的两个 n 阶方阵的加法和乘法, 可以直接验证全体这种 n 阶方阵形成环, 叫做环 R 上的 n 阶方阵环, 表示成 $M_n(R)$. 如果环 R 有幺元素 1_R , 则环

$M_n(R)$ 也有幺元素 $I_n = \begin{pmatrix} 1_R & & \\ & \ddots & \\ & & 1_R \end{pmatrix}$. 进而, 如果 R 是交换环, 我们可以定义方阵 $A = (a_{ij}) \in M_n(R)$

的行列式 $\det A = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$. 基于环 R 的乘法交换性, 我们可以看出 $\det A$ 仍具有行列式通常那些性质, 例如:

- (1) $(\det A)(\det B) = \det(AB);$
- (2) $A(\text{adj}A) = (\text{adj}A)A = (\det A) \cdot I_n.$

其中 $\text{adj}A$ 表示 A 的伴随方阵, 即 $\text{adj}A = (A_{ji})$, 而 A_{ij} 是 A 中元素 a_{ij} 的代数余子式. 上面 (1) 式表明, 当 R 为含幺交换环时, 行列式映射

$$\det : M_n(R) \rightarrow R, \quad A \mapsto \det A$$

是乘法半群的同态 (并且易知这是满同态). 因此若 A 是环 $M_n(R)$ 中的单位, 则 $\det A$ 也是环 R 中的单位. 反之, 如果 $\det A \in U(R)$, 则由上面的 (2) 式可知 $(\det A)^{-1} \text{adj}A$ 是 A 的逆元素, 即 $A \in U(M_n(R))$. 这就完全决定了矩阵环 $M_n(R)$ 的单位群 (其中 R 为含幺交换环):

$$U(M_n(R)) = \{A \in M_n(R) \mid \det A \in U(R)\}$$

. 乘法群 $U(M_n(R))$ 叫做含幺交换环 R 上的 n 次一般线性群, 表示成 $GL(n, R)$. 例如 $GL(n, \mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$, 而对任意域 F , $GL(n, F) = \{A \in M_n(F) \mid \det A \neq 0\}$.

注: 这里 $U(R)$ 表示环 R 的乘法逆元的集合 (单位群)

域

第一章 群

§1 群的典型例子: 循环群, 二面体群, 矩阵群, 对称群

7. 设 m 是正整数, 在 $0, 1, 2, \dots, m-1$ 中, 与 m 互素的整数的个数记作 $\varphi(m)$, 称它为 Euler (欧拉) 函数. 证明: \mathbb{Z}_m 的单位群 \mathbb{Z}_m^* 的阶等于 $\varphi(m)$.

12. 设 $\sigma = (i_1, i_2, \dots, i_r)$, 则对于任意 $\tau \in S_n$, 有

$$\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \dots, \tau(i_r))$$

§2 子群, 陪集, Lagrange 定理, 循环群的子群

2. 设 H, K 都是群 G 的子群, 令 $HK \stackrel{\text{def}}{=} \{hk \mid h \in H, k \in K\}$ 。则 HK 为子群当且仅当 $HK = KH$ 。

5. (1) $S_n = \langle (12), (23), \dots, (n-1\ n) \rangle$; (2) $S_n = \langle (12), (12\dots n) \rangle$.

(1) $(ij) = (1i)(1j)(1i)$, $S_n = \langle (12), (13), \dots, (1n) \rangle$, 因此只要对于 $k \in \{3, 4, \dots, n\}$, 去证 $(1k)$ 可以表示成 $(12), (23), \dots, (n-1, n)$ 这些对换的乘积(它们可以重复出现)。由习题1.1.12得

$$(13) = (23)(12)(23),$$

$$(14) = (34)(13)(34) = (34)(23)(12)(23)(34),$$

...

$$\begin{aligned}(1k) &= (k-1, k)(1, k-1)(k-1, k) \\ &= (k-1, k)(k-2, k-1) \dots (34)(23)(12)(23)(34) \dots (k-2, k-1)(k-1, k).\end{aligned}$$

因此 $S_n = \langle (12), (23), (34), \dots, (n-1, n) \rangle$.

(2) 根据(1), 只要去证对于 $k \in \{2, 3, \dots, n-1\}$, 有 $(k, k+1)$ 可以表示成 $(12), (123\dots n)$ 的整数次幂的乘积。

$$(23) = (123\dots n)(12)(123\dots n)^{-1},$$

$$(34) = (123\dots n)(23)(123\dots n)^{-1} = (123\dots n)^2(12)(123\dots n)^{-2},$$

...

$$\begin{aligned}(k, k+1) &= (123\dots n)(k-1, k)(123\dots n)^{-1} \\ &= (123\dots n)^{k-1}(12)(123\dots n)^{-(k-1)}.\end{aligned}$$

因此 $S_n = \langle (12), (123\dots n) \rangle$.

6. 当 $n \geq 3$ 时, (1) A_n 由 3-轮换生成; (2) $A_n = \langle (123), (124), \dots, (12n) \rangle$.

(1) n 元偶置换可以写为 3-轮换之积 $(1i)(1j) = (1ji)$

(2) 只要证任一 3-轮换 $(ijk) \in \langle (123), (124), \dots, (1n) \rangle$.

$$\begin{aligned}(ijk) &= [(1i)(2j)](12k)[(1i)(2j)]^{-1} \\ &= [(1i)(12)(2i)(2j)](12k)[(1i)(12)(2i)(2j)]^{-1} \\ &= [(12i)(12j)](12k)[(12i)(12j)]^{-1}.\end{aligned}$$

因此 $A_n = \langle (123), (124), \dots, (1n) \rangle$.

9. 如果群 G 的阶为偶数, 则 G 必有 2 阶元素。

反证秒了

10. 证明 Euler 定理：设 n 是正整数，如果整数 a 与 n 互素，则

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

其中 $\varphi(n)$ 是 Euler 函数。

$a \in Z_n^*$, 由 Lagrange 定理 $|a| | |Z_n^*|$, i.e., $|a| | \varphi(n)$

13. 写出 A_4 的所有子群，并证明 A_4 没有 6 阶子群。

A_4 的阶为 $\frac{4!}{2} = 12$, 因此 A_4 的子群的阶只可能是 1, 2, 3, 4, 6, 12. A_4 有：

- 1 个 1 阶子群: $\{(1)\}$
- 3 个 2 阶子群: $\{(1), (12)(34)\}, \{(1), (13)(24)\}, \{(1), (14)(23)\}$
- 4 个 3 阶子群: $\{(1), (123), (132)\}, \{(1), (124), (142)\}, \{(1), (134), (143)\}, \{(1), (234), (243)\}$
- 1 个 4 阶子群: $\{(1), (12)(34), (13)(24), (14)(23)\}$
- 1 个 12 阶子群: A_4

