

《近世代数》 作业 #1 提交日期: 周四 9/12

1. 设 ρ 为集合 S 到集合 T 的映射。证明: ρ 是一满射的充要条件是下列两条件中任一条成立:

(a) 存在 T 到 S 的映射 τ , 使得 $\rho\tau = 1_T$;

(b) 不存在 T 到某集合 U 的两个不同映射 τ_1, τ_2 使得 $\tau_1\rho = \tau_2\rho$

2. ρ 为集合 S 到集合 T 的映射, A, B 是 S 的子集。证明:

$$\rho(A \cup B) = \rho(A) \cup \rho(B),$$

$$\rho(A \cap B) \subset \rho(A) \cap \rho(B),$$

举例说明 $\rho(A \cap B)$ 不一定 等于 $\rho(A) \cap \rho(B)$,

3. 设 $\omega_1, \omega_2 \in \mathbf{C}$ (复数集), 且 $\omega_1/\omega_2 \notin \mathbf{R}$. 在 \mathbf{C} 内定义如下关系 \sim :

$$\alpha \sim \beta \Leftrightarrow \beta = \alpha + a\omega_1 + b\omega_2. \quad (a, b \in \mathbf{Z})$$

证明: (1) 关系 \sim 在 \mathbf{C} 上是一等价关系。

(2). 试求 \mathbf{C} 对上述等价关系的商集 \mathbf{C}/\sim .

《近世代数》HW 2 提交时间 9/19, 周四

1. 设 G 是一个半群, 则 G 是一个群当且仅当以下条件成立

(i) 存在一个元素 e , 使得对所有 $a \in G$, $ea = a$ 成立

(ii) 对任意 $a \in G$, 存在一个元素 a^{-1} , 使得 $a^{-1}a = e$.

(注: e 称为左单位元, 称 a^{-1} 为 a 的左逆元)

2. 证明: 若 G 是一个半群, 则 G 是一个群当且仅当对任意 $a, b \in G$, 方程:

$$ax = b \quad \text{和} \quad ya = b \quad \text{在 } G \text{ 中有解.}$$

(提示: 利用 1 题的结论)

3. 证明: 群 G 是一个 Abel 群当且仅当对任意 $a, b \in G$, 有 $(ab)^2 = a^2b^2$.

4. 证明: 若有限群 G 的阶是偶数, 则 G 中存在一个元 a , 使得 $a^2 = e$.

5. 列出正方形上的全体对称所得到的群的群表. (这个群在课上讲过, 参考笔记)

《近世代数》HW 3 提交时间 9/26, 周四

1. 证明: G 是一个交换群 \iff 映射:

$$\begin{aligned} f: G &\longrightarrow G \\ g &\mapsto g^{-1} \end{aligned}$$

是一个群同构。

2. 设 Q_8 是由矩阵 $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ 按矩阵乘法所生成的群。(其中 $i^2 = -1$)

证明: Q_8 是阶为 8 的非交换群。

(提示: 先验证 $BA = A^3B$, 从而 Q_8 中的元可写成 A^iB^j 的形式, 再注意到 $A^4 = B^4 = I$, 即可得证。)

3. 设 $f: G \longrightarrow H$ 是一个群同态, $A < G, B < H$. 证明:

(a). $\text{Ker } f$ 和 $f^{-1}(B)$ 都是 G 的子群。

(b). $f(A)$ 是 H 的子群。

4. 设 S 是群 G 的一个子集, 在 G 上定义一个关系 \sim :

$$a \sim b \iff ab^{-1} \in S$$

证明: S 是 G 的子群 \iff 关系 \sim 是 G 上的等价关系。

5. 设 G 为一个群, 则 $C(G) = \{g \in G \mid ga = ag, \text{对任意 } a \in G \text{ 成立}\}$ 是 G 的交换子群。

(注: $C(G)$ 称为 G 的中心)

《近世代数》HW 4 提交时间：10/17，周四

1. 若一个群仅有有限个子群，则该群一定是有限群。

2. 设 H 和 K 为群 G 的有限子群，证明： $|HK| = \frac{|H||K|}{|H \cap K|}$.

3. 设 G 为一个群，则：

$$C(G) = \{a \in G | \forall g \in G, ag = ga\}$$

是 G 的正规子群. (注： $C(G)$ 称为 G 的中心)

4. 设 H 为 G 的一个子群，即 $H < G$ ，则 aHa^{-1} 是 G 的子群，并且 $H \cong aHa^{-1}$.

5. 设群 G 是有限群， H 是 G 的一个阶为 n 的子群. 证明：若 H 是唯一的 G 的 n 阶子群，则 H 为 G 的正规子群.

6. 如果 $f: G \rightarrow H$ 是群同态， H 是 Abel 群， $N < G$ 并且 $N \subset \text{Ker} f$. 证明： $N \triangleleft G$

7. 设 H 为 G 的一个子群，证明： $N(H) = \{g \in G | gH = Hg\}$ 是 G 的子群并且 $H \triangleleft N(H)$
(注： $N(H)$ 称为 H 的正规化子)

8. 设 H 为群 G 的指标为 2 的子群，则 H 是 G 的正规子群.

