情報数理 I 要綱 #3

河野

イントロで考えたように群に対しその演算表が得られると群の構造が分かる。その意味で「群が分かった」と言ってもよいだろう。しかし演算表は有限群 (G が有限集合である様な群) でなければ演算表は作ることができないし，集合が大きくなれば演算表を作るのは大変である。ここでは「群が分かる」別の方法を考える。

G を群とし S を G の部分集合とする (部分群とは限らない。というか部分群の場合はでてこない)。S を含む G の最小の部分群を $\langle S \rangle$ と書き，G において S で**生成される**部分群といい，S を G の**生成系**と呼び,「S は G を生成する」という。

$S = \{g_1, \ldots, g_n\}$ のとき $\langle S \rangle$ は $\langle \{g_1, \ldots, g_n\} \rangle$ であるが，$\langle g_1, \ldots, g_n \rangle$ と書く事が多い。

イントロで扱った $M(\Delta_3) = \{id, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$ を例にとる。$S = \{\sigma_1\}$ とする。σ_1 を含む部分群 H は σ_1^2 を含む必要がある。また id を含む必要がある。$H = \{id, \sigma_1, \sigma_2\}$ はそれ自身部分群なので $H = \langle \sigma_1 \rangle$ である。同様に $\langle \tau_1 \rangle = \{id, \tau_1\}$，$M(\Delta_3) = \langle \sigma_1, \tau_1 \rangle$ が分かる。

実は生成系の定義はこれでは不十分である。その様な部分群の存在を一般的に保証する必要がある。そのために次の補題を使う。

補題 1.11 H_1, H_2 を G の部分群とすると $H_1 \cap H_2$ も G の部分群である。

証明　命題 1.8 の 2 つの条件をチェックすればよい。(1) $h, h' \in H_1 \cap H_2$ とする。H_1 は部分群なので $hh' \in H_1$ であり，同様に H_2 も部分群なので $hh' \in H_2$ である。よって $hh' \in H_1 \cap H_2$ である。(2) $h \in H_1 \cap H_2$ とする。H_1, H_2 は部分群なので $h^{-1} \in H_1$ 及び $h^{-1} \in H_2$ が成立する。よって $h^{-1} \in H_1 \cap H_2$ となる。以上により $H_1 \cap H_2$ は部分群である事が分かる。 ∎

この補題を用いると生成される部分群の存在が保証される。G が有限群の場合 S を含む G の部分群をすべて並べそれを $H_1, H_2, \ldots, H_n$ とする。G は条件を満たしているので，その様なものは少なくとも 1 つは存在する。$H_1 \cap H_2 = N_2$ とおくと，補題より N_2 は部分群である。また $N_2 \cap H_2 = N_3$ とおくと N_3 も部分群である。以下これを繰り返すと $N_n = H_1 \cap \cdots \cap H_n$ が部分群である事が分かる。これが S を含む最小の部分群になる。

無限群の場合は無限個の集合の共通部分を考える必要があるので，ここでは扱わないが同様にできる。

1 個の元から生成される群を**巡回群** (*cyclic group*) と呼ぶ。例えば $(\boldsymbol{Z}, +)$ は $\boldsymbol{Z} = \langle 1 \rangle$ となる。何故かというと 1 を含む $\boldsymbol{Z}$ の部分群を H とする。H は 1 を含むので $2 = 1 + 1$ を含む。$3 = 1 + 2$ なので H は 3 を含む。以下同様に (厳密には数学的帰納法で) 自然数 n に対し $n \in H$ が分かる。H は部分群なので $0 \in H$ が成立している。また負の整数 $-n$ に対し，$-n$ は n の逆元であり，$n \in H$ なので $-n \in H$ である。よって $\boldsymbol{Z} = H$ となる。$\boldsymbol{Z}$ は無限集合なので，この群を**無限巡回群** (*infinite cyclic group*) と呼ぶ。

