代数系の基礎要綱 #3

2002–5–9　　河野

次の定理は有用である。

定理 2.10 [ラグランジェの定理] 群 G の部分群 H に対し H の位数 $|H|$ は群 G の位数 $|G|$ の約数である。

定理 2.10 を示すために次の命題を示す。この命題は有限でない群に関しても成立する。

命題 2.11 群 G とその部分群 H に対し G 上の関係 $\sim$ を $g \sim h \Longleftrightarrow g^{-1}h \in H$ で定義する。このときこの関係は同値関係になる。

元 a を含む同値類は $aH = \{\, k \mid \exists h \in H;\, k = ah \,\}$ という形をしている。また aH に含まれる元の数は H に含まれる元の数に等しい; $|aH| = |H|$。

証明　同値関係を示すには 3 つの性質の成立を言えばよい。(**自同律**) 任意の元 g に対し $g^{-1}g = e \in H$ なので $g \sim g$ が分かる。(**対称律**) $g \sim h$ を仮定する。$g^{-1}h \in H$ なので逆元をとると $(g^{-1}h)^{-1} = h^{-1}g$ で，逆元も H に属するので $h \sim g$ が分かる。(**推移律**) $g \sim h$, $h \sim k$ とする。$g^{-1}h \in H$, $h^{-1}k \in H$ より，その積も H の元なので $g^{-1}k = g^{-1}h \cdot h^{-1}k \in H$ となり，$g \sim k$ が分かる。

b を $a \sim b$ となる元とする。このとき $a^{-1}b \in H$ なので，H の元 h が存在して $a^{-1}b = h$ となる。このとき $b = ah$ と書かれる。逆に aH の元 b は H のある元 h を用いて $b = ah$ と書けるので，$a \sim b$ が成立する。

H から aH への写像 f_a を $f_a(h) = ah$ で定義する。$f_{a^{-1}}$ が f_a の逆写像なので f_a は全単射である。よって $|H| = |aH|$ が成立する。

系 2.12 群 G の元 g に対し元 g の位数は群の位数の約数である。

位数の小さい群を決定していこう。位数が 1 である群は $G = \{e\}$ の 1 種類である。

特別な場合として位数が素数の群は次で分かる。

命題 2.13 位数が素数 p の群は位数 p の巡回群に同型である。

証明　群 G の位数は 2 以上なので，G には単位元以外の元が存在する。それを g とする。g の位数は群 G の位数の約数だが，素数なので p または 1 である。1 のときは単位元になるので位数は p となる。このとき $G = \langle\, g \,\rangle$ となるので G は巡回群となる。 ∎

位数 4 の群を考えよう。位数 4 の群はすでに 2 つ登場している。1 つは位数 4 の巡回群 $\boldsymbol{Z}_4$，もう 1 つは位数 2 の巡回群 2 個の直和 $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ である。この 2 つは同型ではない (何故か?)。

群 G を位数 4 の群とする。これが $\boldsymbol{Z}_4$ または $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ に同型である事を示す。群 G の元 g の位数は g が単位元でなければ，4 または 2 である。(**位数 4 の元が存在する場合**) g が位数 4 の元とすると，$G = \langle\, g \,\rangle$ となるので，G は位数 4 の巡回群となる。(**位数 4 の元が存在しない場合**) g を位数 2 の元とする。G には他に位数 2 の元が存在するので $h \neq g$ となる位数 2 の元をとってくる。このとき，e, g, h, gh は互いに異なる G の元なので，$G = \{e, g, h, gh\}$ である。このとき G から $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ への写像 F を $F(e) = (0,0)$, $F(g) = (1,0)$, $F(h) = (0,1)$, $F(gh) = (1,1)$ と決めると F は G から $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ への同型写像である (何故か?)。

演習問題 2.8　$\boldsymbol{Z}_4$ と $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ が同型でない事を示せ。
演習問題 2.9　上の F が同型写像である事を示せ。

引き続き位数の小さい群を調べていくが，そのために少し道具を用意しよう。

群 G の 2 つの部分群 H, K に対し $HK = \{\, g \mid\ g = hk, h \in H, k \in K \,\}$ と置く。HK は G の部分集合ではあるが，一般に部分群にはならない。しかし次が成立する。

命題 2.14

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

証明　$H \bigoplus K$ の位数は $|H| \cdot |K|$ である。$H \bigoplus K$ から HK への上への写像 F を $F(h,k) = hk$ で定義する。HK の任意の元 g に対し $F^{-1}(g)$ の元の個数が $|H \cap K|$ に等しい事を言えば証明が終わる。

