群与 Galois 理论
作业 1

陈宏泰

清华大学数学科学系

cht24@mails.tsinghua.edu.cn

2025 年 10 月 13 日

目录

A. 乘积结构

A1)

证明：性质 1：结合律, $\forall g_1, g_2, g_3 \in G_1, h_1, h_2, h_3 \in G_2$, 有

$$\begin{aligned}
&((g_1, g_2) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1 \cdot_1 g_2, h_1 \cdot_2 h_2) \cdot (g_3, h_3) \\
=& ((g_1 \cdot_1 g_2) \cdot_1 g_3, (h_1 \cdot_2 h_2) \cdot_2 h_3) = (g_1 \cdot_1 (g_2 \cdot_1 g_3), h_1 \cdot_2 (h_2 \cdot_2 h_3)) \\
=& (g_1, h_1) \cdot (g_2 \cdot_1 g_3, h_2 \cdot_2 h_3) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)).
\end{aligned}$$

性质 2：单位元, 设 $1_1, 1_2$ 分别为 G_1, G_2 的单位元, 则 $\forall g \in G_1, h \in G_2$, 有

$$\begin{aligned}
(g, h) \cdot (1_1, 1_2) &= (g \cdot_1 1_1, h \cdot_2 1_2) = (g, h), \\
(1_1, 1_2) \cdot (g, h) &= (1_1 \cdot_1 g, 1_2 \cdot_2 h) = (g, h).
\end{aligned}$$

性质 3：逆元, $\forall g \in G_1, h \in G_2$, 设 g^{-1}, h^{-1} 分别为 g, h 的逆元, 则

$$\begin{aligned}
(g, h) \cdot (g^{-1}, h^{-1}) &= (g \cdot_1 g^{-1}, h \cdot_2 h^{-1}) = (1_1, 1_2), \\
(g^{-1}, h^{-1}) \cdot (g, h) &= (g^{-1} \cdot_1 g, h^{-1} \cdot_2 h) = (1_1, 1_2).
\end{aligned}$$

综上, 在以上乘法下, $G_1 \times G_2$ 构成一个群, 且其单位元是 $(1_1, 1_2)$. □

A2)

证明： $\forall (g_1, h_1), (g_2, h_2) \in G_1 \times G_2$, 有

$$\begin{aligned}
&\pi_1(((g_1, h_1) \cdot (g_2, h_2))) = \pi((g_1 \cdot_1 g_2, h_1 \cdot_2 h_2)) \\
=& g_1 \cdot_1 g_2 = \pi_1((g_1, h_1)) \cdot_1 \pi_1((g_2, h_2)), \\
&\pi_2(((g_1, h_1) \cdot (g_2, h_2))) = \pi((g_1 \cdot_1 g_2, h_1 \cdot_2 h_2)) \\
=& h_1 \cdot_2 h_2 = \pi_2((g_1, h_1)) \cdot_2 \pi_2((g_2, h_2)).
\end{aligned}$$

故 π_1, π_2 为群同态. 而显然 $\ker(\pi_1) = \{(1_1, h) \mid h \in G_2\}, \ker(\pi_2) = \{(g, 1_2) \mid g \in G_2\}$. □

A3)

证明：存在性：令 $G = G_1 \times G_2$, $p_1 = \pi_1$, $p_2 = \pi_2$, 其中 π_1, π_2 为 A2) 中的投影映射. 则对任意的群 H 以及任意的群同态 $\varphi_i : H \to G_i$ $(i = 1, 2)$ 存在

$$\psi : H \to G, \ h \mapsto (\varphi_1(h), \varphi_2(h)),$$

使得 $p_i \circ \psi = \varphi_i$ $(i = 1, 2)$. 若另外存在 ψ' 也满足上述条件, 设 $\psi'(h) = (g_1, g_2)$ 则对任意 $h \in H$, 有 $p_i(\psi'(h)) = \varphi_i(h) = p_i(\psi(h))$ $(i = 1, 2)$, 所以 $g_1 = \varphi_1(h), g_2 = \varphi_2(h)$, 即 $\psi' = \psi$. ψ 唯一性得证. 故而 G, p_1, p_2 满足题设要求, 存在性得证.

唯一性：由存在性已知 $G_1 \times G_2, \pi_1, \pi_2$ 满足题设要求. 设另外存在 G, p_1, p_2 也满足题设要求.

先证明 $G \simeq G_1 \times G_2$:

考虑 $H = G_1 \times G_2$, $\varphi_i = \pi_i$ $(i = 1, 2)$, 则存在唯一的 $\psi : G_1 \times G_2 \to G$, 使得 $p_i \circ \psi = \pi_i$ $(i = 1, 2)$.

