抽象代数习题

Omnscent

2022 年 5 月 19 日

第 1 章　群、环、体、域的基本概念

§1.0　预备知识

问题 1.

设 X 和 Y 是两个集合, $f: X \to Y$ 和 $g: Y \to X$ 是两个映射. 如果 $g \circ f = \mathrm{id}_X$, 则称 g 为 f 的一个**左逆**; 如果 $f \circ g = \mathrm{id}_Y$, 则称 g 为 f 的一个**右逆**. 如果 g 既是 f 的左逆又是 f 的右逆, 则称 g 为 f 的一个**逆**. 证明

(1) f 有左逆当且仅当 f 是单射;

(2) f 有右逆当且仅当 f 是满射;

(3) f 有逆当且仅当 f 是双射;

(4) 如果 f 有左逆 g, 同时又有右逆 h, 则 $g = h$;

(5) 如果 f 有逆, 则 f 的逆唯一, f 的逆记为 f^{-1};

(6) 如果 f 有逆, 则 $\left(f^{-1}\right)^{-1} = f$.

问题 2.

举例说明等价关系的定义中的三个条件是相互独立的（即任意两条不蕴含剩下的一条）.

§1.1　群的基本概念

问题 1.

证明群的定义可以简化为：如果一个非空集合 G 上定义了一个二元运算 $\circ$, 满足：

(1) **结合律**：$(a \circ b) \circ c = a \circ (b \circ c)\ (\forall a, b, c \in G)$;

(2) 存在**左幺元**：存在 $e \in G$, 使得对任意的 $a \in G$, 都有

$$e \circ a = a;$$

(3) 存在**左逆元**：对任意的 $a \in G$, 存在 $b \in G$, 使得

$$b \circ a = e,$$

则 G 关于运算 $\circ$ 构成一个群.

问题 2.

举例说明:在上题中将条件 (3) 改为"存在**右逆元**:对任意的 $a \in G$, 存在 $b \in G$, 使得 $a \circ b = e$", 则 G 不一定是群.

问题 3.

设 G 是一个非空集合, 其中定义了一个二元运算 $\circ$. 证明：如果此运算满足结合律, 并且对于 G 中任意两个元素 a, b, 方程 $a \circ x = b$ 和 $y \circ a = b$ 都在 G 中有解, 则 $(G, \circ)$ 是群.

问题 4.

设 G 是一个非空的有限集合, 其中定义了一个二元运算 $\circ$. 证明：如果此运算满足结合律, 并且对于 G 中任意的三个元素 a, b, c, 都有（左消去律）$ab = ac \Rightarrow b = c$ 以及（右消去律）$ba = ca \Rightarrow b = c$, 则 $(G, \circ)$ 是群.

问题 5.

设 G 是群, $a, b \in G$, 如果 $aba^{-1} = b^r$, 证明 $a^i b a^{-i} = b^{r^i}$.

问题 6.

证明不存在恰有两个 2 阶元素的群.

问题 7.

设 G 是群. 如果对于任意的 $a, b \in G$, 都有 $(ab)^2 = a^2 b^2$, 证明 G 是交换群. 并由此证明：如果 $\exp(G) = 2$, 则 G 交换.

问题 8.

在 S_3 中找出两个元素 x, y, 使得 $(xy)^2 \neq x^2 y^2$.

问题 9.

设 G 是群, i 为任意确定的正整数. 如果对于任意的 $a, b \in G$, 都有 $(ab)^k = a^k b^k, k = i, i+1, i+2$, 证明 G 是交换群.

问题 10.

证明：群 G 为交换群当且仅当 $x \longmapsto x^{-1} (x \in G)$ 是同构映射.

问题 11.

设 S 是群 G 的非空子集, 在 G 中定义一个二元关系 "$\backsim$":$a \backsim b \Longleftrightarrow ab^{-1} \in S$. 证明 $\backsim$ 是一个等价关系当且仅当 S 是 G 的子群.

问题 12.

设 H, K 为群 G 的子群, 证明 $HK \leqslant G$ 当且仅当 $HK = KH$.

问题 13.

设 $n \in \mathbb{Z}$, 则 $n\mathbb{Z}$ 是整数加法群 $\mathbb{Z}$ 的子群. 并证明 $n\mathbb{Z} \cong \mathbb{Z}$.