A_4 没有 6 阶子群：假设 H 是 A_4 的 6 阶子群。由于 A_4 中不是 3-轮换的元素只有 4 个，因此 H 中必有 3-轮换。如果 H 中有一个 3-轮换，那么它的逆也属于 H 。又由于 3-轮换的逆不等于自身，因此 H 中 3-轮换的数目 r 为偶数。由于 H 中有单位元 (1) ，因此 $r = 4$ 或 $r = 2$ 。

情形 1: $r = 4$. 设 $\sigma, \sigma^{-1}, \tau, \tau^{-1}$ 是 H 中的 3-轮换，则 $(1), \sigma, \sigma^{-1}, \tau, \tau^{-1}, \sigma\tau, \sigma\tau^{-1}$ 是 H 中 7 个不同的元素，这与 $|H| = 6$ 矛盾。

情形 2: $r = 2$. 由于 A_4 中含有 8 个 3-轮换，3 个 2 阶元，1 个单位元，因此 6 阶子群 H 一定包含 A_4 的 4 阶子群：

$\{(1), (12)(34), (13)(24), (14)(23)\}$ 。从而 A_4 的这个 4 阶子群也是 H 的一个子群，但是 4 不是 6 的因数，这与 Lagrange 定理矛盾。

综上所述， A_4 没有 6 阶子群。

14. 设 H, K 是群 G 的有限子群，则 $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$

记 $H \cap K = M$, 则 M 是 G 的子群. 又由于 $M \subseteq H$, 因此 M 也是 H 的子群. 设 M 在 H 中的左陪集分解式为 $H = \bigcup_{i=0}^{r-1} h_i M$, 其中 $h_0 = e$. 显见

$$HK = \left(\bigcup_{i=0}^{r-1} h_i M \right) K = \bigcup_{i=0}^{r-1} (h_i M) K = \bigcup_{i=0}^{r-1} h_i (MK) = \bigcup_{i=0}^{r-1} h_i K,$$

其中最后一步是由于 $M \subseteq K$ 且 K 是子群，因此 $MK = K$.

对于 $i, j \in \{0, 1, \dots, r-1\}$, 当 $i \neq j$ 时, 有 $h_i M \cap h_j M = \emptyset$. 假如 $h_i K \cap h_j K \neq \emptyset$, 则存在 $k_1, k_2 \in K$, 使得 $h_i k_1 = h_j k_2$. 从而 $h_j^{-1} h_i = k_2 k_1^{-1} \in H \cap K = M$. 于是 $h_i M = h_j M$, 矛盾. 因此 $h_i K \cap h_j K = \emptyset$. 从而

$$\begin{aligned} |HK| &= \sum_{i=0}^{r-1} |h_i K| = \sum_{i=0}^{r-1} |K| = r|K| = [H : M]|K| \\ |HK| &= \frac{|H|}{|M|}|K| = \frac{|H| \cdot |K|}{|H \cap K|}. \end{aligned}$$

§3 群的同构，群的直积

1. 实数加群 \mathbb{R} 与正实数乘法群 \mathbb{R}^* 同构.

映射 $\phi: x \mapsto e^x$

8. 证明: $Z_3 \times V \cong Z_2 \times Z_6$, 其中 V 是 Klein 群.

由于 $V = Z_2 \times Z_2$, 因此 $Z_3 \times V = Z_3 \times (Z_2 \times Z_2)$, 说明映射 $(a, (b, c)) \mapsto ((a, b), c)$ 是 $Z_3 \times (Z_2 \times Z_2)$ 到 $(Z_3 \times Z_2) \times Z_2$ 的一个同构映射, 从而 $Z_3 \times (Z_2 \times Z_2) \cong (Z_3 \times Z_2) \times Z_2$. 又由于 $Z_3 \times Z_2 \cong Z_6$, 从而说明 $(Z_3 \times Z_2) \times Z_2 \cong Z_6 \times Z_2$. 最后说明 $Z_6 \times Z_2 \cong Z_2 \times Z_6$. 利用同构关系的传递性即可得所要证的结论.

10. D_{12} , $D_4 \times Z_3$, $A_4 \times Z_2$ 这三个24阶非交换群中, 有同构的吗?

D_{12} 有12阶元 σ_{12} , 有12个(反射)二阶元

$D_4 \times Z_3$: 考虑同构映射 $f: D_4 \rightarrow D_4 \times Z_3, x \mapsto (x, \bar{0})$

σ_4 为 D_4 的4阶元, 故 $f(\sigma_4) = (\sigma_4, \bar{0})$ 是 $D_4 \times Z_3$ 的4阶元, 同理 $(e, \bar{1})$ 为 $D_4 \times Z_3$ 的3阶元. 又 $(3, 4) = 1$ 且 $(\sigma_4, \bar{0}) + (e, \bar{1}) = (\sigma_4, \bar{1}) = (e, \bar{1}) + (\sigma_4, \bar{0})$, 故 $(\sigma_4, \bar{1})$ 为 $D_4 \times Z_3$ 中的12阶元. 但是 $D_4 \times Z_3$ 中2阶元 (a, b) 的阶为 $\text{lcm}(|a|, |b|)$, 而 Z_3 没有2阶元, 于是这里 $D_4 \times Z_3$ 中2阶元 (a, b) 只能为 $(a, \bar{0})$ 与 D_4 中2阶元一一对应, 共计4个(反射)

$A_4 \times Z_2$: 由习题1.2.13, A_6 没有6阶元, 若 $A_4 \times Z_2$ 有12阶元 (a, b) , 则根据 $|(a, b)| = \text{lcm}(|a|, |b|), |a| = 12$, 于是 a^2 为 A_4 中6阶元, 矛盾! 于是 $A_4 \times Z_2$ 没有12阶元

综上, 他们三个两两不同构

11. $D_{2n} \cong D_n \times Z_2$ when n is odd.

The dihedral group D_n is presented as:

$$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = I, \tau\sigma\tau = \sigma^{-1} \rangle = \{\sigma^j, \sigma^j\tau \mid 0 \leq j \leq n-1\}$$

Similarly, D_{2n} is presented as:

$$D_{2n} = \langle \gamma, \delta \mid \gamma^{2n} = \delta^2 = I, \delta\gamma\delta = \gamma^{-1} \rangle$$

Consider the elements $(\sigma, \bar{1})$ and $(\tau, \bar{1})$ in $D_n \times Z_2$:

1. Order:

- $|(\sigma, \bar{1})| = \text{lcm}(|\sigma|, |\bar{1}|) = \text{lcm}(n, 2) = 2n$ (since n is odd).
- $|(\tau, \bar{1})| = \text{lcm}(2, 2) = 2$.