另一方面, 考虑 $H = G$, $\varphi_i = p_i$ $(i = 1, 2)$, 则存在唯一的 $\theta : G \to G_1 \times G_2$, 使得 $\pi_i \circ \theta = p_i$ $(i = 1, 2)$. (存在性已证)

考虑复合映射 $\theta \circ \psi : G_1 \times G_2 \to G_1 \times G_2$. 有

$$\pi_i \circ (\theta \circ \psi) = (\pi_i \circ \theta) \circ \psi = p_i \circ \psi = \pi_i.$$

但恒等映射 $\mathrm{id}_{G_1 \times G_2}$ 也满足 $\pi_i \circ \mathrm{id}_{G_1 \times G_2} = \pi_i$, 由 $G_1 \times G_2$ 的泛性质, $\theta \circ \psi = id_{G_1 \times G_2}$.

同理, 考虑复合映射 $\psi \circ \theta : G \to G$. 有

$$p_i \circ (\psi \circ \theta) = (p_i \circ \psi) \circ \theta = \pi_1 \circ \theta = p_i.$$

由 G 的泛性质, $\psi \circ \theta = id_G$.

因此, ψ 和 θ 是互逆的同构, 即 $G \simeq G_1 \times G_2$.

再说明 p_i 在同构意义下唯一:

设 $f : G \to G_1 \times G_2$ 为同构映射, 则 $p_i = \pi_i \circ f$. 则 p_i 本质上就是 G 到 G_1, G_2 的投影映射.

综上, G, p_1, p_2 在同构意义下唯一. 且 $G = G_1 \times G_2$, 特别地, 我们有如下集合的同构:

$$\mathrm{Hom}(H, G_1 \times G_2) \simeq \mathrm{Hom}(H, G_1) \times \mathrm{Hom}(H, G_2), \ \psi \mapsto (\pi_1 \circ \psi, \pi_2 \circ \psi).$$

□

A4)

证明：由 A3) 对泛性质的证明，只需要证明

$$\varphi_i : \mathbb{Z}/n_1 n_2 \mathbb{Z} \to \mathbb{Z}/n_i \mathbb{Z}, \quad \bar{k} \mapsto k \pmod{n_i}, \quad i = 1, 2$$

是群同态即可. 先证明映射是良定义的：若 $\bar{x} = \bar{y}$, 即 $x \equiv y \pmod{n_1 n_2}$，则 $n_1 n_2 \mid (x - y)$。由于 $n_1 \mid n_1 n_2$ 且 $n_2 \mid n_1 n_2$，有：

$$n_1 \mid (x - y), \ n_2 \mid (x - y)$$

因此 $x \equiv y \pmod{n_1}$ 且 $x \equiv y \pmod{n_2}$，故 φ 是良定义的.

再证明映射保持群运算: $\forall \bar{a}, \bar{b} \in \mathbb{Z}/n_1 n_2 \mathbb{Z}$, 有 $\bar{a} + \bar{b} = \overline{a + b}$, 而

$$\varphi_i(\bar{a} + \bar{b}) = \varphi_i(\overline{a + b}) = (a + b)(\mathrm{mod} n_i) = a(\mathrm{mod} n_i) + b(\mathrm{mod} n_i) = \varphi_i(\bar{a}) + \varphi_i(\bar{b}).$$

故 φ_i $(i=1,2)$ 为群同态.

由 A3) 的结论可知, 存在唯一的

$$\psi : \mathbb{Z}/n_1n_2\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ \bar{k} \mapsto (k(\mathrm{mod}\ n_1), k(\mathrm{mod}\ n_2)),$$

使得 $\pi_i \circ \psi = \varphi_i$ $(i=1,2)$. 显然 ψ 为群同态. 而 $|\mathbb{Z}/n_1n_2\mathbb{Z}| = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}| = n_1n_2$, 只需证明 ψ 为单射即可. 设 $\bar{a} \in \ker(\psi)$, 有

$$\pi_i \circ \psi(\bar{a}) = \pi_i(0) = 0 = a(\mathrm{mod}\ n_i) = \varphi_i(\bar{a}),\ i=1,2,$$

则 $\bar{a}=\bar{0}$, 即 $\ker(\psi)=\bar{0}$, ψ 为单射. 因此, ψ 为同构映射, 即

$$\mathbb{Z}/n_1n_2\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

□

A5)

证明: 设有限的循环群 G 的阶为 n, 上课已经证明 $G \simeq \mathbb{Z}/n\mathbb{Z}$.

设 $|C_1| = n_1, |C_2| = n_2$, 则 $C_1 \simeq \mathbb{Z}/n_1\mathbb{Z}$, $C_2 \simeq \mathbb{Z}/n_2\mathbb{Z}$. 由 A4) 可知,

$$C_1 \times C_2 \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \simeq \mathbb{Z}/n_1n_2\mathbb{Z}.$$

故 $C_1 \times C_2$ 为循环群, 且其阶为 n_1n_2. □

A6)

证明: 性质 1: $(A_1 \times A_2, +)$ 为交换群, 其中,$(0_{_1}, 0_{_2})$ 为单位元.