G を有限群とする。集合としての G の要素の個数を $|G|$ で表し，群 G の**位数** (*order*) と呼ぶ。G の元 g に対し $\langle g \rangle$ の位数 $|\langle g \rangle|$ を元 g の**位数** (*order*) といい $o(g)$ で表す。位数 n の巡回群を考えよう。M を平面上の合同変換群とする。σ を原点を中心とする $\dfrac{2\pi}{n}$ 回転とする。このとき $\langle \sigma \rangle = \{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ である事が分かる。この群をこれから C_n と書く。C_n は位数 n の巡回群である。

元の位数を無限の場合にも拡張して定義しておく。G を一般の (有限とは限らない) 群として g をその元とする。$\langle g \rangle \cong \boldsymbol{Z}$ のとき g の位数は無限大であるといい，$o(g) = \infty$ と書く。

命題 1.12 巡回群は $\boldsymbol{Z}$ または C_n と同型である。

これを示すため補題を 1 つ用意する。

補題 1.13 n を負でない整数とする。$n\boldsymbol{Z} = \{ np |\ p \in \boldsymbol{Z} \}$ とすると，$(n\boldsymbol{Z}, +)$ は $(\boldsymbol{Z}, +)$ の部分群である。逆に H を $(\boldsymbol{Z}, +)$ を任意の部分群とする。このときある負でない整数 n が存在して $H = (n\boldsymbol{Z}, +)$ となる。

証明　前半は命題 1.8 の条件 (1),(2) が成立する事を示せばよい。a, b を $n\boldsymbol{Z}$ の元とすると整数 p, q が存在して，$a = np, b = nq$ と書ける。$p + q$ は整数なので $a + b = n(p + q)$ となり，$a + b \in n\boldsymbol{Z}$ が分かる。$a = np \in n\boldsymbol{Z}$ とすると，$-p \in \boldsymbol{Z}$ なので $-a = n(-p) \in n\boldsymbol{Z}$ となる。以上により $n\boldsymbol{Z}$ は部分群である。

H を $\boldsymbol{Z}$ の部分群とする。$H = \{0\}$ の場合 $H = 0\boldsymbol{Z}$ なので，$H \neq \{0\}$ とする。H は 0 以外の元 p を含む。$p < 0$ のとき $-p \in H$ なので H は正の元を含む。H が含む正の元で最小なものを n とする。H は部分群なので $2n = n + n$ を含む。以下同様に (厳密には数学的帰納法) 自然数 p に対し $np \in H$ が分かる。また H は部分群なので $0 \in H$ であり，自然数 p に対し $n(-p) = -(np)$ $(np \in H)$ なので $n(-p) \in H$ が分かる。よって $n\boldsymbol{Z} \subseteq H$ が分かる。

逆に k を H の元とする。割り算の原理から整数 q, r が存在して $k = nq + r$ と書ける。ここで r は $0 \leqq r < n$ を満たしている。k が n で割り切れないと仮定すると $0 < r < n$ である。このとき $r = k + n(-q)$ となり，$k \in H, n(-q) \in H$ なので $r \in H$ となる。しかしこれは n の最小性に矛盾する。よって k は n で割り切れるので，$k \in n\boldsymbol{Z}$ となり，$H = n\boldsymbol{Z}$ が分かる。∎

命題 1.12 の証明をしよう。H を巡回群とすると，ある元 g が存在して $H = \langle g \rangle$ となっている。$\boldsymbol{Z}$ から H への写像 F を $F(n) = g^n$ で定義する。ただし $g^0 = e$(e は単位元), $n = -m$ $(m \in \boldsymbol{N})$ に対しては $g^n = g^{-m} = \left(g^{-1}\right)^m$ と定義する。このとき $g^n g^m = g^{n+m}$ が成立するので F が準同型写像である事が分かる。$F(1) = g$ なので $\mathrm{Im}(F)$ は g を含む H の部分群である。よって定義より $H = \mathrm{Im}(F)$ となる。

