

代数学 C・代数学特論 III 2023 年度前期

レポート 1 (中間レポート)

提出方法：レポートを Webclass で提出して下さい。

提出の際, 写真やスキャンの画質が鮮明かどうかご確認下さい。

提出期限：2023 年 6 月 13 日 (火) 18 時まで。

教員名：コスキヴィルタ・ジャンステファン

問 1.

(1) $n \geq 2$ を自然数とし, アーベル群 $(\mathbb{Z}/n\mathbb{Z}, +)$ を考える. n の正の約数 d に対し,

$$X_d := \{x \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}(x) = d\}$$

とおく.

(a) 以下が成り立つことを示せ.

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} X_d$$

但し, d は n の正の約数全体の集合を走る. また, $\bigsqcup$ とは共通部分のない和集合を意味する.

(b) $\mathbb{Z}/n\mathbb{Z}$ の位数 d の唯一の部分群を H_d とおく. 任意の $x \in \mathbb{Z}/n\mathbb{Z}$ に対し,

$$x \in X_d \iff \langle x \rangle = H_d$$

であることを示せ.

(c) $|X_d| = \varphi(d)$ であることを示せ. ヒント：講義ノート命題 3.12 より, H_d は巡回群である.

(d) 以下が成り立つことを示せ.

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

(2) G を位数 n の有限群とし, その単位元を e とおく. n の正の約数 d に対し,

$$X_d := \{x \in G \mid \text{ord}(x) = d\},$$

$$Y_d := \{x \in G \mid x^d = e\}$$

とおく. 全ての d に対し $|Y_d| \leq d$ であることを仮定する. 以下は, この仮定の下で G が巡回群であることが示される.

(a) d を n の正の約数とし, $X_d \neq \emptyset$ とする. $x \in X_d$ ならば, $Y_d = \langle x \rangle$ が成り立つことを示せ.

(b) $X_d \neq \emptyset$ ならば, $|X_d| = \varphi(d)$ が成り立つことを示せ. ヒント：(2)(a) により, Y_d は位数 d の巡回部分群である.

(c) $\sum_{d|n} |X_d| = n$ であることを示せ. ヒント：分割

(d) $X_n \neq \emptyset$ であることを示せ. ヒント：(2)(b) により, $|X_d| \in \{0, \varphi(d)\}$ である.

- (e) G が巡回群であることを示せ.
- (3) 今, p を素数とし, $G = (\mathbb{Z}/p\mathbb{Z})^\times$ とする.
- (a) 任意の自然数 d に対し, $|\{x \in \mathbb{Z}/p\mathbb{Z} \mid x^d = 1\}| \leq d$ が成り立つことを示せ. ヒント: 多項式 $X^d - 1$ を考える.
- (b) $(\mathbb{Z}/p\mathbb{Z})^\times$ が巡回群であることを示せ.
- (c) $(\mathbb{Z}/13\mathbb{Z})^\times$ の生成元を一つ求めよ.
- (4) p を奇素数とし, $k \geq 1$ とする. 群 $G = (\mathbb{Z}/p^k\mathbb{Z})^\times$ を考える.
- (a) $|G| = p^{k-1}(p-1)$ であることを示せ (1 行以内に解答すること).
- (b) $a \in \mathbb{Z}$, $\gcd(a, p) = 1$, $r \in \mathbb{N}$ とし, $y = 1 + p^r a$ とおく. このとき, $y^p = 1 + p^{r+1} a'$ ($\gcd(a', p) = 1$) と書けることを示せ. ヒント: 二項展開.
- (c) $\beta = \overline{p+1}$ を $\mathbb{Z}/p^k\mathbb{Z}$ における $p+1$ の剰余類とする. G における β の位数が p^{k-1} であることを示せ.
- (d) 自然な準同型

$$f: (\mathbb{Z}/p^k\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times, \quad u + p^k\mathbb{Z} \mapsto u + p\mathbb{Z}$$

を考える. $z \in (\mathbb{Z}/p\mathbb{Z})^\times$ を生成元とし, $f(x) = z$ とする ($x \in (\mathbb{Z}/p^k\mathbb{Z})^\times$). このとき, $\text{ord}(x)$ が $p-1$ の倍数であることを示せ.

- (e) G 内に位数 $p-1$ の元が存在することを示せ. ヒント: 講義ノート命題 3.6.
- (f) G が巡回群であることを示せ. ヒント: 講義ノート命題 3.7.
- (g) $(\mathbb{Z}/169\mathbb{Z})^\times$ の生成元を一つ求めよ.
- (5) 群 $G = (\mathbb{Z}/2^k\mathbb{Z})^\times$ を考える ($k \geq 2$).
- (a) $|G| = 2^{k-1}$ であることを示せ.
- (b) $a \in \mathbb{Z}$, $\gcd(a, 2) = 1$, $r \geq 2$ とし, $y = 1 + 2^r a$ とおく. このとき, $y^2 = 1 + 2^{r+1} a'$ ($\gcd(a', 2) = 1$) と書けることを示せ.
- (c) $\text{ord}(\bar{5}) = 2^{k-2}$ であることを示せ.
- (d) $H = \langle \bar{5} \rangle$ とおく. $\overline{-1} \notin H$ であることを示せ.
- (e) $K = \langle \overline{-1} \rangle$ とおき, 準同型写像

$$\varphi: H \times K \rightarrow G, \quad (u, v) \mapsto uv$$

を考える. φ が同型写像であることを示せ. ヒント: 単射性+濃度

- (f) $(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であることを示せ.