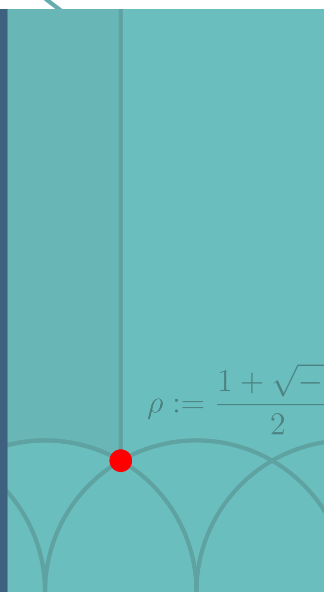
2022 年 7 月 14 日

Algebra Solutions

作者: 正寅

教材: 抽象代数 (张勤海著 第一版)



目录

第 1 章 群论 4
1.1 群与子群 4
1.2 正规子群和商群 11
1.3 同态与同构 16
1.4 直积与半直积 20
1.5 群作用 20
1.6 Sylow 定理 21

第 2 章 环与域 23
2.1 基本概念和例子 23
2.2 理想与同态 27
2.3 极大理想和素理想 30
2.4 整环里的因子分解 30
2.5 域的扩张 32
2.6 代数扩域 35
2.7 多项式的分裂域与正规扩域 37
2.8 有限域 37

第 3 章 Galois 理论 38
3.1 Galois 理论的基本定理 38

第 4 章 补充题目 40
4.1 2021 年期中测试题 43
4.2 2018–2019 年期末测试题 47
4.3 2019 级研究生近世代数试题 53
4.4 2020 级研究生近世代数试题 55

4.5 2021 级近世代数期末试题 60

第 1 章

群论

1.1 群与子群

1. 证明命题 1.1.1, 1.1.2 和 1.1.3.

命题 1.1.1 证明: ($\Rightarrow$) 假设 HK 为子群. 对于任意 $kh \in KH$, 其中 $k \in K$, $h \in H$. 因为 $k = 1k \in HK$, $h = h1 \in HK$ 且 HK 关于乘法封闭, 所以 $kh \in HK$, 故 $KH \subset HK$.

对于任意 $hk \in HK$, 其中 $h \in H$, $k \in K$. 因为 HK 关于取逆封闭, 所以 $(hk)^{-1} \in HK$, 故存在 $x \in H$ 和 $y \in K$ 使得 $(hk)^{-1} = xy \Rightarrow hk = y^{-1}x^{-1} \in KH$. 因而 $HK \subset KH$.

故 $HK = KH$.

($\Leftarrow$) 显然 HK 包含单位元 1, 下证 HK 关于乘法和取逆封闭. 对于任意 $a, b \in HK$, 可分别将 a, b 表为 $a = h_1k_1$, $b = h_2k_2$.

因为 $k_1h_2 \in KH = HK$, 所以存在 $h \in H$ 和 $k \in K$ 使得 $k_1h_2 = hk$, 故

$$ab = h_1k_1h_2k_2 = h_1hkk_2 \in HK,$$

即 HK 关于乘法封闭.

因为

$$a^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK,$$

所以 HK 关于取逆封闭. 从而 HK 为 G 的子群. $\square$

命题 1.1.2 证明: 当 $|G|$ 有限时, 此命题由 Lagrange 定理立即得证. 下面假设 $|G|$ 无限.

首先给出横截的定义: 设 G 为群, $H \leq G$ 且 S 为 G 的子集, 若 H 的每一个右陪集都恰好包含 S 中的一个元素, 则称 S 为 H 在 G 中的右横截. (左横截类似定义)

设 T 为 K 在 H 中的右横截, U 为 H 在 G 中的右横截.

第一步, 设 $g \in G$, 下证存在 $t \in T$ 和 $u \in U$ 使得 $Kg = Ktu$. 对于右陪集 Hg, 存在 $u \in U$ 使得 $Hg = Hu$, 故 $g \in Hu$, 从而存在 $h \in H$ 使得 $g = hu$. 再考虑陪集 Kh, 自然存在 $t \in T$ 使得 $Kh = Kt$, 故 $h \in Kt$, 从而存在 $k \in K$ 使得 $h = kt$. 所以 $g = hu = ktu \in Ktu$, 由此得 $Kg = Ktu$.

第二步, 若存在 $t, t' \in T$ 和 $u, u' \in U$ 使得 $Ktu = Kt'u'$, 下证 $t = t'$, $u = u'$. 因为 $Ktu = Kt'u'$, 所以存在 $k \in K$ 使得 $tu = kt'u'$, 故 $u(u')^{-1} = t^{-1}kt' \in H$, 从而 $Hu = Hu'$. 由横截的定义知 $u = u'$.

结合 $tu = kt'u'$ 和 $u = u'$ 知 $t(t')^{-1} = k \in K$, 故 $Kt = Kt'$, 再次由横截的定义知 $t = t'$.

第三步, 由前两步结论可知 $TU = \{tu \mid t \in T, u \in U\}$ 构成了 K 在 G 中的右横截, 因此

$$|G : K| = |U| \cdot |T| = |G : H| \cdot |H : K|. \qquad \square$$

命题 1.1.3 证明:

$\square$

2. 设 G 为有限群, $|G| = mn$, $(m, n) = 1$, $g \in G$. 证明: G 中存在唯一的元素 x 和 y, 使得 $g = xy = yx$ 且满足 $x^m = y^n = 1$.

证明: 因为 $(m, n) = 1$, 所以存在 $r, s \in \mathbb{Z}$ 使得 $rm + sn = 1$. 令 $x = g^{sn}$, $y = g^{rm}$, 则 $xy = yx = g^{rm+sn} = g$ 且 $x^m = g^{smn} = 1$, $y^n = g^{rmn} = 1$.

下证唯一性, 假设还存在 x' 和 y' 满足 $g = x'y' = y'x'$ 且 $(x')^m = (y')^n = 1$. 由 $xy = x'y'$ 得

$$(xy)^n = x^n y^n = x^n = (x'y')^n = (x')^n (y')^n = (x')^n.$$

则

$$x = x^{rm+sn} = (x^n)^s = ((x')^n)^s = (x')^{sn} = (x')^{rm+sn} = x'.$$

同理可得 $y = y'$, 唯一性得证. □

3. 设 G 为 n 阶群, $a_1, a_2, \ldots, a_n \in G$, 证明: 存在整数 i, j, $1 \le i \le j \le n$, 使得 $a_i a_{i+1} \cdots a_j = 1$.

证明: 考虑集合 $\{a_1, a_1a_2, \ldots, a_1a_2\cdots a_n\}$.

若该集合中存在元素为 1, 则结论自明;

若该集合中不存在元素为 1, 则必有两元素相同, 不妨设 $a_1a_2\cdots a_{i-1} = a_1a_2\cdots a_j$, 利用消去律即得 $a_ia_{i+1}\cdots a_j = 1$. □

4. 设 G 是群, $K = \{a_1, a_2, \ldots, a_n\} \subset G$ 且 $1 \notin K^2$, 证明: 在 n^2 个乘积 a_ia_j 中, 至多有 $\frac{n(n-1)}{2}$ 个元素 $a_ia_j \in K$.

证明: 将 $\{a_ia_j\}_{1\le i,j\le n}$ 这 n^2 个元素表为矩阵形式, 即

$$A = \begin{pmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_n \\ a_2a_1 & a_2a_2 & \cdots & a_2a_n \\ \vdots & \vdots & & \vdots \\ a_na_1 & a_na_2 & \cdots & a_na_n \end{pmatrix}.$$

将 $\{a_i^{-1}a_j\}_{1\le i,j\le n}$ 这 n^2 个元素也表为矩阵形式, 即

$$B = \begin{pmatrix} a_1^{-1}a_1 & a_1^{-1}a_2 & \cdots & a_1^{-1}a_n \\ a_2^{-1}a_1 & a_2^{-1}a_2 & \cdots & a_2^{-1}a_n \\ \vdots & \vdots & & \vdots \\ a_n^{-1}a_1 & a_n^{-1}a_2 & \cdots & a_n^{-1}a_n \end{pmatrix}.$$

B 的主对角线元素皆为 1, 必不属于 K. 由于 $1 \notin K^2$, 故 $K \cap K^{-1} = \varnothing$, 而 B 中任意两对称元素皆互为逆元素, 所以 B 中至多只有 $\frac{n(n-1)}{2}$ 个元素属于 K.

定义映射: $\phi : A\cap K \to B\cap K$, $a_ia_j \mapsto a_i^{-1}a_k$, 其中 $a_k = a_ia_j$. 容易验证 ϕ 为双射, 因此

$$|A\cap K| = |B\cap K| \le \frac{n(n-1)}{2},$$

也即 A 中至多有 $\frac{n(n-1)}{2}$ 个元素属于 K. □

5. 证明交代群 A_4 没有 6 阶子群.

证法 1: 假设 A_4 存在 6 阶子群 H, 则 $|A_4 : H| = \frac{12}{6} = 2$, 因此 H 必为 A_4 的正规子群, 由此可构造商群 A_4/H.

由于 A_4 中含有 8 个 3-轮换, 故可取某一 3-轮换 $x \notin H$. 考虑陪集 H, xH, x^2H, 由于商群 A_4/H 的阶为 2, 故这三个陪集中必有两个相同. 然而我们知道 H 与 xH 不相同, 所以必定是 x^2H 与 H, xH 中的一个相同.

若 $H = x^2H$, 则 $x^2 = x^{-1} \in H \Rightarrow x \in H$, 矛盾.

若 $xH = x^2H$, 则 $x = x^2x^{-1} \in H$, 矛盾.

综上可知假设不成立, 因此 A_4 没有 6 阶子群. □

证法 2: 假设 A_4 存在 6 阶子群 H, 显然 H 必含 3-轮换且 H 仅有一个三阶子群, 那么 H 还包含另外三个 2 阶元.

由此, 3 个 2 阶元与单位元即可组成 H 的 4 阶子群, 然而 $4 \nmid 6$, 这与 Lagrange 定理相矛盾. □

注 交错群 (Alternating group) A_4 是说明 Lagrange 定理逆命题一般不成立的最小群.

注 其实可以把 A_4 中的元素全部列举出来, 即为

$$\begin{aligned} A_4 = \{&(1),(123),(132),(124),(142),(134),(143),(234),(243),\\ &(12)(34),(13)(24),(14)(23)\}. \end{aligned}$$

可以看出, A_4 包含单位元 (阶为 1)、8 个 3-轮换 (阶为 3) 以及三个不相交对换的乘积 (阶为 2).

6. 设 $G = \langle g\rangle$ 是一个 n 阶循环群, 证明:

(i) 对每一个 n 的因子 d, 恰好存在 G 的一个阶为 d 的子群, 即 $\langle g^{\frac{n}{d}}\rangle$;

(ii) 若 d 和 e 是 n 的因子, 则阶为 d 和 e 的子群的交是阶为 $\gcd(d,e)$ 的子群;

(iii) 若 d 和 e 是 n 的因子, 则阶为 d 和 e 的子群的积是阶为 $\operatorname{lcm}(d,e)$ 的子群;

证明: 正式证明之前, 先证明一个引理: 设 n 为正整数且 d,e 皆为 n 的因子, 则

$$\gcd\left(\frac{n}{d},\frac{n}{e}\right)=\frac{n}{\operatorname{lcm}(d,e)},\quad \operatorname{lcm}\left(\frac{n}{d},\frac{n}{e}\right)=\frac{n}{\gcd(d,e)}.$$

第二个等式可由第一个等式推出, 故只需证明第一个等式. 因 $\frac{n}{\operatorname{lcm}(d,e)}\mid\frac{n}{d}$ 且 $\frac{n}{\operatorname{lcm}(d,e)}\mid\frac{n}{e}$, 故 $\frac{n}{\operatorname{lcm}(d,e)}$ 为 $\frac{n}{d}$ 和 $\frac{n}{e}$ 的公因子. 其次, 任取 $\frac{n}{d}$ 和 $\frac{n}{e}$ 的公因子 k, 即 $k\mid\frac{n}{d}$ 且 $k\mid\frac{n}{e}$, 则由于

$$\frac{n}{\operatorname{lcm}(d,e)}=\frac{n\gcd(d,e)}{de}=\frac{n(rd+se)}{de}=r\frac{n}{e}+s\frac{n}{d},$$

故 $k\mid\frac{n}{\operatorname{lcm}(d,e)}$, 所以 $\frac{n}{\operatorname{lcm}(d,e)}$ 为 $\frac{n}{d}$ 和 $\frac{n}{e}$ 的最大公因子, 引理证毕.

(i) 首先, 因为 $|g^{\frac{n}{d}}|=\frac{n}{\gcd(n,\frac{n}{d})}=d$, 故 $\langle g^{\frac{n}{d}}\rangle$ 为阶为 d 的循环群.

然后, 假设 $\langle g^m\rangle$ 也为阶为 d 的循环群, 则

$$\frac{n}{\gcd(n,m)}=d\Rightarrow m=\frac{n}{d}.$$

唯一性得证.

(ii) 利用引理结论得

$$\langle g^{\frac{n}{d}}\rangle\cap\langle g^{\frac{n}{e}}\rangle=\langle g^{\operatorname{lcm}(d,e)}\rangle=\langle g^{\frac{n}{\gcd(d,e)}}\rangle,$$

即阶为 d 的子群和阶为 e 的子群的交为阶为 $\gcd(d,e)$ 的子群.

(iii) 由于循环群为交换群, 故由命题 1.1.1 知子群的积仍为子群, 且

$$\langle g^{\frac{n}{d}}\rangle\langle g^{\frac{n}{e}}\rangle=\langle g^{\gcd\left(\frac{n}{d},\frac{n}{e}\right)}\rangle=\langle g^{\frac{n}{\operatorname{lcm}(d,e)}}\rangle,$$

即阶为 d 的子群和阶为 e 的子群的积为阶为 $\operatorname{lcm}(d,e)$ 的子群. $\square$

7. 证明: 恰有一个极大子群的 n 阶群 G 一定是循环群.

证明: 设 M 是 G 的极大子群, 取 $a \in G\backslash M$. 记 $H = \langle a \rangle$, 若存在极大子群 K 使得 $H \subset K$, 则显然 $K \neq M$, 这与极大子群的唯一性相矛盾. 因此 H 不存在极大子群, 故 $G = H = \langle a \rangle$ 为循环群. □

8. 证明: S_n 的每一个元素可表为若干个对换的乘积, 对换的个数不一定相等, 但对换个数的奇偶性相同.

9. 设 a, b 是群 G 中两个可交换的元素且 $\langle a \rangle \cap \langle b \rangle = \{1\}$, 证明: $|ab| = \frac{|a||b|}{(|a|,|b|)}$.

证明: 记 $m := |a|$, $n := |b|$ 且 $r := |ab|$.

因为

$$(ab)^{\frac{mn}{(m,n)}} = (a^m)^{\frac{n}{(m,n)}}(b^n)^{\frac{m}{(m,n)}} = 1,$$

所以 $r \mid \frac{mn}{(m,n)}$.

又因为

$$(ab)^r = a^r b^r = 1,$$

所以 $a^r = b^{-r} \in \langle b \rangle$, 从而 $a^r \in \langle a \rangle \cap \langle b \rangle = \{1\}$, 所以 $m \mid r$. 同理可知 $n \mid r$, 故 $\mathrm{lcm}(m, n) = \frac{mn}{(m,n)} \mid r$.

综上, $r = \frac{mn}{(m,n)}$, 也即 $|ab| = \frac{|a||b|}{(|a|,|b|)}$. □

注 不能去掉条件 $\langle a \rangle \cap \langle b \rangle = \{1\}$, 否则结论不成立.

例如: 令 $b = a^{-1}$, 则 $|ab| = |e| = 1 \neq \mathrm{lcm}(a, b) = m$.

又例如: 在 12 阶循环群 $\mathbb{Z}/12\mathbb{Z}$ 中, 考虑元素 $a = \bar{2}$ 和 $b = \bar{4}$, 容易验证 $|a| = 6$ 且 $|b| = 3$, 故 $\mathrm{lcm}(|a|, |b|) = 6$. 但是 $a + b = \bar{6}$ 的阶为 2.

10. 证明: 若群 G 中除单位元外其余元素的阶均为 2, 则 G 为交换群.

证明: 假设 G 不为交换群, 则存在 $a, b \in G$ 使得 $ab \neq ba$. 不等式两侧同时乘以 ab 得

$$abab \neq abba.$$

然而 $abab = (ab)^2 = 1$ 且 $abba = ab^2a = a^2 = 1$, 矛盾. □

11. 证明: S_5 可由一个 5-轮换和一个对换生成.

证明: 下证 $S_5 = \langle (12345), (12) \rangle$. 记 $s = (12345)$, $t = (12)$.

事实上, 任何置换都可以表示为对换的乘积, 故只需证 s 和 t 能生成所有的对换即可. 注意到

$$sts^{-1} = (23),$$

类似地

$$s^2ts^{-2} = (34), \quad s^3ts^{-3} = (45), \quad s^4ts^{-4} = (51).$$

由此不难生成其它的所有对换, 例如

$$(13) = (23)(12)(23), \quad (14) = (34)(13)(34).$$

因此 $S_5 = \langle (12345), (12) \rangle$. □

注 此结论可以推广为: S_n 可以由一个对换和一个 n-轮换当且仅当 n 为素数, 见 math.stackexchange.

1.2　正规子群和商群

1. 设 G 为有限群, $H \le G$, $N \trianglelefteq G$, 证明: (i) 若 $(|G:N|, |H|) = 1$, 则 $H \le N$; (ii) 若 $(|G:H|, |N|) = 1$, 则 $N \le H$.

