2023 年《代数学基础》马立明老师班期中测试

考试时间：2023 年 12 月 2 日 19:00–21:15，本卷共 110 分。

一、（15 分）

(a) 求 793 和 1403 的最大公因子和最小公倍数；

(b) 求二元一次方程 $793x + 1403y = 40870$ 的全部整数解，以及正整数解的个数；

(c) 求一次同余方程 $793x \equiv 427 \pmod{1403}$ 的解。

二、（10 分） 设 $(G, \cdot)$ 是有限群，令 A, B 是群 G 的子群。记 $A \cdot B = \{a \cdot b : a \in A, b \in B\}$。证明：

(a) $A \cdot B$ 是群 G 的子群当且仅当 $A \cdot B = B \cdot A$；

(b) 若 A 是群 G 的正规子群，则 $A \cdot B$ 是群 G 的子群，并且 A 是群 $A \cdot B$ 的正规子群。

三、（20 分） 设 m 为大于 1 的正整数，$\mathbb{Z}_m = \{[0], [1], \cdots, [m-1]\}$ 为模 m 的同余类加法群，对任意的整数 a 和 x，令

$$\sigma_a : \mathbb{Z}_m \to \mathbb{Z}_m,\ \sigma([x]) = [ax].$$

(a) 证明 σ_a 为 $\mathbb{Z}_m$ 的自同构（群到自身的同构称为自同构）当且仅当 $\gcd(a, m) = 1$。

(b) 证明 $\sigma_a = \sigma_b$ 当且仅当 $a \equiv b \pmod{m}$；（2 分）证明 $\mathbb{Z}_m$ 的每个自同构必为某个 σ_a。（3 分）

(c) 记 $\mathbb{Z}_m$ 的自同构全体为 $\mathrm{Aut}(\mathbb{Z}_m)$，证明集合 $\mathrm{Aut}(\mathbb{Z}_m)$ 在映射的复合运算下 $\circ$ 构成群。（5 分）

(d) 证明映射 $\tau : \mathbb{Z}_m^\times \to \mathrm{Aut}(\mathbb{Z}_m)$, $[a] \mapsto \sigma_a$ 为群同构。（5 分）

四、（15 分）

(a) 解一次同余方程组

$$\begin{cases} x \equiv 17 \pmod{10}, \\ x \equiv 15 \pmod{12}, \\ x \equiv 12 \pmod{15}. \end{cases}$$

(b) 若 $k \geq 3$，则 5 模 2^k 的阶为 2^{k-2}，并且 $\{(-1)^a 5^b \mid a = 0, 1 \wedge 0 \leq b < 2^{k-2}\}$ 是模 2^k 的缩系。（5 分）

(c) 若 $k \geq 3$，则有群同构 $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$。

五、（20 分） 设 p 是奇素数，n 为正整数，g 为模 p 的原根。

(a) 求 $1 + p$ 模 p^n 的解；

(b) $g(1 + p)$ 为模 p^n 的一个原根吗？为什么？

(c) 求出模 13^{2023} 的一个原根。

(d) 求出整数 13^{2023} 的十进制表示的后两位（十位与个位数）。

六、（20 分） 设 $(G,\cdot)$ 是有限群，其阶为 n，证明：

(a) 素数 p 阶群皆是 Abel 群，并且同构与整数模 p 同余类加法群 $\mathbb{Z}_p$。

(b) 4 阶群皆是 Abel 群，并决定在同构意义下的分类。

(c) 非 Abel 群的最小阶数为 6。

(d) 6 阶非 Abel 群均同构与 S_3。

七、（附加题：6 分） 已知集合 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ 在复数加法和乘法运算下构成含幺交换环。证明以下结论：

(a) 证明 $\mathbb{Z}[\sqrt{-5}]$ 是整环，并求出其乘法单位群。

(b) 2 是 $\mathbb{Z}[\sqrt{-5}]$ 的素元吗？为什么？（含幺交换环 R 的非零元素 p 是素元：p 不是 R 的单位元，并且若 $p \mid ab$，其中 $a, b \in R$，则 $p \mid a$ 或 $p \mid b$。）

(c) 3 是 $\mathbb{Z}[\sqrt{-5}]$ 的不可约元吗？为什么？（含幺交换环 R 的非零元素 p 是不可约元：p 不是 R 的单位元，并且若 $p = ab$，其中 $a, b \in R$，则 a 或 b 为 R 的单位元。）

(d) $\mathbb{Z}[\sqrt{-5}]$ 是唯一分解整环吗？为什么？

(e) 由元素 2 和 $1 + \sqrt{-5}$ 生成的理想是极大理想吗？为什么？

(f) $\mathbb{Z}[\sqrt{-5}]$ 是主理想整环吗？为什么？

八、群论中的 Lagrange 定理（附加题：4 分） 设 $(G,\cdot)$ 是有限群，A 是群 G 的子群。证明：

(a) 在 G 上定义关系 $\sim$：对任意 $g, h \in G$，$g \sim h \Leftrightarrow g^{-1} \cdot h \in A$。则 $\sim$ 是 G 上的等价关系，并求 G 中元素 g 在等价关系 $\sim$ 下的等价类。

(b) 子群 A 的阶整除群 G 的阶。

(c) 对 $g \in G$，使得 $g^n = 1$ 成立的最小正整数 n 称为元素 g 的阶，则元素 g 的阶整除群 G 的阶。

(d) 利用群论中的 Lagrange 定理证明 Euler 定理。