代数学入門

レポート 1 (中間レポート)

教員名：コスキヴィルタ ジャンステファン

提出方法：レポートを Webclass で提出して下さい。

提出期限：2023 年 11 月 30 日 (木) 18 時まで。

問 1. a, b を自然数とする. $a \mid b$ のとき, 任意の自然数 c に対し, 以下が成り立つことを示せ.

$$\frac{a}{\gcd(a, c)} \mid \frac{b}{\gcd(b, c)}.$$

問 2. 群同型 $\mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ が存在しないことを示せ.

問 3. G を群とする.

(1) $x \in G$ を位数 n の元とする. 任意の $k \in \mathbb{Z}$ に対し,

$$\text{ord}(x^k) = \frac{n}{\gcd(k, n)}$$

が成り立つことを示せ.

(2) $x, y \in G$ が交換するもので, $n := \text{ord}(x)$ と $m := \text{ord}(y)$ が互いに素であるとする. このとき, $\text{ord}(xy) = nm$ であることを示せ.

問 4 と問 5 は任意です (正確に解答できた場合は加点となります).

問 4 (任意). G を有限アーベル群とする. G の全ての元の位数の最小公倍数を $e(G)$ とおき, G の冪数という.

- (1) $x, y \in G$ とし, それぞれの位数を n, m とおく. $N = \text{lcm}(n, m)$ とおくと, G 内に位数 N の元が存在することを示せ. ヒント: 問 3(1)+ 問 3(2).
- (2) $x \in G$ を G の元の中で最大位数の元とする. このとき, $\text{ord}(x) = e(G)$ が成り立つことを示せ.
- (3) $e(G)$ は $|G|$ の約数であり, さらに $|G|$ と同じ素因数を持つことを示せ. ヒント: コーシーの定理 (講義ノート系 2.50).

問 5 (任意). フェルマーの小定理より, p が素数のとき, $\text{gcd}(k, p) = 1$ を満たす任意の整数 k に対し $k^{p-1} \equiv 1 \pmod{p}$ が成り立つ (講義ノート定理 1.18 参照).

定義. 素数でない自然数 n がカーマイケル数であるとは, 任意の $k \in \mathbb{Z}$ に対し, $\text{gcd}(k, n) = 1$ のとき

$$k^{n-1} \equiv 1 \pmod{n}$$

が成り立つことをいう.

$n \geq 2$ を素数でない自然数とする.

- (1) n がカーマイケル数である $\iff e((\mathbb{Z}/n\mathbb{Z})^\times) \mid n-1$ であることを示せ. 但し, $e(G)$ は G の冪数である (問 4 参照).
- (2) n をカーマイケル数とし, $n = p_1^{e_1} \dots p_r^{e_r}$ を n の素因数分解とする (ただし, $p_1, \dots, p_r$ は相異なる素数であり, $e_i \geq 1$ であるとする).
 - (a) $p_i \neq 2$ を示せ.
 - (b) $e_1 = \dots = e_r = 1$ であることを示せ. ヒント: $e_i > 1$ のとき p_i は $\varphi(n)$ の素因数である.
 - (c) 各 i に対し, $p_i - 1 \mid n - 1$ であることを示せ. ヒント: $(\mathbb{Z}/p_i\mathbb{Z})^\times$ は巡回群である (講義ノート定理 2.38).
 - (d) $r \geq 3$ であることを示せ.
- (3) 逆に, $p_1, \dots, p_r$ が相異なる素数で $n = p_1 \dots p_r$ とし, 各 i に対し $p_i - 1 \mid n - 1$ が成り立つとする. このとき, n がカーマイケル数であることを示せ.
- (4) 1729 がカーマイケル数であることを示せ.