清华大学 2024-2025 秋季学期，群与 Galois 理论，作业 1

请用 A4 大小的纸张**正反面**用钢笔，签字笔或者圆珠笔书写，并注明自己的姓名、年级（书院或系）和作业的**总页数**。除定理公式所涉及的人名之外，请使用**中文**。本次作业请扫描并上传至网络学堂，具体截止日期请查阅网络学堂，逾期视作零分。

A. 乘积结构

A1) $(G_1, \cdot_1)$ 和 $(G_2, \cdot_2)$ 是群，在 $G_1 \times G_2$ 上如下定义乘法：

$$(g_1, g_2) \cdot (g_1', g_2') := \big(g_1 \cdot_1 g_1', g_2 \cdot_2 g_2'\big).$$

证明，在以上乘法下，$G_1 \times G_2$ 是群并且其单位元为 $(1_1, 1_2)$。这个群被称为 G_1 与 G_2 的**乘积**。

A2) 证明，投影映射

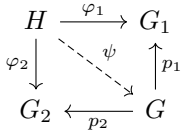
$$\pi_1 : G_1 \times G_2 \to G_1, \quad (g_1, g_2) \mapsto g_1,$$

和

$$\pi_2 : G_1 \times G_2 \to G_2, \quad (g_1, g_2) \mapsto g_2,$$

是群同态。它们的核是什么？

A3) （泛性质）给定群 $(G_1, \cdot_1)$ 和 $(G_2, \cdot_2)$。证明，存在唯一的[1]群 G 以及唯一的群同态 $p_i : G \to G_i$ $(i = 1, 2)$ 使得对任意的群 H 和任意的群同态 $\varphi_i : H \to G_i$ $(i = 1, 2)$，存在唯一的 $\psi : H \to G$，使得 $p_i \circ \psi = \varphi_i$ $(i = 1, 2)$。



特别地，我们有如下的集合之间的同构：

$$\mathrm{Hom}(H, G_1 \times G_2) \simeq \mathrm{Hom}(H, G_1) \times \mathrm{Hom}(H, G_2), \quad \psi \mapsto \big(p_1 \circ \psi, p_2 \circ \psi\big).$$

（提示：利用 A2) 给出 G 的存在性；利用 ψ 的唯一性证明 G 的唯一性）

A4) 给定互素的正整数 n_1 和 n_2。利用 A3) 证明，

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

给出了群同构

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

以上，$\mathbb{Z}/n\mathbb{Z}$ 表示的是（加法）循环群。

A5) C_1 和 C_2 是两个有限阶的循环群，那么，$C_1 \times C_2$ 是否是循环群？

[1] 在同构的意义下

A6) $(A_1,+_1,\cdot_1)$ 和 $(A_2,+_2,\cdot_2)$ 是环。我们在 $A_1\times A_2$ 上如下定义加法 $+$ 和乘法 $\cdot$:

$$(a_1,a_2)+(a_1',a_2'):=\big(a_1+_1a_1',a_2+_2a_2'\big),\ \ (a_1,a_2)\cdot(a_1',a_2'):=\big(a_1\cdot_1a_1',a_2\cdot_2a_2'\big).$$

证明，选取加法单位元 $(0_1,0_2)$ 和乘法单位元 $(1_1,1_2)$，$A_1\times A_2$ 在以上运算下是环。我们把这个环称作是 A_1 与 A_2 的**乘积**。进一步证明，投影映射

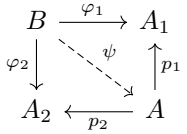
$$\pi_1:A_1\times A_2\to A_1,\ \ (a_1,a_2)\mapsto a_1,$$

和

$$\pi_2:A_1\times A_2\to A_2,\ \ (a_1,a_2)\mapsto a_2,$$

是环同态。

A7)（泛性质）给定环 A_1 和 A_2。证明，存在唯一的[2]环 A 以及唯一的环同态 $p_i:A\to A_i$（$i=1,2$）使得对任意的环 B 和任意的环同态 $\varphi_i:B\to A_i$（$i=1,2$），存在唯一的 $\psi:B\to A$，使得 $p_i\circ\psi=\varphi_i$ $(i=1,2)$。



A8) 给定互素的正整数 m 和 n。证明，我们有**环同构**[3]

$$\mathbb{Z}\big/_{mn\mathbb{Z}}\xrightarrow{\simeq}\mathbb{Z}\big/_{m\mathbb{Z}}\times\mathbb{Z}\big/_{n\mathbb{Z}}.$$