2. Conjugation:

- $(\tau, \bar{1})(\sigma, \bar{1})(\tau, \bar{1}) = (\tau\sigma\tau, \bar{1}) = (\sigma^{-1}, \bar{1})$.
- Moreover, $(\sigma^{-1}, \bar{1})(\sigma, \bar{1}) = (e, \bar{0})$ and $(\sigma, \bar{1})(\sigma^{-1}, \bar{1}) = (e, \bar{0})$.
- Thus, $(\tau, \bar{1})(\sigma, \bar{1})(\tau, \bar{1}) = (\sigma, \bar{1})^{-1}$, and by induction:

$$(\tau, \bar{1})(\sigma, \bar{1})^i(\tau, \bar{1}) = (\sigma, \bar{1})^{-i}, \quad i \in \mathbb{Z}.$$

3. Generating All Elements:

Any element $c = (\sigma^i\tau^j, \bar{k}) \in D_n \times Z_2$ (where $0 \leq i \leq n-1, 0 \leq j, k \leq 1$) can be expressed as:

- If $i+j-k = 0$, then $c = (\sigma, \bar{1})^i(\tau, \bar{1})^j$.
- Otherwise, $c = (\sigma, \bar{1})^i(\tau, \bar{1})^j(I, \bar{1}) = (\sigma, \bar{1})^i(\tau, \bar{1})^j(\sigma, \bar{1})^n$ (since n is odd).

This shows that $D_n \times Z_2$ is generated by $(\sigma, \bar{1})$ and $(\tau, \bar{1})$, with the relations:

$$D_n \times Z_2 = \langle (\sigma, \bar{1}), (\tau, \bar{1}) \mid (\sigma, \bar{1})^{2n} = (\tau, \bar{1})^2 = I, (\tau, \bar{1})(\sigma, \bar{1})(\tau, \bar{1}) = (\sigma, \bar{1})^{-1} \rangle.$$

Then it's easy to see that $D_{2n} \cong D_n \times Z_2$

12. $O_n \cong SO_n \times \{I, -I\}$ when n is odd

$SO_n \cap \{I, -I\} = I$, since n is odd.

It's easy to see that the elements of SO_n commute with the elements of $\{I, -I\}$ and $O_n = SO_n \times \{I, -I\}$.

Then we can obtain that $O_n \cong SO_n \times \{I, -I\}$

§4 群的同态，正规子群，商群，可解群

3. 设 F 是一个域, σ 是 $GL_n(F)$ 到 F^* 的一个映射: $\sigma(A) = |A|, \forall A \in GL_n(F)$. 则 $GL_n(F)/SL_n(F) \cong F^*$.

群同态基本定理

10. $D'_n = \langle \sigma^2 \rangle$ (where $D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = I, \tau\sigma\tau = \sigma^{-1} \rangle$)

Since $\sigma^i \sigma \sigma^{-i} = \sigma^2, \tau \sigma \tau^{-1} = (\tau \sigma \tau^{-1})^2 = (\sigma^{-1})^2 \in \langle \sigma^2 \rangle$, thus $\langle \sigma^2 \rangle \triangleleft D_n$.

$|\sigma^2| = \frac{|\sigma|}{(|\sigma|, 2)} = \frac{n}{(n, 2)}$. Therefore, $|D_n/\langle \sigma^2 \rangle| = \frac{2n}{(n, 2)} / \frac{n}{(n, 2)} = 2(n, 2) \in \{2, 4\}$. It is well known that second-order and fourth-order groups are both Abelian. Hence, $D_n/\langle \sigma^2 \rangle$ is an Abelian group. Thus, $D'_n \subseteq \langle \sigma^2 \rangle$. Since $\sigma^2 = \sigma \tau \sigma^{-1} \tau^{-1} \in D'_n$, thus $\langle \sigma^2 \rangle \subseteq D'_n$. Therefore, $D'_n = \langle \sigma^2 \rangle$. (When n is odd, $|\sigma^2| = n = |\sigma|$, thus $D'_n = \langle \sigma^2 \rangle = \langle \sigma \rangle$.)

12. $S'_n = A_n, n \geq 3$.

Since $[S_n : A_n] = 2$, thus $A_n \triangleleft S_n$, and S_n/A_n is an Abelian group. Therefore, $S'_n \subseteq A_n$.

A_n can be generated by 3-cycles, and for every 3-cycle (ijk) , and we have

$(ijk) = (ijk)^{-2} = (ikj)^2 = [(ij)(ik)]^2 = (ij)(ik)(ij)^{-1}(ik)^{-1} \in S'_n$, Therefore, $A_n \subseteq S'_n$.

Hence, $S'_n = A_n$.

13. $A'_n = A_n, n \geq 5$

When $n \geq 5$, for any 3-cycle swap (a_1, a_2, a_3) in A_n , define $\sigma = (a_1 a_3 a_4 a_2 a_5) \in A_n, \tau = (a_1 a_5 a_2) \in A_n$, then

$$\sigma \tau \sigma^{-1} \tau^{-1} = (a_3 a_1 a_5)(a_1 a_2 a_3) = (a_1 a_2 a_3).$$

Thus, $(a_1 a_2 a_3) \in A'_n$. Since A_n can be generated by 3-cycles, $A_n \subseteq A'_n$. Therefore, $A'_n = A_n$.

Notes: When $n \geq 5$, $S'_n = A_n, A'_n = A_n$. Then S_n is non-solvable, $n \geq 5$.

14. 写出 S_4 的导群列, 由此看出, S_4 是可解群。

Because $S'_4 = A_4, A'_4 = V$, and $V' = \{(1)\}$, it follows that $S_4^{(3)} = \{(1)\}$. Hence, S_4 is solvable.

17. A_n is simple group, $n \geq 5$

A_n can be generated by 3-cycles. That is, for any $a, b \in \{1, 2, \dots, n\}$ where $a \neq b$, take a 3-cycle (ijk) . Then $(ijk) = (ik)(jk)$.

$$\begin{aligned} (ij)(ka) &= (ai)(aj)(bj)(ka)(ai)(aj)(bj)^{-1} \\ &= (ai)(aj)(ab)(bj)(ka)(bj)^{-1}(ab)^{-1}(aj)^{-1}(ai)^{-1} \\ &= (abi)(bja)(abk)(bja)^{-1} = (abi)(abj)(abk)(abi)(abj)^{-1}; \\ (ajk) &= (jka) = (ajb)(akb)(ajb)^{-1} = (abj)^{-1}(abk)^{-1}(abj); \\ (bjk) &= (kbj) = (abk)(abj)(abk)^{-1}. \end{aligned}$$

Therefore, for any $a, b \in \{1, 2, \dots, n\}, a \neq b, A_n$ is generated by the set $M = \{(abl) \mid 1 \leq l \leq n, l \neq a, l \neq b\}$, i.e., $A_n = \langle M \rangle$.

Take any normal subgroup $N \neq \{(1)\}$ of A_n , we want to prove $N = A_n$.

Case 1: Suppose N contains a 3-cycle (abc) , then for any $k \in \{1, 2, \dots, n\}$ and $k \neq a, b, c$, we have

$$(abk) = (cbk)(acb)(cbk)^{-1} \in N.$$

Since $M \subseteq N$, then $\langle M \rangle \subseteq N$. But $A_n \subseteq N$. Therefore, $N = A_n$.