证明: (i) 因为 $(|G:N|, |H|) = 1$, 所以存在整数 m, n 使得 $m|G:N| + n|H| = 1$. 对于任意 $h \in H$, 有

$$\begin{aligned} hN &= h^{m|G:N|+n|H|}N \\ &= h^{m|G:N|}N \\ &= (hN)^{m|G:N|} \\ &= N. \end{aligned}$$

故 $h \in N$, 从而 $H \le N$.

(ii) 因为 $H \le G$, $N \trianglelefteq G$, 所以 $HN = NH$, 故由命题 1.1.1 知 $HN \le G$, 故

$$|HN| \mid |G| = |G:H| \cdot |H|. \tag{$\star$}$$

由第一同构定理知 $HN/N \cong H/H\cap N$, 于是

$$\frac{|HN|}{|N|}=\frac{|H|}{|H\cap N|},$$

即 $|HN|\cdot|H\cap N|=|H|\cdot|N|$, 故

$$|HN|\mid|H|\cdot|N|. \tag{$\star\star$}$$

因为 $(|G:H|,|N|)=1$, 所以存在整数 m 和 n 使得

$$m|G:H|+n|N|=1,$$

结合 $(\star)(\star\star)$ 可得 $|HN|\mid|H|$, 于是 $|HN|=|H|$, 又因为 $H\leq HN$, 所以 $H=HN\Rightarrow N\leq H$. □

2. 设 G 是群, $H\leq G$, $|G:H|=n$ 且 $z\in Z(G)$, 证明: $z^n\in H$.

证明: 设 $N:=N_GH=\{g\in G\mid gHg^{-1}=H\}$, 则 $H\trianglelefteq N$ 且 $N\leq G$.

考虑商群 N/H, 由 $|N:H|\mid|G:H|=n$ 可知对于任意 $xH\in N/H$ 有 $(xH)^n=x^nH=H$, 故 $x^n\in H$. 又因为 $Z(G)\leq N_GH$, 所以对于任意 $z\in Z(G)$, 有 $z^n\in H$. □

3. 设 H 是群 G 的指数有限的子群, 即 $|G:H|=n<\infty$, 证明: H 含有 G 的一个正规子群 N 使得 $|G:N|<\infty$.

证法一: 考虑群作用 $G\times G/H\to G/H$, $(g,xH)\mapsto gxH$. 此作用对应同态

$$\begin{aligned}\phi:G&\longrightarrow\Sigma_{G/H}=S_n\\ g&\longmapsto\sigma_g,\sigma_g(xH)=gxH.\end{aligned}$$

由群同态基本定理知, $G/\ker\phi\cong\operatorname{Im}\phi\leq S_n$. 由于 $\ker\phi$ 为 G 的正规子群,

$$\begin{aligned}\ker\phi&=\{g\in G\mid\sigma_g=\mathrm{id}\}\\ &=\{g\in G\mid\sigma_g(xH)=gxH=xH,\forall xH\in G/H\}\\ &\subseteq\{g\in G\mid\sigma_g(H)=gH=H\}=H.\end{aligned}$$

且 $|G:\ker\phi|=|G/\ker\phi|=|\operatorname{Im}\phi|\leq n!$, 故取 N 为 $\ker\phi$ 即满足要求. □

证法二: 先证明一个引理: 有限个指数有限的子群的交仍然是指数有限的.

由归纳法, 只需证明 2 个子群的情形, 设 G 为群, $H \leq G$, $K \leq G$, 且 $|G:H| < \infty$, $|G:K| < \infty$. 由于 H 稳定地作用在 HK/K 上, 取 $K \in HK/K$, 因 K 的稳定化子为 $G_K = \{h \in H \mid hK = K\} = H \cap K$, 故由轨道-稳定化子定理知

$$HK/K \cong H/H \cap K.$$

故 $|HK:K| = |H:H \cap K|$, 因此

$$|G:H \cap K| = |G:H||H:H \cap K| = |G:H||HK:K| \leq |G:H||G:K| < \infty.$$

设 $\{x_1, x_2, \ldots, x_n\}$ 为 H 在 G 中的一个左陪集代表 (不妨设 $x_1 \in H$). 令

$$N = \bigcap_{i=1}^{n} x_i H x_i^{-1} \subset x_1 H x_1^{-1} = H.$$

由引理知 N 为 G 的指数有限的子群, 故剩下只需证 $N \lhd G$ 即可. 任取 $g \in G$, 因 $\{gx_1, gx_2, \ldots, gx_n\}$ 为 H 在 G 中的另一组左陪集代表, 故存在 $\sigma \in S_n$, 使得 $gx_iH = x_{\sigma(i)}H$ $(1 \leq i \leq n)$, 因此

$$gNg^{-1} = \bigcap_{i=1}^{n} gx_i H x_i^{-1} g^{-1} = \bigcap_{i=1}^{n} x_{\sigma(i)} H x_{\sigma(i)}^{-1} = N.$$

所以就得 $N \lhd G$. □

4. 若群 G 有一个指数为 4 的正规子群, 则 G 也有一个指数为 2 的正规子群.

证明: 假设 N 为 G 的指数为 4 的正规子群, 考虑商群 G/N, 取 $x \notin N$, 则陪集 xN 在商群中的阶 $|xN| = 2$ 或 $|xN| = 4$.

若 $|xN| = 2$, 则 $\langle x \rangle N = N \cup xN$, 故 $|\langle x \rangle N : N| = 2$, 又因为 $|G:N| = |G:\langle x \rangle N| \cdot |\langle x \rangle N : N|$, 故 $|G:\langle x \rangle N| = 2$, 于是 $\langle x \rangle N$ 即为 G 的指数为 2 的正规子群.

若 $|xN| = 4$, 则 $\langle x^2 \rangle N = N \cup x^2 N$, 同理可得 $\langle x^2 \rangle N$ 为 G 的指数为 2 的正规子群. □

5. 设 A 和 B 是群 G 的两个正规子群, $A \cap B = \{1\}$, 证明: A 的元素与 B 的元素可交换.

证明: 对于任意 $a \in A$ 和 $b \in B$, 考虑换位子 $a^{-1}b^{-1}ab$.

因为 A 为正规子群, 所以 $b^{-1}ab \in A$, 从而 $a^{-1}b^{-1}ab \in A$; 因为 B 为正规子群, 所以 $a^{-1}b^{-1}a \in B$, 从而 $a^{-1}b^{-1}ab \in B$, 故 $a^{-1}b^{-1}ab \in A \cap B = \{1\}$, 这说明 $ab = ba$. □

6. 证明: 有限交换单群 $G \neq \{e\}$ 一定是素数阶循环群.

证明: 因在交换群中, 所有子群都正规, 所以在交换单群中没有非平凡的子群. 任取非单位元素 $g \in G$, 由于 G 没有非平凡子群, 就有 $G = \langle g \rangle$, 即 G 为循环群且阶数一定为素数. □

7. 证明: 四元数群 Q_8 的每个子群都是正规子群.

证明: 设 $H \leq Q_8$. 显然当 $H = \{1\}$ 或 $H = Q_8$ 时其为正规子群, 否则 $|H| = 2$ 或 4.

当 $|H| = 4$ 时, $|Q_8 : H| = 2$, 又指数为 2 的子群为正规子群, 故此时 $H \lhd G$. 当 $|H| = 2$ 时, $H = \{1, -1\} \lhd G$. □

8. 设 G 为群, $x, y \in G$, 证明: 若 $[x, y] \in Z(G)$, 则对任意的 $n \in \mathbb{N}$ 有 $[x^n, y] = [x, y]^n$, $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$.[1]

证明: 先证明 $[x^n, y] = [x, y]^n$. 当 $n = 0$ 时等式显然成立, 假设等式对 $n = k$ 成立, 则

$$
\begin{aligned}
[x^{k+1}, y] &= x^{-(k+1)} y^{-1} x^{k+1} y \\
&= x^{-k} \cdot x^{-1} y^{-1} x y \cdot y^{-1} x^k y \\
&= x^{-1} y^{-1} x y \cdot x^{-k} y^{-1} x^k y \\
&= [x, y] \cdot [x^k, y] \\
&= [x, y] \cdot [x, y]^k \\
&= [x, y]^{k+1},
\end{aligned}
$$

[1] 原题有误.

故当 $n=k+1$ 时等式成立, 由归纳法可知对任意 $n\in\mathbb{N}$ 有 $[x^n,y]=[x,y]^n$.

再证明 $(xy)^n=x^ny^n[y,x]^{\frac{n(n-1)}{2}}$. 首先容易由 $[x,y]\in Z(G)$ 证得 $[y,x]\in Z(G)$, 然后注意到一个关系式: 对于任意非负整数 m,n 有

$$x^myx^n=x^mxy\cdot y^{-1}x^{-1}yx\cdot x^{n-1}=x^{m+1}yx^{n-1}\cdot[y,x].$$

当 $n=0$ 时等式显然成立, 假设当 $n=k$ 时等式成立, 即 $(xy)^k=x^ky^k[y,x]^{\frac{k(k-1)}{2}}$, 则不断利用上述关系式得

$$\begin{aligned}(xy)^{k+1}&=xy\cdot x^ky^k[y,x]^{\frac{k(k-1)}{2}}\\&=x^2yx^{k-1}y^k[y,x]^{\frac{k(k-1)}{2}+1}\\&=x^3yx^{k-2}y^k[y,x]^{\frac{k(k-1)}{2}+2}\\&=\cdots\\&=x^{k+1}yx^0y^k[y,x]^{\frac{k(k-1)}{2}+k}\\&=x^{k+1}y^{k+1}[y,x]^{\frac{(k+1)k}{2}},\end{aligned}$$

故当 $n=k+1$ 时等式成立, 由归纳法可知对任意 $n\in\mathbb{N}$, 有 $(xy)^n=x^ny^n[y,x]^{\frac{n(n-1)}{2}}$. □

1.3 同态与同构

1. 设 G 为有限群, $\varphi(x)=x^3$, $x\in G$ 是 G 的一个自同态映射. 证明: 若 $3\nmid|G|$, 则 G 为交换群.

证明: 因 $\varphi(x)=x^3$ 为同态映射, 故对任意 $x,y\in G$, 有 $(xy)^3=x^3y^3$, 也即 $yxyx=x^2y^2$.

先证对于任意 $x\in G$, 都有 $x^2\in Z(G)$. 为此, 考虑换位子 $x^2yx^{-2}y^{-1}$,

因为

$$\begin{aligned}
\left(x^2yx^{-2}y^{-1}\right)^3 &= \left[(x^2yx^{-2})y^{-1}(x^2yx^{-2})y^{-1}\right]x^2yx^{-2}y^{-1}\\
&= y^{-2}\cdot x^2yx^{-2}\cdot x^2yx^{-2}\cdot x^2yx^{-2}y^{-1}\\
&= y^{-2}x^2y^3x^{-2}y^{-1}\\
&= y^{-2}x^{-1}(x^3y^3)x^{-2}y^{-1}\\
&= y^{-2}x^{-1}(xyxyxy)x^{-2}y^{-1}\\
&= y^{-1}(xyxy)x^{-2}y^{-1}\\
&= y^{-1}(y^2x^2)x^{-2}y^{-1}\\
&= 1,
\end{aligned}$$

且 $3\nmid |G|$, 故 $x^2yx^{-2}y^{-1}=1$, 因此 $x^2\in Z(G)$.

于是对任意 $x,y\in G$, 有

$$x^3y^3=(xy)^3=xyxyxy=x(yx)^2y=(yx)^2xy=yxyx^2y=x^2yxy^2,$$

故 $xy=yx$, 从而 G 为交换群. □

2. 设 $\varphi\in\mathrm{Aut}(G)$, $a^{-1}\varphi(a)\in Z(G)$, $a\in G$. 证明: 对任意的 $b\in G'$, 有 $\varphi(b)=b$.

证明: 先证明对任意的 $x,y\in G$, 都有 $[\varphi(x),\varphi(y)]=[x,y]$. 由于对任意 $a\in G$, 都有 $a^{-1}\varphi(a)\in Z(G)$, 故

$$\begin{aligned}
[\varphi(x),\varphi(y)] &= \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)\\
&= \varphi(x)^{-1}\varphi(y)^{-1}\cdot x\cdot x^{-1}\varphi(x)\varphi(y)\\
&= x^{-1}\varphi(x)\cdot\varphi(x)^{-1}\varphi(y)^{-1}x\varphi(y)\\
&= x^{-1}\varphi(y)^{-1}x\varphi(y)\\
&= x^{-1}\varphi(y)^{-1}xy\cdot y^{-1}\varphi(y)\\
&= x^{-1}\cdot y^{-1}\varphi(y)\cdot\varphi(y)^{-1}xy\\
&= x^{-1}y^{-1}xy\\
&= [x,y].
\end{aligned}$$

对于任意的 $b \in G'$, 可将其表为

$$b = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n],$$

故

$$\begin{aligned}\varphi(b) &= \varphi([a_1, b_1]) \cdots \varphi([a_n, b_n]) \\ &= [\varphi(a_1), \varphi(b_1)] \cdots [\varphi(a_n), \varphi(b_n)] \\ &= [a_1, b_1] \cdots [a_n, b_n] = b.\end{aligned}$$

□

3. 设 $G = \langle a \rangle$ 是 30 阶的循环群, $\mathbb{Z}$ 为整数加群. 定义 $\pi(n) = a^n$, 则 π 是 $\mathbb{Z}$ 到 G 的同态映射. 确定 (i) $\ker \pi$; (ii) 找出与子群 $\langle 30 \rangle \leq \langle 15 \rangle \leq \langle 5 \rangle \leq \mathbb{Z}$ 对应的 G 的子群.

解: (i) $\ker \pi = \{n \in \mathbb{Z} \mid a^n = e\} = 30\mathbb{Z}$.

(ii) 相对应的子群分别为 $e \leq \langle a^{15} \rangle \leq \langle a^5 \rangle \leq \langle a \rangle$. □

4. 设 G 为群, $H_1 \lhd G$, $H_2 \lhd G$. 如果 $H_1 \cong H_2$, 是否 $G/H_1 \cong G/H_2$?

证明: 不一定, 例如取 $G = \mathbb{Z}$, $H_1 = 2\mathbb{Z}$, $H_2 = 3\mathbb{Z}$, 则 $H_1 \cong H_2$, 但是 $G/H_1 \ncong G/H_2$. □

5. 设 G 为群, $G' < H \leq G$, 证明: $H \trianglelefteq G$.

证明: 对任意 $g \in G$ 和 $h \in H$, 有 $ghg^{-1} = ghg^{-1}h^{-1}h \in H$, 故 $H \trianglelefteq G$. □

6. 设 $\mathbb{Q}$ 是有理数加群, $\mathbb{Z}$ 是整数加群, 证明:

(i) 对于 $\mathbb{Q}$ 的每一个非零数 k, $q \mapsto kq$ 是 $\mathbb{Q}$ 到 $\mathbb{Q}$ 的自同构;

(ii) $\mathbb{Q}$ 没有有限指数的真子群, 由此得 $\mathbb{Q}/\mathbb{Z}$ 没有有限指数的真子群;

(iii) $\mathbb{Q}$ 没有极大子群.

证明: (i) trivial.

(ii) 设 N 为 $\mathbb{Q}$ 的有限指数的真子群且 $|\mathbb{Q} : N| = n$, 考虑商群 $\mathbb{Q}/N$, 对于任意 $q \in \mathbb{Q}$, 有 $n(q + N) = nq + N = N$, 故 $nq \in N$. 那么对任意 $q \in \mathbb{Q}$, 有 $\frac{q}{n} \in \mathbb{Q}$, 从而 $n\frac{q}{n} = q \in N$, 因此 $N = \mathbb{Q}$, 矛盾.

假设 $N \le \mathbb{Q}/\mathbb{Z}$ 为有限指数的真子群, 考虑两个同态

$$\varphi : \mathbb{Q}/\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})/N, \quad \ker\varphi = N$$

和

$$\sigma : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}, \quad \ker\sigma = \mathbb{Z}.$$

则 $\varphi\circ\sigma : \mathbb{Q} \to (\mathbb{Q}/\mathbb{Z})/N$ 为同态且 $\ker(\varphi\circ\sigma) = \sigma^{-1}(\varphi^{-1}(N)) = \sigma^{-1}(N)$, 由对应定理知 $\ker(\varphi\circ\sigma)$ 为 $\mathbb{Q}$ 的指数有限的真子群, 矛盾.

(iii) 设 H 为 $\mathbb{Q}$ 的任意真子群, 取 $x \in G \setminus H$, $y \in H$ 且 $y \ne 0$. 可以记 $\frac{y}{x} = \frac{a}{b}$, 其中 $a, b \in \mathbb{Z}$ 且 $a \ne 0$. 记 $H' = H + \langle x\rangle$, 则 $H \le H' \le G$.

由 $x \notin H$ 但 $x \in H'$ 知 H 为 H' 的真子群.

我们有 $\frac{x}{a} \notin H' = H + \langle x\rangle$, 事实上, 如若不然, 则可设 $\frac{x}{a} = h + nx$ $(h \in H, n \in \mathbb{Z})$, 则 $x = ah + nax = ah + nby \in H$, 矛盾. 故 H' 为 $\mathbb{Q}$ 的真子群.

综上即知 $H < H' < \mathbb{Q}$, 故 $\mathbb{Q}$ 没有极大子群. □

定理 1 设 G 为群, G' 为 G 的导群 (换位子群), 则 $G' \trianglelefteq G$.