由 A1) 知 $(A_1 \times A_2, +)$ 为群,$(0_{_1}, 0_{_2})$ 为单位元. 而 $\forall (a_1,a_2),(b_1,b_2) \in A_1 \times A_2$, 有

$$(a_1,a_2)+(b_1,b_2) = (a_1 +_{_1} b_1, a_2 +_{_2} b_2) = (b_1 +_{_1} a_1, b_2 +_{_2} a_2) = (b_1,b_2)+(a_1,a_2),$$

故 $(A_1 \times A_2, +)$ 为交换群.

性质 2:

- 乘法满足结合律, $\forall g_1,g_2,g_3 \in A_1, h_1,h_2,h_3 \in A_2$, 有

$$\begin{aligned}
((g_1,g_2)\cdot(g_2,h_2))\cdot(g_3,h_3) &= (g_1 \cdot_{_1} g_2, h_1 \cdot_{_2} h_2)\cdot(g_3,h_3) \\
&= ((g_1 \cdot_{_1} g_2) \cdot_{_1} g_3, (h_1 \cdot_{_2} h_2) \cdot_{_2} h_3) = (g_1 \cdot_{_1} (g_2 \cdot_{_1} g_3), h_1 \cdot_{_2} (h_2 \cdot_{_2} h_3)) \\
&= (g_1,h_1)\cdot(g_2 \cdot_{_1} g_3, h_2 \cdot_{_2} h_3) = (g_1,h_1)\cdot((g_2,h_2)\cdot(g_3,h_3)).
\end{aligned}$$

- $(1_{_1}, 1_{_2})$ 是乘法单位元. $\forall g \in A_1, h \in A_2$, 有

$$\begin{aligned}
(g,h)\cdot(1_{_1},1_{_2}) &= (g \cdot_{_1} 1_{_1}, h \cdot_{_2} 1_{_2}) = (g,h), \\
(1_{_1},1_{_2})\cdot(g,h) &= (1_{_1} \cdot_{_1} g, 1_{_2} \cdot_{_2} h) = (g,h).
\end{aligned}$$

性质 3: 乘法分配律成立, $\forall (a_1,a_2),(b_1,b_2),(c_1,c_2)\in A_1\times A_2$, 有

$$\begin{aligned}
&((a_1,a_2)+(b_1,b_2))\cdot(c_1,c_2)=(a_1+_{_1}b_1,a_2+_{_2}b_2)\cdot(c_1,c_2)\\
=&((a_1+_{_1}b_1)\cdot_{_1}c_1,(a_2+_{_2}b_2)\cdot_{_2}c_2)\\
=&(a_1\cdot_{_1}c_1+_{_1}b_1\cdot_{_1}c_1,a_2\cdot_{_2}c_2+_{_2}b_2\cdot_{_2}c_2)\\
=&(a_1\cdot_{_1}c_1,a_2\cdot_{_2}c_2)+(b_1\cdot_{_1}c_1,b_2\cdot_{_2}c_2)\\
=&(a_1,a_2)\cdot(c_1,c_2)+(b_1,b_2)\cdot(c_1,c_2),\\
&(a_1,a_2)\cdot((b_1,b_2)+(c_1,c_2))=(a_1,a_2)\cdot(b_1+_{_1}c_1,b_2+_{_2}c_2)\\
=&(a_1\cdot_{_1}(b_1+_{_1}c_1),a_2\cdot_{_2}(b_2+_{_2}c_2))\\
=&(a_1\cdot_{_1}b_1+_{_1}a_1\cdot_{_1}c_1,a_2\cdot_{_2}b_2+_{_2}a_2\cdot_{_2}c_2)\\
=&(a_1\cdot_{_1}b_1,a_2\cdot_{_2}b_2)+(a_1\cdot_{_1}c_1,a_2\cdot_{_2}c_2)\\
=&(a_1,a_2)\cdot(b_1,b_2)+(a_1,a_2)\cdot(c_1,c_2).
\end{aligned}$$

综上, $A_1\times A_2$ 在以上运算下是环.

环同态的证明: $\forall (g_1,h_1),(g_2,h_2)\in A_1\times A_2$, 有

$$\begin{aligned}
&\pi_1(((g_1,h_1)+(g_2,h_2)))=\pi((g_1+_{_1}g_2,h_1+_{_2}h_2))\\
=&g_1+_{_1}g_2=\pi_1((g_1,h_1))+_{_1}\pi_1((g_2,h_2)),\\
&\pi_1(((g_1,h_1)\cdot(g_2,h_2)))=\pi((g_1\cdot_{_1}g_2,h_1\cdot_{_2}h_2))\\
=&g_1\cdot_{_1}g_2=\pi_1((g_1,h_1))\cdot_{_1}\pi_1((g_2,h_2)),
\end{aligned}$$

故 π_1 为环同态. 同理, π_2 也为环同态. □

A7)