Case 2: Suppose N contains a permutation σ , and the decomposition of σ into transpositions has at least one r -cycle, where $r \geq 4$, i.e., $\sigma = (a_1a_2\dots a_r)\dots$. Take $\tau = (a_1a_2a_3) \in A_n$, then $\sigma_1 = \tau\sigma\tau^{-1} \in N$. And $\sigma^{-1}(\tau\sigma\tau^{-1}) = \sigma^{-1}\sigma_1 = \sigma^{-1}[(a_1a_2\dots a_r)\dots](a_1a_2a_3)[(a_1a_2\dots a_r)\dots]^{-1}(a_1a_2a_3)^{-1} = \sigma_1^{-1}(a_1a_2a_3)\sigma_1(a_1a_2a_3)^{-1} = \sigma_1^{-1}\sigma_1(a_1a_2a_3)(a_1a_2a_3)^{-1} = (a_1a_3a_r) \in N$. By Case 1, $N = A_n$.

Case 3: Suppose N contains a permutation σ , and the decomposition of σ into transpositions has at least two 3-cycles, i.e., $\sigma = (a_1a_2a_3)(a_4a_5a_6)\dots$. Take $\tau = (a_2a_3a_4) \in A_n$, then $\sigma_1 = \tau\sigma\tau^{-1} \in N$.

$$\begin{aligned} \sigma^{-1}(\tau\sigma\tau^{-1}) &= \sigma^{-1}\sigma_1 = \sigma^{-1}[(a_1a_2a_3)(a_4a_5a_6)\dots](a_2a_3a_4)[(a_1a_2a_3)(a_4a_5a_6)\dots]^{-1}(a_2a_3a_4)^{-1} \\ &= \sigma_1^{-1}\sigma_1[(a_1a_2a_3)^{-1}(a_1a_3a_4)(a_4a_5a_6)](a_1a_2a_4)^{-1} \\ &= (a_3a_1a_4)(a_1a_2a_4a_6), \end{aligned}$$

$(a_1a_4a_4a_2a_3) \in N$. By Case 2, $N = A_n$.

Case 4: Suppose N contains a permutation σ , and the decomposition of σ into transpositions is $\sigma = (a_1a_2)(a_3a_1)\sigma_1$, where σ_1 is a product of some disjoint transpositions. From $\sigma^2 = (a_1a_3a_2)$. From $(a_1a_3a_2) \in N$. By Case 1, $N = A_n$.

Case 5: Suppose N contains a permutation σ which is an even number of disjoint transpositions, i.e., $\sigma = (a_1a_2)(a_3a_4)\sigma_1$, where σ_1 is an even number of disjoint transpositions. Take $\tau = (a_1a_2a_3) \in A_n$, then $\sigma^{-1}(\tau\sigma\tau^{-1}) \in N$.

$$\begin{aligned} \sigma^{-1}(\tau\sigma\tau^{-1}) &= \sigma_1^{-1}\sigma_1[(a_1a_2)(a_3a_4)](a_1a_2a_3)[(a_1a_2)(a_3a_4)]\sigma_1(a_1a_2a_3)^{-1} \\ &= \sigma_1^{-1}\sigma_1(a_3a_4)(a_1a_2a_3)(a_1a_2)(a_3a_4)^{-1} \\ &= (a_1a_3a_4a_2) = (a_2a_4), \end{aligned}$$

Because $\gamma = (a_1a_3)(a_2a_4) \in N$. For $n \geq 5$, there exists $b \in \{1, 2, \dots, n\}$, and $b \neq a_1, a_2, a_3$, take $\delta = (a_3a_1b)$, then $\gamma^{-1}(\delta\gamma\delta^{-1}) \in N$.

$$\gamma^{-1}(\delta\gamma\delta^{-1}) = (\gamma^{-1}\delta\gamma)\delta^{-1} = (a_3a_1b)(a_1ba_3) = (a_1a_3b).$$

Therefore, $(a_1a_3b) \in N$. By Case 1, $N = A_n$.

In summary, $N = A_n$. Therefore, A_n is simple.

15. 如果置换群 G 含有奇置换, 则 G 必有指数为 2 的子群。

Let ψ be a mapping from G to the group of 2nd roots of unity U_2 . ψ maps even permutations to 1 and odd permutations to -1 , then ψ is surjective. Since the product of two even permutations is an even permutation, the product of two odd permutations is an even permutation, the product of an even permutation and an odd permutation is an odd permutation, and the product of an odd permutation and an even permutation is an odd permutation, therefore ψ preserves the operation. Thus ψ is a surjective homomorphism from G to U_2 . Therefore $G/\text{Ker } \psi \cong U_2$. Hence G has a subgroup of index 2, namely $\text{Ker } \psi$. From the definition of ψ , we know that $\text{Ker } \psi$ is the subgroup of G consisting of all even permutations.

16. 设 σ 是群 G 到群 G' 的一个满同态, 记 $K = \text{Ker } \sigma$ 。设 $H' \triangleleft G'$, 令 $\sigma^{-1}(H') \stackrel{\text{def}}{=} \{g \in G \mid \sigma(g) \in H'\}$ 。证明: (1) $\sigma^{-1}(H') \triangleleft G$, 且 $\sigma^{-1}(H') \supseteq K$; (2) $H' \mapsto \sigma^{-1}(H')$ 是 G' 的子群集合到 G 的包含 K 的子群集合的一个双射。

§5 群在集合上的作用, 群的自同构, 轨道-稳定子定理

4. 设 F 是一个域, $GL_n(F)$ 的中心为 $\{kI_n \mid k \in \mathbb{Z}\}$ 。

5. $GL_2(C)$ 的每一个元素

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

引起了扩充复平面 $C \cup \{\infty\}$ 上的一个变换:

$$z \mapsto \frac{az + b}{cz + d},$$

称它为 Möbius (默比乌斯) 变换。证明: (1) 所有 Möbius 变换组成的集合 G 对于变换的乘法成一个群, 称它为 Möbius 群; (2) $GL_2(C)/Z(GL_2(C)) \cong G$.

6. 设 G 是一个群, 证明: 如果 $G/Z(G)$ 是循环群, 则 G 是 Abel 群。

Let $N = Z(G)$. Since G/N is a cyclic group, therefore $G/N = \langle aN \rangle$. For any $x, y \in G$, let $xN = (aN)^r, yN = (aN)^s$, then there exist $n_1, n_2 \in N$ such that $x = a^r n_1, y = a^s n_2$. Thus

$$xyx^{-1}y^{-1} = (a^r n_1)(a^s n_2)(a^r n_1)^{-1}(a^s n_2)^{-1} = a^r a^s a^{-r} a^{-s} n_1 n_1^{-1} n_2 n_2^{-1} = e.$$

Therefore $xy = yx$. Hence G is an Abelian group.