证法一: 对于任意 $u \in G'$ 和任意 $g \in G$, 有

$$gug^{-1} = gug^{-1}u^{-1}u = [g^{-1}, u^{-1}]u \in G',$$

故 $G' \trianglelefteq G$. □

证法二: 换位子群 G' 的每个元素都形如

$$[a_1, b_1][a_2, b_2]\cdots[a_n, b_n].$$

只需证对任意的换位子 $[a, b]$ 都有 $g[a, b]g^{-1} \in G'$ 即可, 事实上, 由于

$$g[a_1, b_1][a_2, b_2]\cdots[a_n, b_n]g^{-1} = (g[a_1, b_1]g^{-1})(g[a_2, b_2]g^{-1})\cdots(g[a_n, b_n]g^{-1}),$$

故当 $g[a_i, b_i]g^{-1} \in G'$ $(1 \le i \le n)$ 时, 有

$$g[a_1, b_1][a_2, b_2]\cdots[a_n, b_n]g^{-1} \in G'.$$

下证 $g[a,b]g^{-1} \in G'$. 设 $\phi: G \to G$ 为任意同态, 则有

$$\phi([a,b]) = \phi(a^{-1}b^{-1}ab) = \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b) = [\phi(a), \phi(b)].$$

特别地, 我们取同态 $\phi(x) = gxg^{-1}$, 则由上述等式知

$$g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}] \in G'.$$

即证所需. □

1.4　直积与半直积

1.5　群作用

1. 证明: 阶为不小于 $r!$ 的有限单群没有指数为 r 的子群.

证明: 假设 G 为有限单群, $|G| \geq r!$, H 为 G 的指数为 r 的子群. G 在陪集空间 G/H 上有自然作用, 由命题 1.5.1 知此作用对应一个从 G 到 $\Sigma_{G/H}$ 的同态: $\varphi: G \to \Sigma_{G/H} = S_r$. 由同态基本定理知 $G/\ker\varphi \cong \operatorname{Im}\varphi \leq S_r$. 由于 $\ker\phi \triangleleft G$ 且 G 为单群, 故 $\ker\varphi = \{e\}$, $G \cong \operatorname{Im}\varphi$, 从而

$$r! \leq |G| = |\operatorname{Im}\varphi| \leq |S_r| = r!,$$

所以 $G \cong S_r$, 而 S_r 不是单群 (A_r 为 S_r 的正规子群, 因任取 $\pi \in S_r, \sigma \in A_r$, $\pi\sigma\pi^{-1}$ 仍为偶置换, 故 $\pi\sigma\pi^{-1} \in A_r$), 这与 G 为单群相矛盾. □

2. 已知 X 为传递的 G 集合, 证明: 群 G 双传递地作用在集合 X 上当且仅当 G_x 传递地作用在集 $X - \{x\}$, $x \in X$ 上.

证明: $(\Rightarrow)$ 任取 $y, z \in X - \{x\}$, 因 G 双传递地作用在 X 上, 故存在 $g \in G$, 使得 $gx = x$, $gy = z$, 由 $gx = x$ 知 $g \in G_x$, 再由 y, z 的任意性知 G_x 传递地作用在 $X - \{x\}$ 上.

$(\Leftarrow)$ 任取 $(x_1, x_2), (y_1, y_2) \in X \times X$ 且 $x_1 \neq x_2$, $y_1 \neq y_2$, 往证存在 $g \in G$, 使得 $gx_1 = y_1$ 且 $gx_2 = y_2$. 因 G 在 X 上传递, 故存在 $h \in G$, 使得

$hx_1 = y_1$, 令 $hx_2 = x_2' \neq y_1$, 由 G_{y_1} 在 $X - \{y_1\}$ 上传递知存在 $k \in G_{y_1}$, 使得 $kx_2' = y_2$. 令 $g = kh$, 则 $gx_1 = khx_1 = ky_1 = y_1$, $gx_2 = khx_2 = kx_2' = y_2$. □

3. 证明: 对群 G 中任意的元素 g, x, $C_G(gxg^{-1}) = gC_G(x)g^{-1}$ 成立.

证明: 对任意 $h = gyg^{-1} \in gC_G(x)g^{-1}$, 其中 $y \in C_G(x)$, 有

$$h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1} = gyxy^{-1}g^{-1} = gxg^{-1},$$

故 $h \in C_G(gxg^{-1})$, 从而 $gC_G(x)g^{-1} \subset C_G(gxg^{-1})$.

在上式中用 $g^{-1}xg$ 替换 x, 得 $gC_G(g^{-1}xg)g^{-1} \subset C_G(x)$, 故 $C_G(g^{-1}xg) \subset g^{-1}C_G(x)g$, 再用 g^{-1} 替换 g, 即得 $C_G(gxg^{-1}) \subset gC_G(x)g^{-1}$, 因此

$$C_G(gxg^{-1}) = gC_G(x)g^{-1}.$$ □

4. 设 G 为有限群, 证明: $|\{(a,b) \in G \times G \mid ab = ba\}| = r|G|$, 其中 r 为 G 的共轭类的个数.

证明: 设 $C_1, \cdots, C_r$ 为 G 的共轭类. 因对任意 $x, y \in C_i$, 有 $|C_G(x)| = |C_G(y)|$, 故

$$\begin{aligned} |\{(a,b) \in G \times G \mid ab = ba\}| &= \sum_{a \in G} |C_G(a)| = \sum_{i=1}^{r} \sum_{a \in C_i} |C_G(a)| \\ &= \sum_{i=1}^{r} |C_i| \cdot |C_G(a)| = \sum_{i=1}^{r} |G| = r|G|. \end{aligned}$$ □

1.6 Sylow 定理

1. 证明: p^2 阶群 G 是交换群, 其中 p 是素数.

证法一: 若 G 中存在 p^2 阶元, 则 G 显然为循环群, 从而为交换群; 若 G 中不存在 p^2 阶元, 则 G 中任意非单位元的阶都为 p.

任取 $x \in G$ 且 $|x| = p$, 因为 $|G : \langle x \rangle| = p$ 为整除 $|G|$ 的最小素数, 故 $\langle x \rangle \lhd G$. 任取 $y \in G$ 且 $|y| = p$, 由 $\langle x \rangle \lhd G$ 知 $yxy^{-1} \in \langle x \rangle$, 故 $yxy^{-1} = x^r$,

其中 $1 \le r \le p-1$, 从而

$$\begin{aligned} y^i x y^{-i} &= y^{i-1}(yxy^{-1})y^{-i+1} = y^{i-1}x^r y^{-i+1} \\ &= y^{i-2}(yx^r y^{-1})y^{-i+2} = y^{i-2}x^{r^2}y^{-i+2} \\ &= \cdots = x^{r^i}. \end{aligned}$$

特别地, $y^{p-1}xy^{1-p} = x^{r^{p-1}}$, 由 Fermat 定理知 $r^{p-1} \equiv 1 \pmod p$, 故 $y^{p-1}xy^{1-p} = x$. 又由于 $|y| = p$, 故 $y^{-1}xy = x \Rightarrow xy = yx$, 由此可知 x 的中心化子 $Z(x) = G \Leftrightarrow x \in Z(G)$, 因此 $Z(G) = G$, 这就说明 G 为交换群. □

注 参考链接: MSE.

上述证明过程用到一个引理:

引理 1 设 G 为有限群, p 为整除 $|G|$ 的最小素数, 若 H 为 G 的指数为 p 的子群, 则 $H \lhd G$.[链接]

证明: 考虑 G 在 H 的陪集空间 $\{xH \mid x \in G\}$ 上的作用:

$$(g, xH) \longmapsto gxH.$$

此作用对应同态 $\phi : G \to S_p$, $g \mapsto \sigma_g$, 其中 $\sigma_g(xH) = gxH$.

记 $K = \ker\phi$, 则 $K \trianglelefteq G$. 若 $g \in K$, 则 $\sigma_g = \mathrm{id}$, 故 $\sigma_g(H) = gH = H \Rightarrow g \in H$, 因此 $K \le H$. 由群同态定理知 G/K 同构于 S_p 的某个子群, 故 $|G/K|$ 整除 $p!$. 又 $|G/K| \mid |G|$ 且 p 为整除 $|G|$ 的最小素数, 故 $|G/K| = p$. 从而

$$p = |G/K| = [G:K] = [G:H][H:K] = p[H:K] \Rightarrow H = K.$$

所以 $H \lhd G$. □

证法二: 证明 p-群必有非平凡的中心. 利用共轭类方程:

$$|G| = |Z(G)| + \sum_x |G : Z(x)|,$$

其中 x 取遍非中心元素的共轭类的代表. 首先, 当 $x \notin Z(G)$ 时, $Z(x)$ 为 G 的真子群, 故 $p \mid |G : Z(x)|$, 从而 $p \mid \sum_x |G : Z(x)|$, 又因 $p \mid |G|$, 故 $p \mid |Z(G)|$. 显然 $Z(G)$ 非空 ($e \in Z(G)$), 因此 p-群的中心是非平凡的.

特别地, 在 p^2 阶群中, $Z(G)$ 非平凡可分为两种可能: $|Z(G)| = p$ 或 $|Z(G)| = p^2$. 若 $|Z(G)| = p$, 则 $|G : Z(G)| = p$, 从而 $G/Z(G)$ 为循环群, 那么 G 为交换群; 若 $|Z(G)| = p^2$, 则 $Z(G) = G$, 从而 G 为交换群. □

第 2 章 环与域

2.1 基本概念和例子

1. 略

证明: 在矩阵环中寻求反例即可. □

2. 设 R 是以 n 为模的剩余类环, 证明:

(i) 若 $n = a^k b$, 则 $[ab]$ 是 R 的幂零元;

(ii) 设 m 为整数, 则 $[m] \in R$ 是幂零元当且仅当 n 的每个素因子也是 m 的一个素因子. 特别地, 确定 $\mathbb{Z}/(72)$ 的幂零元.

证明: (i) 若 $n = a^k b$, 则 $([ab])^k = [a^k b^k] = [b^{k-1} n] = [0]$, 故 $[ab]$ 为幂零元.

(ii)($\Rightarrow$) 因 $[m] \in R$ 为幂零元, 故存在正整数 k 使得 $[m]^k = [m^k] = [0]$, 那么有 $n \mid m^k$. 若素数 $p \mid n$, 则 $p \mid m^k \Rightarrow p \mid m$.

($\Leftarrow$)n 有素数分解 $n = p_1^{k_1} \cdots p_s^{k_s}$, 由条件知 $p_i \mid m (1 \le i \le s)$, 故 $p_1 \cdots p_s \mid m$. 取 $K = \max_{1 \le i \le s}\{k_i\}$, 则 $n = p_1^{k_1} \cdots p_s^{k_s} \mid p_1^K \cdots p_s^K \mid m^k$, 所以 $[m]^k = [m^k] = [0]$, 这说明 $[m]$ 为幂零元. □

3. 证明: $\mathbb{Z}/(k)$ 有幂零元当且仅当存在素数 p 使得 $p^2 \mid k$.

4. 设 a 是环 R 中的元, 若 $a^2 = a$, 则 a 称为幂等元. 若 R 的每个非零元为幂等元, 则称 R 为布尔环. 证明: 布尔环是交换环. 进一步地, 若布尔环是整环, 则它必为二元环.

证明: 对任意 $a \in R$, 有

$$2a = (a+a)^2 = 4a^2 = 4a \Rightarrow 2a = 0.$$

又对任意 $x, y \in R$, 有

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y \Rightarrow xy + yx = 0.$$

故 $xy = xy + (xy + yx) = 2xy + yx = yx$, 也即布尔环为交换环.

若布尔环 R 为整环, 则 R 无零因子. 对于任意的 $a \in R$ 且 $a \neq 0$, 有 $a^2 - a = a(a-1) = 0$, 故 $a = 1$, 也即说明 R 为二元环. □

5. 设 $\mathcal{F}(\mathbb{R})$ 是所有函数 $f : \mathbb{R} \to \mathbb{R}$ 组成的集, 对任意的 $f, g \in \mathcal{F}(\mathbb{R})$, $a \in \mathbb{R}$, 规定: $(f+g)(a) = f(a) + g(a)$, $(fg)(a) = f(a)g(a)$. 证明: $\mathcal{F}(\mathbb{R})$ 是交换幺环且含无限个元 f 使得 $f^2 = f$.

证明: 容易验证 $\mathcal{F}(\mathbb{R})$ 为交换幺环, 取 $f_\alpha = \begin{cases} 1, & x = \alpha \\ 0, & x \neq \alpha, \end{cases}$ 则 $(f_\alpha)_{\alpha \in \mathbb{R}} \subset \mathcal{F}(\mathbb{R})$ 且 $f^2 = f$. □

6. 设 X 是非空集, $\mathcal{P}(X)$ 是 X 的所有子集组成的集. 对于 $A, B \in \mathcal{P}(X)$, 规定 $A + B = A \triangle B$, $AB = A \cap B$. 证明:

(i) $\mathcal{P}(X)$ 为交换幺环且为布尔环;

(ii) $\mathcal{P}(X)$ 恰有一个单位;

(iii) 若 $Y \subset X$, 则 $\mathcal{P}(Y)$ 的单位不同于 $\mathcal{P}(X)$ 的单位.

证明: (i) $\mathcal{P}(X)$ 关于加法成加群:

- $(A+B)+C = (A \triangle B) \triangle C = A \triangle (B \triangle C) = A + (B + C)$
- $A + \emptyset = \emptyset + A = A$
- $A + A = A \triangle A = \emptyset$

$\mathcal{P}(X)$ 关于乘法成半群:

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

$\mathcal{P}(X)$ 满足分配律:

$$(A+B)C=(A\triangle B)\cap C=(A\cap C)\triangle(B\cap C)=AC+BC,$$

$$C(A+B)=CA+CB.$$

综上知 $\mathcal{P}(X)$ 为环, 又 $AB=A\cap B=B\cap A=BA$, 且 $AX=XA=A$, 故 $\mathcal{P}(X)$ 为交换幺环. 又因 $A^2=A\cap A=A$, 故 $\mathcal{P}(X)$ 为布尔环.

(ii) 由 (i) 知 $\mathcal{P}(X)$ 的单位元为 X. 设 $A\in\mathcal{P}(X)$ 为单位, 则存在 $B\in\mathcal{P}(X)$ 使得 $AB=A\cap B=X\Rightarrow A=X$, 即 $\mathcal{P}(X)$ 中的单位只有 X.

(iii) $\mathcal{P}(Y)$ 中的单位为 Y, 显然不同于 $\mathcal{P}(X)$ 的单位 X. □

7. 设 R 是有单位元 1 的交换环, x 是 R 的幂零元, 证明:

(i) 对所有的 $r\in R$, rx 是幂零元;

(ii) $1+x$ 是 R 的单位;

(iii) 一个幂零元与一个单位的和是一个单位.

证明: (i) 因为 x 是 R 的幂零元, 所以存在正整数 n 使得 $x^n=0$, 那么 $(rx)^n=r^nx^n=0$, 从而 rx 是幂零元;

(ii) $(1+x)(1-x+x^2-\cdots+(-1)^{n-1}x^{n-1})=1+(-1)^{n-1}x^n=1$, 故 $1+x$ 是 R 的单位;

(iii) 设 x 为幂零元且 y 为单位, 则 $y+x=y(1+y^{-1}x)$ 仍为单位. □

8. 设 R 是交换幺环, 对任意的 $a,b\in R$, 规定 $a\circ b=a+b-ab$. 证明: R 是域当且仅当 $S=\{r\in R\mid r\neq 1\}$ 关于 $\circ$ 运算是交换群.

证明: 显然对任意的 $a,b\in S$ 都有 $a\circ b=b\circ a$ 且 $a\circ 0=0\circ a=a$, 所以若要使得 S 为交换群, 只需其中任意元素 $a\in S$ 关于 $\circ$ 运算皆有逆元即可.

($\Leftarrow$) 任取 R 中的非零元 a, 有 $a+1\neq 1$, 故 $a+1\in S$. 而 S 关于 $\circ$ 运算为交换群, 故存在 $b\in S$ 使得 $(a+1)\circ b=0$, 即 $a+1+b-(a+1)b=0$, 整理得 $a(b-1)=1$, 也即 $a^{-1}=b-1$. 因此 R 是域.

(⇒) 任取元素 $a \in S$, 由 $a \neq 1$ 知 $a-1 \neq 0$, 故 $a-1$ 在 R 中可逆, 令 $b=(a-1)^{-1}a$, 则

$$\begin{aligned} a \circ b &= a+(a-1)^{-1}a-a(a-1)^{-1}a \\ &= a-(a-1)(a-1)^{-1}a \\ &= 0. \end{aligned}$$

这说明 b 是 a 在 S 中关于 $\circ$ 运算的逆元, 故 S 为交换群. □

9. 设 R 是环, 证明:

(i) u 是 R 的单位当且仅当 u 既是左逆元也是右逆元;

(ii) 若 u 有一个右逆元, 则 u 不是右零因子;

(iii) 若 u 有多于一个的右逆元, 则 u 必为左零因子;

(iv) 若 u 有多于一个的右逆元, 则 u 必有无限多个右逆元.

证明: (i) (⇒) 若 u 是 R 的单位, 则存在 $v \in R$, 使得 $uv=vu=1$, 故 u 既是左逆元也是右逆元.

(⇐) 设 u 既是左逆元也是右逆元, 则存在 $v, w \in R$, 使得 $uv=wu=1$, 从而

$$v=1v=(wu)v=w(uv)=w1=w,$$

因此 u 为单位.

(ii) 设 u 有右逆元 v, 则 $uv=1$. 假设 u 为右零因子, 则存在 $w \in R$, $w \neq 0$, 使得 $wu=0$, 则 $(wu)v=w(uv)=w=0$, 矛盾.

(iii) 设 $v, w \in R$ 都为 u 的右逆元, 则

$$uv=uw=1 \Rightarrow u(v-w)=0.$$

注意 $u \neq 0$ 且 $v-w \neq 0$, 故 u 为左零因子.

