清华大学 2025-2026 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

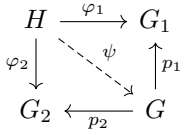
$$\pi_1 : G_1 \times G_2 \to G_1, \quad (g_1, g_2) \mapsto g_1,$$

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 $\cdot$:

$$(a_1, a_2) + (a_1', a_2') := \big(a_1 +_1 a_1', a_2 +_2 a_2'\big), \quad (a_1, a_2) \cdot (a_1', a_2') := \big(a_1 \cdot_1 a_1', a_2 \cdot_2 a_2'\big).$$

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

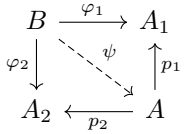
$$\pi_1 : A_1 \times A_2 \to A_1, \quad (a_1, a_2) \mapsto a_1,$$

和

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

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. 有限生成的群

G 是群，$S \subset G$ 是子集。若存在有限子集 $S \subset G$，使得 $\langle S \rangle = G$，则称 G 是**有限生成的**。

C1) 证明，每个有限生成的群均为可数集。

C2) 证明，$(\mathbb{Q}, +)$ 不是有限生成的。

C3) 群 G 是有限生成的，$N \lhd G$ 是正规子群。证明，商群 G/N 是有限生成的。

C4) 给定群 G，$N \lhd G$ 是正规子群。证明，若 N 和 G/N 是有限生成的，则 G 也是有限生成的。

C5)（有限生成群之子群未必有限生成）考虑 $\mathbf{GL}(2;\mathbb{Q})$ 的子群 G，它由两个元素生成：$G = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$。

令

$$H = \left\{ A \in G \middle| A\text{的对角线上的元素均为 } 1 \right\}.$$

证明，H 是 G 的子群并且 H 不是有限生成的。

C6)（有限生成群之有限指标子群有限生成）给定群 G，$H < G$ 是子群。

- 证明，若 $\{g_i H \big| i \in I, g_i \in G\}$ 是 H 在 G 中所有左陪集的集合，则 $\{H g_i^{-1} \big| i \in I, g_i \in G\}$ 是所有右陪集的集合。
- 证明，若 G 是有限生成的且 $[G : H] < \infty$，则 H 是有限生成的。
  （提示：假设有限子集 S 生成 G，$\{g_i H \big| i \in I, g_i \in G\}$ 是 H 的所有左陪集，考虑集合 $\left\{ xsy \middle| x, y \in \{g_i, g_j^{-1} | i \in I\}, s \in S \right\}$。）