$\mathrm{Ker}(F)$ を考える。$\mathrm{Ker}(F) = \{0\}$ のとき F は同型写像で $H \cong \boldsymbol{Z}$ が分かる。よって $\mathrm{Ker}(F) \neq \{0\}$ とする。補題 1.13 より $\mathrm{Ker}(F) = n\boldsymbol{Z}$ (n はある自然数) となる。任意の $k \in \boldsymbol{Z}$に対し $k = nq + r$ となる整数 q, r が存在する (ただし $\leqq r < n$)。$n \in \mathrm{Ker}(F)$ より $F(n) = g^n = e$ なので $g^k = (g^n)^q g^r = g^r$ となる。また $0 \leqq r_1 < r_2 < n$ に対し $g^{r_1} = g^{r_2}$ となったとすると $g^{r_2 - r_1} = e$ となり，$r_1 - r_1 \in \mathrm{Ker}(F)$ となり矛盾。よって $g^{r_1} \neq g^{r_2}$ である。以上から $H = \mathrm{Im}(F) = \{e, g, g^2, \ldots, g^{n-1}\}$ となる。$G : C_n \to H$ を $G(\sigma^k) = g^k$ で定義すると G は同型写像になる。∎

ここで「群が分かる」演算表とは異なる方法を考える。$M(\Delta_3)$ を例にとろう。$M(\Delta_3) = \{id, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_2\}$ であった。$\sigma = \sigma_1, \tau = \tau_1$ とすると $o(\sigma) = 3, o(\tau) = 2, \tau^{-1}\sigma\tau = \sigma^2$ という関係がある。

逆にこの 3 つの関係しか知らないとして群 $M(\Delta_3) = \langle \sigma, \tau \rangle$ が決定できる事を見よう。$M(\Delta_3)$ の元は σ と τ の有限個の積で書けている。元 g の中に $\cdots\tau\sigma\tau\cdots$ という部分があったとする。$\sigma\tau = \tau\sigma^2$ なのでその部分は $\cdots\tau\sigma\tau\cdots = \cdots\tau\tau\sigma^2\cdots = \cdots\sigma^2\cdots$ とできる。また $\cdots\tau\sigma^2\tau\cdots$ という部分があったとすると $\cdots\tau\sigma^2\tau\cdots = \cdots\sigma\tau\tau\cdots = \cdots\sigma\cdots$ とできる。よって元の表記の中に τ は高々1 回しかででこないとしてよい。$\sigma\tau = \tau\sigma^2$ を用いて τ は後ろに移動できるので元の表記として考えられるのは e(単位元), $\sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ の 6 つである。これら 6 個の元はすべて異なる。例えば

$\sigma = \sigma^2$ とすると，$\sigma = e$ となるので $o(\sigma) = 3$ に矛盾する。$\sigma^2 = \sigma\tau$ とすると $\tau = \sigma^4 = \sigma$ このとき $\sigma^2 = \tau^2 = e$ となり $o(\sigma) = 3$ に矛盾等々。積がどうなるかもこの関係式から導かれる。例えば $\sigma\tau$ と $\sigma^2\tau$ の積は $\sigma\tau\sigma^2\tau = \sigma\sigma\tau\tau = \sigma^2$ となる。

ここで重要な概念である**剰余類**とラグランジェの定理に関して述べておく。

定理 1.14 [**ラグランジェの定理**] G を有限群とし，$H \leqq G$ とする。このとき $|H|$ は $|G|$ の約数である。

この定理の帰結として，例えば位数 6 の群の部分群として位数 4 のものはない事が分かる。$M(\Delta_3) = \{id, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$ は位数6の群である。その部分群をすべて書き出すと $\{id\}, \{id, \sigma_1, \sigma_2\}$, $\{id, \tau_1\}, \{id, \tau_2\}, \{id, \tau_3\}, M(\Delta_3)$ の 6 個である。これらの部分群の位数は 1,3,2,2,2,6 ですべて 6 の約数になっている。