(iv) 反证法, 设 u 只有有限个右逆元, 记为 $u_1, u_2, \cdots, u_m$ $(m \geq 2)$. 因

$$u(1-u_iu+u_1)=u-u+uu_1=1, \quad 1 \leq i \leq m$$

且当 $i \neq j$ 时, $1-u_iu+u_1 \neq 1-u_ju+u_1$ (假设相等, 则 $(u_i-u_j)u=0$, 故 $(u_i-u_j)uu_1=u_i-u_j=0$, 矛盾)，故 $1-u_iu+u_1$, $1 \leq i \leq m$ 是 u 的全部右逆元, 因此必存在 k, 使得 $u_1=1-u_ku+u_1 \Rightarrow u_ku=1$. 因为 $m \geq 2$, 故可取 $s \neq k$, 用 u_s 右乘 $u_ku=1$, 得 $u_k=u_s$, 矛盾, 故 u 有无限多个右逆元. □

2.2　理想与同态

1. 设 R 为交换环, 证明: $\mathcal{M}_{nm}(R) \cong \mathcal{M}_n(\mathcal{M}_m(R))$.

证明: 定义映射 $\varphi: \mathcal{M}_{nm}(R) \to \mathcal{M}_n(\mathcal{M}_m(R))$,

$$\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1,nm} \\ r_{21} & r_{22} & \cdots & r_{2,nm} \\ \vdots & \vdots & & \vdots \\ r_{nm,1} & r_{nm,2} & \cdots & r_{nm,nm} \end{pmatrix} \mapsto \begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ \vdots & \vdots & & \vdots \\ M_{n1} & M_{n2} & \cdots & M_{nn} \end{pmatrix},$$

其中 $r_{ij} \in R$, $1 \leq i,j \leq nm$ 且

$$M_{ij} = \begin{pmatrix} r_{(i-1)m+1,(j-1)m+1} & \cdots & r_{(i-1)m+1,jm} \\ \vdots & & \vdots \\ r_{im,(j-1)m+1} & \cdots & r_{im,jm} \end{pmatrix}.$$

再验证 φ 为双射和同态即可. □

2. 设 I,J 是交换幺环 R 的理想, 证明: 若 $I+J=R$, 则 $IJ=I\cap J$.

证明: 由理想的积的定义可知 $IJ \subset I\cap J$ 是显然的, 故只需证 $I\cap J \subset IJ$. 因 $I+J=R$ 且 R 为交换幺环, 故存在 $a \in I$ 和 $b \in J$, 使得 $a+b=1$. 那么对任意 $k \in I\cap J$, 有 $k=k(a+b)=ak+kb \in I+J$. 因此 $IJ=I\cap J$. □

3. 令 $u=\sqrt{2}+\sqrt{3}$, 找一个 $\mathbb{Q}[x]$ 理想 I 使得 $\mathbb{Q}[u] \cong \mathbb{Q}[x]/I$.

解: 考虑满同态映射 $\varphi:\mathbb{Q}[x]\to\mathbb{Q}[u]$, $\sum a_ix^i\mapsto\sum a_iu^i$. 故 $\ker\varphi=\{\sum a_ix^i\mid\sum a_iu^i=0\}$. 由 $u=\sqrt{2}+\sqrt{3}$ 可知 u 满足有理系数方程 $u^4-10u^2+1=0$, 故 $x^4-10x^2+1\in\ker\varphi$. 因 $\ker\varphi$ 为 $\mathbb{Q}[x]$ 的理想且 $\mathbb{Q}[x]$ 为主理想环, 故 $\ker\varphi=(x^4-10x^2+1)$, 由环同态定理得 $\mathbb{Q}[x]/(x^4-10x^2+1)\cong\mathbb{Q}[u]$. □

注 设 F 为域, $F[x]$ 为 F 上的多项式环, 则 $F[x]$ 为主理想环. 事实上, 任取 $F[x]$ 的理想 I, 若 $I=\{0\}$, 则 I 显然为主理想; 若 $I\neq\{0\}$, 设 $d(x)$ 为 I 中次数最低的非零多项式, 对于 I 中任意多项式 $a(x)$, 有 $a(x)=q(x)d(x)+r(x)$, 其中 $\deg r(x)<\deg d(x)$. 因 $a(x)\in I$, $q(x)d(x)\in I$, 故 $r(x)=a(x)-q(x)d(x)\in I$, 而 $\deg r(x)<\deg d(x)$, 因此必有 $r(x)=0$, 从而 $a(x)=q(x)d(x)\Rightarrow I=(d(x))$.

上述结论表明 $\mathbb{Q}[x]$、$\mathbb{R}[x]$、$\mathbb{C}[x]$ 都是主理想环, 但是 $\mathbb{Z}[x]$ 不是主理想环, 因为 $\mathbb{Z}[x]$ 上的理想 $(2,x)$ 不是主理想.

4. 设 I 是 R 的理想, 证明: $R[x]/I[x]\cong(R/I)[x]$.

证明: 考虑映射 $\varphi:R[x]\to(R/I)[x]$, $a_0+\cdots a_nx^n\mapsto(a_0+I)+\cdots+(a_n+I)x^n$. 显然 φ 为满射, 又

$$\begin{aligned}&\varphi(a_0+b_0+\cdots+(a_n+b_n)x^n)\\=&(a_0+b_0+I)+\cdots+(a_n+b_n+I)x^n\\=&(a_0+I)+\cdots+(a_n+I)x^n+(b_0+I)+\cdots+(b_n+I)x^n\\=&\varphi(a_0+\cdots+a_nx^n)+\varphi(b_0+\cdots+b_nx^n),\end{aligned}$$

故 φ 为同态. 然后 φ 的核为

$$\begin{aligned}\ker\varphi&=\{a_0+\cdots+a_nx^n\mid(a_0+I)+\cdots+(a_n+I)x^n=I+\cdots+Ix^n\}\\&=\{a_0+\cdots+a_nx^n\mid a_0,a_1,\cdots,a_n\in I\}\\&=I[x].\end{aligned}$$

因此 $R[x]/I[x]\cong(R/I)[x]$. □

5. 设 p 为素数, 证明: $(p)/(p^m)$ 为 $\mathbb{Z}/(p^m)$ 的幂零理想.

证明: 先证 $(p)/(p^m)$ 为 $\mathbb{Z}/(p^m)$ 的理想, 对任意 $a \in (p)/(p^m)$ 和 $r \in \mathbb{Z}/(p^m)$, 可将其分别表为 $a = kp + (p^m)$, $r = z + (p^m)$, 于是

$$ar = (kp + (p^m))(z + (p^m)) = kzp + (p^m) \in (p)/(p^m),$$

同理可证 $ra \in (p)/(p^m)$, 因此 $(p)/(p^m)$ 为 $\mathbb{Z}/(p^m)$ 的理想.

再证 $(p)/(p^m)$ 为幂零理想 (若理想 I 满足 $I^n = \{\sum a_1a_2\cdots a_n \mid a_i \in I\} = 0$, 则称 I 为幂零理想), 因为 $(p)/(p^m)$ 中的任意 m 个元素的乘积

$$(k_1p + (p^m))(k_2p + (p^m))\cdots(k_mp + (p^m)) = k_1k_2\cdots k_mp^m + (p^m) = (p^m),$$

所以 $\big((p)/(p^m)\big)^m = (p^m)$, 即证 $(p)/(p^m)$ 为幂零理想. □

6. 证明: (i) $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$; (ii) $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/(2)$.

证明: (i) 考虑映射 $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$, $a_0 + \cdots a_nx^n \mapsto a_0$. 容易验证 φ 为满同态, 且

$$\begin{aligned}\ker\varphi &= \{a_0 + \cdots + a_nx^n \mid a_0 = 0\}\\ &= \{a_1x + \cdots a_nx^n\}\\ &= \{(a_1 + \cdots a_nx^{n-1})x\} = (x).\end{aligned}$$

故 $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

也可以定义映射 $\phi : \mathbb{Z} \to \mathbb{Z}[x]/(x)$, $n \mapsto n + (x)$, 证明 ϕ 为同构映射.

(ii) 考虑映射 $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/(2)$, $a_0 + \cdots a_nx^n \mapsto \begin{cases}\bar{0} & \text{若 } a_0 \text{ 为偶数}\\ \bar{1} & \text{若 } a_0 \text{ 为奇数,}\end{cases}$ 容易验证 φ 为满同态映射, 且 $\ker\varphi = \{a_0 + \cdots + a_nx^n \mid a_0 \text{ 为偶数}\} = (2,x)$, 因此 $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/(2)$.

也可以定义映射 $\phi : \mathbb{Z} \to \mathbb{Z}[x]/(2,x)$, $n \mapsto n + (2,x)$. 然后验证 ϕ 为满同态且 $\ker\phi = 2\mathbb{Z}$. □

2.3　极大理想和素理想

2.4　整环里的因子分解

1. 设 F 是域, 令 $R = \{a_0 + a_2x^2 + \cdots + a_nx^n \mid a_i \in F\} \subset F[x]$. 证明: x^5 和 x^6 在 R 里没有最大公因子.

证明: x^5 和 x^6 在 R 中的公因子有 $1, x^2, x^3$ (注意 $x \notin R$, 故在 R 中 x^4 不是 x^5 的因子, x^5 不是 x^6 的因子). 若 x^5 和 x^6 在 R 中有最大公因子, 其必为 x^3, 但在 R 中 x^2 不是 x^3 的因子, 故 x^5 和 x^6 在 R 中没有最大公因子. □

2. 设 R 是唯一分解环, F 是 R 的商域, $\alpha \in F$, 证明: α 可以写为 $\frac{a}{b}$ 的形式, 其中 $a, b \in R$ 且 $(a, b) = 1$.

证明: 由于 F 是 R 的商域, 故对任意 $\alpha \in F$, 存在 $a_1, b_1 \in R$, 使得 $\alpha = \frac{a_1}{b_1}$. 因 R 是唯一分解环, 故 (a_1, b_1) 存在, 令 $a = \frac{a_1}{(a_1,b_1)}$, $b = \frac{b_1}{(a_1,b_1)}$, 则 $\alpha = \frac{a}{b}$ 且 $(a, b) = 1$. □

3. 设 R 是唯一分解环, F 是 R 的商域, $\alpha \in F$, $f(x) \in R[x]$ 是首项系数为 1 的多项式. 证明: 若 $f(\alpha) = 0$, 则 $\alpha \in R$.

证明: 设 $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in R[x]$, 则

$$f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0.$$

由上一题知存在 $a, b \in R$ 且 $(a, b) = 1$, 使得 $\alpha = \frac{a}{b}$, 故

$$\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{a}{b}\right) + a_n = 0,$$

整理得

$$a^n = -(a_1a^{n-1} + \cdots + a_{n-1}ab^{n-2} + a_nb^{n-1})b,$$

故 $b \mid a^n$, 又 $(a, b) = 1$, 由命题 2.4.6(iv) 知 $b \mid a^{n-1}$, 依次递推可得 $b \mid a$, 从而 $\alpha = \frac{a}{b} \in R$. □

4. 在 $\mathbb{Z}[x]$ 里, (x^2+1, x^5+x^3+1) 是否为一个主理想? 在 $\mathbb{Q}[x]$ 里, 它是否为一个主理想? 等于怎样一个主理想?

证明: 由定义知

$$(x^2+1, x^5+x^3+1) = \{(x^2+1)p(x) + (x^5+x^3+1)q(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}.$$

因 $(x^2+1)(-x^3) + (x^5+x^3+1) = 1$, 故 $1 \in (x^2+1, x^5+x^3+1)$, 于是 $(x^2+1, x^5+x^3+1) = \mathbb{Z}[x]$.

同理在 $\mathbb{Q}$ 中, (x^2+1, x^5+x^3+1) 为主理想且等于 $\mathbb{Q}[x]$. $\square$

5. 设 R 是主理想环, $R \subset S$, S 是整环, $a, b \in R$. 证明: 若 d 是 a, b 在 R 中的最大公因子, 则 d 也是 a, b 在 S 中的最大公因子.

证明: 用 $(\cdot)_R$ 和 $(\cdot)_S$ 分别表示相应集合在 R 和 S 中生成的理想. 因在 R 中, $d \mid a$ 且 $d \mid b$, 故 $a \in (d)_R$ 且 $b \in (d)_R$, 从而 $(a,b)_R \in (d)_R$. 由于 R 为主理想环, 故设 $(a,b)_R = (e)_R$, 则在 R 中 $e \mid a$ 且 $e \mid b$, 故在 R 中 $e \mid d$, 所以 $(d)_R \subset (e)_R = (a,b)_R$, 因此 $(d)_R = (a,b)_R$.

任取 a, b 在 S 中的因子 c, 则 $(a,b)_S \subset (c)_S$, 显然 $(a,b)_R \subset (a,b)_S$, 故 $(d)_R \subset (c)_S \Rightarrow d \in (c)_S$, 所以在 S 中 $c \mid d$, 故 d 是 a, b 在 S 中的最大公因子. $\square$

6. 设 I 是主理想环, $a, b \in I$, 证明 $(a) + (b) = I$ 当且仅当 $(a, b) = 1$.

证明: $(\Rightarrow)$ 若 $(a) + (b) = I$, 则存在 $u, v \in I$, 使得 $ua + vb = 1$. 设 $c \mid a$ 且 $c \mid b$, 则 $c \mid ua + vb$, 即 $c \mid 1$, 也即 c 为单位, 所以 $(a, b) = 1$.

$(\Leftarrow)$ 由定理 2.4.10 知存在 $u, v \in I$, 使得 $ua + vb = (a, b) = 1$, 故 $1 \in (a) + (b)$, 从而 $(a) + (b) = I$. $\square$

7. 设 F 是域, $f(x) \in F[x]$. 决定 $F[x]/(f(x))$ 的所有理想.

证明: 由环的第四同构定理知 $I/(f(x))$ 为 $F[x]/(f(x))$ 的理想当且仅当 I 为 $F[x]$ 的包含 $(f(x))$ 的理想, 而 $F[x]$ 为主理想环, 故可设 $I = (p(x))$, $p(x) \in F[x]$. 由于 $(f(x)) \subset I = (p(x))$, 故 $p(x) \mid f(x)$, 因此 $F[x]/(f(x))$ 的所有理想为 $(p(x))/(f(x))$, 其中 $p(x) \mid f(x)$. $\square$

8. 决定 $\mathbb{Z}[x]/(2,x^3+1)$ 的所有理想.

证法一: 因 $\mathbb{Z}[x]/(2,x^3+1)\cong\mathbb{Z}_2[x]/(x^3+1)$, 故我们考虑 $\mathbb{Z}_2/(x^3+1)$ 的理想. 由于 $\mathbb{Z}_2$ 为域, 故 $\mathbb{Z}_2[x]$ 为主理想环, 从而是唯一分解环, 在 $\mathbb{Z}_2[x]$ 中, x^3+1 有唯一分解 $x^3+1=(x+1)(x^2+x+1)$. 由第 13 题结论知 $\mathbb{Z}_2[x]/(x^3+1)$ 的所有理想为 $(p(x))/(x^3+1)$, 其中 $p(x)\mid(x+1)(x^2+x+1)$, 也即有四个理想

$$
\begin{aligned}
&(1)/(x^3+1)=\mathbb{Z}_2[x]/(x^3+1) && (x+1)/(x^3+1)\\
&(x^2+x+1)/(x^3+1) && ((x+1)(x^2+x+1))/(x^3+1)=0
\end{aligned}
$$

因此 $\mathbb{Z}[x]/(2,x^3+1)$ 有四个理想: $\mathbb{Z}[x]/(2,x^3+1)$, $(2,x+1)/(2,x^3+1)$, $(2,x^2+x+1)/(2,x^3+1)$ 和 (0). □

证法二: $I/(2,x^3+1)$ 为 $\mathbb{Z}[x]/(2,x^3+1)$ 的理想当且仅当 I 为 $\mathbb{Z}[x]$ 的包含 $(2,x^3+1)$ 的理想. 故需要向理想 $(2,x^3+1)$ 中添加元得到包含 $(2,x^3+1)$ 的理想, 任取 $f(x)\in\mathbb{Z}[x]$, $f(x)$ 模 x^3+1 后得到次数不超过 2 的多项式, 再将得到的多项式模 2 得到各项系数为 0 和 1 的多项式, 因此可供选择的 $f(x)$ 有: 0、1、x、x^2、$x+1$、x^2+1、x^2+x 和 x^2+x+1. 注意到

$$
\begin{aligned}
&(2,x^3+1,x)=(2,x^3+1,x^2)=(2,x^3+1,1)=(1)=\mathbb{Z}[x]\\
&(2,x^3+1,x+1)=(2,x^3+1,x^2+1)=(2,x^3+1,x^2+x)=(2,x+1)\\
&(2,x^3+1,x^2+x+1)=(2,x^2+x+1)
\end{aligned}
$$

所以 $\mathbb{Z}[x]/(2,x^3+1)$ 的理想有四个, 分别为平凡理想 $\mathbb{Z}[x]/(2,x^3+1)$、(0) 和非平凡理想 $(2,x+1)/(2,x^3+1)$、$(2,x^2+x+1)/(2,x^3+1)$. □

2.5　域的扩张

1. 设 E 是 F 的有限扩域, 证明: (i) $[E:F]=1\iff E=F$; (ii) 若 $\alpha\in E$ 是 F 上的代数元, 则 $n\mid[E:F]$ (这里 n 为 α 的次数).

证明: (i) ($\Leftarrow$) 显然. ($\Rightarrow$) 若 $[E:F]=1$, 则 E 为 F 上的一维向量空间, 故存在 $e\in E$, 使得 $E=\{fe\mid f\in F\}$, 故 $|E|=|F|$, 又 $F\subset E$, 故 $E=F$.

(ii) 因 $[E:F]=[E:F(\alpha)][F(\alpha):F]$, 且 $[F(\alpha):F]=n$, 故 $n\mid[E:F]$. □

2. 设 $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$, 求 $[E:\mathbb{Q}]$, 并给出 E 在 $\mathbb{Q}$ 上的一个基.

证明: $[E:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=4$, E 在 $\mathbb{Q}$ 上的一个基为 $1,\sqrt{2},\sqrt{3},\sqrt{6}$. □

3. 证明: $\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}(\sqrt{-1})$ 作为 $\mathbb{Q}$ 上的向量空间是同构的, 但作为域是不同构的.

