5 群の例: 整数の剰余群

$\mathbb{Z}$ を整数全体の集合とする. 自然数 $n \in \mathbb{N}$ をひとつとる. 各整数 $a \in \mathbb{Z}$ について, n を法として a と合同な整数全体の集合を $\bar{a}$ と書くことにする:

$$\bar{a} = \{z \in \mathbb{Z} \mid z \equiv a \pmod{n}\}.$$

この $\bar{a}$ を,「a を含む mod n の**剰余類**」と呼ぶ. $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ と書けば,

$$\bar{a} = a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\}$$

である. mod n の剰余類全体の集合を $\mathbb{Z}/n\mathbb{Z}$ と書く[2]. $\mathbb{Z}/n\mathbb{Z}$ は実際には n 個の元からなる有限集合であり,

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

と書ける. だから, 平たく言えば, これは整数を n で割った「余り」全体の集合とみなせる. 以下, 特に誤解の恐れがないときは $\bar{a}$ を単に a と書くこともある.

ここで, $\mathbb{Z}/n\mathbb{Z}$ の演算 $+$ を

$$\bar{a} + \bar{b} = \overline{a+b}$$

により定義する.

問題 5.0 この演算 $+$ が well-defined (きちんと定義されている) かどうかを確かめよ. 具体的には, $a, a', b, b' \in \mathbb{Z}$, $\bar{a} = \bar{a'}$, $\bar{b} = \bar{b'}$ のときにちゃんと $\overline{a+b} = \overline{a'+b'}$ になるのかどうかがあまり明らかではないので, それを確かめよ.

問題 5.1 (1) $(\mathbb{Z}/n\mathbb{Z}, +)$ が群になることを示せ.
(2) さらに, $\mathbb{Z}/n\mathbb{Z}$ は巡回群であることを示せ.

この群 $\mathbb{Z}/n\mathbb{Z}$ を mod n の**剰余群**と呼ぶ.

問題 5.2 次の元の位数を求めよ.
(1) $2 \in \mathbb{Z}/100\mathbb{Z}$
(2) $3 \in \mathbb{Z}/100\mathbb{Z}$
(3) $100 \in \mathbb{Z}/101\mathbb{Z}$

---

[1]ホームページ http://www.math.tsukuba.ac.jp/~amano/lec2012-2/e-algebra-ex/index.html

[2]教科書の記述などとは少し異なりますが, 本質的には同じものです. 「集合の集合」なので少し分かりにくいですが, 線形代数で学んだ「商空間」と似たようなものなので, それを思い出しながら理解してください.