（提示：使用中国剩余定理）

A9) A 和 B 是环，$A^\times$ 和 $B^\times$ 是它们的乘法可逆元所构成的（乘法）群。证明，我们有群同构

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

其中，$\times_{\text{ring}}$ 代表着环的乘积，$\times_{\text{group}}$ 代表着群的乘积。

B. 域的有限乘法子群是循环群

给定正整数 n，Euler 的 ϕ-函数给出 $1,\cdots,n$ 中与 n 互素的数的个数:

$$\phi(n)=\big|\big\{1\leqslant k\leqslant n\big|(k,n)=1\big\}\big|.$$

B1) 证明，$\left|\left(\mathbb{Z}\big/_{n\mathbb{Z}}\right)^\times\right|=\phi(n)$，其中，$\left(\mathbb{Z}\big/_{n\mathbb{Z}}\right)^\times$ 是环 $\mathbb{Z}\big/_{n\mathbb{Z}}$ 的可逆元组成的（乘法）子群。

B2) 证明，ϕ 具有如下乘性：对任意互素的正整数 n 和 m，有

$$\phi(nm)=\phi(n)\phi(m).$$

进一步，如果 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是它的素因子分解，其中，p_i 为不同的素数而指标 α_i 均为正整数，证明:

$$\phi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k}).$$

[2]在同构的意义下

[3]请与 A4) 仔细对比

B3) 证明，对任意正整数 n，对任意与 n 互素的整数 a，有 $a^{\phi(n)} \equiv 1 \ (\mathrm{mod} n)$。特别地，当 p 为素数时，这给出了 Fermat 小定理。

B4) (有限循环群子群的分类) 证明，作为加法群，对每个 n 的因子 d，$\mathbb{Z}/n\mathbb{Z}$ 恰有一个阶为 d 的循环子群 C_d。进一步，$\mathbb{Z}/n\mathbb{Z}$ 的每个子群均形如 C_d，其中，$d|n$。

B5) 证明，对任意的正整数 n，我们有公式

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

B6) K 是域，$G < K^\times$ 是有限群，$|G| = n$。对任意的 $d|n$，令 G_d 为 G 中阶为 d 的元素组成的集合。证明，

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

B7) 证明，G 是循环群。

B8) 证明，$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 是循环群，其中，p 是素数。

B9) 对于奇素数 p 和 $m \geqslant 2$，我们证明 $\left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$ 是循环群：

- 证明，$(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}$，其中 $k \geqslant 0$。据此证明 $\overline{p+1} \in \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$ 的阶为 p^{m-1}。
- 证明，存在 $\overline{k} \in \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$，其阶为 $p-1$。
- 证明，存在 $\bar{l} \in \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$，使得 $\langle \bar{l} \rangle = \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$。

B10) 对于 $m \geqslant 2$，我们给出 $\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times$ 的结构：

- 证明，$(1+2^2)^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}$，其中 $k \geqslant 0$。据此证明，$\overline{5} \in \left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times$ 的阶为 2^{m-2}。
- 证明，映射（以下左边是加法群，右边是乘法群）

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z} \longrightarrow \left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times, \quad (a,b) \mapsto (-1)^a 5^b \mod 2^m.$$

是群同构。

B11) (Gauss) 证明，对任意正整数 n，$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 是循环群当且仅当 n 形如 $1, 2, 4, p^m$ 或 $2p^m$，其中，$m \geqslant 1$ 而 p 为奇素数。此时，$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 的每个生成元 $\bar{l}$ 都被称为 n 的**原根**。

C. 线性群中元素的阶的几个命题

C1) 令 $\mathbf{M}_n(\mathbb{Z})$ 为整系数的 $n \times n$ 矩阵的集合，令

$$\mathbf{GL}(n;\mathbb{Z}) = \left\{ A \in \mathbf{M}_n(\mathbb{Z}) \middle| \ A\text{可逆并且 } A^{-1} \in \mathbf{M}_n(\mathbb{Z}) \right\}.$$

- 证明，$\mathbf{GL}(n;\mathbb{Z}) = \left\{ A \in \mathbf{M}_n(\mathbb{Z}) \middle| \det(A) = \pm 1 \right\}$。
- 如果 $A \in \mathbf{GL}(2;\mathbb{Z})$ 的阶有限，证明，$\mathrm{ord}(A) \in \{1,2,3,4,6\}$。

- 证明，存在只依赖于 n 的常数 C_n，若 $A \in \mathbf{GL}(n;\mathbb{Z})$ 的阶有限，则 $\big|\mathrm{ord}(A)\big| \leqslant C_n$。

C2) p 是素数，q 是 p 的幂，域 $\mathbb{F}_q$ 有 q 个元素。我们已知 $\mathbf{GL}(n;\mathbb{F}_q)$ 共有 $\prod_{k=0}^{n-1}(q^n - q^k)$ 个元素。