《近世代数》HW 5 提交时间：10/24，周四

1. 设 $\langle 6 \rangle, \langle 30 \rangle$ 为 \mathbb{Z} 的子群，则 $\langle 6 \rangle / \langle 30 \rangle \cong \mathbb{Z}_5$.
2. 设 $C(G) = \{a \in G \mid \forall g \in G, ag = ga\}$ ，是群 G 的中心. 证明：如果 $G/C(G)$ 是循环群，则 G 是 Abel 群.
3. 计算 \mathbb{Z}_6 到 \mathbb{Z}_6 的所有同构. (注：群 G 到自己的同构的全体，称为自同构，记为 $\text{Aut}(G)$)
4. 以 V 表示全体 n 维实向量的集合， $GL(n, R)$ 在 V 上作用为左乘，即对于 $A \in GL(n, R)$ 及 $\alpha \in V$

$$GL(n, R) \times V \longrightarrow V$$

$$(A, \alpha) \longmapsto A\alpha$$

试求所有轨道. (注： $GL(n, R)$ = 全体 $n \times n$ 实可逆矩阵)

5. 设 S 表示所有 $n \times n$ 实对称矩阵的集合，定义 $GL(n, R)$ 在 S 上的作用如下：对于 $A \in GL(n, R)$ 及 $B \in S$

$$GL(n, R) \times S \longrightarrow S$$

$$(A, B) \longmapsto ABA^T$$

其中 A^T 表示矩阵 A 的转置，试求轨道的个数.

《近世代数》HW 6 提交时间：11/7，周四

1. 设 H 为 G 的子群，集合 $S = \{H \text{ 在 } G \text{ 中的全体左陪集}\}$ ，定义 G 在 S 上的作用如下：

$$\begin{aligned} G \times S &\longrightarrow S \\ (g, aH) &\longmapsto gaH \end{aligned}$$

则此作用诱导出一个群同态： $\phi: G \longrightarrow A(S)$ 并且核 $\text{Ker}\phi$ 包含于 H 中. 即 $\text{Ker}\phi \subset H$. (注：这里 $A(S)$ 表示集合 S 上的全体双射)

2. 设 G 为有限群， H 为 G 的指标为 p 的子群， p 为 $|G|$ 的最小素数因子. 证明： $H \triangleleft G$ (**提示**：首先考虑定义一个如上题 G 在集合 $S = \{H \text{ 在 } G \text{ 中的全体左陪集}\}$ 的一个作用，然后利用上题的结论和 Lagrange 定理，证明 $\text{Ker}\phi = H$.)

《近世代数》中期试卷提交时间 11/18, 周一

1A. 设 $X = \{aba^{-1}b^{-1} \mid a, b \in G\}$ 为群 G 的一子集, 定义 G 的换位子群 $[G, G]$ 如下:

$$[G, G] = \langle X \rangle \quad (\text{即 } X \text{ 生成的子群}).$$

证明: $[G, G] \triangleleft G$ 并且商群 $G/[G, G]$ 是 Abel 群.

1B. 设 $X = \{aba^{-1}b^{-1} \mid a, b \in G\}$ 为群 G 的一子集, 定义 G 的换位子群 $[G, G]$ 如下:

$$[G, G] = \langle X \rangle \quad (\text{即 } X \text{ 生成的子群}).$$

设 $H < G$, 且 $[G, G] \subset H$. 证明: $H \triangleleft G$, 并且 G/H 是 Abel 群.

1C. 设 G 为 Abel 群, 集合

$$H = \{a \in G \mid \text{存在某个整数 } n \text{ 使得 } a^n = e\}$$

即 G 中全体阶有限的元素组成的集合.

证明:

(a) H 是 G 的子群. (群 H 也称为挠群或周期群)

(b) 若 $(\mathbb{Q}, +)$ 是有理数加法群, $(\mathbb{Z}, +)$ 是 \mathbb{Q} 的整数加法子群, 则 \mathbb{Q}/\mathbb{Z} 是挠群.

2A. 设群 $G = \{\tau_a \mid a \in \mathbb{R}\}$, 群 G 的乘法如下:

$$\tau_a * \tau_b = \tau_{a+b}$$

定义 G 在平面 \mathbb{R}^2 上的一个关系如下:

$$\begin{aligned} G \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (\tau_a, (x, y)) &\longmapsto (x + a, \quad y + 2ax + a^2) \end{aligned}$$

证明:

(a) 以上关系是群 G 在平面 \mathbb{R}^2 上的一个作用.

(b) 任意一个轨道是平面 \mathbb{R}^2 上的一条抛物线.

2B. 设群 $G = \{\tau_a \mid a \neq 0, a \in \mathbb{R}\}$, 群 G 的乘法如下:

$$\tau_a * \tau_b = \tau_{ab}$$

定义 G 在平面 \mathbb{R}^2 上的一个关系如下:

$$\begin{aligned} G \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (\tau_a, (x, y)) &\longmapsto (ax, \quad a^{-1}y) \end{aligned}$$

证明:

- (a) 以上关系是群 G 在平面 \mathbb{R}^2 上的一个作用.
- (b) 平面 \mathbb{R}^2 中任意不在坐标轴上点的轨道是一条双曲线.