证明: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{-1}):\mathbb{Q}]=2$, 维数相同的向量空间是同构的.

假设存在域同构 $\varphi:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{-1})$, 由于 $\varphi(1)=1$, 故对任意整数 n, 有 $\varphi(n)=n$, 继而对任意有理数 $\frac{n}{m}$, $n\in\mathbb{Z},m>0$, 有 $\varphi(\frac{n}{m}\cdot m)=m\varphi(\frac{n}{m})=n\Rightarrow\varphi(\frac{n}{m})=\frac{n}{m}$, 也即 φ 固定 $\mathbb{Q}$ 中元不动.

由于 φ 为同构, 故存在 $w=a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, 使得 $\varphi(w)=\sqrt{-1}$, 故

$$\begin{aligned}-1=(\sqrt{-1})^2=\varphi(w^2)&=\varphi(a^2+2b^2+2\sqrt{2}ab)\\&=\varphi(a^2)+\varphi(2b^2)+\varphi(2\sqrt{2}ab)\\&=a^2+2b^2+2ab\varphi(\sqrt{2}),\end{aligned}$$

由此可得 $\varphi(\sqrt{2})=-\frac{a^2+2b^2+1}{2ab}\in\mathbb{Q}$, 这说明

$$\varphi(\mathbb{Q}(\sqrt{2}))\subset\mathbb{Q}\subsetneq\mathbb{Q}(\sqrt{-1}),$$

与假设 $\varphi(\mathbb{Q}(\sqrt{2}))=\mathbb{Q}(\sqrt{-1})$ 相矛盾. □

4. 设 $F(\alpha)$ 是域 F 的单代数扩域, 证明: 若 $[F(\alpha):F]$ 是奇数, 则 $F(\alpha)=F(\alpha^2)$.

证明: $[F(\alpha):F]=[F(\alpha):F(\alpha^2)][F(\alpha^2):F]$, 由于 α 为 $F(\alpha^2)$ 上多项式 $x^2-\alpha$ 的根, 故 α 在 $F(\alpha^2)$ 上的极小多项式的次数至多为 2, 所以 $[F(\alpha):F(\alpha^2)]=1$ 或 2. 当 $[F(\alpha):F(\alpha^2)]=2$ 时, $[F(\alpha):F]$ 为偶数, 矛盾, 故必有 $[F(\alpha):F(\alpha^2)]=1$, 从而 $F(\alpha)=F(\alpha^2)$. □

5. 设 E 是域 F 的扩域, $\alpha\in E$, 证明: α 是 F 上的代数元当且仅当 $[F(\alpha):F]<\infty$.

证明: $(\Rightarrow)$ 因 α 是 F 上的代数元, 故存在 $0\neq f(x)\in F[x]$, 使得 $f(\alpha)=0$, 故 $[F(\alpha):F]=\deg p(x)\leq\deg f(x)<\infty$. □

6. 设 α 是 $\mathbb{Q}[x]$ 上多项式 x^2-5x+7 的根, 试把 $\frac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}$ 写成关于 α 的多项式.

解: 设 $\frac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}=A+B\alpha$, 则

$$1-7\alpha+2\alpha^2=(1+\alpha-\alpha^2)(A+B\alpha).$$

利用条件 $\alpha^2=5\alpha-7$ 和待定系数法可求得 $A=\frac{9}{2}$, $B=-\frac{7}{4}$. □

7. 求 $\mathbb{Q}(\sqrt[3]{2})$ 中元 $1+\sqrt[3]{2}+\sqrt[3]{4}$ 的逆元.

解: 由于 $(\sqrt[3]{2}-1)(1+\sqrt[3]{2}+\sqrt[3]{4})=1$, 故逆元为 $\sqrt[3]{2}-1$. □

8. 求 $[\mathbb{Q}(\sqrt{3+2\sqrt{2}}):\mathbb{Q}]$.

解: 令 $u=\sqrt{3+2\sqrt{2}}$, 则 $u^2=3+2\sqrt{2}\Rightarrow u^4-6u^2+1=0$, 即 u 在 $\mathbb{Q}$ 上的极小多项式为 x^4-6x^2+1, 因此 $[\mathbb{Q}(\sqrt{3+2\sqrt{2}}):\mathbb{Q}]=4$. □

9. 证明: $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

证明: 显然 $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$, 故

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})][\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}],$$

因 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$, 故

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2}+\sqrt{3})]=1,$$

因此 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. □

2.6　代数扩域

一个域 K 称为代数闭域, 若 $K[x]$ 中每个次数大于零的多项式在 K 内有一个根. 此定义等价于: 若 $K[x]$ 中每个次数大于零的多项式的根都在 K 中. 事实上, 设 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$ 有一个根 $x_0 \in F$, 则 $f(x)$ 可分解为 $f(x) = (x - x_0)g(x)$, 其中 $g(x) \in F[x]$ 为 $n-1$ 次多项式, 由条件知 $g(x)$ 在 F 中也有根, 同样可以分解, 如此进行下去, 便得到 $f(x)$ 的所有根都在 F 中.

1. 设 E 是 F 的代数扩域, α 是 E 上的代数元, 证明: α 是 F 上的代数元.

证明: 因 α 是 E 上的代数元, 故存在 E 中元 $e_0, e_1, \cdots, e_n \neq 0$ 使得 $e_0 + e_1\alpha + \cdots + e_n\alpha^n = 0$, 因此 α 为 $F(e_0, \cdots, e_n)$ 上的代数元, 从而 $F(e_0, \cdots, e_n, \alpha)$ 为 $F(e_0, \cdots, e_n)$ 的有限扩域, 又因为 $F(e_0, \cdots, e_n)$ 为 F 的有限扩域, 所以 $F(e_0, \cdots, e_n, \alpha)$ 为 F 的有限扩域, 当然也为 F 的代数扩域. □

2. 设 E 是 F 的代数扩域, $\alpha, \beta \in E$, $[F(\alpha) : F] = m$, $[F(\beta) : F] = n$. 证明: $[F(\alpha, \beta) : F(\beta)] = m$ 当且仅当 $[F(\alpha, \beta) : F(\alpha)] = n$.

证明: 只需利用等式

$$\begin{aligned}[F(\alpha, \beta) : F] &= [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] \\ &= [F(\alpha, \beta) : F(\beta)][F(\beta) : F]\end{aligned}$$

及题给条件即可. □

3. 设 F 是域, $x^n - a \in F[x]$, α 是 $x^n - a$ 在 F 的某个扩域 E 内的根. 证明: 若 $[F(\alpha) : F] = n$, $m \mid n$, 则 $[F(\alpha^m) : F] = n/m$, $[F(\alpha) : F(\alpha^m)] = m$.

证明: 若 $[F(\alpha) : F] = n$, 则 α 在 F 上的极小多项式即为 $x^n - a$, 从而 α^m 在 F 上的极小多项式为 $x^{\frac{n}{m}} - a$, 故 $[F(\alpha^m) : F] = n/m$, $[F(\alpha) : F(\alpha^m)] = m$. □

4. 设 F, K, E 均为域且满足 $F \subset K \subset E$, 证明: E 是 F 的代数扩域当且仅当 E 是 K 的代数扩域且 K 是 F 的代数扩域.

证明: $(\Rightarrow)$ 因 E 是 F 的代数扩域, 故 E 中任意元都是 K 上的代数元且 K 中任意元都是 F 上的代数元, 即 E 是 K 的代数扩域且 K 是 F 的代数扩域.

$(\Leftarrow)$ 因 E 是 K 的代数扩域, 故对任意 $e \in E$, e 是 K 上的代数元, 又 K 是 F 的代数扩域, 故由第一题知 e 为 F 上的代数元, 从而 E 是 F 的代数扩域. □

5. 设 E 是 F 的代数扩域, A 是 F 在 E 中的代数闭包, 则 A 在 E 中是代数闭的.

证明: 即证 A 在 E 中的代数闭包即为 A 自身. 任取 $x \in E \setminus A$, 若 x 为 A 上的代数元, 注意到 A 为 F 的代数扩域, 故由第一题结论知 x 为 F 上的代数元, 这与 A 的定义相矛盾, 故 x 不是 A 上的代数元, 从而 A 在 E 中的代数闭包即为 A 自身. □

6. 设 E 是 F 的扩域, 证明: E 是 F 的有限扩域当且仅当 E 是由 F 上有限个代数元生成的.

证明: $(\Rightarrow)$ 设 $[E : F] = n$ 且 E 作为 F 上的向量空间有一组基 $e_1, \cdots, e_n$, 则 $E = F(e_1, \cdots, e_n)$. 由于有限扩域为代数扩域, 故 e_i 皆为 F 上的代数元.

$(\Leftarrow)$ 即为定理 2.6.5. □

7. 设 E 是域 F 的扩域, $f(x) \in F[x]$ 是素数 p 次不可约多项式, $[E : F] < \infty$. 证明: 若 $f(x)$ 在 $E[x]$ 里可约, 则 $p \mid [E : F]$.

证明: 因 $f(x)$ 在 $E[x]$ 中可约, 故 $f(x)$ 在 $E[x]$ 中可分解为 $f(x) = g(x)h(x)$, 其中 $g(x)$ 不可约且 $\deg g(x) < p$. 设 α 是 $g(x)$ 的一个根, 则 $L = E(\alpha)$ 是 E 的扩域且 $[L : E] = \deg g(x)$, 又 $[L : F] = [L : F(\alpha)][F(\alpha) : F]$, 故 $p \mid [L : F]$, 所以 $p \mid [L : E][E : F]$, 但 $p \nmid [L : E]$, 因此 $p \mid [E : F]$. □

2.7　多项式的分裂域与正规扩域

1. 设 E 是 n 次多项式 $f(x)$ 在 F 上的分裂域, 证明: $[E:F] \mid n!$. $[E:F] = n!$ 何时成立?

2.8　有限域

1. 令 F 是特征为 2 的素域, 找出 $F[x]$ 中的所有三次不可约多项式.

解: 特征为 2 的素域同构于 $\mathbb{Z}_2$, 而 $\mathbb{Z}_2[x]$ 上的三次多项式有 $x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+x, x^3+x^2+1, x^3+x^2+x+1$. 若三次多项式可约, 则其必可分解出一次因式, 从而该三次多项式必然在 $\mathbb{Z}_2$ 上有根. 因此所有三次不可约多项式只有 x^3+x+1 和 x^3+x^2+1. $\square$

2. 证明: 有限域不可能是代数闭域.

证明: 设 $F = \{a_1, \cdots, a_n\}$ 为有限域, 因多项式 $(x-a_1)(x-a_2)\cdots(x-a_n)-1$ 在 F 上无根, 所以 F 不是代数闭域. $\square$

3. 证明: 当 $n \geq 3$ 时, $x^{2^n}+x+1$ 是 $F_2[x]$ 中不可约多项式.

第 3 章

Galois 理论

3.1 Galois 理论的基本定理

1. 设 $f(x)=x^3-2\in\mathbb{Q}[x]$, 计算 $f(x)$ 的 Galois 群.

证明: 第一步, 计算 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域. $f(x)=0\Rightarrow x=\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$, 其中 ω 为三次本原单位根, 故 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域为 $E=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=\mathbb{Q}(\sqrt[3]{2},\omega)$.

第二步, 计算 $[E:\mathbb{Q}]$.

$$[E:\mathbb{Q}]=[E:\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}].$$

ω 在 $\mathbb{Q}(\sqrt[3]{2})$ 上的极小多项式为 x^2+x+1, 故 $[E:\mathbb{Q}(\sqrt[3]{2})]=2$, 且 E 作为 $\mathbb{Q}(\sqrt[3]{2})$ 上的向量空间具有一组基 $1,\omega$.

$\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^3-2, 故 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, 且 $\mathbb{Q}(\sqrt[3]{2})$ 作为 $\mathbb{Q}$ 上的向量空间具有一组基 $1,\sqrt[3]{2},\sqrt[3]{4}$.

因此 $[E:\mathbb{Q}]=6$, 且 E 在 $\mathbb{Q}$ 上的一组基为 $1,\sqrt[3]{2},\sqrt[3]{4},\omega,\sqrt[3]{2}\omega,\sqrt[3]{4}\omega$.

第三步, 求 $\mathrm{G}(E/\mathbb{Q})$. 对任意 $\sigma\in\mathrm{G}(E/\mathbb{Q})$, σ 由其在 $\sqrt[3]{2}$ 和 ω 上的取值唯一确定. 由于 σ 置换 $x^2+x+1=0$ 的根, 故 $\sigma(\omega)\in\{\omega,\omega^2\}$. 又由于 σ 置换 $x^3-2=0$ 的根, 故 $\sigma(\sqrt[3]{2})\in\{\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}$. 由此我们便可以得到六个自同构, 但为叙述方便, 选取两个自同构 $\sigma,\tau\in\mathrm{G}(E/\mathbb{Q})$ 满足:

$$\begin{cases}\sigma(\sqrt[3]{2})=\sqrt[3]{2}\omega\\ \sigma(\omega)=\omega\end{cases}\qquad\begin{cases}\tau(\sqrt[3]{2})=\sqrt[3]{2}\\ \tau(\omega)=\omega^2\end{cases}$$

	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	ω	ω^2
1	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	ω	ω^2
σ	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	ω	ω^2
σ^2	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	ω	ω^2
τ	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}\omega$	ω^2	ω
$\sigma\tau$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$	ω^2	ω
$\sigma^2\tau$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}$	ω^2	ω

则可得下表 □

2. 证明 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 是 $\mathbb{Q}$ 的 Galois 扩张, 并求其 Galois 群.

证明: 由于 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 是可分多项式 $f(x)=(x^2-2)(x^2-3)(x^2-5)$ 在 $\mathbb{Q}$ 上的分裂域, 故 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 是 $\mathbb{Q}$ 的 Galois 扩张, 且 $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}]=8$, 令

$$\sigma:\begin{cases}\sqrt{2}\mapsto-\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\\ \sqrt{5}\mapsto\sqrt{5}\end{cases}\qquad \tau:\begin{cases}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto-\sqrt{3}\\ \sqrt{5}\mapsto\sqrt{5}\end{cases}\qquad \pi:\begin{cases}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\\ \sqrt{5}\mapsto-\sqrt{5}\end{cases}$$

则 $\mathrm{G}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})=\{\mathrm{id},\sigma,\tau,\pi,\sigma\tau,\sigma\pi,\tau\pi,\sigma\tau\pi\}$. □

第 4 章 补充题目

1. 求有理数域上多项式 $x^3 - x^2 - x - 2$ 的分裂域 E, 并求 $[E : \mathbb{Q}]$.

证明: 因 $x^3 - x^2 - x - 2 = (x-2)(x^2+x+1)$, 故 $E = \mathbb{Q}(\omega)$, 其中 ω 为三次单位根, 且 ω 在 $\mathbb{Q}$ 上的极小多项式为 x^2+x+1, 故 $[E : \mathbb{Q}] = 2$. $\square$

2. 设 $x^3 - a$ 是 $\mathbb{Q}[x]$ 上不可约多项式, α 为 $x^3 - a$ 的一个根, 证明: $\mathbb{Q}(\alpha)$ 不是 $x^3 - a$ 在 $\mathbb{Q}$ 上的分裂域.

证明: 因 α 在 $\mathbb{Q}$ 上极小多项式的次数为 3, 故 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. 假设 $\mathbb{Q}(\alpha)$ 为 $x^3 - a$ 的分裂域, 因 $\alpha, \omega\alpha \in \mathbb{Q}(\alpha)$, 故 $\omega \in \mathbb{Q}(\alpha)$, 因此 $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\alpha)$, 但 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, 矛盾. $\square$

3. 证明: $\mathbb{Q}(\sqrt[3]{5})$ 不是 $\mathbb{Q}$ 的正规扩张.

证明: $\sqrt[3]{5}$ 的极小多项式为 $x^3 - 5$, 注意到 $\sqrt[3]{5}\omega$ 为 $x^3 - 5$ 的根, 但 $\sqrt[3]{5}\omega \notin \mathbb{Q}(\sqrt[3]{5})$. $\square$

4. 设 a, b 为含幺环 R 中的元, 则 $1 - ab$ 可逆 $\Leftrightarrow$ $1 - ba$ 可逆.

证明: 只需证明必要性, 充分性证明同理. 此题可采用形式分析. 若 $1 - ab$ 可逆, 则

$$(1-ab)^{-1} = 1 + ab + abab + ababab + \cdots.$$

则从形式上看

$$
\begin{aligned}
(1-ba)^{-1} &= 1+ba+baba+bababa+\cdots \\
&= 1+b(1+ab+abab+\cdots)a \\
&= 1+b(1-ab)^{-1}a.
\end{aligned}
$$

下面验证 $1-ba$ 的逆确实为 $1+b(1-ab)^{-1}a$.

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

类似地 $(1+b(1-ab)^{-1}a)(1-ba)=1$, 证毕. □

5. 求环 $\mathbb{Z}[\sqrt{-1}]$ 的单位群, 证明此环为整环但不是域.

证明: 定义 $\phi:\mathbb{Z}[\sqrt{-1}]\to\mathbb{Z}$, $a+b\sqrt{-1}\mapsto a^2+b^2$, 则可验证对任意 $a+b\sqrt{-1},c+d\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$, 有

$$
\phi((a+b\sqrt{-1})(c+d\sqrt{-1}))=\phi(a+b\sqrt{-1})\phi(c+d\sqrt{-1}).
$$

若 $a+b\sqrt{-1}$ 为单位, 则存在 $c+d\sqrt{-1}$ 使得

$$
(a+b\sqrt{-1})(c+d\sqrt{-1})=1,
$$

则

$$
\phi(a+b\sqrt{-1})\phi(c+d\sqrt{-1})=(a^2+b^2)(c^2+d^2)=1.
$$

因此 $a+b\sqrt{-1}=\pm1$ 或 $\pm\mathrm{i}$, 即 $\mathbb{Z}[\sqrt{-1}]$ 的单位群为 $\{\pm1,\pm\mathrm{i}\}$.