问题 14.

证明：S_4 的子集 $B = \{(1), (12)(34), (13)(24), (14)(23)\}$ 是一个子群, 且 B 与四次单位根群 μ_4 不同构.

问题 15.

令

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{-\frac{2\pi i}{n}} \end{pmatrix},$$

证明集合 $\{B, B^2, \cdots, B^n, AB, AB^2, \cdots, AB^n\}$ 在矩阵乘法下构成群, 并且此群与二面体群 D_{2n} 同构.

问题 16.

证明偶数阶群中必有元素 $a \neq e$, 满足 $a^2 = e$.

问题 17.

对 $n > 2$, 证明在有限群 G 中阶为 n 的元素个数是偶数.

问题 18.

对于群中的任意二元素 a, b, 证明 ab 与 ba 的阶相等.

问题 19.

在群 $\mathrm{SL}_2(\mathbb{Q})$ 中, 证明元素

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

的阶为 4, 元素

$$b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

的阶为 3, 而 ab 为无限阶元素.

问题 20.

设 G 是交换群, 证明 G 中的全体有限阶元素构成 G 的一个子群.

问题 21.

如果 G 只有有限多个子群, 证明 G 是有限群.

问题 22.

设 H, K 为有限群 G 的子群, 证明 $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

问题 23.

证明指数为 2 的子群必为正规子群.

问题 24.

证明不存在恰有两个指数为 2 的子群的群.

问题 25.

写出二面体群 D_{20} 的全部正规子群.

问题 26.

设 S 为 G 的非空子集, 令

$$\begin{aligned} C_G(S) &= \{x \in G | xa = ax, \forall a \in S\}, \\ N_G(S) &= \{x \in G | xSx^{-1} = S\} \end{aligned}$$

($C_G(S)$ 和 $N_G(S)$ 分别称为 S 在 G 中的**中心化子**和**正规化子**). 证明:

(1) $C_G(S)$ 和 $N_G(S)$ 都是 G 的子群;

(2) $C_G(S) \trianglelefteq N_G(S)$.

问题 27.

设 H, K 为 G 的正规子群, 证明:

(1) $HK = KH$;

(2) $HK \trianglelefteq G$;

(3) 如果 $H \cap K = \{e\}$, 则 G 同构于 $G/H \oplus G/K$ 的子群.

问题 28.

设 $m, n \in \mathbb{Z}$. 证明 $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus Z/n\mathbb{Z}$ 当且仅当 m 与 n 互素.

问题 29.

设 G 为有限群, $N \trianglelefteq G$,$|N|$ 与 $|G/N|$ 互素. 如果 G 的元素 a 的阶整除 $|N|$, 证明 $a \in N$.

问题 30.

设 H, K 是群 G 的子群, 证明 $H \cap K$ 的任一左陪集是 H 的一个左陪集与 K 的一个左陪集的交.

问题 31.

设 H, K 都是群 G 的指数有限的子群, 证明 $H \cap K$ 在 G 中的指数也有限.

问题 32.

设 H 是群 G 的指数有限的子群, 证明 G 有指数有限的正规子群.

问题 33.

设 p 为素数. 证明所有的 p 阶群必为循环群, 因此也是交换群.

问题 34.

试定出所有互不同构的 4 阶群.

问题 35.

证明阶小于 6 的群皆交换, 举例说明存在 6 阶非交换群.

问题 36.

设 G 是 n 阶群, 整数 m 与 n 互素. 如果 $g, h \in G$, 且 $g^m = h^m$, 证明 $g = h$. 再证明对于任一 $x \in G$, 存在唯一的 $y \in G$ 使得

$$y^m = x$$

问题 37.

设 G 是群, $g \in G$. 若 $o(g) = n$, 则 $o(g^m) = n/(m, n)$.

问题 38.

设 $H \leqslant G, K \leqslant G, a, b \in G$. 若 $Ha = Kb$, 则 $H = K$.

问题 39.

设 A, B, C 为 G 的子群, 并且 $A \leqslant C$, 证明

$$AB \cap C = A(B \cap C)$$

问题 40.

设 A, B, C 为群 G 的子群, 并且 $A \leqslant B$. 如果 $A \cap C = B \cap C, AC = BC$, 证明 $A = B$.