2C. 设群 $G = \{\tau_\theta \mid 0 \leq \theta < 360^\circ\}$, 群 G 的乘法如下:

$$\tau_{\theta_1} * \tau_{\theta_2} = \tau_{[\theta_1 + \theta_2]}$$

其中 $[\theta_1 + \theta_2]$ 是 $\theta_1 + \theta_2$ 对模 360° 的主余数. 现把平面 \mathbb{R}^2 与复数 \mathbb{C} 等同, 即点 $(x, y) = z \in \mathbb{C}$, $|z| = \sqrt{x^2 + y^2}$. 定义 G 在平面 $\mathbb{R}^2 = \mathbb{C}$ 上的一个关系如下:

$$\begin{aligned} G \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (\tau_\theta, z) &\longmapsto ze^{i\theta} \end{aligned}$$

证明:

- (a) 以上关系是群 G 在平面 \mathbb{R}^2 上的一个作用.
- (b) 平面 \mathbb{R}^2 上除坐标原点外, 任意一点的轨道是一个圆.

《近世代数》HW 7 提交时间：11/14，周四

1. 设 G 为有限群, P 为 G 的 *Sylow* p -子群, $N \triangleleft G$, 证明: PN/N 是 G/N 的 *Sylow* p -子群.
2. 设 G 为有限群, P 为 G 的 *Sylow* p -子群. 证明:
 - (a) P 在 $N_G(P)$ 中的共轭子集只有一个.
 - (b) $N_G(P) = N_G(N_G(P))$.
3. 设 G 的阶为 100, 证明 G 中必有阶为 25 的正规子群.
4. 设 G 的阶为 168, G 中有多少个阶为 7 元素.
5. 找出 S_4 的所有 *Sylow* 2-子群及 *Sylow* 3-子群.

《近世代数》HW 8 提交时间：11/21，周四

1. 设 R 为一非交换环, $a, b \in R$. 如果 $a, b, ab - 1$ 都可逆, 试证明:

$a - b^{-1}$ 和 $(a - b^{-1})^{-1} - a^{-1}$ 也可逆, 并且

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

2. 证明: $\mathbb{Z}(i) = \{a + bi \mid a, b \in \mathbb{Z}\}$ 关于整数的加法、乘法组成一个整环.

(注: $\mathbb{Z}(i)$ 称为**高斯整数环**)

3. 环 R 称为一个 *Boolean* 环, 如果 $\forall a \in R$, 都有 $a^2 = a$. 证明: 任何一个 *Boolean* 环都是交换环, 并且 $\forall a \in R$, 有 $a + a = 0$.

4. 设 R 是一个非零环, 并且对任意 $a \in R, a \neq 0$, 都存在唯一的元 $b \in R$ 使得 $aba = a$. 证明:

(a). R 没有零因子.

(b). $bab = b$

(c). R 有单位元 1_R .

(d). R 是除环.

《近世代数》HW 9 提交时间：11/28，周四

1. 证明集合：

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

关于实数的加法、乘法组成一个域，在此域中，试求出 $-2 + \sqrt[3]{2} + 3\sqrt[3]{4}$ 的逆元.

2. 设 I 为交换环 R 的一个理想，定义集合：

$$\text{Rad}(I) = \{r \in R \mid \text{存在整数 } n \text{ 使得 } r^n \in I\}$$

证明： $\text{Rad}(I)$ 是 R 的理想. (注： $\text{Rad}(I)$ 称为 R 的**根理想**)

3. 证明： \mathbb{Z}_m 是主理想环. 特别当 m 为素数时， \mathbb{Z}_m 是域.

《近世代数》HW 10 提交时间：12/5 周四

1. 求环 \mathbb{Z}_{28} 的所有素理想和极大理想.
2. 证明：设 I 是整数环 \mathbb{Z} 的非零理想，则以下条件等价：

$$I \text{ 是素理想} \iff I \text{ 是极大理想} \iff I = (p), p \text{ 是素数}$$

3. 证明环同态第三定理：设 I, J 为环 R 的理想，若 $I \subset J$ ，则 J/I 是商环 R/I 的理想，并且有： $(R/I)/(J/I) \cong R/J$