定理を示すために剰余類というものを考える。G を群 H をその部分群とする。このとき G に次の様な同値関係を定義する。G の g, h が $g^{-1}h \in H$ となるとき g と h は同値であるといい，$g \sim h$ と書く。この関係は次の 3 つを見たし同値関係になる。1) **反射率**：$a \sim a$, 2) **対称律**：$a \sim b$ ならば $b \sim a$, 3) **推移律**：$a \sim b, b \sim c$ ならば $a \sim c$。

演習問題 1.1　上で定義した関係が反射律，対称律，推移律を満たすことを示せ。

記法を定義しておく。群 G の部分集合 (勿論部分群でもよい) を S とする。G の元 g に対し集合 $\{gs |\ s \in S\}$ を gS と書く。また $\{sg |\ s \in S\}$ を Sg と書く。$\left\{s^{-1} \middle|\ s \in S\right\}$ を S^{-1} と書く。2 つの部分集合 S_1, S_2 に対し $\{s_1 s_2 |\ s_1 \in S_1, s_2 \in S_2\}$ を $S_1 S_2$ と書く。

一般に G 上に同値関係があると，G の元はお互いに同値な元の類に分割される。この類を群 G の H に関する (**左**) **剰余類**と呼ぶ。剰余類は G のある元 g を用いて $gH = \{gh |\ h \in H\}$ と書かれる。G の元は剰余類に分割されるので，G の元 , g_1(通常単位元 e を選ぶ), $\ldots, g_n$ が存在して $G = g_1 H \cup \cdots \cup g_n H$ と書ける。これらの剰余類は共通部分を持たないので $G = g_1 H + \cdots + g_n H$ とも書かれる。

$G = M(\Delta_3)$, $H = \{id, \sigma_1, \sigma_2\}$ とする。このとき $id \sim \sigma_1 \sim \sigma_2 \not\sim \tau_1 \sim \tau_2 \sim \tau_3$ なので $G = H + \tau_1 H$ となる。

$H = \{id, \tau_1\}$ とすると，$id \sim \tau_1$, $\sigma_1 \sim \tau_3$, $\sigma_2 \sim \tau_2$ なので $G = H + \sigma_1 H + \sigma_2 H$ となる。$\sigma_1 H = \tau_3 H$, $\sigma_2 H = \tau_2 H$ なので $G = H + \tau_3 H + \tau_2 H = H + \tau_2 H + \tau_3 H$ と書いてもよい。

一般に G の H に関する剰余類の個数を G における H の**指数** (*index*) といい $|G : H|$ と表す。ラグランジェの定理は次の命題の系として出て来る。

命題 1.15 G を有限群 H をその部分群とすると，$|G : H| = \dfrac{|G|}{|H|}$ である。

証明　$G = H + g_2 H + \cdots + G_n H$ を剰余類による分割とする。H から $g_i H$ への写像 f_i を $f_i(g) = g_i g$ で定義すると，f_i は H から $g_i H$ の上への一対一写像になる。よって $|g_i H| = |H|$ なので $|G| = n|H|$ となる。∎

剰余類には右剰余類というものもある。G を群 H をその部分群とする。G の元 g, h が $gh^{-1} \in H$ となるとき g と h は同値であるといい $g \sim h$ と書く。この関係は同値関係となり同値類による類別ができるが，この同値類を右剰余類という。右剰余類はある元 g を用いて Hg と書かれ，$G = Hg_1 + \cdots + Hg_n$ という分解が得られる。

