暗号の数理問題解説 #4

河野

演習問題 *1.8　(星印∗のついた問題は全員に課す問題ではない。興味があり，意欲のある人はチャレンジしてみて下さい。) 剰余群を定義するとき G を可換群として定義したが，一般の群に対しても H がある種の性質をみたすとき定義できる。G を群とし，H を部分群とする。H が次の性質を満たすとき**正規部分群** (*normal subgroup*) と呼ぶ。

$$\text{任意の } g \in G \text{ と任意の } h \in H \text{ に対し } g^{-1}hg \in H \text{ が成立する。}$$

次を示せ。G を群とし，H をその正規部分群とする。このとき剰余類 G/H に $[a] \cdot [b] = [ab]$ によって演算を定義できる。

代表元によらず積が定義できることを示せばよいので，$[a] = [a']$ かつ $[b] = [b']$ のとき $[ab] = [a'b']$ を示せばよい。$[a] = [a']$ より $a'a^{-1} \in H$ となっている。$[b] = [b']$ より $b'b^{-1} \in H$ となっている。$(a'b')(ab)^{-1} \in H$ が示されれば $[ab] = [a'b']$ が成立し証明が終わる。

$$(a'b')(ab)^{-1} = (a'b')b^{-1}a^{-1} = a'(b'b^{-1})a^{-1}$$

となるここで $h = b'b^{-1}$ とおくと $h \in H$ である。

$$a'ha^{-1} = a'eha^{-1} = a'(a^{-1}a)ha^{-1} = (a'a^{-1})aha^{-1} = (a'a^{-1})\left(a^{-1}\right)^{-1}ha^{-1}$$

となるが $a'a^{-1} \in H$ かつ $\left(a^{-1}\right)^{-1}ha^{-1} \in H$ より $a'ha^{-1} \in H$ となる。

演習問題 *1.9　乗法群 $\mathbb{S}^1$ が巡回群でないことを示せ。

$\mathbb{S}^1$ が巡回群だと仮定して矛盾を導く。$\mathbb{S}^1$ が巡回群だとすると，ある元 $z \in \mathbb{S}^1$ が存在して $\mathbb{S}^1 =< z >$ となっている。$z =\in \mathbb{S}^1$ なのである実数 $\theta \in \mathbb{R}$ が存在して $z = e^{i\theta\pi}$ となっている。θ は有理数であるか有理数でないかのいずれかである。θ が有理数のとき $m \in \mathbb{Z}$ と $n \in \mathbb{N}$ を用いて $\theta = \dfrac{m}{n}$ と表すことができる。このとき

$$z^{2n} = \left(e^{i\theta\pi}\right)^{2n} = \left(e^{i\frac{m}{n}\pi}\right)^{2n} = e^{i\frac{m}{n}2n\pi} = e^{i2n\pi} = 1$$

このとき $< z >$ は有限群になるがこれは $\mathbb{S}^1$ が無限集合ということに矛盾する。

よって $\theta \notin \mathbb{Q}$ とする。$i \in \mathbb{S}^1$ なのである $k \in \mathbb{Z}$ が存在して $i = z^k$ と書ける。$i^4 = 1$ なので $z^{4k} = \left(z^k\right)^4 = i^4 = 1$ となる。$1 = z^{4k} = \left(e^{i\theta\pi}\right)^{4k} = e^{i4\theta k\pi}$ となるので $4\theta k = m \in \mathbb{Z}$ となる。このとき $\theta = \dfrac{k}{4} \in \mathbb{Q}$ となるので矛盾。