《近世代数》HW 11 提交时间：12/12，周四

1. 证明：在 $\mathbb{Z}_2[x]$ 中多项式 $x^3 + x^2 + 1$ 是不可约的，并利用这一结论构造一个有 8 个元的有限域.
2. 证明： $\sqrt{3} + \sqrt{5}$ 是 \mathbb{Q} 上的代数元，并且求 $\sqrt{3} + \sqrt{5}$ 在 \mathbb{Q} 上的极小多项式.
3. 设 $x^3 - 3x - 1 \in \mathbb{Q}[x]$ ，证明：
 - (a). $x^3 - 3x - 1$ 是 \mathbb{Q} 上的不可约多项式；
 - (b). 若 α 为 $x^3 - 3x - 1$ 的一个根，则 \mathbb{Q} 的代数单扩张 $\mathbb{Q}(\alpha)$ 是域 \mathbb{Q} 上的三维向量空间，并且可以取 $\{1, \alpha, \alpha^2\}$ 作为 $\mathbb{Q}(\alpha)$ 的基；
 - (c). 在域 $\mathbb{Q}(\alpha)$ 中求元 $\alpha^4 + 2\alpha^3 + 3$ 的逆元. (提示：由于 $\alpha^4 + 2\alpha^3 + 3 \in \mathbb{Q}(\alpha)$ 由 (b)，首先在基 $\{1, \alpha, \alpha^2\}$ 下，把元 $\alpha^4 + 2\alpha^3 + 3$ 线性表示出来，然后再找其逆元.)

《近世代数》习题答案 (仅供参考)

HW #1

1. 假设 ρ 是满射, 则对 $\forall t \in T$ 取 $s_t \in \rho^{-1}(t)$, 定义 $\tau : T \rightarrow S$ 如下:
 $\tau(t) = s_t$, 易见 $\rho\tau = 1_T$. 现在若存在 τ_1, τ_2 使得, $\tau_1\rho = \tau_2\rho$, 则 $\tau_1\rho\tau = \tau_2\rho\tau \Rightarrow \tau_1 1_T = \tau_2 1_T \Rightarrow \tau_1 = \tau_2$, 矛盾. 从而, 不存在不同的 τ_1, τ_2 使得 $\tau_1\rho = \tau_2\rho$. 反之, 若 ρ 有右逆, 即 $\rho\tau = 1_T$. 则对任意 $t \in T$, 取 $s = T(t) \in S$, 显然, $\rho(s) = \rho(T(t)) = t$, 从而 ρ 为满射.

2 略.

3 (1) 只需证明以下三个条件成立, 则 \sim 是复数 \mathbb{C} 上的等价关系.

(a) (自反性) $\alpha \sim \alpha$, since $\alpha = \alpha + 0\omega_1 + 0\omega_2$.

(b) (对称性) $\alpha \sim \beta \Rightarrow \beta = \alpha + a\omega_1 + b\omega_2$, for some intergers a, b .
Obviously, we have that $\alpha = \beta - a\omega_1 - b\omega_2$, i.e. $\beta \sim \alpha$.

(c) (传递性) 若 $\alpha \sim \beta, \beta \sim \gamma$, 则 $\beta = \alpha + a\omega_1 + b\omega_2$, and $\gamma = \beta + c\omega_1 + d\omega_2$,
where $a, b, c, d \in \mathbb{Z}$. Hence, $\gamma = \alpha + (a+c)\omega_1 + (b+d)\omega_2$, so $\alpha \sim \gamma$.

(2). 不失一般性, 可以取 $\omega_1 = i, \omega_2 = 1$. 则设 $\alpha = x + iy$, 可知, 在该等价关系下 α 作为代表元所在的类

$$[\alpha] = \{x + a + (y + b)i | a, b \in \mathbb{Z}\} = \{(x + a, y + b) | a, b \in \mathbb{Z}\}$$

即平面上的点格, 从而得到的商集 \mathbb{C}/\sim 等同于把正方形两组对边等同起来, 所以我们得到一个环面.

HW#2

1. 证明: " \Rightarrow " 显然. 现证: " \Leftarrow " 由假设, 若 $a \in G$, 由 (ii), $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = a(ea^{-1}) = aa^{-1}$, 故 $aa^{-1} = e$, 所以 a^{-1} 是 a 的逆. 注意到 $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$ 对任意 $a \in G$ 成立, 故 e 是单位元. 故, G 是群.

2. 证明: " \implies " 显然. 现证: " \impliedby " 由假设, 对于方程 $ya = a$ 在 G 中有解, 记这个解为 $y = e$, 即 $ea = a$, 现在需证明, $\forall b \in G$, 都有 $eb = b$, 则 e 为 G 的左单位元. 实际上, 由假设 $ax = b$ 在 G 中有解, 记这个解为 $x = c$, 即 $b = ac$, 注意到 $eb = e(ac) = (ea)c = ac = b$, 所以 e 为 G 的左单位元. 用同样的技巧可以证明: $\forall a \in G$, 存在 $d \in G$ 使得 $da = e$, 即 a 的左逆元. 最后由 (1) 题的结论, 推出 G 是群.
3. 证明: " \implies " 显然. 现证: " \impliedby " 由假设, $(ab)^2 = a^2b^2$, 因为 G 为群, 所以消去律成立,

$$(ab)^2 = a^2b^2 \iff abab = a^2b^2 \iff abab = aabb \iff ba = ab$$

4. 证明: 由于有限群 G 的阶是偶数, 群中除单位元 e 外, 其余元都成对出现, 从而必有一元 $a \in G$ 使得 $a^2 = e$.
5. 参考笔记.