7. 分别求 D_{2m-1}, D_{2m} 的中心, 其中 $m \geq 2$.

$$\begin{aligned} \sigma^i \in Z(D_n) &\Leftrightarrow \tau \sigma^i = \sigma^i \tau \\ &\Leftrightarrow \tau \sigma^i \tau^{-1} = \sigma^i \\ &\Leftrightarrow (\tau \sigma \tau^{-1})^i = \sigma^i \\ &\Leftrightarrow \sigma^{-i} = \sigma^i \\ &\Leftrightarrow \sigma^{2i} = I \\ &\Leftrightarrow n \mid 2i. \end{aligned}$$

Case 1: $n = 2m - 1$

$$\sigma^i \in Z(D_{2m-1}) \Leftrightarrow 2m - 1 \mid i \Leftrightarrow i = 0 \Leftrightarrow \sigma^i = I.$$

由于 $\tau \notin Z(D_{2m-1})$, 故

$$Z(D_{2m-1}) = \{I\}.$$

Case 2: $n = 2m$

$$\sigma^i \in Z(D_{2m}) \Leftrightarrow m \mid i \Leftrightarrow i = 0 \text{ 或 } m \Leftrightarrow \sigma^i = I \text{ 或 } \sigma^m.$$

由于 $\tau \notin Z(D_{2m})$, 故

$$Z(D_{2m}) = \{I, \sigma^m\}.$$

8. 求 S_n 的中心, 其中 $n \geq 3$.

Since $S_n = \langle (12), (13), \dots, (1n) \rangle$, therefore

$$\begin{aligned} \tau \in Z(S_n) &\Leftrightarrow \tau(1i)\tau^{-1} = (1i), i = 2, 3, \dots, n \\ &\Leftrightarrow \tau(1) = 1, \tau(i) = i, i = 2, 3, \dots, n; \text{ or } \tau(1) = i\tau(i) = 1, i = 2, 3, \dots, n \end{aligned}$$

Since τ is a mapping, thus when $n \geq 3$, the second case cannot occur. Therefore $\tau \in Z(S_n) \Leftrightarrow \tau = (1)$.

Hence $Z(S_n) = \{(1)\}$.

14. Determine all conjugacy classes of D_{2m-1} and D_{2m} , where $m \geq 2$.

From Exercise 1.5.7, we know that

$$Z(D_{2m-1}) = \{I\}, \quad Z(D_{2m}) = \{I, \sigma^m\}.$$

For D_{2m-1} : It is obvious that

$$\begin{aligned} C_{D_{2m-1}}(\sigma^i) &= \langle \sigma \rangle, \quad 1 \leq i \leq 2m-2; \\ C_{D_{2m-1}}(\sigma^i\tau) &= \{I, \sigma^i\tau\}, \quad 0 \leq i \leq 2m-2; \\ C_{D_{2m-1}}(I) &= D_{2m-1}. \end{aligned}$$

Then by the **Orbit-Stabilizer Theorem**,

$$|D_{2m-1}(\sigma^j)| = 2, \quad 1 \leq j \leq 2m-2, \quad |D_{2m-1}(I)| = 1, \quad |D_{2m-1}(\sigma^i\tau)| = 2m-1, \quad 1 \leq i \leq 2m-1.$$

And since

$$\begin{aligned} \sigma\sigma\sigma^{-1} &= \sigma, \\ \sigma^2\tau\sigma\tau\sigma^{-2} &= \sigma^{2m-2} \in D_{2m-1}(\sigma); \\ \sigma\sigma^2\sigma^{-1} &= \sigma^2, \\ \sigma^2\tau\sigma^2\tau\sigma^{-2} &= \sigma^{2m-3} \in D_{2m-1}(\sigma^2); \\ &\vdots \\ \sigma\sigma^k\sigma^{-1} &= \sigma^k, \\ \sigma^2\tau\sigma^k\tau\sigma^{-2} &= \sigma^{2m-1-k} \in D_{2m-1}(\sigma^k), \end{aligned}$$

we have

$$D_{2m-1}(\sigma^k) = \{\sigma^k, \sigma^{2m-1-k}\}, \quad 1 \leq k \leq m-1; \quad D_{2m-1}(I) = \{I\}.$$

For the remaining $2m-1$ elements $\sigma^j\tau$, find x such that $\sigma^x(\sigma^j\tau)\sigma^{-x} = \sigma^{j+2x}\tau \equiv \sigma^i\tau$

$$\Leftrightarrow j + 2x \equiv i \pmod{2m-1} \Leftrightarrow 2x \equiv i - j \pmod{2m-1}.$$

By number theory, $(2, 2m-1) = 1$, so this congruence equation has a solution for x .

Thus, $\{\sigma^j\tau \mid 1 \leq j \leq 2m-1\}$ is contained in one conjugacy class.

By the **Orbit Decomposition Theorem**, this conjugacy class is $D(\tau)$.

For D_{2m} : Similarly, we can obtain that

$$\begin{aligned} C_{D_{2m}}(\sigma^i) &= \langle \sigma \rangle, 1 \leq i \leq 2m-1 \setminus \{m\}; \\ C_{D_{2m}}(I) &= C_{D_{2m}}(\sigma^m) = D_{2m}; \\ D_{2m}(\sigma^k) &= \{\sigma^k, \sigma^{2m-k}\}, 1 \leq k \leq m-1; D_{2m}(\sigma^m) = \{\sigma^m\}; D_{2m}(I) = \{I\} \end{aligned}$$

For the remaining $2m$ elements $\sigma^j\tau$, find x such that $\sigma^x(\sigma^j\tau)\sigma^{-x} = \sigma^{j+2x}\tau \equiv \sigma^i\tau$

$$\Leftrightarrow j + 2x \equiv i \pmod{2m} \Leftrightarrow 2x \equiv i - j \pmod{2m} \Leftrightarrow i \equiv j \pmod{2}.$$

So $\{\sigma^{2i}\tau \mid 1 \leq i \leq m\}$, $\{\sigma^{2j-1}\tau \mid 1 \leq j \leq m\}$ each is contained in one conjugacy class.

By the **Orbit Decomposition Theorem**, the two conjugacy classes are $D(\tau)$, $D(\sigma\tau)$.

In conclusion, the $m+1$ conjugacy classes of D_{2m-1} are

$$D_{2m-1}(I) = \{I\} \quad D_{2m-1}(\sigma^k) = \{\sigma^k, \sigma^{2m-1-k}\}, 1 \leq k \leq m-1 \quad D_{2m-1}(\tau) = \{\sigma^j\tau \mid 1 \leq j \leq 2m-1\};$$

the $m+3$ conjugacy classes of D_{2m-1} are

$$D_{2m}(I) = \{I\} \quad D_{2m}(\sigma^k) = \{\sigma^k, \sigma^{2m-k}\}, 1 \leq k \leq m-1 \quad D_{2m}(\sigma^m) = \{\sigma^m\} \quad D_{2m}(\tau) \quad D_{2m}(\sigma\tau)$$

15. 设 σ 的不相交的轮换分解式 (包含所有的 1-轮换) 为

$$\sigma = (a_1 a_2 \dots a_{l_1})(b_1 b_2 \dots b_{l_2}) \dots (q_1 q_2 \dots q_{l_r})$$

其中 $l_1 \geq l_2 \geq \dots \geq l_r$, 且 $l_1 + l_2 + \dots + l_r = n$. 则我们把有序数组 (l_1, l_2, \dots, l_r) 称为置换 σ 的型 (type), 也称为 n 的一个分拆 (partition). 证明: (1) σ_1 与 σ_2 在 S_n 中共轭当且仅当 σ_1 与 σ_2 同型; (2) S_n 中共轭类的个数等于 n 的分拆的个数.