演習問題 1.2　上に書いた事を証明せよ。

一般に左剰余類による分解と右剰余類による分解は一致しない。$G = M(\Delta_3)$, $H = \{id, \tau_1\}$ とすると，左剰余類は $H = idH = \tau_1 H = \{id, \tau_1\}$, $\sigma_1 H = \tau_3 H = \{\sigma_1, \tau_3\}$, $\sigma_2 H = \tau_2 H = \{\sigma_2, \tau_2\}$ となり分解は $G = H + \sigma_1 H + \sigma_2 H$ と書けた。一方右剰余類は $H = Hid = H\tau_1 = \{id, \tau_1\}$, $H\sigma_1 = H\tau_2 = \{\sigma_1, \tau_2\}$, $H\sigma_2 = H\tau_3 = \{\sigma_2, \tau_3\}$ となり分解は $G = H + H\sigma_1 + H\sigma_2$ と書ける。このとき例えば σ_1 を含む左剰余類 $\sigma_1 H$ と右剰余類 $H\sigma_1$ は集合として同じではない。

一方左剰余類と右剰余類が一致するような部分群 H も存在する。$H = \{id, \sigma_1, \sigma_2\}$ とすると左剰余類は $H = idH = \sigma_1 H = \sigma_2 H = \{id, \sigma_1, \sigma_2\}$, $\tau_1 H = \tau_2 H = \tau_3 H = \{\tau_1, \tau_2, \tau_3\}$ であった。右剰余類は $H = Hid = H\sigma_1 = H\sigma_2 = \{id, \sigma_1, \sigma_2\}$, $H\tau_1 = H\tau_2 = H\tau_3 = \{\tau_1, \tau_2, \tau_3\}$ となり，例えば τ_1 を含む左剰余類 $\tau_1 H$ と右剰余類 $H\tau_1$ は集合として一致している。

G の部分群 H が g の任意の元 g に対し g を含む左剰余類と右剰余類が一致するとき H を G の **正規部分群** (*normal subgroup*) と呼ぶ。このとき $H \trianglelefteq G$ と書く。$H \neq G$ のときは $H \triangleleft G$ と書く。

命題 1.16 H が G の正規部分群である必要十分条件は G の任意の元 g に対し $g^{-1}Hg \subseteq H$ が成立する事である。

演習問題 1.3　命題 1.16 を証明せよ。

N, H を群 G の 2 つの部分群とする。NH は一般には G の部分群とはならないが H に関する左剰余類に分割する事はできる：$NH = g_1 H + \cdots + g_n H$。このとき $n = |NH : H|$ と定義し，NH における H の指数という。

命題 1.17 G の部分群 N, H に対し $|NH : H| = |N : N \cap H|$ が成立する。

証明　$N = g_1(N \cap H) + \cdots + g_n(N \cap H)$ を N の $N \cap H$ に関する剰余類への分割とする。$g_1 H + \cdots + g_n H$ が NH の H による剰余類への分割である事を示す。

$g_i N = g_j N$ が成立しているとする。このとき $g_j^{-1} g_i \in H$ が成立している。$g_i, g_j \in N$ なので $g_j^{-1} g_i \in N$ が成立し，$g_j^{-1} g_i \in N \cap H$ が得られる。剰余類への分割を与えている事から $g_i = g_j$ が分かる。

次に $NH = g_1 H + \cdots + g_n H$ を示す。このためには NH の任意の元が $g_1 H + \cdots + g_n H$ に含まれている事を示せばよい。nh を NH の任意の元とする。n は $g_1(N \cap H) + \cdots + g_n(N \cap H)$ に含まれているので，ある g_i と $N \cap H$ の元 h' が存在して $n = g_i h'$ と書ける。このとき $nh = g_i h' h$ であり，$h'h \in H$ なので $nh \in g_i H$ が分かる。∎

命題 1.18 G の部分群 N, H に対し $NH = HN$ が成立するとき NH は G の部分群である。特に N または H が正規部分群のとき NH は部分群である。

演習問題 1.4　命題 1.18 を示せ。

演習問題 1.5　$H < G$ が $|G : H| = 2$ となるとき H は G の正規部分群である。