群の学習の要（２０１８年2月２１日作成、２０１８年3月2日修正）

集合 S に対して $\mathfrak{P}(S)$ を S のべき集合とする。

$\mathbb{N}$ を自然数全体のなす集合とする。$\mathbb{N} = \{1, 2, 3, \ldots\}$ である。$\mathbb{Z}$ を整数全体のなす集合とする。$\mathbb{R}$ を実数全体のなす集合とする。$x, y \in \mathbb{R}$ に対して $J_{x,y} := \{r \in \mathbb{Z} | x \leq r \leq y\}$ とおく。

除法の原理　『$\forall r \in \mathbb{Z},\ \forall d \in \mathbb{N},\ \exists m \in \mathbb{Z},\ \exists k \in J_{0,d-1},\ r = dm + k$』
この m に対して 『$m \in J_{\frac{r-(d-1)}{d}, \frac{r}{d}}$』が成り立つ事を意識せよ。

【除法の原理は指定されない限りいちいち証明しなくて良い。】

空でない集合 G が『群』であるとは、演算 $G \times G \to G,\ (x, y) \mapsto xy$, が与えられていて『$\forall x, \forall y, \forall z \in G,\ (xy)z = x(yz)$』, 『$\exists e \in G,\ \forall x \in G,\ ex = xe = x$』および『$\forall x \in G,\ \exists x^{-1} \in G,\ x^{-1}x = xx^{-1} = e$』を満たすときにいう。 単位元 e が G の元であることを強調するとき e を e_G と書く。

G を群とする。$x \in G$ とする。$r \in \mathbb{Z}$ に対して $x^r \in G$

$$x^r := \begin{cases} e & (r = 0 \text{ のとき}) \\ xx^{r-1} & (r \in \mathbb{N} \text{ のとき}) \\ (x^{-1})^{-r} & (-r \in \mathbb{N} \text{ のとき}) \end{cases}$$

により定義する。公式

$$『\forall m, \forall n \in \mathbb{Z},\ (x^m)(x^n) = x^{m+n} \text{ および } (x^m)^n = x^{mn}』$$

が成り立つ。【この公式は指定されない限りいちいち証明しなくて良い。】

群 G の空でない部分集合 H が『G の部分群』であるとは、『$\forall x, \forall y \in H,\ xy \in H$』および『$\forall x \in H,\ x^{-1} \in H$』を満たすときにいう。

G を群とし、$x \in G$ とする。$\langle x \rangle := \{x^r | r \in \mathbb{Z}\}$ とおく。$\langle x \rangle$ は G の部分群である。【この事は指定されない限りいちいち証明しなくて良い。】

群 G の空でない部分群 N が『G の正規部分群』であるとは、『$\forall a \in G,\ \forall x \in N,\ axa^{-1} \in N$』を満たすときにいう。

G を群とし、N を G の正規部分群とする。$x \in N$ に対して $xN \in \mathfrak{P}(G)$ を $xN := \{xn | n \in N\}$ により定義する。

$$『\forall a, \forall b \in G,\ (ab)N = \{yz | y \in aN, z \in bN\}』 \quad \cdots\cdots ⓘ$$

が成り立つ。[$\because$　右辺⊂左辺を示す。　$y \in aN$, $z \in bN$ とする。$n_1 \in N$ を $y = an_1$ となるものとする。$n_2 \in N$ を $z = bn_2$ となるものとする。$yz = an_1bn_2 = abb^{-1}n_1bn_2$ である。$b = (b^{-1})^{-1}$ であるので $b^{-1}n_1b = b^{-1}n_1(b^{-1})^{-1}$ である。N は G の正規部分群であるので $b^{-1}n_1b \in N$ である。N は G の部分群であるので $b^{-1}n_1bn_2 \in N$ である。従って $yz \in (ab)N$ である。ゆえに右辺⊂左辺が成り立つ。左辺⊂右辺を示す。　$w \in (ab)N$ とする。$n_3 \in N$ を $w = abn_3$ となるものとする。$abn_3 = aebn_3$ である。N は G の部分群であるので $e \in N$ である（$\because$ $n \in N$ とすると $e = nn^{-1} \in N$）。ゆえに $w \in$ 右辺が成り立つ。ゆえに左辺⊂右辺が成り立つ。ゆえに左辺＝右辺が成り立つ。]

