群論はじめの一歩(3)

3.1 剰余類

H を群G の部分群とするとき、次の同値関係 “~ “が定義できる

$x \sim y$ ⇔ ある$h \in H$ に対して$x = yh$と書ける

同値関係:①反射律 reflexive②対称律 symetric③推移律 transitive

① $e \in H$ であるから、$x = xe$ は $x \sim x$ を意味する

②$x \sim y$ ⇔ $y \sim x$ 。なぜなら $x \sim y$のとき$x = yh$ ， $h \in H$と書ける。このとき、h^{-1} を右から“かける”と$y = xh^{-1}$ となる。$h^{-1} \in H$ であるから$y \sim x$を意味する。

③$x \sim y, y \sim z \Rightarrow x \sim z$ 。なぜなら$x = yh_1, y = zh_2$ ，$h_1, h_2 \in H$ であるが、これから$x = yh_1 = zh_2h_1$ となり、$h_1h_2 \in H$ に注意すれば$x \sim z$がわかる。■

G上の同値関係はGの分割をもたらす。すなわち、$E_x = \{y \in G | x \sim y\}$ とおくと、

①$G = \cup E_x$	②$E_x = E_y$ か$E_x \cap E_y = \phi$ のいずれかである。

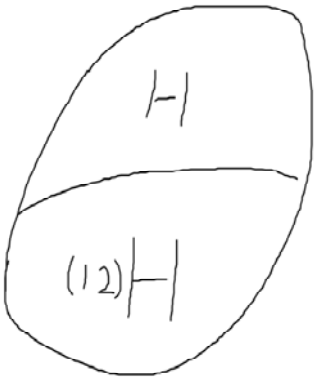
①については、$G \supset \cup E_x$は定義から明らかだが、$x \sim x$がいつも成り立ち和集合はすべての$x \in G$ についてとるわけだから$G \subset \cup E_x$も言える。

②については、$x \sim y \Leftrightarrow E_x = E_y$ を言えばよい。$x \approx y$ で$E_x \cap E_y \neq \phi$とすると$z \in E_x \cap E_y$ がとれ、$z \sim x, z \sim y$ から$x \sim y$ となり矛盾を招くから。そこで、

より、$E_x \subset E_y$ をしめす。$z \in E_x$ とすると、$z \sim x$ であり、$x \sim y$ より、$z \sim y$ すなわち、$z \in E_y$ 。同様にして $E_x \supset E_y$ が示され、結局 $E_x = E_y$ となる。■

定義より、$E_x = \{y \in G | x \sim y\} = \{y \in G | y = xh, h \in H\} = xH$ と書き直される。そして、xH は G における H の左剰余類と呼ばれる。(left coset in G modulo H)。

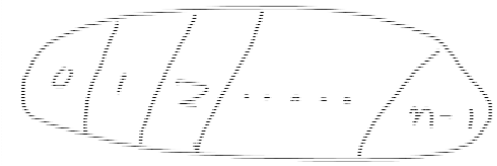
[例 $G = (S_3, \circ)$] $H = \{e, (123), (132)\}$ とする。このとき $eH = H = \{e, (123), (132)\}$ 、$(12)H = \{(12), (23), (13)\}$ となり、$G = H \cup (12)H$ のように分割される。



[例 $G = (\mathbb{Z}, +)$]

$H = n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$ n の倍数。

$0+H, 1+H, \cdots, (n-1)+H$ のように n 個の剰余類に分割される。つまり整数を n でわったときあまりは、$0, 1, 2, \cdots, n-1$ のものに分割



剰余類は右剰余類 Hx も同様に定義されるが、左剰余類と右剰余類は一般には異なる。G が可換群（アーベル群）の場合は右剰余類と左剰余類は同じである。

［例 $G=(S_3,\circ)$］ S_3 は可換群でないことを以前見た。そこで、$H=\{e,(12)\}$ とおくと、

左剰余類 $(13)H=\{(13),(123)\}$ ，$(23)H=\{(23),(132)\}$

右剰余類 $H(13)=\{(13),(132)\}$，$H(23)=\{(23),(123)\}$

というように異なっている。

3.2 剰余類の大きさ

命題 G における H の剰余類の濃度（個数）は H と同じ濃度（個数）である。

証明）$x\in G$ を一つ固定する。そして、$\eta_x : H\to xH$ なる写像 $\eta_x(h)=xh$ を考える。η_x が全単射であることを示せば証明は終わる。