容易验证 $\mathbb{Z}[\sqrt{-1}]$ 为交换幺环且没有零因子, 故为整环 (事实上, 可以进一步验证其为欧式环). 取 $2\in\mathbb{Z}[\sqrt{-1}]$, 显然 2 没有乘法逆元, 故 $\mathbb{Z}[\sqrt{-1}]$ 不是域. □

6. 证明: 若整环 R 只有有限多个理想, 则 R 为域.

证明: 任取非零元 $\alpha\in R$, 考虑理想 $(\alpha),(\alpha^2),\cdots$, 由于 R 只有有限多个理想, 故存在正整数 $m<n$, 使得 $(\alpha^m)=(\alpha^n)$, 则 $\alpha^m\in(\alpha^n)$, 从而 $\alpha^m=\alpha^n\beta\Rightarrow\alpha^m(1-\alpha^{n-m}\beta)=0$, 而 R 没有零因子且 $\alpha^m\neq 0$, 故 $1-\alpha^{n-m}\beta=0$, 因此 α 可逆. 从而 R 为域. □

7. 设 u 是多项式 x^3-6x^2+9x+3 的一个实根.

(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$;

(2) 将 u^4, $(u+1)^{-1}$, $(u^2-6u+8)^{-1}$ 表示成 $1,u,u^2$ 的 $\mathbb{Q}$-线性组合.

证明: (1) 取素数 3, 由于 $3\nmid 1$, $3\mid(-6)$, $3\mid 9$, $3\mid 3$ 且 $3^2\nmid 3$, 故由 Eisenstein 判别法知 x^3-6x^2+9x+3 在 $\mathbb{Q}$ 上不可约, 因此其就是 u 在 $\mathbb{Q}$ 上的极小多项式, 从而 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2) 利用 $u^3=6u^2-9u-3$, 有

$$u^4=u(6u^2-9u-3)=27u^2-57u-18.$$

由于

$$(u+1)(u^2-7u+16)=u^3-6u^2+9u+16=13,$$

故 $(u+1)^{-1}=\frac{1}{13}(u^2-7u+16)$. 利用辗转相除法可得

$$1=\frac{1}{35}(x^2-9x+1)(x^2-6x+8)-\frac{1}{35}(x-9)(x^3-6x^2+9x+3).$$

在上式中取 $x=u$, 得 $1=\frac{1}{35}(u^2-9u+1)(u^2-6u+8)$, 故

$$(u^2-6u+8)^{-1}=\frac{1}{35}(u^2-9u+1).$$ □

8. 设 α 是 $\mathbb{Q}$ 上的超越元, $u=\frac{\alpha^3}{1+\alpha}$, 求 $[\mathbb{Q}(\alpha):\mathbb{Q}(u)]$.

解: 下证 x^3-ux-u 是 α 在 $\mathbb{Q}(u)$ 上的不可约多项式. 反证法, 假设 x^3-ux-u 在 $\mathbb{Q}(u)$ 上可约, 则 $x^3-ux-u=0$ 在 $\mathbb{Q}(u)$ 内有根 β, 记 $\beta=\frac{f(u)}{g(u)}$, 其中 $f(x),g(x)\in\mathbb{Q}[x]$, 则

$$\left(\frac{f(u)}{g(u)}\right)^3-u\frac{f(u)}{g(u)}-u=0,$$

即
$$(f(u))^3 - uf(u)(g(u))^2 - u(g(u))^3 = 0.$$
故 u 为 $\mathbb{Q}$ 上的代数元, 从而 $\mathbb{Q}(u)$ 为 $\mathbb{Q}$ 的有限扩张, 于是
$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(u)][\mathbb{Q}(u):\mathbb{Q}] < \infty.$$
这表明 α 在 $\mathbb{Q}$ 上为代数元, 矛盾. 因此 $x^3 - ux - u$ 是 α 在 $\mathbb{Q}(u)$ 上的极小多项式, 从而 $[\mathbb{Q}(\alpha):\mathbb{Q}(u)] = 3$. □

9. 设 $K = \mathbb{Q}(\alpha)$ 为 $\mathbb{Q}$ 的单扩张, 其中 α 在 $\mathbb{Q}$ 上代数, 求证: $|\operatorname{Aut}(K)| \leq [K:\mathbb{Q}]$.

证明: $[K:\mathbb{Q}]$ 等于 α 在 $\mathbb{Q}$ 上的极小多项式 $p(x)$ 的次数 n, 且 K 作为 $\mathbb{Q}$ 上的向量空间具有一组基: $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$. 任取 $\sigma \in \operatorname{Aut}(K)$, σ 由其在 α 上的作用唯一确定. 设 $p(x)$ 的全部根为 $\{\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n\}$, 由于 σ 将 $p(x)$ 的根映为 $p(x)$ 的根, 故
$$\sigma(\alpha) \in \{\alpha_1, \alpha_2, \cdots, \alpha_n\} \cap K.$$
因此 $|\operatorname{Aut}(K)| \leq n = [K:\mathbb{Q}]$. □

4.1　2021 年期中测试题

1. 设 G 是群, G_1, G_2 是 G 的有限子群, 证明:
$$|G_1G_2| = \frac{|G_1|\,|G_2|}{|G_1 \cap G_2|}.$$

证法一: 考虑 G_1 在陪集空间 G/G_2 上的自然作用, 取 $G_2 \in G/G_2$, G_2 的轨道为 $\{gG_2 \mid g \in G_1\}$, 而 G_2 的稳定化子为
$$\{g \in G_1 \mid gG_2 = G_2\} = G_1 \cap G_2.$$
于是由轨道-稳定化子定理得
$$|\{gG_2 \mid g \in G_1\}| = |G_1/G_1 \cap G_2| = \frac{|G_1|}{|G_1 \cap G_2|},$$

而 $|\{gG_2 \mid g \in G_1\}| = \frac{|G_1G_2|}{|G_2|}$, 因此

$$\frac{|G_1G_2|}{|G_2|} = \frac{|G_1|}{|G_1 \cap G_2|}. \qquad \square$$

证法二: 所证等式等价于

$$\frac{|G_1G_2|}{|G_2|} = \frac{|G_1|}{|G_1 \cap G_2|}.$$

考虑两个陪集族

$$G_1G_2/G_2 :\ = \{hG_2 \mid h \in G_1\}$$

和

$$G_1/G_1 \cap G_2 :\ = \{hG_1 \cap G_2 \mid h \in G_1\}.$$

下面在两个陪集族上建立双射, 为此考虑映射

$$\begin{aligned} \phi\colon G_1G_2/G_2 &\longrightarrow G_1/G_1 \cap G_2 \\ hG_2 &\longmapsto hG_1 \cap G_2 \end{aligned}$$

ϕ 合理定义: 当 $h_1G_2 = h_2G_2$ 时, 有 $h_1h_2^{-1} \in G_2$, 又因为 $h_1h_2^{-1} \in G_1$, 所以 $h_1h_2^{-1} \in G_1 \cap G_2$, 从而 $h_1G_1 \cap G_2 = h_2G_1 \cap G_2$, 这说明 ϕ 是合理定义的.

ϕ 是单射: 设 $h_1G_1 \cap G_2 = h_2G_1 \cap G_2$, 则 $h_1h_2^{-1} \in G_1 \cap G_2 \Rightarrow h_1h_2^{-1} \in G_2 \Rightarrow h_1G_2 = h_2G_2$.

ϕ 是满射: 显然.

因此 G_1G_2/G_2 的陪集个数等于 $G_1/G_1 \cap G_2$ 的陪集个数, 故

$$\frac{|G_1G_2|}{|G_2|} = \frac{|G_1|}{|G_1 \cap G_2|}. \qquad \square$$

证法三: 因 $G_1 \cap G_2 \le G_1$, 故可考虑陪集空间 $G_1/G_1 \cap G_2$. 设 $|G_1/G_1 \cap G_2| = m$ 且 $G_1 = h_1(G_1 \cap G_2) \cup h_2(G_1 \cap G_2) \cup \cdots \cup h_m(G_1 \cap G_2)$, 其中 $h_i \in G_1$ 且 $h_ih_j^{-1} \notin G_2, i \neq j$.

下证 G_1G_2 可表示为如下不相交的陪集之并

$$G_1G_2 = h_1G_2 \cup h_2G_2 \cup \cdots \cup h_mG_2. \tag{$\star$}$$

首先因 $h_ih_j^{-1} \notin G_2, i \neq j$, 故 $(h_iG_2)_{i=1}^m$ 两两不相交. 其次对任意的 $hk \in G_1G_2$, 因 $G_1 = h_1(G_1\cap G_2)\cup h_2(G_1\cap G_2)\cup\cdots\cup h_m(G_1\cap G_2)$, 故存在 $h_i \in G_1$ 和 $g \in G_1 \cap G_2$ 使得 $h = h_ig$, 那么 $hk = h_igk \in h_iG_2$, 即证 $(\star)$.

所以 $|G_1G_2| = m|G_2| = \frac{|G_1||G_2|}{|G_1\cap G_2|}$. □

2. 证明: 若 Abel 群 $G = H_1 + H_2 + \cdots + H_n, H_i$ 都是有限群, 则有

$$\big|G\big| \mid \big|H_1\big|\big|H_2\big|\cdots\big|H_n\big|,$$

且 $|G| = |H_1|\,|H_2|\cdots|H_n| \Leftrightarrow G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$.

证明: 考虑映射 $\phi : H_1 \oplus H_2 \oplus \cdots \oplus H_n \to G = H_1 + H_2 + \cdots + H_n$, $(h_1, h_2, \cdots, h_n) \mapsto h_1 + h_2 + \cdots + h_n$. 验证 ϕ 为满同态, 故

$$H_1 \oplus H_2 \oplus \cdots \oplus H_n / \ker\phi \cong G,$$

所以 $|G| \mid |H_1||H_2|\cdots|H_n|$.

当 $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$, 显然 $|G| = |H_1||H_2|\cdots|H_n|$;

当 $|G| = |H_1||H_2|\cdots|H_n|$ 时, $|\ker\phi| = 1 \Rightarrow \ker\phi = \{0\}$, 故 $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$. □

3. 设 G 和 G' 分别是阶为 m 和 n 的有限循环群, 证明: 存在 G 到 G' 的满同态的充要条件是 $n \mid m$.

证明: $(\Rightarrow)$ 设 $\phi : G \to G'$ 为满同态, 则 $G/\ker\phi \cong G'$, 故 $\frac{|G|}{|\ker\phi|} = |G'|$, 也即 $\frac{m}{|\ker\phi|} = n \Rightarrow n \mid m$.

$(\Leftarrow)$ 设 g, h 分别为 G 和 G' 的生成元, 定义 $\phi : G \to G'$, $g^a \mapsto h^a$, 则

$$\phi(g^ag^b) = \phi(g^{a+b}) = h^{a+b} = h^ah^b = \phi(g^a)\phi(g^b).$$

又因 $m \geq n$, 故 ϕ 为满射, 从而为满同态. □

4. 在剩余类环 $\mathbb{Z}_n$ 中, 记满足 $(a,n)=1$ 的剩余类 $[a]$ 的个数为 $\varphi(n)$, 证明:

(1) 令 $R=\{[a]\in\mathbb{Z}_n \mid (a,n)=1\}$, 则 R 关于剩余类的乘法构成一个群;

(2) 若 $(a,n)=1$, 则 $a^{\varphi(n)}\equiv 1 \pmod n$ (欧拉定理).

证明: (1) (i) 结合律显然满足; (ii) $[1]$ 为单位元, 即 $[a][1]=[1][a]=[a]$; (iii) 任取 $[a]\in R$, 由于 $(a,n)=1$, 故存在整数 r,s, 使得 $ar+ns=1$, 从而 $[a][r]=[ar]=[1-ns]=[1]$, 即 $[r]$ 为 $[a]$ 的逆元. 综上即知 R 关于剩余类的乘法构成一个群.

(2) 任取 $[a]\in R$, 由 Lagrange 定理知 $[a]$ 的阶为 $\varphi(n)$ 的因子, 故 $[a]^{\varphi(n)}=\left[a^{\varphi(n)}\right]=[1]$, 所以 $a^{\varphi(n)}\equiv 1 \pmod n$. □

5. 设 I,J 是环 R 的理想且 $R=I+J$, 证明: $R/(I\cap J)\cong R/I\oplus R/J$.

证明: 定义映射

$$\begin{aligned}\phi: R &\longrightarrow R/I\oplus R/J\\ r &\longmapsto (r+I, r+J).\end{aligned}$$

首先, ϕ 为同态: 对于任意 $r_1,r_2\in R$, 有

$$\phi(r_1+r_2)=(r_1+r_2+I, r_1+r_2+J)=\phi(r_1)+\phi(r_2),$$

$$\phi(r_1r_2)=(r_1r_2+I, r_1r_2+J)=(r_1+I, r_1+J)(r_2+I, r_2+J)=\phi(r_1)\phi(r_2).$$

其次, ϕ 为满射: 任取 $(r_1+I, r_2+J)\in R/I\oplus R/J$, 由于 $R=I+J$, 故存在 $r_{1I}, r_{2I}\in I$, $r_{1J}, r_{2J}\in J$, 使得 $r_1=r_{1I}+r_{1J}$ 且 $r_2=r_{2I}+r_{2J}$. 取 $r=r_{1J}+r_{2I}$, 则

$$\phi(r)=(r_{1J}+r_{2I}+I, r_{1J}+r_{2I}+J)=(r_1+I, r_2+J).$$

又因 $\ker\phi=\{r\in R \mid (r+I, r+J)=(I,J)\}=I\cap J$, 故

$$R/(I\cap J)\cong R/I\oplus R/J. \qquad \square$$

6. 设 R 是交换环, P 是 R 的真理想, 证明: P 是 R 的素理想 $\Leftrightarrow$ 对 R 的任意两个理想 I, J, 若 $IJ \subseteq P$, 则 $I \subseteq P$ 或 $J \subseteq P$, 其中 $IJ = \{ij \mid i \in I, j \in J\}$.

证明: $(\Rightarrow)$ 若 $IJ \subseteq P$, 假设 $I \nsubseteq P$, 则存在 $x \in I$, 使得 $x \notin P$. 由于 $IJ \subseteq P$, 故对任意 $y \in J$, $xy \in P$, 但 $x \notin P$, 故 $y \in P$, 从而 $J \subseteq P$.

$(\Leftarrow)$ 设 $ab \in P$, 则 $(a)(b) \subseteq P \Rightarrow (a) \subseteq P$ 或 $(b) \subseteq P$, 故 $a \in P$ 或 $b \in P$, 因此 P 为素理想. □

7. 设 R 是唯一分解整环, $a \in R$ 且 $a \neq 0$, 证明: R 仅有有限多个主理想包含 a.

证明: 设 $a \in (b)$, 则 $b \mid a$, 由于 a 为唯一分解整环, 故整除 a 的元素 b 有限. □

8. 证明:

(1) $p(x) = x^3 + x + 1$ 是 $\mathbb{Z}_2[x]$ 中的不可约多项式;

(2) $\mathbb{Z}_2[x]/(x^3 + x + 1)$ 是域.

证明: (1) 由于 $\deg p(x) = 3$, 故 $p(x)$ 可约 $\iff$ $p(x)$ 在 $\mathbb{Z}_2$ 中有根. 但 $p(0) \neq 0$, $p(1) \neq 0$, 故 $p(x)$ 不可约.

(2) 由于 $\mathbb{Z}_2$ 为域, 故 $\mathbb{Z}_2[x]$ 为主理想环. 设 I 为理想且 $(x^3 + x + 1) \subset I \subseteq \mathbb{Z}_2[x]$, 由于 $\mathbb{Z}_2[x]$ 为主理想环, 故可设 $I = (a(x))$, 则 $x^3 + x + 1 \in (a(x))$, 故存在 $b(x) \in \mathbb{Z}_2[x]$ 使得 $x^3 + x + 1 = a(x)b(x)$, 而 $x^3 + x + 1$ 不可约, 故 $a(x) = 1 \Rightarrow I = \mathbb{Z}_2[x]$, 即证 $(x^3 + x + 1)$ 为极大理想, 所以 $\mathbb{Z}_2[x]/(x^3 + x + 1)$ 是域. (教材定理 2.4.9: 在主理想环中素元生成的主理想为极大理想) □

4.2　2018–2019 年期末测试题

1. 设 G 是一个阶为偶数的有限群, 证明 G 中阶大于 2 的元素的个数一定为偶数, G 中阶等于 2 的元素的个数一定为奇数.

证明: 任取 G 中阶大于 2 的元 a, 必有 $a \neq a^{-1}$, 且 a^{-1} 的阶等于 a 的阶, 故 G 中阶大于 2 的元素可两两组队, 因此阶数大于 2 的元素的个数一定为偶数, 从而 G 中阶等于 2 的元素的个数一定为奇数. □

2. 设 G 为群, 如果 $G/Z(G)$ 为循环群, 则 G 为交换群.

证明: 因商群 $G/Z(G)$ 为循环群, 故存在 $g \in G$, 使得 $G/Z(G) = \langle gZ(G)\rangle$. 对任意 $g_1, g_2 \in G/Z(G)$, 存在正整数 m_1, m_2 使得

$$g_1Z(G) = g^{m_1}Z(G), \quad g_2Z(G) = g^{m_2}Z(G).$$

故 $g_1 = g^{m_1}z_1$, $g_2 = g^{m_2}z_2$, 其中 $z_1, z_2 \in Z(G)$, 于是

$$g_1g_2 = g^{m_1}z_1g^{m_2}z_2 = g^{m_2}z_2g^{m_1}z_1 = g_2g_1.$$

因此 G 为交换群. □

3. 证明域 F 关于乘法的有限子群 G 为循环群.