问题 41.

设 G 是群. 令 $Z(G) = \bigcap\limits_{g \in G} C_G(g)$. 称 $Z(G)$ 为 G 的**中心**. 证明 $Z(G)$ 是 G 的正规子群.

问题 42.

证明 2 阶正规子群必属于群的中心.

问题 43.

证明 A_4 没有 6 阶子群.

问题 44.

证明 $Z(A \oplus B) = Z(A) \oplus Z(B)$.

问题 45.

证明：有限群 G 是二面体群的充分必要条件是 G 可由两个 2 阶元素生成.

§1.2 环的基本概念

问题 1.

如果把整数环 $\mathbb{Z}$ 中的加法和乘法的定义互换, 即对于 $a, b \in \mathbb{Z}$, 定义 $a \oplus b = ab, a \odot b = a + b$, 试问 $(\mathbb{Z}; \oplus, \odot)$ 是否构成环？

问题 2.

在集合 $S = \mathbb{Z} \times \mathbb{Z}$ 上定义

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc) \end{aligned}$$

证明 $(S; +, \cdot)$ 是交换幺环.

问题 3.

设 R 是交换幺环. 对于 $a, b \in R$, 定义

$$\begin{aligned} a \oplus b &= a + b - 1, \\ a \odot b &= a + b - ab, \end{aligned}$$

证明 $(R; \oplus, \odot)$ 是交换幺环.

问题 4.

设 $(G;+)$ 是交换群. 对于 $\varphi, \phi \in \mathrm{End}\,(G)$, 定义加法:

$$\begin{aligned} \varphi + \phi: \quad & G \to G, \\ & g \longmapsto \varphi\,(g) + \phi\,(g)\,, \quad g \in G. \end{aligned}$$

又定义 $\varphi \cdot \phi$ 为 φ 与 ϕ 的复合 $\varphi \circ \phi$. 证明 $(\mathrm{End}\,(G)\,;+,\cdot)$ 构成幺环（称为 G 的**自同态环**）.

问题 5.

设 $G = (\mathbb{Z};+)$, 求 $\mathrm{End}\,(G)$.

问题 6.

设 G 为 n 阶循环群, 求 $\mathrm{End}\,(G)$.

问题 7.

设 $G = \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, 求 $\mathrm{End}\,(G)$.

问题 8.

给出环 R 和它的子环 S 的例子, 使得他们满足以下条件之一:

(1) R 有 1, 但 S 没有 1;

(2) R 有 1, 但 S 有 1;

(3) R 与 S 都有 1;

(4) R 不交换, 但 S 交换.

问题 9.

设 R 是环. 如果存在 $e_l \in R$, 满足 $e_l a = a\,(\forall a \in R)$, 则称 e_l 为 R 的一个**左幺元**. 类似地, 如果存在 $e_r \in R$, 满足 $ae_r = a\,(\forall a \in R)$, 则称 e_r 为 R 的一个**右幺元**. 证明:

(1) 如果 R 有左幺元又有右幺元, 则 R 有幺元;

(2) 如果 R 有左幺元但没有非零零因子, 则 R 有幺元;

(3) 如果 R 有左幺元但没有右幺元, 则 R 至少有两个左幺元.

问题 10.

设 R 是环, $a \in R, a \neq 0$. 如果存在 $b \in R, b \neq 0$, 使得 $aba = 0$, 证明 a 是 b 的一个左零因子或右零因子.

问题 11.

设 R 是有限幺环, $a, b \in R$ 且 $ab = 1$. 证明 $ba = 1$

*** 问题 12.**

设 R 是幺环, $a, b \in R, ab = 1$ 但 $ba \neq 1$. 证明由无穷多个 $x \in R$ 满足 $ax = 1$.

问题 13.

设 R 是环, $a \in R$. 如果存在正整数 n 使得 $a^n = 0$, 则称 a 为一个**幂零元**. 证明：如果 a 是幺环中的幂零元, 则 $1 - a$ 可逆.

问题 14.

证明：在交换环 R 中全体幂零元组成一个理想（称为 R 的**幂零根**或**小根**）.

问题 15.

证明幺环中理想的加、乘法满足分配律. 即设 I, J, K 是幺环 R 的理想, 则

$$
\begin{aligned}
(I + J) K &= IK + JK, \\
K (I + J) &= KI + KJ.
\end{aligned}
$$

问题 16.