HW#3

1. 证明: (\iff): $\forall g_1, g_2 \in G, g_1g_2 = f((g_1g_2)^{-1}) = f(g_2^{-1}g_1^{-1}) = f(g_2^{-1})f(g_1^{-1}) = g_2g_1$ 从而, G 是 Abel 群. (\implies) 显然.
2. 证明: 若令 $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ 由简单的矩阵乘法, 我们可得: 由集合 X 生成的群 $\langle X \rangle$ 由以下元素组成.

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E,$$

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, A^2B = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, A^3B = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

并且注意到

$$BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, B^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

由此易见: $A^3B = BA$. 故 Q_8 的任何一个元素都是 A^iB^j 的形式, 所以 Q_8 有 8 个元的非交换群.

3. 参考笔记.

4. 证明: (\implies), 设 S 是 G 的子群, 欲证 \sim 是等价关系, 我们要验证以下性质: (1) 自反性: $\forall a \in G, a \sim a \iff aa^{-1} = e \in S$, (2) 对称性: 若 $a \sim b \iff ab^{-1} \in S$, 则由于 S 是群, 故 $ab^{-1} \in S \implies ba^{-1} \in S \iff b \sim a$. (3) 传递性: 若 $a \sim b, b \sim c$ 则, $ab^{-1} \in S, bc^{-1} \in S$ 从而, $ac^{-1} = ab^{-1}bc^{-1} \in S \iff a \sim c$.

(\impliedby) 假设 \sim 是 G 上的一个等价关系, $\forall a, b \in S$, 则由等价关系的定义, 易见 $a \sim e$ 并且 $e \sim b$, 从而对于任意 $a, b \in S$, 我们都有 $a \sim b \implies ab^{-1} \in S$, 从而 S 是子群.

5. 显然.

HW#4

1. 证明: 任取一个非单位元 $a \in G$, 得到 G 的一个循环子群: $\langle a \rangle$, 而且其阶是有限的. 否则 $\langle a \rangle \cong \mathbb{Z}$, 然而 \mathbb{Z} 有无限多子群, 这与假设矛盾. 由同样的方法, 可得到 G 的所有循环子群, 但是这样的子群, 只有有限个, 从而 G 是有限群.

2. 证明: 设 $C = H \cap K$ 是 K 的一个指标为 $n = \frac{|K|}{|H \cap K|}$ 的子群. 则 K 是 C 的右陪集的不交并: $Ck_1 \cup Ck_2 \cdots \cup Ck_n, \quad k_i \in k$. 因 $HC = H$, 故 HK 是 $Hk_1 \cup Hk_2 \cdots \cup Hk_n, \quad k_i \in k$ 不交并, 因此 $|HK| = |H| \cdot n = |H||K|/|H \cap K|$.

3. G 的中心为:

$$C(G) = \{a \in G | \forall g \in G, ag = ga\}$$

则, 对 $\forall g \in G$, 需证明 $\forall c \in C(G), gcg^{-1} \in C(G)$. Obviously, $gcg^{-1} = cgg^{-1} = c \in C(G)$, so $C(G) \triangleleft G$.

4. 证明: 任取 $g_1, g_2 \in aHa^{-1}$, 则 $g_1 = ah_1a^{-1}, g_2 = ah_2a^{-1}$, 那么,

$$g_1g_2^{-1} = ah_1a^{-1}(ah_2a^{-1})^{-1} = ah_1h_2^{-1}a^{-1} \in aHa^{-1}.$$

从而, $aHa^{-1} < G$. 易见,

$$\phi: H \longrightarrow aHa^{-1}, \text{ given by } h \longmapsto aha^{-1}$$

是群同构, 故 $aHa^{-1} \cong H$.

5. 证明: 由上题结论, $aHa^{-1} \cong H$ 和 H, aHa^{-1} 都是 G 的阶为 n 的子群, 由假设知: $aHa^{-1} = H$, 即 $H \triangleleft G$.
6. 证明: 由群同态第一定理: $G/\ker f \cong \text{Im } f$, 而 $\text{Im } f < H$, H 是 Abel 群, 所以 $\text{Im } f$ 是 Abel 群, 故 $G/\ker f$ 是 Abel 群, 然而 Abel 群的任意子群都是正规子群, 所以子群 $N/\ker f$ 是 $G/\ker f$ 的正规子群. 由同构群之间的正规子群的一一对应关系, 可得到: N 是 G 的正规子群, 即 $N \triangleleft G$.
7. 直接由正规子群的定义验证.
8. 由于 H 在 G 中的指标是 2, 即 H 在 G 中的作陪集的个数是 2, 同时有陪集的个数也是 2. 故可设 $G = H \cup aH = H \cup Ha$, 从而 $aH = Ha$, 即 $H \triangleleft G$.

HW# 5

1. 证明: 定义映射:

$$\phi: \langle 6 \rangle \longrightarrow \mathbb{Z}_5$$

$$6m \longmapsto [m]_5$$

易验证 ϕ 是满同态. 则由群同态基本定理: $\langle 6 \rangle / \ker \phi \cong \mathbb{Z}_5$. 而 $\text{Ker } \phi = \{6m \mid 6m = 5n\} = \langle 30 \rangle$, 故 $\langle 6 \rangle / \langle 30 \rangle \cong \mathbb{Z}_5$.