证明：存在性：令 $A=A_1\times A_2$, $p_1=\pi_1$, $p_2=\pi_2$, 其中 π_1,π_2 为 A6) 中的投影映射.
则对任意的环 B 以及任意的环同态 $\varphi_i: B\to A_i$ $(i=1,2)$ 存在

$$\psi: B\to A,\ b\mapsto(\varphi_1(b),\varphi_2(b)),$$

使得 $p_i\circ\psi=\varphi_i$ $(i=1,2)$. 若另外存在 ψ' 也满足上述条件, 设 $\psi'(b)=(a_1,a_2)$ 则对任意 $b\in B$, 有 $p_i(\psi'(b))=\varphi_i(b)=p_i(\psi(b))$ $(i=1,2)$, 所以 $a_1=\varphi_1(b),a_2=\varphi_2(b)$, 即 $\psi'=\psi$.
ψ 唯一性得证. 故而 A,p_1,p_2 满足题设要求, 存在性得证.

唯一性：由存在性已知 $A_1\times A_2,\pi_1,\pi_2$ 满足题设要求. 设另外存在 A,p_1,p_2 也满足题设要求.

先证明 $A\simeq A_1\times A_2$:

考虑 $B=A_1\times A_2$, $\varphi_i=\pi_i$ $(i=1,2)$, 则存在唯一的 $\psi: A_1\times A_2\to A$, 使得 $p_i\circ\psi=\pi_i$ $(i=1,2)$.

另一方面, 考虑 $B = A$, $\varphi_i = p_i$ $(i = 1, 2)$, 则存在唯一的 $\theta : A \to A_1 \times A_2$, 使得 $\pi_i \circ \theta = p_i$ $(i = 1, 2)$. (存在性已证)

考虑复合映射 $\theta \circ \psi : A_1 \times A_2 \to A_1 \times A_2$. 有

$$\pi_i \circ (\theta \circ \psi) = (\pi_i \circ \theta) \circ \psi = p_i \circ \psi = \pi_i.$$

但恒等映射 $\mathrm{id}_{A_1 \times A_2}$ 也满足 $\pi_i \circ \mathrm{id}_{A_1 \times A_2} = \pi_i$, 由 $A_1 \times A_2$ 的泛性质, $\theta \circ \psi = id_{A_1 \times A_2}$.

同理, 考虑复合映射 $\psi \circ \theta : A \to A$. 有

$$p_i \circ (\psi \circ \theta) = (p_i \circ \psi) \circ \theta = \pi_1 \circ \theta = p_i.$$

由 A 的泛性质, $\psi \circ \theta = id_A$.

因此, ψ 和 θ 是互逆的同构, 即 $A \simeq A_1 \times A_2$.

再说明 p_i 在同构意义下唯一:

设 $f : A \to A_1 \times A_2$ 为同构映射, 则 $p_i = \pi_i \circ f$. 则 p_i 本质上就是 A 到 A_1, A_2 的投影映射.

综上, A, p_1, p_2 在同构意义下唯一. 且 $A \simeq A_1 \times A_2$. □

A8)

证明：由 A7) 对泛性质的证明，只需要证明

$$\varphi_i : \mathbb{Z}/n_1n_2\mathbb{Z} \to \mathbb{Z}/n_i\mathbb{Z}, \quad \bar{k} \mapsto k \,(\mathrm{mod}\ n_i)\,, \quad i = 1, 2$$

是环同态即可. A4) 中已经证明了 φ_i 是良定义的且为 (加法) 群同态, 只需再验证映射保持乘法和乘法单位元即可. $\forall \bar{a}, \bar{b} \in \mathbb{Z}/n_1n_2\mathbb{Z}$, 有 $\bar{a} \cdot \bar{b} = \overline{ab}$, 而

$$\varphi_i(\bar{a} \cdot \bar{b}) = \varphi_i(\overline{ab}) = ab(\mathrm{mod}\ n_i) = (a(\mathrm{mod}\ n_i)) \cdot (b(\mathrm{mod}\ n_i)) = \varphi_i(\bar{a}) \cdot \varphi_i(\bar{b}).$$

乘法单位元 $\bar{1} \in \mathbb{Z}/n_1n_2\mathbb{Z}$, 由中国剩余定理,

$$x \equiv 1 \pmod{n_1n_2} \Leftrightarrow x \equiv 1 \pmod{n_1} \quad \text{且} \quad x \equiv 1 \pmod{n_2}$$

故 $\varphi_i(\bar{1}) = 1(\mathrm{mod}\ n_i)$ 为 $\mathbb{Z}/n_i\mathbb{Z}$ 的乘法单位元. 从而 φ_i 为环同态.