设 I 是交换幺环 R 的一个理想. 令

$$
\mathrm{rad} I = \left\{ x \in R | \text{存在正整数} n \text{使得} x^n \in I \right\}.
$$

证明 $\mathrm{rad} I$ 是 R 的理想（$\mathrm{rad} I$ 称为 I 的**根理想**）.

问题 17.

证明域 K 上的 n 阶全矩阵环 $\mathrm{M}_n(K)$ 没有非平凡理想（这种环称为**单环**）.

问题 18.

设 R 和 S 都是幺环, $\varphi : R \to S$ 是把 R 的幺元映到 S 的幺元的满同态, 判断下述命题是否正确（给出证明或反例）:

(1) φ 把幂零（幂等）元映为幂零（幂等）元（环中的元素 a 称为**幂等元**, 如果 $a^2 = a$）;

(2) φ 把零因子映为零因子;

(3) φ 把整环映为整环;

(4) 如果 S 是整环, 则 R 是整环;

(5) φ 把可逆元映为可逆元;

(6) 对于 $a \in R$, 如果 $\varphi(a)$ 可逆, 则 a 可逆.

问题 19.

设 R 是幺环, T 是整环, $\varphi : R \to T$ 是环同态. 证明 $\varphi(1_R) = 1_T$（1_R 和 1_T 分别为 R 和 T 的幺元）.

问题 20.

证明习题 3 中构造的环与原来的环 R 同构.

问题 21.

设 R 是幺环, $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ 是环 R 的一个内直和, I 为 R 的一个理想. 证明

$$I = (I \cap R_1) \oplus (I \cap R_2) \oplus \cdots \oplus (I \cap R_n) .$$

§1.3 体、域的基本概念

问题 1.

设 R 是非零交换幺环. 证明 R 是单环当且仅当 R 是域.

问题 2.

设 K 是域, $\varphi : K \to R$ 是环同态. 证明 $\varphi(K) = \{0\}$ 或 φ 是单射.

问题 3.

证明有限整环是域.

问题 4.

在 p–进制域 $\mathbb{Q}_p$ 中证明 $\sum_{i=1}^{\infty} p^i = \frac{1}{1-p}$

问题 5.

证明 p–进整数环 $\mathbb{Z}_p$ 的可逆元素乘法群

$$\mathbb{Z}_p^{\times} = \left\{ a \in \mathbb{Z}_p \middle| \, |a|_p = 1 \right\} .$$

问题 6.

证明 p–进整数环 $\mathbb{Z}_p$ 的任一非零理想皆形如

$$\{a \in \mathbb{Z}_p | v_p(a) \geqslant n\} ,$$

其中 n 为非负整数.

问题 7.

证明 p–进整数环 $\mathbb{Z}_p$ 的任一非零理想皆形如 $\mathfrak{M}^n$, 其中 $\mathfrak{M}$ 为 $\mathbb{Q}_p$ 的赋值理想, n 为非负整数.

问题 8.

证明 p–进整数环 $\mathbb{Z}_p$ 等于可逆元素乘法群与赋值理想 $\mathfrak{M}$ 的无交并.

问题 9.

证明 $\mathbb{H}_0 = \{a + bI + cJ + dK \in \mathbb{H} | a, b, c, d \in \mathbb{Q}\}$ 是四元数体 $\mathbb{H}$ 的子体.

问题 10.

求四元数体 $\mathbb{H}$ 的中心（即 $\mathbb{H}$ 中与所有元素乘法可交换的全体元素）.

问题 11.

证明四元数体的单位元素 $\{\pm 1, \pm I, \pm J, \pm K\}$ 在乘法下组成一个群, 叫做**四元数群**, 记作 Q_8. 证明 Q_8 的每个子群都是正规子群.

问题 12.

证明四元数群 Q_8 与 4 阶循环群的直和存在非正规子群.

问题 13.

设 L 是含有两个以上元素的环. 如果对于每个非零元素 $a \in L$, 都存在唯一的元素 $b \in L$ 使得 $aba = a$, 证明:

(1) L 无非零零因子;

(2) $bab = b$;

(3) L 有 1;

(4) L 是体.

问题 14.

