6 群の例: $\mathbb{Z}/p\mathbb{Z}$ の乗法群

前回の $\mathbb{Z}/n\mathbb{Z}$ には和 $+$ だけでなく, 積 $\cdot$ を

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

により定めることができる.

問題 6.0 この積 $\cdot$ が well-defined かどうか確かめよ.

実は $\mathbb{Z}/n\mathbb{Z}$ は前回定義した和 $+$ と上記の積 $\cdot$ により**環**の構造をもつ (時間があれば, 環の定義を調べて確かめてみてください).

問題 6.1 (1) p を素数とする. 任意の $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ $(a, b \in \mathbb{Z})$ について,

$$\bar{a} \cdot \bar{b} = \bar{0} \quad \Leftrightarrow \quad \bar{a} = \bar{0} \text{ または } \bar{b} = \bar{0}$$

が成立することを示せ.
(2) n が素数でないときは上記は成立しない. つまり, ある $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ が存在して $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ かつ $\bar{a} \cdot \bar{b} = \bar{0}$ が成立する. そのような例を挙げよ.

p を素数とするとき, 上記の (1) がいえれば, $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ について, もし $\bar{a} \neq 0$ かつ $\bar{b} \neq \bar{0}$ ならば $\bar{a} \cdot \bar{b} \neq \bar{0}$ であることが分かる. 言い換えれば,

$$(\mathbb{Z}/p\mathbb{Z})^\times := (\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\} = \{\bar{1}, \cdots, \overline{p-1}\}$$

とおくと, $(\mathbb{Z}/p\mathbb{Z})^\times$ は乗法 $\cdot$ により閉じている.

問題 6.2 上で定義した $(\mathbb{Z}/p\mathbb{Z})^\times$ は乗法 $\cdot$ により群をなすことを示せ.

次回のプリントで証明するが, 実は $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群になることが知られている.

問題 6.3 (1) $(\mathbb{Z}/5\mathbb{Z})^\times$ が巡回群であることを確かめよ.
(2) $(\mathbb{Z}/13\mathbb{Z})^\times$ が巡回群であることを確かめよ.

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