From exercise 1.1.12, this is quite easy to prove.

16. 求 S_4 的共轭类的个数, 以及每个共轭类的代表和元素数目。

$4 = 4, 4 = 3 + 1, 4 = 2 + 2, 4 = 2 + 1 + 1, 4 = 1 + 1 + 1 + 1$. Therefore, the partitions of 4 have 5 types. Thus, S_4 has 5 conjugacy classes, and their representatives are: $(1234), (123), (12)(34), (12), (1)$. The number of elements in the corresponding conjugacy classes are respectively: $\frac{1}{4}4! = 6$, $\frac{1}{3}(4 \cdot 3 \cdot 2) = 8$, $\frac{1}{2}[\frac{1}{2}(4 \cdot 3)] = 3$, $\frac{1}{2}(4 \cdot 3) = 6, 1$.

17. 求 A_4 的共轭类的个数, 以及每个共轭类的代表和元素数目。

In A_4 , the necessary condition for permutations σ_1 and σ_2 to be conjugate is that σ_1 and σ_2 are of the same type, but this is not a sufficient condition.

For example, (123) and (132) are of the same type, but they are not conjugate in A_4 . This is because the only τ that satisfies $\tau(123)\tau^{-1} = (132)$ are $(23), (13), (12)$, which are all odd permutations and do not belong to A_4 . Using the necessary condition for conjugacy and checking, we find that A_4 has 4 conjugacy classes, with representatives: $(1), (12)(34), (123), (132)$. The number of elements in the corresponding conjugacy classes are: 1, 3, 4, 4.

18. 设 σ 是一个 n -轮换。求 σ 的共轭类的元素数目, 以及 $C_{S_n}(\sigma)$ 的阶。

Based on the conclusion of problem 1.5.15, the conjugacy class of an n -cycle σ consists exactly of all n -cycles. Thus, the number of elements in the conjugacy class of σ is $\frac{n!}{n} = (n - 1)!$ (**Circular arrangement**). Therefore, $|C_{S_n}(\sigma)| = \frac{n!}{(n-1)!} = n$. Since $\sigma \in C_{S_n}(\sigma)$ and the order of σ is n , it follows that $C_{S_n}(\sigma) = \langle \sigma \rangle$.

19. 求 O_2 的所有共轭类。

O_2 consists of all 2×2 orthogonal matrices. According to Advanced Algebra, there are only two types of 2×2 orthogonal matrices:

$$A_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \quad B_\varphi = \begin{pmatrix} \cos \varphi & \sin \varphi \\ \sin \varphi & -\cos \varphi \end{pmatrix},$$

where $0 \leq \theta < 2\pi, 0 \leq \varphi < 2\pi$. Two elements in O_2 are conjugate if and only if these two matrices are orthogonally similar. Since similar matrices have the same determinant, and $|A_\theta| = 1, |B_\varphi| = -1$, for any θ and φ , A_θ and B_φ are not conjugate. Since B_φ is a real symmetric matrix, B_φ must be orthogonally similar to a diagonal matrix with its main diagonal elements being the eigenvalues of B_φ .

Since

$$|\lambda I - B_\varphi| = (\lambda - \cos \varphi)(\lambda + \cos \varphi) - \sin^2 \varphi = \lambda^2 - 1,$$

the eigenvalues of B_φ are 1 and -1 . Therefore, B_φ is conjugate to $\text{diag}\{1, -1\}$, $0 \leq \varphi < 2\pi$. Thus, $\{B_\varphi \mid 0 \leq \varphi < 2\pi\}$ is a conjugacy class of O_2 .

Given θ ($0 \leq \theta < 2\pi$), for any ψ ($0 \leq \psi < 2\pi$),

$$\begin{aligned} A_\psi A_\theta A_\psi^{-1} &= A_\theta, \\ B_\psi A_\theta B_\psi^{-1} &= \begin{pmatrix} \cos(\psi - \theta) & \sin(\psi - \theta) \\ \sin(\psi - \theta) & -\cos(\psi - \theta) \end{pmatrix} \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix} = A_{-\theta} = A_{2\pi - \theta}. \end{aligned}$$

Therefore, when $0 < \theta < \pi$, the conjugacy class of A_θ is $\{A_\theta, A_{2\pi - \theta}\}$. The conjugacy class of $A_0 = I$ is $\{I\}$, and the conjugacy class of $A_\pi = -I$ is $\{-I\}$. In summary, the complete conjugacy classes of O_2 are:

$$\{I\}, \quad \{-I\}, \quad \{B_\varphi \mid 0 \leq \varphi < 2\pi\}, \quad \{A_\theta, A_{2\pi - \theta}\}, \quad 0 < \theta < \pi.$$

20. 群 G 的子群 H 为正规子群当且仅当 H 是 G 的一些共轭类的并集。

21. (1) 求 S_5 的共轭类的个数, 以及每个共轭类的代表和元素数目; (2) 证明: S_5 只有三个正规子群, 即 $\{(1)\}, A_5, S_5$ 。

(1): The partitions of 5 have 7 types, so S_5 has 7 conjugacy classes. Their representatives are:

$(1), (12), (12)(34), (123), (123)(45), (1234), (12345)$.

The number of elements in the corresponding conjugacy classes are:

1, 10, 15, 20, 20, 30, 24.

(2): The normal subgroups of S_5 should be unions of some conjugacy classes. The order of a subgroup must be a divisor of $|S_5| = 120$, and the subgroup must contain the identity element. Therefore, the non-trivial normal subgroups of S_5 cannot be the union of two conjugacy classes. The union of three conjugacy classes only has $1 + 15 + 24 = 40$ as a divisor of 120, but $(12)(34)(12345) = (1)(245)(3)$ does not belong to this union. The union of four conjugacy classes only has $1 + 15 + 20 + 24 = 60$ as a divisor of 120, one of which is exactly A_5 , and another union is not closed under the operation. The union of five or six conjugacy classes does not have an element count that is a divisor of 120. Therefore, the normal subgroups of S_5 are only three: $\{(1)\}, A_5, S_5$.

22. 设 G 为 p -群, $N \triangleleft G$, 且 $|N| = p$ 。证明: $N \subseteq Z(G)$ 。

Since $N \triangleleft G$, there is a conjugation action of group G on set N

Let Ω_0 denote the set of fixed points of the conjugation action of group G on N . Since the set of fixed points of the conjugation action of G on G is $Z(G)$, we have $\Omega_0 = Z(G) \cap N$. Since G is a p -group, according to Proposition 4 of this section, $|Z(G) \cap N| \equiv |N| \pmod{p}$. Since $|N| = p$ and $Z(G) \cap N < N$, we have $|Z(G) \cap N| = p$. Thus, $N = Z(G) \cap N \subseteq Z(G)$.