设 L 是体, $a, b \in L, ab \neq 0, 1$. 证明**华罗庚等式**:

$$a - \left(a^{-1} + \left(b^{-1} - a\right)^{-1}\right)^{-1} = aba.$$

问题 15.

设 F 是特征 $p > 0$ 的域. 证明

$$(a + b)^p = a^p + b^p, \ \forall a, b \in F.$$

问题 16.

给出两个有限非交换群 G, 分别适合：

(1) $g^3 = e, \forall g \in G$;

(2) $g^4 = e, \forall g \in G$.

第 2 章 群

§2.1 几种特殊类型的群

问题 1.

设 g 为群 G 中的 rs 阶元素, 其中 r 与 s 互素. 证明存在 $a, b \in G$ 满足 $g = ab, o(a) = e, o(b) = s$ 且 a, b 都是 g 的方幂.

问题 2.

如果群 G 中的元素 g 的阶与正整数 k 互素, 证明方程 $x^k = g$ 在 $\langle g \rangle$ 内恰有一个解.

问题 3.

证明有理数加法群的任一有限生成子群都是循环群.

问题 4.

设 G 是有限生成的交换群. 如果 G 的每个生成元的阶都有限, 证明 G 是有限群.

*** 问题 5.**

证明有限生成群的指数有限的子群也是有限生成的.

*** 问题 6.**

设 G 是群. 对于任一正整数 k, 令 $G^k = \left\{g^k | g \in G\right\}$. 证明 G 是循环群的充分必要条件是 G 的任意一个子群都是 G^k 这样的集合.

*** 问题 7.**

设 p 是素数, n 是正整数, $G = \mathrm{Z}_{p^n}$. 试确定 $\mathrm{Aut}\,(G)$.

问题 8.

写出互不同构的所有的 36 阶交换群.

问题 9.

求 $\mathrm{Z}_3 \oplus \mathrm{Z}_9 \oplus \mathrm{Z}_9 \oplus \mathrm{Z}_{243}$ 的 9 阶循环和非循环子群的个数.

问题 10.

证明 S_n 可以由 $n-1$ 个对换 $(1\ 2), (1\ 3), \cdots, (1\ n)$ 生成, 也可以由 $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ 生成.

问题 11.

证明 S_n 可以由对换 $(1\ 2)$ 和轮换 $(1\ 2\ \cdots\ n)$ 生成.

问题 12.

如果 n 是大于 2 的偶数, 证明 A_n 可以由 $(1\ 2\ 3), (1\ 2\ 4), \cdots (1\ 2\ n)$ 生成, 也可以由 $(1\ 2\ 3), (2\ 3\ 4), \cdots, (n-2\ n-1\ n)$ 生成.

问题 13.

证明：如果 n 是大于 2 的偶数, A_n 可以由 $(1\ 2\ 3)$ 和 $(2\ 3\ \cdots\ n)$ 生成; 如果 n 是大于 2 的奇数, 则 A_n 可以由 $(1\ 2\ 3)$ 和 $(1\ 2\ \cdots\ n)$ 生成.

问题 14.

设 $\sigma = (1\ 2\ \cdots\ n)$, 证明 σ 在 S_n 中的中心化子是 $\langle\sigma\rangle$, 并证明 σ 在 S_n 中的共轭类含有 $(n-1)!$ 个元素.

问题 15.

设 $n > 2$, 证明 $Z(S_n) = \{(1)\}$.

问题 16.

设 $n \geqslant 5$, 证明 S_n 中只有一个非平凡的真正规子群, 即 A_n.

问题 17.

设 G 是群, $N \trianglelefteq G, N \cap G' = \{e\}$. 证明 $N \leqslant Z(G)$.

问题 18.

证明可解群的子群和商群都是可解群.

问题 19.

设 H, K 都是群 G 的正规子群, G/H 与 G/K 都可解. 证明 $G/H \cap K$ 也可解.

问题 20.

如果群 G 恰有两个自同构, 证明 G 必为交换群.

问题 21.

证明阶大于 2 的有限群至少有两个自同构.

问题 22.

证明 $\mathrm{Aut}\,(\mathbb{Z}_2 \oplus \mathbb{Z}_2) \cong S_3$.

§2.2 群在集合上的作用和 Sylow 定理

问题 1.