①単射：$\eta_x(h_1)=\eta_x(h_1)$ を仮定する。すなわち、$xh_1=xh_2$ となるが消去法則を使って、$h_1=h_2$ となる。

②全射：$z\in xH$ を任意にとる。そのとき、ある $h\in H$ を見つけ出して $z=xh$ とできる。つまり $\eta_x(h)=z$ となる h が取れる。■

定義：①G の位数 $|G|$ とは G の要素の個数のことである（有限の場合）。

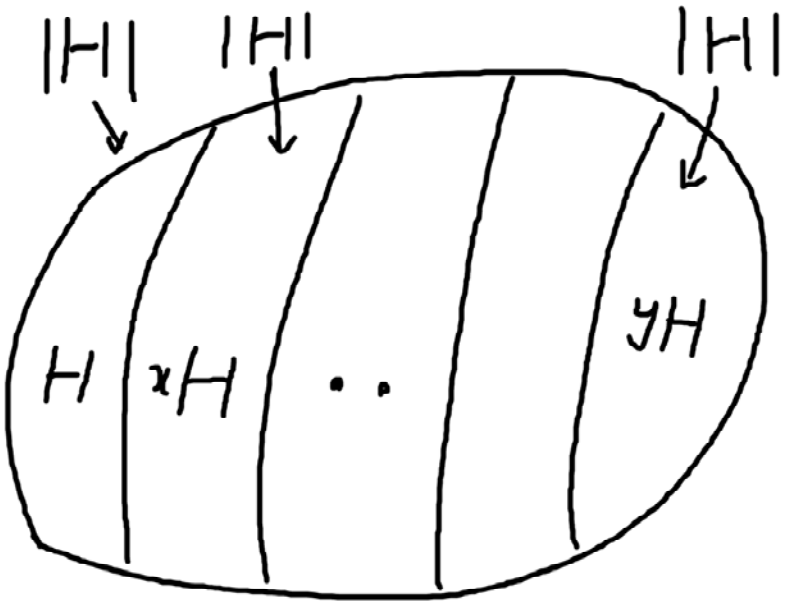
② $x \in G$ の位数$|x|$ は$x^n = e$ となる最小の自然数$n \geq 1$ のことである。

③G におけるH の指数$[G:H]$ とは、H に対する剰余類（右、左）の個数のことである。

3.3 ラグランジュの定理

定理 G を有限群、H をGの部分群とする。 Hの位数はGの位数の約数である。

3.1 節で$G = \cup E_x$を示した。ここで、$E_x = xH$ と書けるが、$|xH| = |H|$ である。なぜなら、xH は$H = \{h_1, \cdots, h_k\}$とすると、$xH = \{xh_1, \cdots, xh_k\}$であり個数は変わらない。したがって、$G$の位数は剰余類の個数$\times$ H の位数（$|G| = (\#\cos ets)|H|$ ）。剰余類への分割$G = H \cup xH \cup \cdots \cup yH$ は下図のように



おなじ大きさに分割されているわけである。■

証明の最後の式は、$|G|=(\#\cos ets)|H|=[G:H]|H|$であり、

$$[G:H]=\frac{|G|}{|H|}$$

という美しい等式として表される。

系　$x\in G$に対して、位数$|x|$はGの位数$|G|$の約数である。

部分群として$H=\{x,x^2,\cdots\}=\langle x\rangle$ を考えれば上記の定理が適用できる■

[例 （$\mathbb{Z}/10,+$）]

群$(\mathbb{Z}/10,+)$というのは整数で 10 で割った余りが等しいものは同一視してその演算は＋であるが10を法とする合同演算をおこなう。たとえば、

$23=3$ ， $5+8=3$ のようにする。

$(\mathbb{Z}/10,+)=\{0,1,\cdots,9\}$ の部分群として、$H_1=\{0,5\}$ ， $H_2=\{0,2,4,6,8\}$ があり、

$|H_1|=2$,$|H_2|=5$であり、10 の約数は、$2,5$ であるから、自明なもの

$e=\{0\},G=\{0,1,\cdots,9\}$ を除くと$(\mathbb{Z}/10,+)$の部分群は、H_1,H_2 だけであることがわかる。

また、$g=5$ の位数は$g^2=5+5=0$であるから位数$|g|$ は 2、$g=2$ の位数は$g^5=2+2+2+2+2=0$ より位数は 5.　これらを一覧表にすると、

g	$\lvert g \rvert$
0	1
5	2
$2,4,6,8$	5
$1,3,7,9$	10

となる。