证法一: 任意取 $d \mid n$, 令 $G_d = \{x \in G \mid o(x) = d\}$. 假设 $G_d \neq \emptyset$, 则存在 $y \in G_d$, 显然 $\langle y\rangle \subseteq \{x \in G \mid x^d = 1\}$. 但是 $\#\langle y\rangle = d$, 故 $\langle y\rangle = \{x \in G \mid x^d = 1\}$. 因此 G_d 就是 d 阶循环群 $\langle y\rangle$ 的生成元构成的集合, 故 $\#G_d = \varphi(d)$.

上述过程说明对于 $\forall d \mid n$, G_d 或者为空集或者满足 $\#G_d = \varphi(d)$, 故

$$n = \#G = \sum_{d|n} \#G_d \leq \sum_{d|n} \varphi(d) = n.$$

故对任意的 $d \mid n$, 有 $\#G_d = \varphi(d)$, 特别地, $\#G_n = \varphi(n)$, 因此 G 为循环群. □

证法二: 在有限交换群 G 中存在元素 g, 使得 g 的阶是 G 中所有元素的阶的倍数, 记 $o(g) = n$, 则 G 中所有元素都满足方程

$$x^n = e.$$

但是在域中满足 $x^n = e$ 的元素个数不超过 n, 故 $|G| \leq n$. 显然, $n \leq |G|$, 因而 $|G| = n$, 这就说明 $G = \langle g\rangle$ 为循环群. □

证法三: 由有限交换群的结构定理知 $G\cong\mathbb{Z}_{p_1^{r_1}}\oplus\cdots\oplus\mathbb{Z}_{p_s^{r_s}}$, 其中 $p_1,p_2,\cdots,p_s$ 不一定两两互异, 记此同构为

$$\begin{aligned}\phi: G &\longrightarrow \mathbb{Z}_{p_1^{r_1}}\oplus\cdots\oplus\mathbb{Z}_{p_s^{r_s}}\\ a &\longmapsto (a_1,\cdots,a_s).\end{aligned}$$

令 $m=\operatorname{lcm}(p_1^{r_1},\cdots,p_s^{r_s})$, 对任意 $a_i\in\mathbb{Z}_{p_i^{r_i}}$, 有 $p_i^{r_i}a_i=0$, 故 $ma_i=0$. 因此对任意 $a\in G$, 有

$$\phi(a^m)=m(a_1,\cdots,a_s)=0\Rightarrow a^m=1.$$

即 G 中每个元素都满足 $x^m=1$, 而在域 F 中方程 $x^m-1=0$ 至多只有 m 个根, 故 $|G|\le m$. 显然 $m\le|G|$, 故 $m=|G|=p_1^{r_1}\cdots p_s^{r_s}$, 这说明 $p_1,p_2,\cdots,p_s$ 两两互异, 故 $G\cong\mathbb{Z}_m$ 为循环群. □

注 这是一个一般性的结论, 值得关注. 任何一个域 F 去掉其中的零元素得到的集合 $F^*=F\setminus\{0\}$ 关于乘法构成一个群, 本题要说明的就是 F^* 的有限子群一定是循环群.

相关链接: (1) MSE 上关于这个问题的讨论. (2) 一个 PDF.

4. 设交换幺环 R 只有一个极大理想 M, 证明 $R\setminus M$ 中的元素都是 R 中的单位.

证明: 若 $x\in R$ 不是单位, 则 (x) 为 R 的真理想, 而 M 为唯一的极大理想, 故 $(x)\subset M\Rightarrow x\in M$, 因此 $R\setminus M$ 中的元都是单位. □

5. 证明: 设 R 为特征为素数 p 的交换环, 则 $a\mapsto a^p$ 为 R 的自同态.

证明: 记映射 $\phi: a\mapsto a^p$, 则

$$\phi(a+b)=(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^kb^{p-k}=a^p+b^p=\phi(a)+\phi(b),$$

$$\phi(ab)=(ab)^p=a^pb^p=\phi(a)\phi(b).$$

故 ϕ 为 R 的自同态. □

6. 如果在环 R 中对于每个元素 x 均存在大于 1 的自然数 n (n 可能与 x 有关) 使得 $x^n = x$, 证明 R 的每个素理想都是极大理想.

证明: 设 P 为 R 的素理想, 任取 $x \in R \setminus P$, 存在 $n > 1$ 使得 $x^n = x$, 即 $x(x^{n-1} - 1) = 0 \in P$, 但 $x \notin P$, 故 $x^{n-1} - 1 \in P$, 因此 $(x, P) = (1) = R$, 由此可知 P 为极大理想. □

7. 证明代数闭域为无限域.

证明: 假设代数闭域 F 为有限域, 记 $F = \{a_1, \cdots, a_n\}$, 考虑方程 $(x - a_1)(x - a_2)\cdots(x - a_n) - 1 = 0$, 显然其在 F 中没有根, 这与 F 为代数闭域相矛盾. □

8. 证明: 整环 $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ 关于 $\mathbb{Z}[\sqrt{2}]^*$ 到 $\mathbb{Z}^{\geq 0}$ 的映射

$$\phi(m + n\sqrt{2}) = |m^2 - 2n^2|$$

是一个欧式环.

证明: 可以验证 $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ 对任意的 $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$ 成立.

任取 $m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ 且 $m_2 + n_2\sqrt{2} \neq 0$, 则

$$\frac{m_1 + n_1\sqrt{2}}{m_2 + n_2\sqrt{2}} = \frac{\left(m_1 + n_1\sqrt{2}\right)\left(m_2 - n_2\sqrt{2}\right)}{m_2^2 - 2n_2^2} = s + t\sqrt{2},$$

其中 $s = \frac{m_1m_2 - 2n_1n_2}{m_2^2 - 2n_2^2}$, $t = \frac{n_1m_2 - m_1n_2}{m_2^2 - 2n_2^2}$. 选取整数 q_1, q_2 使得 $|q_1 - s| \leq \frac{1}{2}$, $|q_2 - t| \leq \frac{1}{2}$, 则

$$\frac{m_1 + n_1\sqrt{2}}{m_2 + n_2\sqrt{2}} = \left(q_1 + q_2\sqrt{2}\right) + (s - q_1) + (t - q_2)\sqrt{2}.$$

即

$$\begin{aligned} m_1 + n_1\sqrt{2} = & \left(q_1 + q_2\sqrt{2}\right)\left(m_2 + n_2\sqrt{2}\right) \\ & + \left[(s - q_1) + (t - q_2)\sqrt{2}\right]\left(m_2 + n_2\sqrt{2}\right). \end{aligned}$$

记 $r_1+r_2\sqrt{2}=[(s-q_1)+(t-q_2)\sqrt{2}]\left(m_2+n_2\sqrt{2}\right)\in\mathbb{Z}[\sqrt{2}]$, 则

$$m_1+n_1\sqrt{2}=\left(q_1+q_2\sqrt{2}\right)\left(m_2+n_2\sqrt{2}\right)+r_1+r_2\sqrt{2}.$$

由于

$$\begin{aligned}\phi\left(r_1+r_2\sqrt{2}\right)&=\phi\left(s-q_1+(t-q_2)\sqrt{2}\right)\phi\left(m_2+n_2\sqrt{2}\right)\\&=\left|(s-q_1)^2-2(t-q_2)^2\right|\phi\left(m_2+n_2\sqrt{2}\right)\\&\leq\left((s-q_1)^2+2(t-q_2)^2\right)\phi\left(m_2+n_2\sqrt{2}\right)\\&\leq\frac{3}{4}\phi\left(m_2+n_2\sqrt{2}\right)<\phi\left(m_2+n_2\sqrt{2}\right).\end{aligned}$$

故 $\mathbb{Z}[\sqrt{2}]$ 为欧式环. □

9. 如果 $f(x)$ 为域 F 上的一个多项式, E_1 和 E_2 都是该多项式的分裂域, 证明 E_1 与 E_2 同构.

证明: 对 $[E_1:F]$ 作数学归纳法.

若 $[E_1:F]=1$, 即 $f(x)=\prod_{i=1}^{n}(x-\alpha_i)$, 其中 $\alpha_i\in F$, 则 $E_1=E_2=F$, 取 $\sigma:E_1\to E_2$ 为 id 即可.

假设 $[E_1:F]<n$ 时命题为真. 下面假设 $[E_1:F]=n$ $(n\geq 2)$, 故 $f(x)$ 存在次数大于或等于 2 的不可约因式, 设

$$f(x)=f_1(x)g(x),\quad f_1(x),g(x)\in F[x],\deg f_1(x)\geq 2.$$

其中 $f_1(x)$ 是 $f(x)$ 在 $F[x]$ 中的一个次数大于或等于 2 的不可约因式. 设 $\alpha\in E_1$ 是 $f_1(x)$ 的一个零点, $\alpha'\in E_2$ 是 $f_1(x)$ 的一个零点, 则

$$\begin{aligned}\sigma:F(\alpha)&\longrightarrow F(\alpha')\\g(\alpha)&\longmapsto g(\alpha'),\quad g(x)\in F[x]\end{aligned}$$

是域同构且 $\sigma|_F=\mathrm{id}$. 由于 $[F(\alpha):F]=\deg f_1(x)\geq 2$, 所以 $[E_1:F(\alpha)]<n$. 显然 E_1 是 $f(x)$ 在 $F(\alpha)$ 上的分裂域, E_2 是 $f(x)$ 在 $F(\alpha')$ 上的分裂域, 由归纳假设, 存在同构 $\tilde{\sigma}:E_1\to E_2$ 且 $\tilde{\sigma}|_{F(\alpha)}=\sigma$, 于是 $\tilde{\sigma}|_F=\sigma|_F=\mathrm{id}$, 所以当 $[E:F]=n$ 时命题成立. □

10. 设 $a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$, 且 $a^2+b^2=p$, p 为素数, 证明 $\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle\cong\mathbb{Z}_p$.

证明: 考虑映射

$$\begin{aligned}\phi:\mathbb{Z}&\longrightarrow\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle,\\ n&\longmapsto n+\langle a+b\mathrm{i}\rangle.\end{aligned}$$

首先, ϕ 为同态: 对任意 $m,n\in\mathbb{Z}$, 有

$$\phi(m+n)=m+n+\langle a+b\mathrm{i}\rangle=\phi(m)+\phi(n).$$

$$\phi(mn)=mn+\langle a+b\mathrm{i}\rangle=\phi(m)\phi(n).$$

其次, ϕ 为满射: 因 a^2+b^2 为素数, 故 $(a,b)=1$, 故存在整数 r,s 使得 $ra+sb=1$, 对任意 $m+n\mathrm{i}+\langle a+b\mathrm{i}\rangle\in\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle$, 取 $k=m+bnr-ans$, 则

$$m+n\mathrm{i}-k=n\mathrm{i}+ans-bnr=(a+b\mathrm{i})(ns+nr\mathrm{i})\in\langle a+b\mathrm{i}\rangle.$$

故

$$\phi(k)=k+\langle a+b\mathrm{i}\rangle=(m+n\mathrm{i})+\langle a+b\mathrm{i}\rangle.$$

又因

$$\begin{aligned}\ker\phi&=\{n\mid n=(a+b\mathrm{i})(c+d\mathrm{i})\}\\&=\{n\mid n=ac-bd+(ad+bc)\mathrm{i}\}\\&=\left\{-\frac{d}{b}(a^2+b^2)\mid b\text{ 整除 }d\right\}\\&=\langle a^2+b^2\rangle.\end{aligned}$$

所以 $\mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle\cong\mathbb{Z}_{a^2+b^2}$. □

注 在证明 ϕ 为满射时, 我们要寻找 k 使得

$$k+\langle a+b\mathrm{i}\rangle=m+n\mathrm{i}+\langle a+b\mathrm{i}\rangle.$$

即要求 $m+n\mathrm{i}-k\in\langle a+b\mathrm{i}\rangle$, 故

$$m+n\mathrm{i}-k=(a+b\mathrm{i})(p+q\mathrm{i})=(ap-bq)+(aq+bp)\mathrm{i}.$$

所以要求 $m-k=ap-bq$ 且 $n=aq+bp$, 我们的目标是利用已知值 a,b,r,s,m,n 表示 k. 注意

$$k=m-ap+bq.$$

于是需要想办法替换掉 p,q. 这时注意 $n=ap+bq=n\cdot 1=n(ra+sb)=anr+bns$, 故令 $p=nr$, $q=ns$ 即可.

4.3　2019 级研究生近世代数试题

1. 证明: p^2 阶群 G 是循环群, 其中 p 是素数.

证明: 见第 1.6 节: Sylow 定理. □

2. 证明有理数加法群的任一有限生成子群为循环群.

证明: 设 $\frac{m_1}{n_1},\dots,\frac{m_k}{n_k}$ 为群 $G<\mathbb{Q}$ 的生成元, 则对于 $\forall g\in G$, 有

$$g=a_1\frac{m_1}{n_1}+\cdots+a_k\frac{m_k}{n_k}=\frac{a_1m_1n_2\cdots n_k+\cdots+a_km_kn_1\cdots n_{k-1}}{n_1\cdots n_k},$$

其中 $a_1,\dots,a_k$ 为整数, 显然 G 为循环群 $\left\langle\frac{1}{n_1\cdots n_k}\right\rangle$ 的子群, 从而 G 为循环群. □

3. 设 G 为群, 证明 $G/Z(G)$ 同构于 G 的内在同构群 (内自同构群).

证明: 内自同构群为 $\mathrm{In}(G)=\{\sigma_g\in\mathrm{Aut}(G)\mid\sigma_g(x)=gxg^{-1},\forall x\in G\}$. 考虑映射 $\phi:G\to\mathrm{In}(G)$, $g\mapsto\sigma_g$. 显然 ϕ 为满射, 又由于

$$\sigma_{g_1g_2}(x)=g_1g_2xg_2^{-1}g_1^{-1}=\sigma_{g_1}\sigma_{g_2}(x),$$

故 $\phi(g_1g_2)=\sigma_{g_1g_2}=\sigma_{g_1}\sigma_{g_2}=\phi(g_1)\phi(g_2)$, 故 ϕ 为满同态. 并且 ϕ 的核为

$$\begin{aligned}\ker\phi&=\{g\in G\mid \sigma_g=\mathrm{id}\}\\&=\{g\in G\mid gxg^{-1}=x,\forall x\in G\}\\&=Z(G).\end{aligned}$$

从而由群同态基本定理, 得 $G/Z(G)\cong \mathrm{In}(G)$. □

4. 证明: $\mathbb{Z}[\mathrm{i}]/(3+\mathrm{i})\cong\mathbb{Z}_{10}$.

证明: 考虑映射 $\phi:\mathbb{Z}[\mathrm{i}]\to\mathbb{Z}_{10}$, $a+b\mathrm{i}\mapsto\overline{a-3b}$ 即可. □

5. 设 I,J 为交换幺环 R 的理想, 证明: 若 $I+J=R$, 则 $IJ=I\cap J$.

证明: 显然 $IJ\subset I\cap J$. 下证 $I\cap J\subset IJ$, 任取 $r\in I\cap J$, 由于 $I+J=R$, 故存在 $a\in I,b\in J$ 使得 $a+b=1$, 从而 $r=r(a+b)=ar+rb\in IJ$, 因此 $I\cap J\subset IJ$. □

6. 设 U 为 R 的理想, 证明 $r(U)=\{x\mid xu=0,\ \forall u\in U\}$ 为 R 的理想.

证明: 按定义直接验证. □

7. 证明对任意的域, 其中的有限乘法子群一定是循环群.

证明: 见 2018–2019 年期末测试题第三题. □

8. 构造一个有 9 个元素的域, 并给出它的加法和乘法.

解: 考虑 $\mathbb{Z}_3[x]/(x^2+1)$, 此为含有 9 个元素的域, 其中元素为

$$[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2].$$

加法为 $[f(x)+g(x)]=[f(x)+g(x)]$, 乘法为 $[f(x)][g(x)]=[f(x)g(x)]$. □

9. 设 E 是 F 的代数扩域, A 是 F 在 E 中的代数闭包, 证明 A 在 E 中是代数闭的.

证明: 即证 A 在 E 中的代数闭包即为 A 自身. 任取 $x\in E\setminus A$, 若 x 为 A 上的代数元, 注意到 A 为 F 的代数扩域, 故由第一题结论知 x 为 F 上的代数元, 这与 A 的定义相矛盾, 故 x 不是 A 上的代数元, 从而 A 在 E 中的代数闭包即为 A 自身. □

10. 设 K 为多项式 $(x^2+3)(x^2+5)$ 在 $\mathbb{Q}$ 上的分裂域, 求 $\mathrm{G}(K/\mathbb{Q})$, 找出所有子群并写出它们对应的中间域.

解: 第一步, 求出 K. 因为 $(x^2+3)(x^2+5)=0$ 的根为 $\pm\sqrt{3}\mathrm{i}, \pm\sqrt{5}\mathrm{i}$, 故 $K=\mathbb{Q}(\sqrt{3}\mathrm{i}, \sqrt{5}\mathrm{i})$.

第二步, 求 $[K:\mathbb{Q}]$.

$$[K:\mathbb{Q}]=[K:\mathbb{Q}(\sqrt{3}\mathrm{i})][\mathbb{Q}(\sqrt{3}\mathrm{i}):\mathbb{Q}]=4$$

且 K 作为 $\mathbb{Q}$ 上的向量空间具有一组基: $1, \sqrt{3}\mathrm{i}, \sqrt{5}\mathrm{i}, \sqrt{15}$.