设 G 是有限群, $H < G$ 且 $|G:H| = n > 1$. 证明 G 必含有一个指数整除 $n!$ 的非平凡正规子群或者 G 同构于 S_n 的一个子群.

问题 2.

设 G 是有限群, p 为 $|G|$ 的最小素因子. 证明 G 的指数为 p 的子群（如果存在）必正规.

问题 3.

证明 p^2 阶群必交换（这里 p 是素数）, 并且这种群在同构意义下只有两个.

问题 4.

证明 p 群是可解群.

问题 5.

证明非交换 6 阶群必同构于 S_3.

问题 6.

写出 S_4 的一个 Sylow2 子群和一个 Sylow3 子群.

问题 7.

设 G 是群, $H \trianglelefteq G, K \trianglelefteq G$, 且 $H \cap K = \{e\}$, 则 H 和 K 之间元素的乘法可交换.

问题 8.

定出所有互不同构的 15 阶群.

问题 9.

定出所有互不同构的 10 阶群.

问题 10.

设 p, q 是不同的素数. 证明不存在 pq 阶单群.

问题 11.

设 p, q 是不同的素数. 证明 p^2q 阶群必含有正规的 Sylow 子群.

问题 12.

证明不存在 56 阶单群.

*** 问题 13.**

证明 60 阶单群必同构于 A_5.

问题 14.

设 p 为素数, 群 G 的阶为 p^3. 如果 G 非交换, 证明 $G' = Z(G)$.

问题 15.

设 G 为 p 群, $N \trianglelefteq G, |N| = p$. 证明 $N \leqslant Z(G)$.

问题 16.

证明不存在群 G 满足 $G' \cong S_3$.

问题 17.

证明不存在群 G 满足 $G' \cong S_4$.

问题 18.

证明 $A_n (n > 4)$ 中每个 3 轮换都可以表成一个换位子. 由此证明 $A_n = A_n$.

问题 19.

设 G 为有限群, $N \trianglelefteq G$, P 为 N 的一个 Sylow p 子群. 证明 $G = NN_G(P)$.

问题 20.

设 G 是有限群, 且 G 有一个非平凡的循环的 Sylow2 子群. 证明 G 有指数为 2 的子群.

问题 21.

设 p 是素数, $F = \mathbb{Z}/p\mathbb{Z}, G = \mathrm{GL}_n(F)$. 具体写出 G 的一个 Sylow p 子群.

§2.3 合成群列

问题 1.

证明整数加法群 $\mathbb{Z}$ 没有合成群列.

问题 2.

写出 Z_6 的两种合成群列.

问题 3.

写出 S_3 和 S_4 的合成群列.

问题 4.

设 $F=\mathbb{Z}/2\mathbb{Z}$, 试写出 $\mathrm{GL}_2(F)$ 的一个合成群列.

§2.4 自由群

问题 1.

证明 S_4 由元素 a,b 生成, 而 a,b 适合 $a^2=b^3=e,(ab)^4=e$.

问题 2.

证明 A_4 由元素 a,b 生成, 而 a,b 适合 $a^2=b^3=e,(ab)^3=e$.

问题 3.

设群 G 由元素 a,b 生成, 有定义关系 $a^4=b^4=e,a^2=b^2,b^{-1}ab=a^{-1}$. 证明 G 为第 1 章 §1.3 的习题 11 定义的 8 阶四元数群.

问题 4.

设 F 是的自由群, G,H 是群. 设 $\alpha:F\to G$ 是同态, $\beta:H\to G$ 是满同态, 则存在同态 $\gamma:F\to H$ 使得 $\alpha=\beta\gamma$. (本习题的结论常称为是**自由群的万有性质**或**自由群的投射性质**)

$$\begin{tikzcd}
& G \\
F \arrow[ur, "\alpha"] \arrow[dr, "\gamma"'] & \\
& H \arrow[uu, "\beta"']
\end{tikzcd}$$

图 1: 第四题图

§2.5 正多面体及有限旋转群

问题 1.

证明 S_4 只有一个 12 阶子群, 即 A_4.

问题 2.

证明 S_5 只有一个 60 阶子群, 即 A_5.

问题 3.

应用本节的结果给出空间正多面体的一个分类.

