

代数学基礎演習 II

1. 12 次巡回群 $\langle \sigma \mid \sigma^{12} = e \rangle \simeq \mathbb{Z}/12\mathbb{Z}$ の部分群をすべて求めよ。
2. (i) 3 次対称群 $\mathfrak{S}_3$ の部分群をすべてあげよ。
 (ii) 上で与えた非自明な部分群 H (4 つ存在) のそれぞれについて, $\mathfrak{S}_3$ での相異なる左 H コセットをすべて具体的にかきあげ, それらを用いて $\mathfrak{S}_3$ の左 H コセット分割を与えよ。
3. $\mathbb{Z}$ 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。
4. 「 H が G の部分群」 $\iff$ 「任意の $x, y \in H$ に対して $x^{-1}y \in H$ 」を示せ。
5. n 次巡回群 $G = \langle \sigma \mid \sigma^n = e \rangle$ は n の任意の約数 m を位数とする部分群 H_m を丁度 1 つだけもつことを H_m を具体的に与えることによって示せ。さらに H_m それぞれは m 次巡回群であることを示せ。
6. 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。
7. $G = \langle \sigma \mid \sigma^n = e \rangle$ を n 次巡回群とする。 σ^k の位数を n や (n, k) (n と k の最大公約数) を用いてあらわせ。
8. (A) 「 G は有限アーベルで, かつさらに任意の $n = 1, 2, \dots$ に対し $x^n = e$ を満たす G の元の個数は n 以下である」ならば G は巡回群であることを次のようにして示せ:
 G の元のうち位数が最大のものをひとつとって α とする。 $N = \text{ord } \alpha$ とおく。 G の任意の元 β をとり, $n = \text{ord } \beta$ とする。
 (i) もし $n \nmid N$ ならば, ある素数のべき $q = p^r$ で $q \mid n$ であるが $q \nmid N$ をみたすものが存在する。これについて $\alpha\beta^{n/q}$ の位数を調べて矛盾を導き, 従って $n \mid N$ であることを示せ。
 (ii) 仮定 (A) より $\beta \in \{e, \alpha^{N/n}, \alpha^{2N/n}, \dots\}$ であり, 従って G は巡回群であることを結論せよ。
9. (i) 乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$ (定義は Notation 参照) の元を具体的にすべてあげよ。

(ii) $2^{-1}, 3^{-1}, 6^{-1} \in (\mathbb{Z}/7\mathbb{Z})^\times$ をそれぞれ求めよ。

(iii) $(\mathbb{Z}/7\mathbb{Z})^\times$ 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。

10. (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。

11. 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 $1, 2, \dots, n-1$ のうち n と互いに素なものの全体であることを示せ。

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

12. 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。

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 ($a + b \pmod n$) 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

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

$$2 + 3 = 3 + 2 \equiv 0 \pmod 5, \quad 2 + 4 = 4 + 2 \equiv 1 \pmod 5, \quad 4 + 4 \equiv 3 \pmod 5$$

など。また 0 が単位元, 1 の逆元 $-1 \equiv 4 \pmod 5$, 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 ($ab \pmod n$) 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 $(\mathbb{Z}/n\mathbb{Z})^\times$ とかくと, これは乗法に関して可換群となる。

たとえば $(\mathbb{Z}/17\mathbb{Z})^\times$ において

$$6 \cdot 3 = 18 \equiv 1, \quad 8 \cdot 15 = 120 \equiv 1 \pmod{17}$$

より $6^{-1} = 3 \in (\mathbb{Z}/17\mathbb{Z})^\times$, $8^{-1} = 15 \in (\mathbb{Z}/17\mathbb{Z})^\times$ など。また $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$, $5^{-1} = 5$ である。