- 对任意的 $A \in \mathbf{GL}(n;\mathbb{F}_q)$，证明，集合 $\big\{P(A)\big|P \in \mathbb{F}_q[X]\big\}$ 至多有 q^n 个元素。以上，对于 $P(X) = \sum_{k=0}^{n} a_k X^k$，其中，$a_k \in \mathbb{F}_q$，我们定义 $P(A) = \sum_{k=0}^{n} a_k \cdot A^k$。
- 证明，对任意的 $A \in \mathbf{GL}(n;\mathbb{F}_q)$，$\mathrm{ord}(A) \leqslant q^n - 1$。
- 给定如下的结论：存在 $K = \mathbb{F}_q$ 的域扩张 $L = \mathbb{F}_{q^n}$，使得 $[L:K] = n$。证明，存在 $A \in \mathbf{GL}(n;\mathbb{F}_q)$，$\mathrm{ord}(A) = q^n - 1$。

所以，$\mathbf{GL}(n;\mathbb{F}_q)$ 中元素的阶的最大值恰好是 $q^n - 1$。

D. 有限群乘积的消去定理

我们先证明群论中三个标准的定理：

- （第二同构定理）G 是群，$K < G$，$N \lhd G$。证明，$N \cap K \lhd K$ 并且有自然的群同构：

$$K\big/_{N \cap K} \xrightarrow{\simeq} NK\big/_{N},$$

其中，首先说明 $NK = \big\{x \cdot y\big|x \in N, y \in K\big\}$ 是 G 的子群。

- （第三同构定理）G 是群，$K \lhd G$，$H \lhd G$ 并且 $K < H$。证明，$H\big/_K \lhd G\big/_K$ 并且有自然的群同构：

$$\big(G\big/_K\big)\Big/\big(H\big/_K\big) \xrightarrow{\simeq} G\big/_H.$$

- （子群对应定理）$\varphi : G \twoheadrightarrow G'$ 是满的群同态，我们有如下双射：

$$\big\{H\big|H < G, H \supset \mathrm{Ker}(\varphi)\big\} \xrightarrow{1:1} \big\{H'\big|H' < G'\big\},\quad H \mapsto \varphi(H).$$

进一步，假设以上对应把 H 映射成 H'，那么，H 是 G 的正规子群当且仅当 H' 是 G' 的正规子群。

下面证明有限群乘积的消去定理。给定有限群 G, G'，以下两个数值是非负整数：

$$M\big(G,G'\big) = \big|\mathrm{Hom}(G,G')\big|,\quad I\big(G,G'\big) = \big|\big\{\varphi \in \mathrm{Hom}(G,G')\big|\varphi \text{ 为单射}\big\}\big|.$$

D1) 证明如下等式，其中，以下是对所有 G 的正规子群 H 来求和：

$$M\big(G,G'\big) = \sum_{H \lhd G} I\left(G\big/_H, G'\right)$$

D2) 证明，对每个 G 的正规子群 H 存在整数 λ_H，使得

$$I\big(G,G'\big) = \sum_{H \lhd G} \lambda_H \cdot M\left(G\big/_H, G'\right).$$

特别地，以上等式中的系数 $\big\{\lambda_H\big|H \lhd g\big\}$ 不依赖于 G'。

D3) 假设 G_1, G_2, G' 是有限群并且 $G_1 \times G' \simeq G_2 \times G'$。证明，$I\big(G_1, G'\big) = I\big(G_2, G'\big)$。

D4) （消去定理）证明，若 G_1, G_2, G' 是有限群并且 $G_1 \times G' \simeq G_2 \times G'$，则 $G_1 \simeq G_2$。

D5) 令 G_1 和 G_2 为有限维 $\mathbb{F}_2$-线性空间，G' 为 $\mathbb{F}_2$-线性空间且其基有可数无限个元素。证明，$G_1 \times G' \simeq G_2 \times G'$。特别地，这一组 G_1, G_2, G' 不满足消去定理。

Algebra is the metaphysics of arithmetic.

— John Ray

练习题（不提交）

1. G 是群，$H \subset G$ 是有限子集并且对乘法封闭[4]。证明，H 是子群。

2. 假设 $\{G_i\}_{i\in I}$ 是 G 的一族正规子群，那么，$\bigcap_{i\in I} G_i$ 也是正规子群。

3. 有限集 G 上定义了满足结合律的乘法 $G \times G \to G$，$(g_1, g_2) \mapsto g_1 \cdot g_2$。假设以下两点成立：

   - 对任意的 $g, x, y \in G$，有 $g \cdot x = g \cdot y \quad \Rightarrow \quad x = y$;
   - 对任意的 $g, x, y \in G$，有 $x \cdot g = y \cdot g \quad \Rightarrow \quad x = y$。