第 3 章 环

§3.1 环的若干基本知识

（除特殊声明外, 此习题中的环都是指交换幺环. ）

问题 1.

设 I, J 为环 R 的理想, I, J 互素, 证明 $IJ = I \cap J$.

问题 2.

设 $I_1, \cdots, I_n$ 为环 R 的两两互素的理想, 证明

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

问题 3.

设 I, J, K 为环 R 的理想, $IJ \subseteq K$ 且 I 与 K 互素, 证明 $J \subseteq K$.

问题 4.

设 I, J, K 为环 R 的理想, $I, J \supseteq K$ 且 I 与 J 互素, 证明 $IJ \supseteq K$.

问题 5.

设 p 是一个素数, n 是大于 1 的整数, $R = \mathbb{Z}/(p^n)$, 证明:

(1) R 的元素不是可逆元就是幂零元;

(2) R 只有一个素理想, 记作 P;

(3) 商环 R/P 是域.

问题 6.

设 $\mathfrak{M}$ 是 p 进整数环 $\mathbb{Z}_p$ 的赋值理想, 证明对于任意正整数 n, 有 $\mathbb{Z}_p/\mathfrak{M}^n \cong \mathbb{Z}/(p^n)$.

问题 7.

设 $\varphi : R \to R_1$ 是把 1 映成 1 的环同态. 如果 Q 是 R_1 的素理想, 证明 $P = \varphi^{-1}(Q)$ 是 R 的素理想. 如果 Q 是 R_1 的极大理想, $\varphi^{-1}(Q)$ 一定是 R 的极大理想吗?

问题 8.

若环 R 的一个素理想 P 包含有限多个理想 $I_i\,(1 \leqslant i \leqslant n)$ 的交, 证明 P 包含某个 I_i.

问题 9.

若环 R 的一个理想 I 含于有限多个素理想 $P_i\,(1 \leqslant i \leqslant n)$ 的并, 证明 I 含于某个 P_i.

问题 10.

证明有限环的素理想都是极大理想.

问题 11.

设 p 为素数, 写出分式环 $\mathbb{Z}_{(p)}$（表成 $\mathbb{Q}$ 的子集）.

问题 12.

设 P 为环 R 的素理想（于是 R 可以视为 R_p 的子环）.

(1) 对于 R 的任一理想 I, 证明 $I \cdot R_p$ 是 R_p 的理想;

(2) 对于 R 的任一素理想 Q, 证明 $Q \cdot R_p$ 是 R_p 的素理想或平凡理想 (1).

(3) 证明 $P \cdot R_p$ 是 R_p 唯一的极大理想;

(4) 证明 $Q \longmapsto Q \cdot R_p$ 给出 R 含于 P 的素理想的集合到 R_p 的素理想的集合的双射.

§3.2 整环内的因子分解理论

问题 1.

构造一个不满足因子链条件的整环.

问题 2.

设 R 是满足因子链条件的整环, 证明 R 是唯一分解整环当且仅当 R 中任意两个元素都有最大公因子.

问题 3.

设 R 是唯一分解整环, S 是 R 的一个乘法封闭子集, $0 \notin S$. 证明分式环 $S^{-1}R$ 也是唯一分解整环.

问题 4.

举例说明唯一分解整环的子环不一定是唯一分解整环.

问题 5.

设 R 是唯一分解整环, P 是 R 的素理想. 举例说明商环 R/P 不一定是唯一分解整环.

问题 6.

证明一元多项式环 $\mathbb{Z}[x]$ 的任一主理想都不是极大理想.

问题 7.

设 K 是域. 系数在 K 中的形式幂级数 $\sum_{i=0}^{\infty} a_i x^i (a_i \in K, x为不定元)$ 的全体在通常的加法和乘法下构成一个环, 称为 K 上的一元**形式幂级数环**, 记为 $K[[x]]$.

(1) 设 $f(x) = \sum_{i=0}^{\infty} a_i x^i \in K[[x]]$, 证明 $f(x)$ 是 $K[[x]]$ 的可逆元当且仅当 $a_0 \neq 0$;

(2) 证明 $K[[x]]$ 是主理想整环.

问题 8.

证明：主理想整环中的非零素理想是极大理想.

问题 9.

设 R 是主理想整环, $a, b, d \in R$, 则 $(a, b) = (d)$ 当且仅当 d 是 a, b 的最大公因子.

