定理 2.2 の証明

担当：大矢 浩徳 (OYA Hironori)

本資料では，代数学 I 第 3 回講義資料定理 2.2 の証明を行う．

定理 2.2

$n \in \mathbb{Z}_{>0}$ とする．k を n の約数としたとき，

$$H_k \coloneqq \{[ka]_n \mid a \in \mathbb{Z}\} \subset \mathbb{Z}/n\mathbb{Z}$$

は $(\mathbb{Z}/n\mathbb{Z}, +)$ の位数 n/k の部分群である．さらに，$(\mathbb{Z}/n\mathbb{Z}, +)$ の部分群はこの形のもので尽くされる．

証明. H_k が位数 n/k の部分群であること：任意の 2 元 $[ka]_n, [kb]_n \in H_k$ に対し，

$$[ka]_n + [kb]_n = [ka + kb]_n = [k(a+b)]_n \in H_k, \qquad -[ka]_n = [-ka]_n = [k(-a)]_n \in H_k$$

となるので，命題 1.5 より H_k は $\mathbb{Z}/n\mathbb{Z}$ の部分群である．さらに，$n = \ell k$ としたとき，$[\ell k]_n = [n]_n = [0]_n$ であることに注意すると，H_k は具体的には

$$H_k = \{[0]_n, [k]_n, [2k]_n, \ldots, [(\ell-1)k]_n\}$$

と書ける．よって，H_k の元の個数は $\ell = n/k$ 個である．
部分群が H_k の形のものに限られること：まず，

$$H_1 = \{[a]_n \mid a \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$$
$$H_n = \{[na]_n \mid a \in \mathbb{Z}\} = \{[0]_n\}$$

なので，自明な部分群は確かに H_k の形で表されることがわかる (1 も n も n の約数であることに注意)．次に，$\mathbb{Z}/n\mathbb{Z}$ の非自明な部分群 H が必ず n のある約数 k を用いて H_k の形で書けることを示そう．$[k]_n \in H$ となる $1 \leq k \leq n-1$ で最小のものを k_0 とする．(H は非自明なので $[0]_n$ 以外の元を少なくとも 1 つは含むため，このような k_0 は必ず 1 つ定まる．) このとき，

$$H = H_{k_0} \coloneqq \{[k_0 a]_n \mid a \in \mathbb{Z}\}$$

であることを示す．H は部分群であるから，$[k_0]_n$ を何度も足し合わせたもの，およびその逆元を全て含むので，

$$H_{k_0} = \{[k_0 a]_n \mid a \in \mathbb{Z}\} \subset H$$

である．次に，$[m]_n \in H$ かつ $[m]_n \notin H_{k_0}$ となる $[m]_n$ $(1 \leq m \leq n-1)$ が存在したとする．このとき，m を k_0 で割った商を q，余りを r とすると，$0 \leq r < k_0$ で，

$$m = k_0 q + r$$

である．いま，$[k_0 q]_n \in H_{k_0} \subset H$ であることに注意すると，H は部分群であることより，

$$[m]_n - [k_0 q]_n = [r]_n \in H$$

である．ここで，$r < k_0$ なので $r \geq 1$ だと，これは k_0 の最小性に反する．よって，$r = 0$，つまり，$m = k_0 q$ となる．しかし，このとき $[m]_n = [k_0 q]_n \in H_{k_0}$ となり，$[m]_n$ の取り方に矛盾する．よって，背理法により，このような $[m]_n$ は存在せず，$H = H_{k_0}$ であることがわかる．

最後に k_0 が n の約数であることを示そう．n を k_0 で割った商を q'，余りを r' とすると，$0 \leq r' < k_0$ で，

$$n = k_0 q' + r'$$

である．ここで，$[n]_n = [0]_n \in H_{k_0}, [k_0 q']_n \in H_{k_0}$ であることより，H_{k_0} が部分群であることに注意すると，

$$[n]_n - [k_0 q']_n = [r']_n \in H_{k_0} = H$$

となる．ここで，$r' < k_0$ なので $r' \geq 1$ だと，これは再び k_0 の最小性に反する．よって，$r' = 0$，つまり，$n = k_0 q'$ となる．よって，k_0 は n の約数である． □