2. 证明: $G/C(G)$ 是循环群, 则存在 $g \in G$

$$G/C(G) = \langle gC(G) \rangle = \{g^m C(G) \mid m \in \mathbb{Z}\}$$

任取 $g_1, g_2 \in G$, 考虑 $g_1 C(G), g_2 C(G) \in G/C(G)$, 则, $g_1 C(G) = g^m C(G)$, $g_2 C(G) = g^n C(G)$ 并且:

$$\exists h_1, h_2 \in C(G), s.t.: g_1 = g^m h_1, \quad g_2 = g^n h_2$$

所以,

$$g_1 g_2 = g^m h_1 g^n h_2 = g^{m+n} h_1 h_2$$

$$g_2 g_1 = g^n h_2 g^m h_1 = g^{m+n} h_2 h_1$$

因 $h_1, h_2 \in C(G)$, 故 $g_2 g_1 = g_1 g_2$, 从而 G 是 Abel 群.

3. 证明: 注意到任何群同构把生成元映射到生成元, 而 \mathbb{Z}_6 的生成元为: $[1], [5]$. 所以对 $\forall \phi \in \text{Aut}(\mathbb{Z}_6)$, ϕ 唯一的由生成元的像确定. 从而, $\text{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

4. 证明: 由定义 $A \in GL(n, R)$ 及 $\alpha \in V$

$$\begin{aligned} GL(n, R) \times V &\longrightarrow V \\ (A, \alpha) &\longmapsto A\alpha \end{aligned}$$

对向量空间 V 来说, 任意非零 $\alpha, \beta \in V$, 都存在 $A \in GL(n, R)$ 使得 $A\alpha = \beta$, therefore,

$$\text{orb}(\alpha) = \begin{cases} 0 & \text{for } \alpha = 0 \\ V - \{0\}, & \text{for } \alpha \neq 0 \end{cases}$$

5. 证明: 我们知道: 任意的对称阵都合同于一个对角阵. 即 $\forall B \in S, \exists A \in GL(n, R)$ 使得: $ABA^T = D$, 其中 D 为如下对角阵:

$$D = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{bmatrix} \quad (1)$$

这里 $d_i \in \{0, -1, 1\}$, 考虑矩阵 B 的秩, 设 $r(B) = m$, 则 $0 \leq m \leq n$, 并且对应的对角阵 D 有 $m+1$ 个彼此不合同的类型, 从而, $\text{orb}(B)$ 有 $m+1$ 个不同的可能, 所以总共轨道的个数为: $1 + 2 + 3 + \cdots + n + (n+1) = (n+1)(n+2)/2$.

HW# 6

1. 证明: $\text{Ker}\phi = \{g \in G \mid \phi(g) = \text{Id}_S\}$, 故 $\forall g \in \text{ker}\phi, g(H) = gH = H$, 从而 $g \in H$ 由此可得 $\text{Ker}\phi \subset H$
2. 证明: 首先考虑定义一个如上题 G 在集合 $S = \{H \text{ 在 } G \text{ 中的全体左陪集}\}$ 上的一个作用 ϕ , 由假设知 $|S| = p$, 并且诱导出 $\phi: G \rightarrow A(S)$ 的群同态, 其中 $A(S)$ 是集合 S 上的全体排列, 由群同态基本定理, $G/\text{Ker}\phi \cong \phi(G)$. 从而 $|G/\text{Ker}\phi|$ 整除 $p!$. 同时由上题的结论: $\text{Ker}\phi \subset H$, 现证明: $H \subset \text{Ker}\phi$, 那么就有 $H = \text{Ker}\phi$ 但 $\text{ker}\phi \triangleleft G$, 从而 $H \triangleleft G$. 实际上, 由 Lagrange 定理, 我们有:

$$|G/\text{Ker}\phi| = [G : \text{ker}\phi] = [G : H][H : \text{ker}\phi] = p[H : \text{ker}\phi]$$

从而 $|G/\text{Ker}\phi| = 1$, 或 p 由假设, p 为 $|G|$ 的最小素数因子, 故 $[H : \text{ker}\phi] = 1$, 从而有 $H = \text{Ker}\phi$, 即为证.

HW# 7

1. 证明: 设 $|G| = p^n m$, $(p, m) = 1$, $|N| = p^\lambda q$, $(p, q) = 1$. 则群 G 的 Sylow p -群的阶 $|P| = p^n$, 群 N 的 Sylow p -群的阶为 p^λ . 故:

$$|G/N| = |G|/|N| = p^n m / p^\lambda q = p^{n-\lambda} m / q, \quad (p, m/q) = 1$$

从而 G/N 的 Sylow p -群的阶为 $p^{n-\lambda}$. 由第二群同态定理: $PN/N \cong P/P \cap N$ 和 $|PN| = |P||N|/|P \cap N|$, 并且注意到 $P \cap N$ 为 N 的 Sylow p -群, 所以 $|P \cap N| = p^\lambda$. 由此可得:

$$|PN/N| = |P||N|/|P \cap N||N| = |P|/|P \cap N| = p^n / p^\lambda = p^{n-\lambda}$$

因此, G/N 的 p -子群 PN/N 的阶为 $p^{n-\lambda}$, 从而 PN/N 是 G/N 的 Sylow p -群.