问题 10.

设 R 是主理想整环, D 是包含 R 的主理想整环, $a, b, d \in R$, d 是 a, b 在 R 中的最大公因子. 证明 d 也是 a, b 在 D 中的最大公因子.

问题 11.

设 R 是主理想整环, P 是 R 的一个非零素理想. 证明在分式环 R_P 上可以定义一个绝对值函数, 满足第一章 §1.3 例 3.3 中的三个条件.

问题 12.

设 K 是代数数域 (见第 1 章 §1.3 例 1.3). K 的元素 α 称为一个**代数整数**, 如果 α 是一个首项系数为 1 的整系数多项式的零点. 设 d 是无平方因子的整数, $K = \mathbb{Q}\left(\sqrt{d}\right)$.

(1) 如果 $d \equiv 2, 3 \pmod 4$, 证明 K 中代数整数的集合等于

$$\left\{a + b\sqrt{d} | a, b \in \mathbb{Z}\right\};$$

(2) 如果 $d \equiv 1 \pmod 4$, 证明 K 中代数整数的集合等于

$$\left\{a + b\frac{1+\sqrt{d}}{2} \middle| a, b \in \mathbb{Z}\right\}.$$

由此证明 K 中的代数整数的全体构成一个环, 称为 K 的**代数整数环**.

问题 13.

证明 $\mathbb{Q}\left(\sqrt{-3}\right)$ 的代数整数环是欧几里得环.

问题 14.

证明 $\mathbb{Q}(\sqrt{2})$ 的代数整数环是欧几里得环.

问题 15.

证明 $\mathbb{Q}(\sqrt{5})$ 的代数整数环是欧几里得环.

问题 16.

证明环 $\mathbb{Z}[i]$(其中 $i=\sqrt{-1}$) 的可逆元素乘法群为 $\{\pm 1, \pm i\}$.

问题 17.

设 p 为素数. 如果 $p \equiv 1 \pmod 4$, 证明存在 $a, b \in \mathbb{Z}$, 使得

$$p = a^2 + b^2$$

问题 18.

证明环 $\mathbb{Z}[i]$ 的不可约元 (在相伴意义下) 有且仅有以下三种:

(1) $1+i$;

(2) $a+bi$, 其中 $a, b \in \mathbb{Z}$ 满足 $a^2+b^2 \equiv 1 \pmod 4$ 为素数;

(3) $p \equiv 3 \pmod 4$ 为素数.

问题 19.

设 K 是域, $K[x,y]$ 是 K 上的二元多项式环,

$$R = K[x,y] / \left(x^3 - y^3\right).$$

(1) 证明 R 是整环;

(2) 令 $P_0 = (\bar{x}, \bar{y}) \, (\subseteq R)$, 证明 P_0 是 R 的极大理想, 且

$$\left(P_0 \cdot R_{P_0}\right) / \left(P_0 \cdot R_{P_0}\right)^2$$

作为 K 向量空间的维数为 2;

(3) 令 $P_1 = (\bar{x}-1, \bar{y}-1) \, (\subseteq R)$, 证明 P_1 是 R 的极大理想, 且 $\left(P_1 \cdot R_{P_1}\right) / \left(P_1 \cdot R_{P_1}\right)^2$ 作为 K 向量空间的维数为 1.

问题 20.

设 R 是唯一分解整环, K 为 R 的分式域, $f(x)$ 是 $R[x]$ 中的首项系数为 1 的多项式. 如果 $g(x)$ 是 $f(x)$ 在 $K[x]$ 中的首项系数为 1 的因子, 证明 $f(x) \in R[x]$.

问题 21.(Eisenstein 判别法)

设 R 是唯一分解整环, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$. 如果存在 R 的不可约元 p 满足 $p \nmid a_n, p | a_i\ (\forall i < n), p^2 \nmid a_0$, 证明 $f(x)$ 在 $F[x]$ 中不可约 (F 是 R 的分式域).

问题 22.

判断下列多项式在一元多项式环 $\mathbb{Q}(i)[x]$ 中是否可约:

(1) $x^{p-1} + x^{p-2} + \cdots + 1$, 其中 p 为素数;

(2) $x^4 + (8+i)x^3 + (3-4i)x + 5$.