$$『\forall a \in G,\ a^{-1}N = \{v^{-1} | v \in aN\}』 \quad \cdots\cdots ⓘⓘ$$

が成り立つ。[$\because$　右辺⊂左辺を示す。　$n_4 \in N$ を $v = an_4$ となるものとする。$v^{-1} = n_4^{-1}a^{-1} = a^{-1}an_4^{-1}a^{-1}$ である。N は G の部分群であるので $n_4^{-1} \in N$ である。N は G の正規部分群であるので $an_4^{-1}a^{-1} \in N$ である。従って $v^{-1} \in a^{-1}N$ である。ゆえに右辺⊂左辺が成り立つ。左辺⊂右辺を示す。$u \in$ 左辺とする。$n_5 \in N$ を $u = a^{-1}n_5$ となるものとする。$u = (u^{-1})^{-1} = (n_5^{-1}a)^{-1} = (aa^{-1}n_5^{-1}a)^{-1}$ である。$a^{-1}n_5^{-1}a = a^{-1}n_5^{-1}(a^{-1})^{-1}$ であり N が G の正規部分群であるので $a^{-1}n_5^{-1}a \in N$ である。ゆえに $u \in$ 右辺が成り立つ。ゆえに左辺⊂右辺が成り立つ。ゆえに左辺＝右辺が成り立つ。]

G を群とし、N を G の正規部分群とする。$\mathfrak{P}(G)$ の部分集合 G/N を $G/N := \{xN | x \in G\}$ により定義する。ⓘ, ⓘⓘ により G/N は演算を $(xN)(yN) := (xy)N$ （$x, y \in G$）とする群である。$e_{G/N} = N$ である。群 G/N を正規部分群 N による G の『剰余群』という。

有限集合 S に対して $|S|$ を S の元の個数とする。有限集合 S の部分集合 T も有限集合であり $|T| \leq |S|$ である。

$$『有限群\ G\ と\ G\ の部分群\ H\ に対して\ \frac{|G|}{|H|} \in \mathbb{N}\ が成り立つ。』 \quad \cdots\cdots ⓘⓘⓘ$$

［∵　$x \in G$ に対して $xH \in \mathfrak{P}(G)$ を $xH := \{xh | h \in H\}$ により定義する。$x, y \in G$ に対して

$$「xH \cap yH \neq \emptyset \text{ ならば } xH = yH \text{ が成り立つ。」} \quad \cdots\cdots ①$$

（∵ $z \in xH \cap yH$ とする。$h_1 \in H$ を $z = xh_1$ となるものとする。$h_2 \in H$ を $z = yh_2$ となるものとする。$w \in xH$ とする。$h_3 \in H$ を $w = xh_3$ となるものとする。このとき $w = xh_3 = zh_1^{-1}h_3 = yh_2h_1^{-1}h_3$ より $w \in yH$ が成り立つ。ゆえに $xH \subset yH$ が成り立つ。同様にして $yH \subset xH$ が示される。ゆえに $xH = yH$ が成り立つ。） ① より

$$\begin{gathered}「\exists A \in \mathfrak{P}(G),\ A \neq \emptyset,\ G = \cup_{a \in A} aH, \\ 「\forall a_1, \forall a_2 \in A,\ a_1H \cap a_2H \neq \emptyset \Rightarrow a_1 = a_2」」 \\ \cdots\cdots ②\end{gathered}$$

が成り立つ。

$$「\forall x \in G,\ |xH| = |H| \text{ が成り立つ。」} \quad \cdots\cdots ③$$

（∵写像 $f : H \to xH,\ f(h) := xh,$ は全単射）。②, ③ より ② の A に対して $|G| = |A||H|$ が成り立つ。ゆえに $\frac{|G|}{|H|} = |A| \in \mathbb{N}$ が成り立つ。］

G を有限群とする。$x \in G$ とする。$d := |\langle x \rangle|$ とする。

$$『「\langle x \rangle = \{x^r | r \in J_{0,d-1}\}」 \text{ および } 「x^d = e」 \text{ が成り立つ。』} \cdots\cdots ⓘⓥ$$