2. (a) 注意到 $P \triangleleft N(P)$, 所以 P 在 $N(P)$ 中的共轭子集只有一个. (b) $x \in N(N(P)) \implies xN(P)x^{-1} = N(P) \implies xPx^{-1} < N(P) \implies xPx^{-1} = P \implies x \in N(P) \implies N(N(P)) < N(P)$. 从而 $N(N(P)) = N(P)$.

3. 证明: $100 = 2^2 \cdot 5^2$, 由 Sylow 第一定理知 G 有阶为 25 的子群. 设 n_5 表示阶为 25 的 Sylow 5-子群的个数, 则由 Sylow 第三定理:

$$n_5 | 4, \quad n_5 \equiv 1 \pmod{5} \implies n_5 = 1 \implies \text{阶为 25 的 Sylow 5-子群是正规子群.}$$

4. 证明: $168 = 2^3 \cdot 3 \cdot 7$, 由 Sylow 第一定理知 G 有阶为 7 的子群. 设 n_7 表示阶为 7 的 Sylow 7-子群的个数, 则由 Sylow 第三定理:

$$n_7 | 24, \quad n_7 \equiv 1 \pmod{7} \implies n_7 = 1 \text{ 或 } n_7 = 8$$

下一步需确定 n_7 是 1 还是 8. 一般方法是, 考虑所有可能的 n_2, n_3 (即 Sylow-2 和 Sylow 3-子群的个数), 然后考虑所有可能的组合, 如 $n_3 = 1, 4, 7, 28$. $n_2 = 1, 3, 7, 21$. $n_7 = 1, 8$. (但这比较复杂! 有兴趣的同学可以尝试.)

5. S_3 的所有 Sylow 2-子群及 Sylow 3-子群,

解: $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, $|S_3| = 2 \cdot 3$, 故 S_3 有 Sylow 2-子群及 Sylow 3-子群, 并且由 Sylow 定理可知: $n_2 = 3, n_3 = 1$.

S_3 的所有 Sylow 2-子群:

$$\langle (12) \rangle = \{(1), (12)\}$$

$$\langle (23) \rangle = \{(1), (23)\}$$

$$\langle (13) \rangle = \{(1), (13)\}$$

S_3 的所有 Sylow 3-子群:

$$\langle 123 \rangle = \{(1), (123), (132)\}$$

故可以得到 $\langle 123 \rangle = \{(1), (123), (132)\}$ 为 S_3 唯一的非平凡的正规子群. (S_4 的所有 Sylow p -子群: 可以类似的去做, 同学们自己试试看!)

HW# 8

1. 证明: 由假设, $a, b, ab - 1$ 都可逆, 并且:

$$(a - b^{-1})b(ab - 1)^{-1} = (ab - 1)(ab - 1)^{-1} = 1 \implies (a - b^{-1})^{-1} = b(ab - 1)^{-1}, \text{ 即 } (a - b^{-1}) \text{ 可逆. 同时可验证 } (a - b^{-1})^{-1} - a^{-1} \text{ 可逆:}$$

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

得证.

2. 直接按环的定义验证, 并且易见 $\mathbb{Z}[i]$ 对乘法可交换, 没有零因子, 故是整环.

3. 证明: 由假设 $\forall a \in R$ 都有 $a^2 = a$. 所以, $\forall a, b$,

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

同时注意到,

$$(a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a = a + a \implies a + a = 0$$

综上所述, $a = -a$, 所以, $ab = ba$. 即 *Boolean* 环是交换环.

4. (a). 设 R 中有零因子, 即在 R 中 $\exists a \neq 0, c \neq 0$ 使得, $ca = 0$, 现在考察: $a(b - c)a = aba - aca = a - aca = a \implies a(b - c)a = a$, 但由假设对于任意 $a \neq 0 \exists$ 唯一元 b 使得: $aba = a$, 从而有 $b - c = b \implies c = 0$. 矛盾! 故没有零因子.

(b). $a(bab - b) = abab - ab = (aba)b - ab = ab - ab = 0$, 但 R 没有零因子, 所以: $bab - b = 0 \iff bab = a$

(c). 对任意 $a \neq 0$, 则存在唯一的 $b \in R$, 使得: $aba = a, bab = b$, 现在证明: ba 就是单位元 1_R . 实际上, $\forall c \in R$, 假设 $cba = \lambda$, 则 $(cba)b = \lambda b \iff cb = c \implies c = \lambda$ (因为没有零因子), 从而 $\forall c \in R$, 假设 $cba = \lambda = c \implies ba = 1_R$.