   证明，G 在此乘法下是群。

4. 试给出所有（在同构意义下）阶数不超过 5 的群。

5. G 是群，$H < G$ 是子群并且 $[G : H] = 2$。证明，$H \lhd G$ 是正规子群。如果 $[G : H] = n$，其中，$n \geqslant 3$，结论是否成立?

6. G 是群，$H < G$ 是子群并且 $[G : H] = n$。证明，如果 H 是唯一的指标为 n 的子群，那么 $H \lhd G$ 是正规子群。

7. (循环群的分类) G 是循环群。证明，或 $G \simeq \mathbb{Z}$，或有正整数 n 使得 $G \simeq \mathbb{Z}/n\mathbb{Z}$，二者必居其一。

8. G 是 mn 阶的交换群，其中，m, n 为互素。如果存在 $g, h \in G$，使得其阶分别为 m 和 n，证明，G 为循环群。

9. G 是群并且它只有有限个子群。证明，G 是有限群。

10. G 是群。对任意的 $g \in G$，共轭映射 $\mathrm{Int}(g)$ 的定义如下：

$$\mathrm{Int}(g) : G \to G, \quad h \mapsto \mathrm{Int}(g)(h) = ghg^{-1}.$$

    证明，以上映射给出群同态：

$$G \to \mathrm{Aut}(G), \quad g \mapsto \mathrm{Int}(g).$$

    并且 $\mathrm{Ker}(\mathrm{Int}) = \mathrm{Z}(G)$ 而 $\mathrm{Im}(\mathrm{Int}) \lhd \mathrm{Aut}(G)$ 是正规子群。

11. 试在二面体群 $\mathfrak{D}_4$ 中找到两个子群 $K < H < G$，使得 $K \lhd H$，$H \lhd \mathfrak{D}_4$，但是 K 不是 $\mathfrak{D}_4$ 的正规子群? 这表明正规子群的关系并不传递。

12. G 是群，K 和 H 为其子群并且 $K \lhd H$，$H \lhd G$。证明，如果 H 是循环群，那么 $K \lhd G$。

13. (四元数群) 令 $\mathbf{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$，一共有 8 个元素。定义 1 为单位元；对任意的 $\pm x \in \mathbf{Q}_8$，令 $(-1) \cdot (\pm x) = (\pm x) \cdot (-1) = \mp x$；定义乘法：

$$i \cdot j = -j \cdot i = k,\ j \cdot k = -k \cdot j = i,\ k \cdot i = -i \cdot k = j,\ i^2 = j^2 = k^2 = -1.$$

    证明，以上给出群结构。试找出它所有的子群并证明这些子群都是正规子群。$\mathbf{Q}_8$ 与二面体群 $\mathfrak{D}_4$ 是否同构?

[4]即对任意的 $h_1, h_2 \in H$，$h_1 \cdot h_2 \in H$。

14. (Cayley 定理：每个（有限）群都同构于（有限）对称群的子群）G 是群。令 $X = G$，定义映射：

$$\varphi : G \to \mathfrak{S}_X,\ \ g \mapsto \varphi(g) : x \mapsto g \cdot_G x,\ \ \forall x \in X.$$

证明，G 是单的群同态（从而，$G \simeq \mathrm{Im}(\varphi)$）。

15. 证明，$\mathbb{Q}/\mathbb{Z}$ 是无限群但是每个元素的阶都是有限的。

16. G 是群，定义映射

$$\mathrm{Inv} : G \to G,\ g \mapsto g^{-1}.$$

证明，G 是交换群当且仅当 Inv 是群同态。

17. G 是群，如果对任意的 $g \in G$，$g^2 = 1$，证明，G 是交换群

18. $\mathbb{Z}/p\mathbb{Z}$ 是 p-阶加法循环群，其中，p 是素数。证明，$\mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right)$ 是循环群。如果把 p 替换成 6 或者 8，结论是否成立?

19. G 是群，H, K 为其子群。我们定义 $H \cdot K = \{h \cdot k | h \in H, k \in K\}$。证明，$H \cdot K$ 为子群当且仅当 $H \cdot K = K \cdot H$。

20. G 是群，H, K 为其有限子群。证明，

$$|H \cdot K| = \frac{|H||K|}{|H \cap K|}.$$

21. G 是群，H, K 为其子群。证明，$H \cap K < H$ 并且

$$[H : H \cap K] \leqslant [G : K].$$

假设 $[G : K]$ 有限，进一步证明以上等号成立当且仅当 $G = K \cdot H$。

22. G 是群，H, K 为其有限指标的子群。证明，

$$[G : H \cap K] \leqslant [G : H][G : K].$$

并且等号成立当且仅当 $G = K \cdot H$。

23. $\varphi : G \to A$ 是群同态，A 是交换群。证明，G 中任意的包含 $\mathrm{Ker}(\varphi)$ 的子群都是正规子群。