由 A7) 的结论可知, 存在唯一的

$$\psi : \mathbb{Z}/n_1n_2\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ \bar{k} \mapsto (k(\mathrm{mod}\ n_1), k(\mathrm{mod}\ n_2)),$$

使得 $\pi_i \circ \psi = \varphi_i$ $(i = 1, 2)$, 显然 ψ 为环同态. 而 $|\mathbb{Z}/n_1n_2\mathbb{Z}| = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}| = n_1n_2$, 只需证明 ψ 为单射即可. 设 $\bar{a} \in \ker(\psi)$, 有

$$\pi_i \circ \psi(\bar{a}) = \pi_i(0) = 0 = a(\mathrm{mod}\ n_i) = \varphi_i(\bar{a}),\ i = 1, 2,$$

则 $\bar{a}=\bar{0}$, 即 $\ker(\psi)=\bar{0}$, ψ 为单射. 因此, ψ 为同构映射, 即

$$\mathbb{Z}/n_1n_2\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

□

A9)

证明：由 A7) 对泛性质的证明，只需要证明

$$\varphi_1 : (A \times_{\text{ring}} B)^\times \to A^\times,\ (a,b) \mapsto a$$
$$\varphi_2 : (A \times_{\text{ring}} B)^\times \to B^\times,\ (a,b) \mapsto b$$

是群同态即可, 运算是 $A^\times$ 与 $B^\times$ 上的乘法运算. 显然有

$$(a,b) \in (A \times_{\text{ring}} B)^\times \Leftrightarrow a \in A^\times, b \in B^\times,$$

故映射是良定义的. $\forall (a_1,b_1),(a_2,b_2) \in \left(A \times_{\text{ring}} B\right)^\times$, 有

$$\varphi_1((a_1,b_1)\cdot(a_2,b_2)) = \varphi_1((a_1\cdot a_2, b_1\cdot b_2)) = a_1\cdot a_2 = \varphi_1((a_1,b_1))\cdot\varphi_1((a_2,b_2)),$$
$$\varphi_2((a_1,b_1)\cdot(a_2,b_2)) = \varphi_2((a_1\cdot a_2, b_1\cdot b_2)) = b_1\cdot b_2 = \varphi_2((a_1,b_1))\cdot\varphi_2((a_2,b_2)).$$

故 φ_1,φ_2 为群同态.

由 A7) 的结论可知, 存在唯一的

$$\psi : (A \times_{\text{ring}} B)^\times \to A^\times \times B^\times, (a,b) \mapsto (a,b),$$

使得 $\pi_i \circ \psi = \varphi_i\ (i=1,2)$. 显然 ψ 为群同态. 而 $|(A \times_{\text{ring}} B)^\times| = |A^\times \times B^\times| = |A^\times||B^\times|$, 只需证明 ψ 为单射即可. 设 $(a,b) \in \ker(\psi)$, 有

$$\pi_1 \circ \psi((a,b)) = \pi_1(1_A, 1_B) = 1_A = a = \varphi_1((a,b)),$$
$$\pi_2 \circ \psi((a,b)) = \pi_2(1_A, 1_B) = 1_B = b = \varphi_2((a,b)),$$

则 $(a,b)=(1_A,1_B)$, 即 $\ker(\psi)=(1,1)$, ψ 为单射. 因此, ψ 为同构映射, 即

$$(A \times_{\text{ring}} B)^\times \simeq A^\times \times B^\times.$$

□

B. 域的有限乘法子群是循环群

B1)

证明： 显然有

$$\begin{aligned}
&x \in (\mathbb{Z}/n\mathbb{Z})^{\times} \\
\Leftrightarrow &\exists y \in (\mathbb{Z}/n\mathbb{Z})^{\times}, \text{s.t. } xy = 1 \in (\mathbb{Z}/n\mathbb{Z})^{\times} \\
\Leftrightarrow &\exists y, m, \text{s.t. } xy + mn = 1 \\
\Leftrightarrow &(x, n) = 1
\end{aligned}$$

所以，$|(\mathbb{Z}/n\mathbb{Z})^{\times}| = \phi(n)$. □

B2)

证明： 由 A8), A9) 可知,

$$(\mathbb{Z}/nm\mathbb{Z})^{\times} \simeq (\mathbb{Z}/n\mathbb{Z} \times_{\text{ring}} \mathbb{Z}/m\mathbb{Z})^{\times} \simeq (\mathbb{Z}/n\mathbb{Z})^{\times} \times_{\text{group}} (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

对两边取阶，有 $\phi(nm) = \phi(n)\phi(m)$.

进一步，如果 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 则由上式知

$$\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}).$$

而 $\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}(1 - \frac{1}{p_i})$. 因此

$$\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).$$

□

B3)

证明： 对任意正整数 n, 由 B1) 知 $|(\mathbb{Z}/n\mathbb{Z})^{\times}| = \phi(n)$, $\forall a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, 由 Lagrange 定理有 $a^{\phi(n)} = 1 \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, 即 $a^{\phi(n)} \equiv 1 \pmod n$. 因此, $\forall a \in \mathbb{Z}$ 且 $(a, n) = 1$, 有 $a^{\phi(n)} \equiv 1 \pmod n$.