第三步, 求 $\mathrm{G}(K/\mathbb{Q})$. 任取 $\sigma \in \mathrm{G}(K/\mathbb{Q})$, σ 将 $\sqrt{3}\mathrm{i}$ 映为 $\pm\sqrt{3}\mathrm{i}$, 将 $\sqrt{5}\mathrm{i}$ 映为 $\pm\sqrt{5}\mathrm{i}$, 故取 $\sigma, \tau \in \mathrm{G}(K/\mathbb{Q})$ 满足

$$\sigma: \begin{cases} \sqrt{3}\mathrm{i} \mapsto -\sqrt{3}\mathrm{i} \\ \sqrt{5}\mathrm{i} \mapsto \sqrt{5}\mathrm{i} \end{cases} \qquad \tau: \begin{cases} \sqrt{3}\mathrm{i} \mapsto \sqrt{3}\mathrm{i} \\ \sqrt{5}\mathrm{i} \mapsto -\sqrt{5}\mathrm{i} \end{cases}$$

则 $\mathrm{G}(K/\mathbb{Q})=\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$. 并且 $\mathrm{G}(K/\mathbb{Q})$ 的子群和对应的中间域分别为:

$G_1=\{\mathrm{id}\}$, $K^{G_1}=K$;

$G_2=\{\mathrm{id}, \sigma\}$, $K^{G_2}=\mathbb{Q}(\sqrt{5}\mathrm{i})$;

$G_3=\{\mathrm{id}, \tau\}$, $K^{G_3}=\mathbb{Q}(\sqrt{3}\mathrm{i})$;

$G_4=\{\mathrm{id}, \sigma\tau\}$, $K^{G_4}=\mathbb{Q}(\sqrt{15})$;

$G_5=\mathrm{G}(K/\mathbb{Q})$, $K^{G_5}=\mathbb{Q}$. □

4.4　2020 级研究生近世代数试题

1. 设 M 和 N 分别是群 G 的正规子群, 且 $M\cap N=\{1\}$, 证明: 对任意 $a\in M, b\in N$, 有 $ab=ba$.

证明: 证明 $a^{-1}b^{-1}ab\in M\cap N=\{1\}$ 即可. □

2. 设 p 是一个素数, $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 有多少个 p^2 阶子群?

证明: 原题出自近世代数三百题第 87 页, 答案为 p^2+p+1.

因 $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 中元的阶只可能为 $1,p,p^2,p^3$, 故我们分别求出阶为 $1,p,p^2,p^3$ 的元素个数. 任取 $(a,b)\in\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$, 有

$$|(a,b)|=\operatorname{lcm}(|a|,|b|).$$

(1) 阶为 1 的元只有单位元 $(1,1)$;

(2) 阶为 p 的元分为三类:

- $|a|=1,|b|=p$, 共有 $1\times(p-1)=p-1$ 个
- $|a|=p,|b|=1$, 共有 $(p-1)\times 1=p-1$ 个
- $|a|=p,|b|=p$, 共有 $(p-1)\times(p-1)=(p-1)^2$ 个

故有 p^2-1 个 p 阶元.

(3) 阶为 p^3 的元: 设 $|(a,b)|=p^3$, 则必需 $|a|=p^3$, 而 b 可任意选择, 在 $\mathbb{Z}_{p^3}$ 中有 $\varphi(p^3)=p^2(p-1)$ 个 p^3 阶元, 因此 $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 中 p^3 阶元共有 $p^2(p-1)\cdot p^2=p^4(p-1)$ 个.

(4) 阶为 p^2 的元: 由群的阶减去上述三类之和, 即有

$$p^5-1-(p^2-1)-p^4(p-1)=p^2(p^2-1)$$

个 p^2 阶元.

设 H 为 $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 的 p^2 阶子群, 由有限交换群的结构定理知 $H\cong\mathbb{Z}_{p^2}$ 或 $H\cong\mathbb{Z}_p\oplus\mathbb{Z}_p$.

当 $H\cong\mathbb{Z}_{p^2}$ 时, H 由 p^2 阶元生成, 但每个 p^2 阶循环群中有 $\varphi(p^2)=p(p-1)$ 个生成元, 故共有

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

个 p^2 阶循环群.

当 $H\cong\mathbb{Z}_p\oplus\mathbb{Z}_p$ 时, H 由 p^2-1 个 p 阶元和一个单位元组成, 故 H 恰好包含 $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 中全部 p 阶元, 所以这样的 H 只有一个.

综上可得, $\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$ 共有 p^2+p+1 个 p^2 阶子群. $\square$

3. 设 D 为整环, m 和 n 为互素的正整数, $a, b \in D$. 如果 $a^m = b^m$, $a^n = b^n$, 求证 $a = b$.

证明: 由于 $(m, n) = 1$, 故存在整数 r, s 使得 $rm + sn = 1$. 不妨设 $r > 0$, $s < 0$, 则 $rm = 1 - sn > 0$. 由于 $a^m = b^m$, 故 $a^{rm} = b^{rm}$, 即 $a^{1-sn} = b^{1-sn}$, 也即 $a \cdot a^{-sn} = b \cdot b^{-sn}$. 由于 $a^n = b^n$, 故 $a^{-sn} = b^{-sn} =: c$, 则 $ac = bc \Rightarrow (a-b)c = 0$. 若 $c = 0$, 则 $a = b = 0$; 若 $c \neq 0$, 则 $a - b = 0 \Rightarrow a = b$. □

4. 设 $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, 且 $a^2 + b^2 = p$, p 为素数, 证明 $\mathbb{Z}[\mathrm{i}]/\langle a + b\mathrm{i}\rangle \cong \mathbb{Z}_p$.

证明: 见 2018–2019 年最后一题. □

5. 求多项式 $x^4 - 3x$ 在 $\mathbb{Q}$ 上的分裂域 (在 $\mathbb{Q}$ 上的) Galois 群的全部子群以及子群的不动域.

证明: 第一步, 求分裂域. 由 $x^4 - 3x = 0$ 得 $x = 0, \sqrt[3]{3}, \sqrt[3]{3}\omega, \sqrt[3]{3}\omega^2$, 其中 ω 为三次本原单位根. 因此 $x^4 - 3x$ 在 $\mathbb{Q}$ 上的分裂域为 $E = \mathbb{Q}(\sqrt[3]{3}, \omega)$.

第二步, 计算 $[E : \mathbb{Q}]$.

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2 \times 3 = 6.$$

且 E 在 $\mathbb{Q}$ 上的一组基为 $1, \sqrt[3]{3}, \sqrt[3]{9}, \omega, \sqrt[3]{3}\omega, \sqrt[3]{9}\omega$.

第三步, 求 $\mathrm{G}(E/\mathbb{Q})$. 任取 $\sigma \in \mathrm{G}(E/\mathbb{Q})$, 由于 σ 将 ω 映为 ω 或 ω^2, 将 $\sqrt[3]{3}$ 映为 $\sqrt[3]{3}$、$\sqrt[3]{3}\omega$ 或 $\sqrt[3]{3}\omega^2$, 故可取 $\sigma, \tau \in \mathrm{G}(E/\mathbb{Q})$ 满足条件

$$\sigma : \begin{cases} \omega \mapsto \omega \\ \sqrt[3]{3} \mapsto \sqrt[3]{3}\omega \end{cases} \qquad \tau : \begin{cases} \omega \mapsto \omega^2 \\ \sqrt[3]{3} \mapsto \sqrt[3]{3} \end{cases}$$

则 $\mathrm{G}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, Galois 群中各自同态关于根的置换见表 4.1. 相应的子群以及固定域分别为:

$G_1 = \{\mathrm{id}\}$, $E^{G_1} = E$;

$G_2 = \{\mathrm{id}, \sigma, \sigma^2\}$, $E^{G_2} = \mathbb{Q}(\omega)$;

$G_3 = \{\mathrm{id}, \tau\}$, $E^{G_3} = \mathbb{Q}(\sqrt[3]{3})$;

$G_4 = \{\mathrm{id}, \sigma\tau\}$, $E^{G_4} = \mathbb{Q}(\sqrt[3]{3}\omega^2)$;

表 4.1: $\mathrm{G}(E/\mathbb{Q})$ 关于根的置换

	$\sqrt[3]{3}$	$\sqrt[3]{3}\omega$	$\sqrt[3]{3}\omega^2$	ω	ω^2
1	$\sqrt[3]{3}$	$\sqrt[3]{3}\omega$	$\sqrt[3]{3}\omega^2$	ω	ω^2
σ	$\sqrt[3]{3}\omega$	$\sqrt[3]{3}\omega^2$	$\sqrt[3]{3}$	ω	ω^2
σ^2	$\sqrt[3]{3}\omega^2$	$\sqrt[3]{3}$	$\sqrt[3]{3}\omega$	ω	ω^2
τ	$\sqrt[3]{3}$	$\sqrt[3]{3}\omega^2$	$\sqrt[3]{3}\omega$	ω^2	ω
$\sigma\tau$	$\sqrt[3]{3}\omega$	$\sqrt[3]{3}$	$\sqrt[3]{3}\omega^2$	ω^2	ω
$\sigma^2\tau$	$\sqrt[3]{3}\omega^2$	$\sqrt[3]{3}\omega$	$\sqrt[3]{3}$	ω^2	ω

$G_5 = \{\mathrm{id}, \sigma^2\tau\}$, $E^{G_5} = \mathbb{Q}(\sqrt[3]{3}\omega)$;

$G_6 = G$, $E^{G_6} = \mathbb{Q}$. □

6. 设 R 为交换幺环, 若对任意 $a \in R$, a 或 $1-a$ 可逆, 证明: $N = \{a \in R \mid a$ 为不可逆元$\}$ 为 R 的理想.

证明: 任取 $a_1, a_2 \in N$, 假设 $a_1 - a_2$ 可逆, 则存在 $b \in R$, 使得 $(a_1 - a_2)b = 1$, 即 $a_1 b = 1 + a_2 b$. 由于 a_2 不可逆, 故 $-a_2 b$ 不可逆, 故 $1-(-a_2 b) = 1+a_2 b$ 可逆, 从而 $a_1 b$ 可逆, 由 $a_1 b$ 可逆可得 a_1 可逆, 矛盾. 因此 $a_1 - a_2 \in N$.

任取 $a \in N$, $r \in R$, 由于 a 不可逆, 故 ar 不可逆, 故 $ar \in N$.

因此 N 为 R 的理想. □

7. 证明代数闭域为无限域.

证明: 2018–2019 第七题. □

8. 证明: 若 $f(x)$ 为 $\mathbb{R}$ 上的不可约多项式, 则其次数为 1 或 2.

证明: 设 $f(x) \in \mathbb{R}[x]$ 为不可约多项式, 由代数学基本定理知 $f(x) \in \mathbb{C}[x]$ 有根 $z_0 \in \mathbb{C}$.

若 $z_0 \in \mathbb{R}$, 则 $f(x) = (x - z_0)g(x)$, $g(x) \in \mathbb{R}[x]$. 由于 $f(x)$ 不可约, 故 $g(x)$ 必为非零常数且 $\deg f(x) = 1$.

若 $z_0 \notin \mathbb{R}$, 则 $f(\overline{z_0}) = \overline{f(z_0)} = 0$, 因此在 $\mathbb{C}[x]$ 中 $f(x)$ 可被 $x - z_0$ 和 $x - \overline{z_0}$ 整除, 又 $1 \cdot (x - z_0) + (-1)(x - \overline{z_0}) = \overline{z_0} - z_0 = -2\,\mathrm{Im}(z_0)\mathrm{i} \neq 0$ 为 $\mathbb{C}[x]$ 中单位, 故 $f(x)$ 可以被 $(x - z_0)(x - \overline{z_0}) = x^2 - 2\,\mathrm{Re}(z_0)x + |z_0|^2 \in \mathbb{R}[x]$ 整

除, 即 $f(x) = (x^2 - 2\operatorname{Re}(z_0)x + |z_0|^2)g(x)$, 其中 $g(x) \in \mathbb{R}[x]$ 必为非零常数且 $\deg f(x) = 2$. □

9. 设 F 为域, $E = F(a)$ 为 F 的单扩域, $b \in E - F$. 证明: a 在 $F(b)$ 上为代数的.

证明: 因 $b \in E - F$, 故存在 $g(x), h(x) \in F[x]$, 使得 $b = \frac{g(a)}{h(a)}$, 故 $g(a) - bh(a) = 0$, 令 $f(x) = g(x) - bh(x) \in F(b)[x]$, 则 $f(a) = 0$, 所以 a 在 $F(b)$ 上为代数的. □

10. 设域 F 的特征为 0, E 是 F 的扩域, 并且 $[E : F] = 4$. 证明存在一个满足条件 $F \subset I \subset E$ 的 F 的二次扩域 I 的充要条件是: $E = F(\alpha)$, 而 α 在 F 上的极小多项式是 $x^4 + ax^2 + b$.

证明: ($\Rightarrow$) 第一步, 首先证明存在 $\alpha \in E \setminus I$, 使得 α 在 I 上的极小多项式为 $x^2 - a$, $a \in I$. 对任意 $\alpha_1 \in E \setminus I$, 设 α_1 的极小多项式为 $x^2 + k_1x + k_0$, 设此极小多项式的另一个根为 α_2, 则由韦达定理知 $\alpha_1 + \alpha_2 = -k_1 \in I$. 记 $\alpha = \alpha_1 - \alpha_2$, 断言 $\alpha \notin I$, 否则, 由 $\alpha_1 + \alpha_2 \in I$ 且 $\alpha_1 - \alpha_2 \in I$ 可推知 $\alpha_1 \in I$, 矛盾. 于是 α 在 I 上的极小多项式为二次多项式. 令 $f(x) = x^2 - a \in I[x]$, 其中 $a = k_1^2 - 4k_0$, 则

$$f(\alpha) = (\alpha_1 - \alpha_2)^2 - (k_1^2 - 4k_0) = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 - (k_1^2 - 4k_0) = 0,$$

所以 α 在 I 上的极小多项式即为 $f(x) = x^2 - a \in I[x]$.

第二步, 若 $a \in I \setminus F$, 设 a 在 F 上的极小多项式为 $x^2 + \ell_1x + \ell_0$, 令 $g(x) = x^4 + \ell_1x^2 + \ell_0$, 则由 $\alpha^2 = a$ 得

$$g(\alpha) = \alpha^4 + \ell_1\alpha^2 + \ell_0 = a^2 + \ell_1a + \ell_0 = 0.$$

下证 $g(x)$ 是 α 在 F 上的极小多项式. 实际上, 也就是要证明扩张次数 $[F(\alpha) : F] = 4$, 由于

$$E = I(\alpha) \supset F(\alpha) \supset F(\alpha^2) = F(a) = I \supset F.$$

故

$$4 = [E : F] = [E : F(\alpha)][F(\alpha) : I][I : F],$$

结合 $[F(\alpha) : I] > 1$ 和 $[I : F] = 2$ 即得 $[F(\alpha) : F] = 4$. 所以此时 $g(x) = x^4 + \ell_1 x^2 + \ell_0$ 就是 α 在 F 上的极小多项式.

若 $a \in F$, 则 $F(\alpha^2) = F(a) = F$, 故 $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)] \leq 2$, 而 $\alpha \notin F$, 故 $[F(\alpha) : F] = 2$, 因此此时 $g(x)$ 必然不是 α 在 F 上的极小多项式. 类似于第一步知, 存在 $\beta \in I \setminus F$, 使得 β 在 F 上的极小多项式为 $x^2 - b \in F[x]$, 令 $\gamma = \alpha + \beta$, 则

$$\gamma^4 = (a+b)^2 + 4ab + 2(a+b) \cdot 2\alpha\beta,$$

且

$$\gamma^2 = (\alpha+\beta)^2 = a + b + 2\alpha\beta.$$

结合上面两式得 $\gamma^4 - 2(a+b)\gamma^2 + (a-b)^2$. 令 $h(x) = x^4 - 2(a+b)x^2 + (a-b)^2 \in F[x]$, 则 $h(\gamma) = 0$, 下证 $h(x)$ 为 γ 在 F 上的极小多项式. 即需证 $[F(\gamma) : F] = [F(\alpha+\beta) : F] = 4$. 事实上, 由于 $\alpha + \beta \in F(\alpha+\beta)$, 故 $\frac{a-b}{\alpha+\beta} = \frac{\alpha^2-\beta^2}{\alpha+\beta} = \alpha - \beta \in F(\alpha+\beta)$, 因此 $\alpha, \beta \in F(\alpha+\beta) \Rightarrow F(\alpha+\beta) = F(\alpha, \beta) = E$, 故 $[F(\alpha+\beta) : F] = [E : F] = 4$. $\square$

4.5　2021 级近世代数期末试题

1. 设交换群 G 中元素 a 及 b 的阶分别为 m, n, 证明或否定 ab 的阶为 m, n 的最小公倍数.

2. 设 S 为复平面中的单位圆, 关于乘法构成群. 证明 $\mathbb{R}/\mathbb{Z} \cong S$.

3. 给出 63 阶交换群的所有同构类.

4. 求出群 $\mathbb{Z}_{12}$ 的自同构群.

5. 证明: 若一个整环只有有限多个理想, 则它是一个域.

6. 证明: $\mathbb{Q}[x, y, z]$ 中的理想 $(x^2 - 2, y^2 + 1, z)$ 为真理想.

7. 设 I 为主理想环, a, b 为 I 中元素. 证明 $(a) + (b) = I$ 当且仅当 $(a, b) = 1$ (即 a, b 互素).

8. 设 K 为域 F 的扩域, E 为域 K 的扩域, 证明 E 为 F 的代数扩域当且仅当 E 为 K 的代数扩域且 K 为 F 的代数扩域.

9. 设 $p(x)$ 为特征为 0 的域 F 上的不可约多项式且它有一根可以用根式表示, 则它的所有根都可以用根式表示.

10. 求 $(x^2+3)(x^3-2)$ 在 $\mathbb{Q}$ 上的分裂域 K, 并求 $\mathrm{G}(K/\mathbb{Q})$, 找出其所有子群并写出它们所对应的中间域.