代数学基礎演習 II

1. $\mathbb{Z}$ は整数の加法によってアーベル群となる (0 が単位元，$a \in \mathbb{Z}$ の逆元は $-a \in \mathbb{Z}$)。これを加法群 $\mathbb{Z}$ とよぶ。特に $\mathbb{Z}$ は $1 \in \mathbb{Z}$ で生成される無限巡回群である；$\mathbb{Z} = \langle 1 \rangle = \{n1 \mid n \in \mathbb{Z}\}$.

(i) $a \in \mathbb{Z}$ に対して $a\mathbb{Z} := \{a \text{ の倍数全体 }\} = \{na \mid n \in \mathbb{Z}\}$ と定める。これは $\mathbb{Z}$ の部分群であることを示せ。

(ii) $a, b \in \mathbb{Z}$ の最小公倍数を m とすると $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ であることを示せ。

(iii) 加法群 $\mathbb{Z}$ の任意の部分群 H に対して $H = a\mathbb{Z}$ を満たす $a \in \mathbb{Z}$ が存在する，つまり $\mathbb{Z}$ の部分群は $a\mathbb{Z}$ $(a \in \mathbb{Z})$ たちで尽くされることを示せ。

2. 位数 12 の巡回群 $\langle \sigma \mid \sigma^{12} = e \rangle \simeq \mathbb{Z}/12\mathbb{Z}$ の部分群をすべて求めよ。

3. n 次巡回群 G $(\simeq \langle \sigma \mid \sigma^n = e \rangle)$ は n の任意の約数を位数とする部分群を丁度 1 つだけもつことを示せ。さらにそれぞれの部分群は巡回群であることを示せ。

4. 位数が素数 p である群は p 次巡回群と同型であることを示せ。

5. (i) 3 次対称群 $\mathfrak{S}_3$ の部分群をすべて書きあげよ。

(ii) 上で与えた非自明な部分群のそれぞれについて，$\mathfrak{S}_3$ での相異なる左コセットをすべて具体的に与え，それらを用いて $\mathfrak{S}_3$ の左コセット分割を明示せよ。

6. G を群，$H < G$ を部分群とする。

(i) $a \in G$ に対して

$$aHa^{-1} := \{aha^{-1} \mid H\}$$

と定めるとこれは G の部分群であることを示せ。この aHa^{-1} を部分群 H の G における共役とよぶ。またすべての $a \in G$ に対して $aHa^{-1} = H$ をみたす G の部分群 H を正規部分群とよび, $H \lhd G$ で表す。

(ii) $\mathfrak{S}_3$ の非自明な部分群のうち正規部分群であるものはどれか。また正規でない部分群 $H < \mathfrak{S}_3$ に対しては $\sigma H \sigma^{-1} \neq H$ となる $\sigma \in \mathfrak{S}_3$ を具体的に与えよ。

7. (i) 乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$ の元を具体的にすべてあげよ。

(ii) $(\mathbb{Z}/7\mathbb{Z})^\times$ は巡回群であることを生成元を与えることによって示せ。

8. (i) $(\mathbb{Z}/8\mathbb{Z})^\times$ の元を具体的にすべてあげよ。

(ii) $(\mathbb{Z}/8\mathbb{Z})^\times$ は巡回群であるかないか，具体的に調べて判定せよ。

9. 整数 m, n の最大公約数を d（特に m, n が互いに素なら $d = 1$）とするとき，$am + bn = d$ を満たす整数 a, b が存在する（Euclid 互除法によって証明できる）。これを利用して以下に答えよ。

(i) $(\mathbb{Z}/n\mathbb{Z})^\times$ は $1, 2, \ldots, n-1$ のうち n と互いに素なもの全体であることを示せ。

(ii) 特に素数 p に対して $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$, $\#(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$, よって $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup (\mathbb{Z}/p\mathbb{Z})^\times$ は体であることを示せ。

10. p は素数，n は自然数とする。$\#(\mathbb{Z}/p^n\mathbb{Z})^\times$ を p, n を用いた式であらわせ。

11. 次の同値を示せ：「有限群 G が巡回群である $\iff$ 任意の自然数 m に対して $x^m = e$ を満たす G の元 x の個数は m 以下である」

Notation

正の整数 n に対して，整数を n で割った余り全体の集合を $\mathbb{Z}/n\mathbb{Z}$ とかく。

(i) $\mathbb{Z}/n\mathbb{Z}$ は自然に加法 $(a + b \mod n)$ が定義できて，それによって可換群となる；例えば $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ において

$$2 + 2 \equiv 4 \mod 5, \quad 1 + 4 = 4 + 1 \equiv 0 \mod 5,$$

$$2{+}3 = 3{+}2 \equiv 0 \mod 5, \quad 2{+}4 = 4{+}2 \equiv 1 \mod 5, \quad 4{+}4 \equiv 3 \mod 5$$

など。また 0 が単位元，1 の逆元 $-1 \equiv 4 \mod 5$，など。さらに $n = 1$ のとき $\mathbb{Z}/1\mathbb{Z} = \{0\}$，$n > 1$ のとき $\mathbb{Z}/n\mathbb{Z}$ は 1 で生成される位数 n の巡回群である;

$$\mathbb{Z}/n\mathbb{Z} = \langle 1 \mid n1 \equiv 0 \rangle \simeq \langle \sigma \mid \sigma^n = e \rangle; \quad 1 \mapsto \sigma, \quad k1 \mapsto \sigma^k$$

(ii) $\mathbb{Z}/n\mathbb{Z}$ には自然に乗法 $(ab \mod n)$ も定義できる。このとき単位元は $1 \in \mathbb{Z}/n\mathbb{Z}$ であるが，$0 \in \mathbb{Z}/n\mathbb{Z}$ の逆元は存在しない。よって $\mathbb{Z}/n\mathbb{Z}$ 全体は乗法に関して群にはならない。一方で乗法に関する $\mathbb{Z}/n\mathbb{Z}$ の可逆元全体を $(\mathbb{Z}/n\mathbb{Z})^\times$ とすると，これは乗法に関して可換群となる。