特别地, 当 $n = p$ 为素数时, $|(\mathbb{Z}/p\mathbb{Z})^{\times}| = p - 1$, 有 $a^{p-1} \equiv 1 \pmod p$, 即 Fermat 小定理. □

B4)

证明： 由于 d 是 n 的因子, 知道 $d \mid n$, 设 $m = n/d$, 于是令 $C_d = \langle m \rangle$, 于是 C_d 是 $\mathbb{Z}/n\mathbb{Z}$ 的子群, 且 $|C_d| = d$.

下面证明 C_d 是唯一的: 设 H 是 $\mathbb{Z}/n\mathbb{Z}$ 的一个 d 阶子群, 则 $\forall a \in H$, 有 $da \equiv 0 \pmod n$(由 Lagrange 定理). 于是 $n \mid da$, 由于 $n = md$, 则 $md \mid da$, 即 $m \mid a$. 于是 $H \subset \langle m \rangle = C_d$. 又 $|H| = |C_d| = d$, 故 $H = C_d$. 因此, C_d 是唯一的.

进一步, 设 H 是 $\mathbb{Z}/n\mathbb{Z}$ 的任意子群, 设 $|H| = d$, 则 $d \mid n$. 由上面已经证明了存在唯一的 d 阶子群 C_d, 故 $H = C_d$. 因此, $\mathbb{Z}/n\mathbb{Z}$ 的子群与 n 的因子之间存在一一对应关系, 且形如 C_d.

□

B5)

证明： 对任意正整数 n, 有

$$\begin{aligned}\sum_{d|n}\phi(d) &= \sum_{d|n}\phi(\frac{n}{d}) \quad (d\text{与}\frac{n}{d}\text{都遍历}n\text{的所有因子})\\ &= \sum_{d|n}|\{1\leq k\leq \frac{n}{d} \mid (k,\frac{n}{d})=1\}|\\ &= \sum_{d|n}|\{d\leq kd\leq n \mid (kd,n)=d\}|\\ &= \sum_{d|n}|\{d\leq m\leq n \mid (m,n)=d\}|.\end{aligned}$$

注意到最后一个等式决定了 $\{1,2,\ldots,n\}$ 的一个划分, 与划分对应的等价关系是:

$$m_1 \sim m_2 \Leftrightarrow (m_1,n)=(m_2,n).$$

因此上式等于 n, 即

$$\sum_{d|n}\phi(d) = n.$$

□

B6)

证明： 对每个 $d \mid n$, 定义:

$$G_d = \{g\in G \mid \mathrm{ord}(g)=d\}$$

由 Lagrange 定理, 每个元素的阶整除 n, 故

$$G = \bigsqcup_{d|n} G_d \quad (\text{不交并})$$

现在固定 $d \mid n$. 如果 $G_d = \emptyset$, 则 $|G_d| = 0$.

如果 $G_d \neq \emptyset$, 取 $g \in G_d$, 则 $\mathrm{ord}(g) = d$. 考虑循环子群 $H = \langle g\rangle$, 它是 G 的 d 阶子群. 对于 $a \in H$, 设 $a = g^m$, 于是

$$\begin{aligned}a\text{的阶为}d &\Leftrightarrow a^d = 1\text{且}a^k\neq 1, \forall 0<k<d\\ &\Leftrightarrow g^{md}=1\text{且}g^{mk}\neq 1, \forall 0<k<d\\ &\Leftrightarrow d\mid md\text{且}d\nmid mk, \forall 0<k<d\\ &\Leftrightarrow (m,d)=1.\end{aligned}$$

故而 H 中恰有 $\phi(d)$ 个 d 阶元素. 又在域 K 中, x^d-1 最多有 d 个根, 而 $H=\{1,g,g^2,\ldots,g^{d-1}\}$ 中已经提供了 d 个互不相同的根, 故所有 d 阶元素都在 H 中. 因此, $|G_d|=\phi(d)$ 当 $G_d\neq\emptyset$, 否则为 0. 因此

$$n=|G|=\sum_{d|n}|G_d|=\sum_{d|n,G_d\neq\emptyset}\phi(d).$$

□

B7)

证明： 由 B6) 知,

$$n=\sum_{d|n,G_d\neq\emptyset}\phi(d).$$

由 B5) 知,

$$n=\sum_{d|n}\phi(d).$$

因此, $\sum_{d|n,G_d=\emptyset}\phi(d)=0$. 由于 $\phi(d)>0$, 故 $G_d\neq\emptyset,\forall d\mid n$.

设 $g_n\in G_n$, 则 $\mathrm{ord}(g_n)=n$. 于是 g_n 为 G 的一个生成元, 故 G 为循环群. □

B8)

证明： $\mathbb{Z}/p\mathbb{Z}$ 为域, $(\mathbb{Z}/p\mathbb{Z})^\times$ 为 $\mathbb{Z}/p\mathbb{Z}$ 的乘法群. 由 B7) 知, $\mathbb{Z}/p\mathbb{Z}$ 的有限子群是循环群. □

B9)

B10)

B11)

以上三问在初等数论课程中已被证明, 这里不再赘述.