23. 设 G 是一个群, G 的所有子群组成的集合记作 Ω 。令 $G \times \Omega \rightarrow \Omega : (a, H) \mapsto aHa^{-1}$ 。容易看出这给出了群 G 在 Ω 上的一个作用。 H 的轨道 $G(H)$ 是由 H 的所有共轭子群组成的。 H 的稳定子群 $G_H = \{g \in G \mid gHg^{-1} = H\}$ 称为 H 在 G 中的正规化子 (normalizer), 记作 $N_G(H)$ 。显然, $H \triangleleft N_G(H)$ 。证明: 如果 G 为有限群, $H < G$, 则 H 的共轭子群的个数等于 $[G : N_G(H)]$ 。

This follows immediately from the Orbit-Stabilizer Theorem.

24. 设 H 是有限群 G 的一个非平凡子群, 则 $G \neq \bigcup_{g \in G} gHg^{-1}$.

The number of conjugacy classes of H equals $[G : N_G(H)]$, and $|gHg^{-1}| = |H|$. Since H is non-trivial and the identity element e of G belongs to each conjugacy class, we have $|\bigcup_{g \in G} gHg^{-1}| < [G : N_G(H)]|H|$. If $G = \bigcup_{g \in G} gHg^{-1}$, then

$$|G| = |\bigcup_{g \in G} gHg^{-1}| < [G : N_G(H)]|H| = \frac{|G|}{[G : N_G(H)]}|H|.$$

This implies that $|N_G(H)| < |H|$. This contradicts with $H \subseteq N_G(H)$. Therefore, $G \neq \bigcup_{g \in G} gHg^{-1}$.

25. 设 G 为一个 $2k$ 阶群, k 为奇数, 证明: G 必有指数为 2 的子群。

Consider the left multiplication of group G on set G . Since $|G| = 2k$, there is an isomorphism

$$\begin{aligned} \psi : G &\rightarrow S_{2k}, a \mapsto \psi_{(a)}, \psi_{(a)}x := a \circ x = ax. \\ a \in \ker \psi &\Leftrightarrow \psi_{(a)} = I \Leftrightarrow ax = x, \forall x \in G \Leftrightarrow a = e \end{aligned}$$

Then by the **Fundamental Theorem of Homomorphisms**

$$G \cong \text{Im } \psi, |G| = |\text{Im } \psi| = 2k$$

By the exercise 1.2.9, there exists 2-order element $\psi_{(a)}$ in $\text{Im } \psi$. According to the **cycle decomposition** of a permutation, $\psi_{(a)}$ must be the product of some 2-cycles. Suppose $\psi_{(a)}$ has a fixed point x , then $ax = x$. Thus, $\varphi(a) = \varphi(e) = (1)$, which is a contradiction.

And since there are a total of $2k$ elements, k disjoint 2-cycles are needed to cover all the elements. Therefore, the cycle decomposition of $\varphi(a)$ is

$$\varphi(a) = (i_1 i_2)(i_3 i_4) \cdots (i_{2k-1} i_{2k}),$$

which contains k transpositions. Since k is odd, $\varphi(a)$ is an odd permutation. According to exercise 1.4.15, the permutation group $\text{Im}\varphi$ must have a subgroup \widetilde{H} of index 2. Thus, G has a subgroup $\varphi^{-1}(\widetilde{H})$ of index 2.

26. Let H be a subgroup of the group G , then the kernel of the left multiplication action of G on the left coset set $(G/H)_l$ is equal to $\bigcap_{x \in G} xHx^{-1}$.

a belongs to the kernel of the left multiplication action of group G on the left coset set $(G/H)_l$

$$\Leftrightarrow a \circ xH = xH, \forall xH \in (G/H)_l \Leftrightarrow axH = xH, \forall xH \in (G/H)_l$$

$$\Leftrightarrow x^{-1}ax \in H, \forall x \in G \Leftrightarrow a \in xHx^{-1}, \forall x \in G.$$

Therefore, the kernel of the left multiplication action of group G on the left coset set $(G/H)_l$ is equal to $\bigcap_{x \in G} xHx^{-1}$.

27. 设 G 为一个有限群, $H < G$, 且 $[G : H] = n > 1$ 。证明: G 或者有一个指数整除 $n!$ 的非平凡正规子群, 或者 G 同构于 S_n 的一个子群。

Consider the group G acting on the left coset set $(G/H)_l$ by left multiplication. Since $[G : H] = n > 1$, there is a homomorphism ϕ from G to S_n .

Case 1: $\text{Ker}\phi = \{e\}$. Then $G \cong \text{Im}\phi$. Thus, G is isomorphic to a subgroup of S_n .

Case 2: $\text{Ker}\phi \neq \{e\}$. Then $G/\text{Ker}\phi \cong \text{Im}\phi$. Therefore, $[G : \text{Ker}\phi] = |\text{Im}\phi|$, and $\text{Im}\phi \leq S_n$, so $|\text{Im}\phi|$ is a factor of $n!$. Hence, the normal subgroup $\text{Ker}\phi$ of G has an index that divides $n!$. According to problem 1.5.26, $\text{Ker}\phi = \bigcap_{x \in G} xHx^{-1}$. Thus, $\text{Ker}\phi \subseteq H$. Since $H \neq G$, $\text{Ker}\phi \neq G$. Therefore, $\text{Ker}\phi$ is a non-trivial normal subgroup of G .

32. 设群 G 与群 H 分别作用在集合 Ω 和 W 上。令

$$(g, h) \circ (x, y) \stackrel{\text{def}}{=} (g \circ x, h \circ y),$$

易证明这给出了群 $G \times H$ 在集合 $\Omega \times W$ 上的一个作用, 称它是乘积作用 (product action)。 $\Omega \times W$ 里的元素 (x, y) 的轨道 $(G \times H)(x, y) = G(x) \times H(y)$, (x, y) 的稳定子群 $(G \times H)_{(x, y)} = G_{(x)} \times H_{(y)}$ 。-->

§6 Sylow定理

1. 证明不存在阶为 148 的单群。
2. 证明不存在阶为 36 的单群。
3. 证明不存在阶为 56 的单群。
4. 证明不存在阶为 30 的单群。
5. 证明 6 阶群或者是循环群，或者同构于 S_3 。
6. 决定 10 阶群的类型。
7. 决定 15 阶群的类型。
8. 决定 35 阶群的类型。
9. 决定 21 阶群的类型。
10. 设 p, q 都是素数，且 $p < q$ 。决定 pq 阶群的类型。
11. 设 p, q 是不同的素数。证明 p^2q 阶群必包含一个正规的 Sylow 子群。
12. 设群 G 的阶为 p^3 ，其中 p 是素数。证明：如果 G 是非交换群，则 $|Z(G)| = p$ ，且 $Z(G) = G'$ 。
13. 设 p 是素数。计算 S_p 中 Sylow p -子群的个数。由此证明 Wilson 定理：

$$(p-1)! \equiv -1 \pmod{p}.$$

14. 设 G 为一个有限群, $N \triangleleft G$, P 是 N 的一个 Sylow p -子群。证明: $G = N \cdot N_G(P)$.