最初に $g = e$ の時を示す。$F^{-1}(e)$ から $H \cap K$ への写像 u を次の様に決める。$(h,k) \in F^{-1}(e)$ を任意にとってくる。このとき $hk = e$ より $h = k^{-1}$。k^{-1} は K の元なので h は $H \cap K$ の元である。このとき $u(h,k) = h$ とする。この u は全単射である (何故か?)。一般の g に対しては以下の様に $F^{-1}(g)$ から $H \cap K$ への写像 u_g を決める。$hk = g$ となる h と k を 1 組固定する。$(h',k') \in F^{-1}(g)$ を任意にとってくる。$h_1 = h^{-1}h'$, $k_1 = k'k^{-1}$ と置くと，$h_1 \in H$, $k_1 \in K$ である。$hk = g = h'k'$ より，$hk = hh_1k_1k$ なので $h_1k_1 = e$ である。前と同様に $h_1 \in H \cap K$ が分かる。このとき $u_g(h',k') = h_1$ とする。この u_g は全単射である (何故か?)。

演習問題 2.10　証明中の u 及び u_g が全単射である事を示せ。

群 G の元 a に対し写像 J_a を $J_a(g) = a^{-1}ga$ で定義する。

命題 2.15 任意の a に対し J_a は G 上の同型写像である。

特に部分群 H に対し $J_a(H)$ はまた G の部分群になる。これを H の**共役部分群** (*conjugate subgroup*) という。また元 g に対し $J_a(g) = a^{-1}ga$ を g の**共役元** (*conjugate element*) という。部分群 H が任意の $a \in G$ に対し $J_a(H) = H$ という性質を持つとき**正規部分群** (*normal subgroup*) といい，$H \triangleleft G$ と書く。H が正規部分群のとき J_a を H に制限した写像 (これも同じ記号 J_a で表す) は H 上の同型写像を与える。

命題 2.16 G を群とし，H, K をその部分群とする。
(1) HK が部分群をなすための必要十分条件は $HK = KH$ が成り立つ事である。
(2) H, K の少なくとも一方が正規部分群なら HK は部分群をなす。
(3) H, K ともに正規部分群ならば HK も正規部分群である。

証明
(1) $HK = KH$ が成立しているとする。HK の任意の元 hk と $h'k'$ に対し $hk \cdot h'k' \in HK$ を示す。$kh' \in KH = HK$ なので $h_1 \in H$ と $k_1 \in K$ が存在して $kh' = h_1k_1$ となる。このとき $hkh'k' = hh_1k_1k'$ が成立し, $hh_1 \in H$, $k_1k' \in K$ なので成立する。次に任意の $hk \in H$ に対し $(hk)^{-1} \in HK$ を示す。$hk^{-1} = k^{-1}h^{-1}$ で，上と同様の議論で $k^{-1}h^{-1} = h_1k_1$ となる $h_1 \in H$ と $k_1 \in K$ が存在するのでこれも HK の元である。よって HK は部分群になる。

HK が部分群であると仮定する。任意の元 $k \in K$ と $h \in H$ に対し，k も h も HK の元なので $kh \in HK$ が成立する。よって $KH \subseteq HK$ となる。G の部分集合 A に対し $A^{-1} = \left\{ a^{-1} \,\middle|\, a \in A \right\}$ と置く。H, K は部分群なので $H^{-1} = H$, $K^{-1} = K$ が成立する。$KH \subseteq HK$ より $(KH)^{-1} \subseteq (HK)^{-1} = K^{-1}H^{-1}$ が成立するので，$HK \subseteq KH$ が得られ，$HK = KH$ が分かる。

(2) $H \triangleleft G$ とする。任意の $k \in K$ に対し $k^{-1}Hk = H$ となるので，$HK = KH$ が分かる。よって (1) より HK は部分群をなす。

(3) 演習問題に。

演習問題 2.11　(3) を証明せよ。

演習問題 2.12　命題の証明で用いた A^{-1} に関する性質を抜き出し証明せよ。

演習問題 2.13　郡 G の部分群 H に対し $\dfrac{|G|}{|H|}$ を**指数** (*index*) という。指数 2 の部分群は正規部分群である事を示せ。

次の 2 つの定理は有限群論では基本的である。

定理 2.17 [Sylow's theorem] 有限群 G に対しその位数を割り切る素数を p とする。このとき位数が p の冪である群を **p–群** (*p–group*) という。また群の位数を割り切る最大の p 冪を p^e とするとき，位数 p^e の部分群を**シロー p–部分群** (*Sylow p–subgroup*) と呼ぶ。

(1) 群 G の位数 p を割り切る各素数 p に対しシロー p–部分群は存在する。

(2) G の p–部分群はあるシロー p–部分群に含まれる。

(3) シロー p–部分群はお互いに共役である。

(4) シロー p–部分群の個数は $kp + 1$ 個である。

定理 2.18 G を有限アーベル群とする。このとき正整数 $d_1, \ldots, d_n$ が存在して

$$G \cong \boldsymbol{Z}_{d_1} \bigoplus \cdots \bigoplus \boldsymbol{Z}_{d_n}$$

が成立する。d_i $(i = 1, \ldots, n)$ に各 d_i が d_{i+1} を割り切るという条件をつけるとこの数は G に対し一意的に決まる。

演習問題 ****2.14　(1) 定理 2.17 を証明せよ。

(2) 定理 2.18 を証明せよ。