C. 有限生成的群

C1)

证明：设 G 是有限生成的群, $G=\langle S\rangle$, 其中 $S\subset G$ 为有限子集. 由讲义**例子 2.10** 的 3), $\langle S\rangle$ 具有如下描述:

$$\langle S\rangle=\{s_1^{n_1}s_2^{n_2}\cdots s_k^{n_k}\mid k\in\mathbb{N},s_i\in S,n_i\in\mathbb{Z},s_i\neq s_{i+1}\}.$$

由于下标 k 是可数的, n_i 是可数的, 故 G 为可数集. □

C2)

证明：若 $\mathbb{Q}=\langle q_1,q_2\cdots q_n\rangle$, 取 N 为各 q_i 分母的最大公倍数, 则所有生成元的分母整除 N, 故生成群包含于 $\frac{1}{N}\mathbb{Z}$. 但 $\frac{1}{N+1}\notin\frac{1}{N}\mathbb{Z}$, 矛盾. 因此 $(\mathbb{Q},+)$ 不是有限生成的. □

C3)

证明：设群 G 由有限子集 $S=\{g_1,g_2,\ldots,g_n\}$ 生成, 即 $G=\langle S\rangle$. 由于 $N\lhd G$ 为正规子群, 有自然的商映射

$$\pi:G\to G/N,\ g\mapsto gN.$$

由群同态的性质, $G/N=\langle\pi(S)\rangle$, 其中 $\pi(S)=\{\pi(g_i)\mid g_i\in S\}$ 为有限子集. 故 G/N 为有限生成的. □

C4)

证明：设 N 由有限子集 $T=\{n_1,n_2,\ldots,n_m\}$ 生成, 即 $N=\langle T\rangle$. 设 G/N 由有限子集 $S=\{g_1N,g_2N,\ldots,g_kN\}$ 生成, 即 $G/N=\langle S\rangle$. 取 $S'=\{g_1,g_2,\ldots,g_k\}$, 则 S' 为 G 的有限子集.

下面证明 $G=\langle S'\cup T\rangle$:

设 $H=\langle S'\cup T\rangle$, 则 $H\subset G$. 而对任意 $g\in G$, 由 $G/N=\langle S\rangle$, 有

$$gN=(g_{i_1}N)^{n_1}\cdot(g_{i_2}N)^{n_2}\cdots(g_{i_k}N)^{n_k}=g_{i_1}^{n_1}g_{i_2}^{n_2}\cdots g_{i_k}^{n_k}N,\ 其中g_{i_j}\in S'\subset H,k,n_j\in\mathbb{Z}.$$

因此, $g_{i_k}^{-n_k}\cdots g_{i_2}^{-n_2}g_{i_1}^{-n_1}g\in N=\langle T\rangle\subset H$, 故 $g\in H\Rightarrow G\subset H$. 综上, $G=H=\langle S'\cup T\rangle$.

因此, G 为有限生成的. □

C5)

证明：注意到 G 的两个生成元都是上三角矩阵, 且上三角矩阵对于加减、乘法、取逆封闭, 故 G 中的元素均为上三角矩阵.

先证明 H 是 G 的子群:

- $H\neq\emptyset$, 因为单位元 $I_2\in H$.
- H 对乘法封闭: $\forall A_1,A_2\in H$, 有 $A_1A_2\in G$, 且显然 A_1A_2 的对角线元素全为 1, 故 $A_1A_2\in H$.

– H 对取逆封闭: $\forall A\in H$, 有 $A^{-1}\in G$, 且显然 A^{-1} 的对角线元素全为 1, 故 $A^{-1}\in H$.

综上, H 为 G 的子群.

再证明 H 不是有限生成的:

首先需要刻画 H, 令 $A=\begin{pmatrix}2&0\\0&1\end{pmatrix},B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, 则 $G=\langle A,B\rangle$. 计算可知:

$$A^n=\begin{pmatrix}2^n&0\\0&1\end{pmatrix},\quad A^{-n}=\begin{pmatrix}2^{-n}&0\\0&1\end{pmatrix},\quad A^nBA^{-n}=\begin{pmatrix}1&2^n\\0&1\end{pmatrix},\text{ 其中}n\in\mathbb{Z}.$$

故 $\begin{pmatrix}1&2^n\\0&1\end{pmatrix}\in H$, 其中 $n\in\mathbb{Z}$.