(d). 由于 R 中没有零因子, 故左右消去律成立, 从而由假设, 对任意 $a \neq 0$, 则存在唯一的 $b \in R$, 使得: $aba = a \implies ab = 1_R$, $bab = b \implies ba = 1_R$, 所以, 任何非零元都有逆, 即 R 是除环.

HW#9

1. 证明: 直接按照域的概念验证. 至于求 $-2 + \sqrt[3]{2} + 3\sqrt[3]{4}$ 的逆元, 可以设 $x + y\sqrt[3]{2} + z\sqrt[3]{4}$ 为其逆元, 则 $(-2 + \sqrt[3]{2} + 3\sqrt[3]{4})(x + y\sqrt[3]{2} +$

$z\sqrt[3]{4} = 1$, 由此得到一个关于 x, y, z 的线性方程组, 可求出 x, y, z , 即就找到了 $-2 + \sqrt[3]{2} + 3\sqrt[3]{4}$ 的逆元.

2. 直接按理想的定义验证.
3. 参考课堂笔记.

HW#10

1. 由环同态基本定理, \mathbb{Z}_{28} 的理想都是形如: $I/(28)$, 其中 I 是 \mathbb{Z} 的包含理想 (28) 的 \mathbb{Z} 的理想, 从而 \mathbb{Z}_{28} 的素理想或极大理想都是 $I/(28)$, 其中 I 满足: $(28) \subset I$, I 是 \mathbb{Z} 的素理想或极大理想. 由环同态第三定理: $\mathbb{Z}/28/I/(28) \cong \mathbb{Z}/I$. 从而, $I/(28)$ 是素理想或极大理想 $\iff \mathbb{Z}/I$ 是整环或域. 但 \mathbb{Z}/I 是整环或域 $\iff I = (p)$, p 是素数, 只需找 28 的素因子: 2, 7, 那么由其生成的理想 I 就满足: $(28) \subset I$, I 是 \mathbb{Z} 的素理想或极大理想, 综上所述, $(2)/(28), (7)/(28)$ 为 \mathbb{Z}_{28} 的素理想同时也是极大理想.
2. 参考笔记.
3. 参考群同态第三定理的证明

HW# 11

1. 证明: 由于多项式 $x^3 + x^2 + 1$ 在 \mathbb{Z}_2 上没有根, 故不可约. 所以理想 $(x^3 + x^2 + 1)$ 是 $\mathbb{Z}_2[x]$ 的极大理想, 从而 $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ 是域. 同时注意到:

$$\mathbb{Z}_2[x]/(x^3 + x^2 + 1) = \{au^2 + bu + c \mid a, b, c \in \mathbb{Z}_2\}$$

这个域是含有 8 个元的域.

2. 证明: 注意到: $(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}$, $(8 + 2\sqrt{15})^2 = 124 + 32\sqrt{15}$, 取多项式 $P(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$, 易见 $P(\sqrt{3} + \sqrt{5}) = 0$, 故 $\sqrt{3} + \sqrt{5}$ 是 \mathbb{Q} 上的代数元. 因

$$P(x) = x^4 - 16x^2 + 4 = (x^2 - 8)^2 - 60 = (x^2 - 8 - 2\sqrt{15})(x^2 - 8 + 2\sqrt{15})$$

, 所以 $P(x)$ 在 \mathbb{Q} 上不可约, 从而 $P(x) = x^4 - 16x^2 + 4$ 是 $\sqrt{3} + \sqrt{5}$ 在 \mathbb{Q} 上的极小多项式.

3. (a). 易见 $x^3 - 3x - 1$ 在 \mathbb{Q} 上没有根, 从而不可约.

(b) 若 α 为 $x^3 - 3x - 1$ 的一个根, 则 \mathbb{Q} 的代数单扩张:

$\mathbb{Q}(\alpha) \cong \mathbb{Q}(x)/(x^3 - 3x - 1)$ 是域 \mathbb{Q} 上的三维向量空间, 并且可以取 $\{1, \alpha, \alpha^2\}$ 作为 $\mathbb{Q}(\alpha)$ 的基; (c). 由于 $\alpha^4 + 2\alpha^3 + 3 \in \mathbb{Q}(\alpha)$:

$$\alpha^4 + 2\alpha^3 + 3 = (\alpha^3 - 3\alpha - 1)(\alpha + 2) + 3\alpha^2 + 7\alpha + 5 = 3\alpha^2 + 7\alpha + 5.$$

所以 $(\alpha^4 + 2\alpha^3 + 3)^{-1} = (3\alpha^2 + 7\alpha + 5)^{-1}$. 设 $(3\alpha^2 + 7\alpha + 5)^{-1} = a + b\alpha + c\alpha^2 \in \mathbb{Q}(\alpha)$, 则

$$(3\alpha^2 + 7\alpha + 5)(a + b\alpha + c\alpha^2) = 1$$

再注意到 $\alpha^3 = 3\alpha + 1$, 化简上式得到关于 a, b, c 的线性方程组, 解此方程组即可.(上式要首先用关系 $\alpha^3 = 3\alpha + 1$ 化为关于 α 的二次式, 然后用待定系数法, 得到关于 a, b, c 的线性方程组, 同学们自己补出细节!)