15. 证明: 如果有限群 G 有一个循环的 Sylow 2-子群, 则 G 有一个指数为 2 的子群。

§7 有限Abel群的结构

1. 决定 12 阶 Abel 群的互不同构的类型。

2. 决定 108 阶 Abel 群的互不同构的类型。

3. 决定 360 阶 Abel 群的互不同构的类型。

4. 决定 144 阶 Abel 群的互不同构的类型。

5. 决定 216 阶 Abel 群的互不同构的类型。

6. 求下列群的初等因子: (1) $Z_{16} \times Z_{15} \times Z_{20}$; (2) $Z_9 \times Z_{45}$; (3) $Z_4 \times Z_{14} \times Z_{16}$.

7. 设 G 是 100 阶 Abel 群。① 证明 G 必含有 10 阶元; ② G 的初等因子应当怎样才能使 G 不含大于 10 的元素?

8. 证明: 如果有限 Abel 群的阶没有平方因子, 则它必为循环群。

9. 证明: 一个 Abel p -群如果恰好有 $p-1$ 个 p 阶元, 则它一定是循环群。

10. 设 V 是域 Z_2 上的 n 维线性空间, 决定 V 的加法群的结构, 写出它的初等因子, 它是不是初等 Abel 2-群?

11. 设 V 是域 Z_p 上的 n 维线性空间, p 是素数。 V 的加法群是不是初等 Abel p -群?

§8 自由群, 群的表现

1. 把下列由字母表 $X = \{x, y, z\}$ 形成的字化简成既约字: (1) $w_1 = x^{-1}y^4y^{-1}y^{-3}zz^{-2}y^{-1}z^{-1}$; (2)

$$w_2 = z^{-2}y^3x^{-2}x^{-2}yx^2z^{-3}z^3; (3) w_3 = z_3^2yxx^{-1}xz^{-1}y^2z^{-1}y^{-1}.$$

2. w_1, w_2, w_3 同第 1 题, 求 $w_1w_2w_3$ 。

3. 在 3-辫群 B_3 中, 求 b_1^2, b_2^2, b_1b_2 , 其中 b_1, b_2 是初等辫子(见 §8 的图 1-10)。

4. 在 3-辫群 B_3 中, 分别写出 b_1^2, b_2^2, b_1b_2 产生的 S_3 中的置换。

5. 找出 B_3 中的两个不同的辫子, 它们都产生置换 (132)。

6. 在 4-辫群 B_4 中, 求 b_1b_3, b_3b_1 和 $b_3b_1b_3^{-1}$, 其中 b_1, b_3 都是初等辫子(见 §8 的图 1-14)。从所画的图看, b_1b_3 与 b_3b_1 相等吗?

7. 设 G 和 G' 是两个群, x_1, x_2, \dots, x_n 称为一个字, 其中每个 x_i 属于无交并 $G \cup G'$ (即, 把 G 的元素与 G' 的元素看成不同的元素形成的并集, 注意即使 $G = G'$, 在求无交并 $G \cup G'$ 时, 也需要把前一个集合 G 与后一个集合 G' 的元素看成不同的元素)。称一个字是既约的, 如果 x_i 与 x_{i+1} 不在同一个群里 ($1 \leq i < n$), 并且 x_i 不是 G 或 G' 的单位元 ($1 \leq i \leq n$)。可证明每一个字能化简成唯一的既约字(类似于本节定理 1 的证法)。两个既约字 w_1 与 w_2 相乘就是在 w_1 后面接着写 w_2 , 然后把它化简成既约字。所有既约字连同字空间的集合对于上述乘法成一个群, 称它为 G 与 G' 的自由积 (free product), 记作 $G * G'$ 。证明: $Z * Z \cong F_2$, 其中 F_2 代表由 2 个元素生成的自由群。

第二章 环

§1 环的类型和性质, 理想

2. 有限整环是域。

只要证有限整环 R 的每个非零元可逆. 设 $R = \{a_1, a_2, \dots, a_n\}$. 任取 R 的一个非零元 a , 则 aa_1, aa_2, \dots, aa_n 两两不等 (假如 $aa_j = aa_l$, 由于整环 R 没有非平凡的零因子, 因此从 $a(a_j - a_l) = 0$ 得出 $a_j - a_l = 0$, 即 $a_j = a_l$). 于是 $\{aa_1, aa_2, \dots, aa_n\} = R$.

从而必有某个 $j \in \{1, 2, \dots, n\}$, 使得 $aa_j = 1$. 因此 a 可逆, 从而 R 是一个域.

4. 设 R 是有单位元的环, 则 R 的每一个非平凡的理想都不能含有单位元。

$$r = 1 \cdot r \in I \Rightarrow R \subset I$$

5. 域 F 没有非平凡的理想。

$$1 = aa^{-1} \in I, \text{ 由上题即可}$$

6. 设 R 是一个有单位元的交换环, 如果 R 没有非平凡的理想, 则 R 是一个域。

任取 R 的一个非零元 a , 考虑 $Ra := \{ra \mid r \in R\}$. 由于 $r_1a - r_2a = (r_1 - r_2)a \in Ra$, $r(r_1a) = (rr_1)a \in Ra$, $(r_1a)r = (r_1r)a \in Ra$, 因此 Ra 是 R 的一个理想. 由已知条件得, $Ra = R$. 于是 $1 \in Ra$. 故 $\exists b \in R$, 使得 $1 = ba$. 从而 a 可逆, 于是, R 是一个域.

10. 设 D 是一个除环, 证明 $M_n(D)$ 是单环。

任取 $M_n(D)$ 的一个理想 J , 且 $J \neq \{0\}$. 于是有 $A \in J$, 且 $A \neq 0$. 从而有一个元素 $a_{kl} \neq 0$. 由于 $E_{ik}AE_{lj} = a_{kl}E_{ij}$, 因此 $a_{kl}E_{ij} \in J$. 从而 $E_{ij} = a_{kl}^{-1}(a_{kl}E_{ij}) \in J$. 于是 $E_{ij} = E_{ik}E_{kl}E_{lj} \in J$, $1 \leq i, j \leq n$. 因此对于任意 $B = (b_{ij}) \in M_n(D)$, 有

$$B = \sum_{i=1}^n \sum_{j=1}^n b_{ij}E_{ij} \in J$$

. 从而 $M_n(D) \subseteq J$. 又有 $J \subseteq M_n(D)$, 因此 $J = M_n(D)$. 这证明了 $M_n(D)$ 没有非平凡的理想. 于是 $M_n(D)$ 是单环.

第三章 域扩张及其自同构

§1 域扩张, 分裂域, 正规扩张, 可分扩张

§2 域扩张的自同构群, Galois 扩张, Galois 基本定理

§3 本原元素, 迹与范数