反证法, 若 H 为有限生成的, 则存在 $S=\left\{\begin{pmatrix}1&n_1\\0&1\end{pmatrix},\begin{pmatrix}1&n_2\\0&1\end{pmatrix},\cdots,\begin{pmatrix}1&n_k\\0&1\end{pmatrix}\right\}$, 其中 $n_i\in\mathbb{Z}$, 使得 $H=\langle S\rangle$. 而 $\langle S\rangle\simeq\langle n_1,n_2,\cdots n_k\rangle_{(\mathbb{Q},+)}$, 因为

$$\begin{pmatrix}1&a\\0&1\end{pmatrix}\begin{pmatrix}1&b\\0&1\end{pmatrix}=\begin{pmatrix}1&a+b\\0&1\end{pmatrix},\quad\begin{pmatrix}1&a\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&-a\\0&1\end{pmatrix},\quad a,b\in\mathbb{Q}.$$

设 N 为所有 n_i 的分母的最大公倍数, 则对 H 中的任意元素形如 $\begin{pmatrix}1&2^{-n}\\0&1\end{pmatrix},n>N$, 因为 2^{-n} 的分母不整除 N, 故 $2^{-n}\notin\langle n_1,n_2,\cdots n_k\rangle_{(\mathbb{Q},+)}$, 故 $\begin{pmatrix}1&2^{-n}\\0&1\end{pmatrix}\notin\langle S\rangle$. 矛盾. 因此, H 不是有限生成的.

综上, 有限生成的群的子群不一定是有限生成的. □

C6)

证明:

- 首先 Hg_i^{-1} 显然是 H 的一个右陪集. 而 $Hg_i^{-1}=Hg_j^{-1}\Leftrightarrow g_ig_j^{-1}\in H$, 证明与 $g_iH=g_jH\Leftrightarrow g_ig_j^{-1}$ 类似, 这里不再赘述. 由 $\{g_iH\mid i\in I,g_i\in G\}$ 是 H 在 G 中所有左陪集的集合知, $\left\{Hg_i^{-1}\mid i\in I,g_i\in G\right\}$ 中的元素两两不交.

  下面证明 $\left\{Hg_i^{-1}\mid i\in I.g_i\in G\right\}$ 包含所有右陪集. $\forall g\in G,\exists i\in I,\text{s.t.}g^{-1}\in g_iH$, 即 $\exists h\in H,\text{s.t.}g^{-1}=g_ih$. 从而 $g=h^{-1}g_i^{-1}\in Hg_i^{-1}$. 故 $\left\{Hg_i^{-1}\mid i\in I,g_i\in G\right\}$ 包含所有右陪集.

  综上, $\left\{Hg_i^{-1}\mid i\in I,g_i\in G\right\}$ 是所有右陪集的集合.

- 假设有限子集 S 生成 G, $\{g_iH\mid i\in I,g_i\in G\}$ 是 H 的所有左陪集, 由 $[G:H]<\infty$, 知 I 为有限指标集. 由上一小问知 $\left\{Hg_i^{-1}\mid i\in I,g_i\in G\right\}$ 是所有右陪集. 并且取左陪集代表元集合 $\{g_i\mid i\in I\}$, 不妨取 $g_1=1_G$.

考虑:

$$T=\left\{xsy \mid x,y\in\left\{g_i,g_i^{-1}\mid i\in I\right\},s\in S\right\}\cap H$$

由于 I,S 都是有限集, 于是 T 也是有限集. $\forall h\in H$, 有 $h=s_1s_2\cdots s_k$, 其中 $s_i\in S\cup S^{-1}$ 对于 $s_1,\exists i_1\in I,h_1\in H,$s.t.

$$s_1=hg_{i_1}^{-1}\Rightarrow s_1g_{i_1}=h_1\in H,$$

而对于 $s_j(2\leq j\leq k),\exists i_j\in I,h_j\in H,$s.t.

$$g_{i_{j-1}}^{1}s_j=hg_{i_j}^{-1}\Rightarrow g_{i_{j-1}}^{-1}s_jg_{i_j}=h_j\in H.$$

从而有:

$$\begin{aligned}h&=(s_1g_{i_1})(g_{i_1}^{-1}s_2g_{i_2})\cdots(g_{i_{j-1}}^{-1}s_jg_{i_j})\cdots(g_{i_{k-1}}^{-1}s_kg_{i_k})g_{i_k}^{-1}\\&=(g_1^{-1}s_1g_{i_1})(g_{i_1}^{-1}s_2g_{i_2})\cdots(g_{i_{j-1}}^{-1}s_jg_{i_j})\cdots(g_{i_{k-1}}^{-1}s_kg_{i_k})g_{i_k}^{-1},\end{aligned}$$

而 h 与右边前 k 个元素都在 H 中, 所以 $g_{i_k}^{-1}\in H\Rightarrow g_{i_k}=1_G$.

所以 $H=\langle T\rangle$, H 是有限生成的.

□

D. 线性群中元素的阶的几个命题

D1)

证明：

- $\forall A \in \mathbf{GL}(n,\mathbb{Z})$, 由于 $A \in \mathbf{M}_n(\mathbb{Z})$, $\det(A) \in \mathbb{Z}$, 而由于，又 $\det(A)\det(A^{-1}) = 1$, 故而 $\det(A) = \pm 1$.

-

$\square$