［∵　写像 $\varphi : J_{0,d-1} \to \langle x \rangle$ を $\varphi(k) := x^k$ により定義する。φ は単射である事を背理法により示す。φ が単射でないとする。このとき「$\exists m, \exists n \in J_{0,d-1},\ m < n,\ \varphi(m) = \varphi(n)$」が成り立つ。$k := n - m$ とする。$k \in J_{1,d-1}$ である。$X := \{x^r | r \in J_{0,k-1}\}$ とする。$y \in \langle x \rangle$ とする。$s \in \mathbb{Z}$ を $y = x^s$ となるものとする。除法の原理より「$\exists t \in \mathbb{Z},\ \exists r \in J_{0,k-1},\ s = kt + r$」が成り立つ。このとき

$$\begin{aligned}&y = x^s = x^{kt+r} = x^{kt}x^r = (x^k)^t x^r = (x^{n-m})^t x^r = (x^{n+m(-1)})^t x^r \\ &= (x^n x^{m(-1)})^t x^r = (x^n (x^m)^{-1})^t x^r = (x^n (x^n)^{-1})^t x^r = ex^r = x^r \in X\end{aligned}$$

が成り立つ。ゆえに $\langle x \rangle \subseteq X$ が成り立つ。$|X| \leq k \leq d-1$ より $|\langle x \rangle| \leq d-1$ となり $|\langle x \rangle| = d$ に矛盾する。ゆえに φ は単射である。$|\langle x \rangle| = d = |J_{0,d-1}|$ より φ は全単射である。従って「$\langle x \rangle = \{x^r | r \in J_{0,d-1}\}$」が成り立つ。$x^d \in \langle x \rangle$ より 「$\exists u \in J_{0,d-1},\ x^d = x^u$」が成り立つ。$u \in J_{1,d-1}$ であれば

$\varphi(u-1) = x^{u-1} = x^u x^{-1} = x^d x^{-1} = x^{d-1} = \varphi(d-1)$ となり，φ が単射である事に矛盾である。ゆえに「$x^d = e$」が成り立つ。］

G を有限群とする。このとき

$$『「\forall x \in G,\ x^{|G|} = e\ 」が成り立つ。』\ \cdots\cdots ⓥ$$

［∵　$d := |\langle x \rangle|$ とする。ⓘⓥ より $x^d = e$ がなりたつ。$k := |G|$ とする。ⓘⓘⓘ より $\frac{k}{d} \in \mathbb{N}$ が成り立つ。ゆえに $x^k = (x^d)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$ が成り立つ。］

G を有限群とする。$x \in G$ とする。$d := |\langle x \rangle|$ とする。$r \in \mathbb{N}$ を $\frac{d}{r} \in \mathbb{N}$ となるものとする。

$$『「\exists k \in \mathbb{N},\ |\langle x^k \rangle| = r」が成り立つ。』\cdots\cdots ⓥⓘ$$

［∵　$k := \frac{d}{r}$ とする。「$\forall t \in J_{0,r-1},\ kt < k(t+1)$」かつ「$kr = d$」であるので ⓘⓥ より写像 $\psi : J_{0,r-1} \to \langle x^k \rangle,\ \psi(t) := x^{kt}$, は単射であり、$(x^k)^r = e$ である。従って ⓘⓥ より「$|\langle x^k \rangle| = r$」が成り立つ。］

G を有限群とし、N を G の正規部分群とする。このとき G/N は有限群であり、$|G/N| = \frac{|G|}{|N|}$ が成り立つ。［∵この事は ⓘⓘⓘ の証明と同様にして示される。］

G を有限群とし、N を G の正規部分群とする。このとき

$$『「\forall h \in G/N,\ \exists x \in G,\ |\langle h \rangle| = |\langle x \rangle|」が成り立つ。』\cdots\cdots ⓥⓘⓘ$$

［∵　$y \in G$ を $h = yN$ となるものとする。$r := |\langle h \rangle|$ および $d := |\langle y \rangle|$ とおく。除法の原理より「$\exists n \in \mathbb{Z},\ \exists k \in J_{0,r-1},\ d = nr + k$」が成り立つ。ⓘⓥ より $h^r = e_{G/N}$ および $y^d = e_G$ が成り立つ。従って

$$h^k = (h^r)^n h^k = h^d = (yN)^d = y^d N = eN = N = e_{G/N}$$

が成り立つ。ⓘⓥ より $k = 0$ が成り立つ。ゆえに $\frac{d}{r} = n \in \mathbb{Z}$ が成り立つ。$d > 0,\ r > 0$ より $\frac{d}{r} \in \mathbb{N}$ である。よって ⓥⓘ より ⓥⓘⓘ が成り立つ。］