2017.9.29

代数学概論第三（田口）　講義ノート

1. 群の定義

定義 1.1. 集合 G が 群 (group) であるとは、二項演算

$$G \times G \ \to \ G; \quad (g, h) \ \mapsto \ g \cdot h$$

が定義されてをり、以下の三つの公理を満たす事である：

(G1) 任意の $f, g, h \in G$ に対し $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.
(G2) 或る元 $e \in G$ が存在して、任意の $g \in G$ に対し $e \cdot g = g \cdot e = g$.
(G3) 任意の $g \in G$ に対し或る $g' \in G$ が存在して $g \cdot g' = g' \cdot g = e$.

G が 有限群（resp. 無限群）であるとは集合として有限（resp. 無限）である事である。G が有限群のとき、G の元の個数を G の 位数 (order) と言ふ。

群 G が 可換群 (commutative group) または アーベル群 (abelian group) であるとは、さらに次の公理を満たす事である：

(G4) 任意の $g, h \in G$ に対し $g \cdot h = h \cdot g$.

注意 1.2. (G2) の元 e を G の 単位元 (identity element) と呼ぶ。群の単位元は唯一つである。

(G3) の元 g' を g の 逆元 (inverse) と呼ぶ。g の逆元は（各 g につき）唯一つである。多くの場合、これを g^{-1} と記す。

G の演算の記号 $\cdot$ は他の記号で書かれる事も多い（記号を略して gh と「積」の様に書かれる事も多い）。特に可換群の場合は「プラス」の記号 $+$ で書かれる事も少なくない（その場合は g の逆元を $-g$ と記す）。

単位元の記号としては、 e の他、1 や （アーベル群の場合には） 0 が使はれる事もある。

定義 1.3. 群 G の元 g と正の整数 n に対し、g を n 回掛けたもの $g \cdot \cdots \cdot g$ を g^n と記す。$g^0 = e$ と定義する。負の整数 $-n$ に対し $g^{-n} = (g^{-1})^n$ と定義する。

群 G が 巡回群 (cyclic group) であるとは、ある元 $g \in G$ が存在して、任意の $h \in G$ は $h = g^n$ $(n \in \mathbb{Z})$ と書ける事である。

巡回群は有限の事も無限の事もある。

例 1.4. (1) 集合 X に対し、$\mathrm{Aut}(X)$ により、X から X 自身への全単射全体の集合を表す。$G = \mathrm{Aut}(X)$ とおくと、写像の合成 $f \circ g$ により G には二項演算

$$G \times G \ \to \ G; \quad (f, g) \ \mapsto \ f \circ g$$

が定義され、これに関して G は群を成す。その単位元は恒等写像 id_X であり、$f \in G$ の逆元は f の逆写像 f^{-1} である。

特に X が有限集合 $\{1,\dots,n\}$ のとき、$\mathrm{Aut}(X)$ を S_n (又は $\mathfrak{S}_n$) と記し、n 次対称群 (nth symmetric group) と呼ぶ。$|S_n| = n!$ である。S_n の元は

$$\begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix}, \quad (j_1 \cdots j_{k_1})(j_{k_1+1} \cdots j_{k_1+k_2}) \cdots (j_{k_1+\cdots+k_{r-1}+1} \cdots j_n)$$

等の形で表示される。S_n の元を 置換 (permutation) と言ふ。置換は見かけ（上の様な表示の仕方）が違つても同じ元を表す事がある事に注意せよ。

(2) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ... 等は加法に関しアーベル群をなす。剰余環 $\mathbb{Z}/m\mathbb{Z}$ も同様。$\mathbb{Z}$ は無限巡回群であり $\mathbb{Z}/m\mathbb{Z}$ は（$m \neq 0$ ならば）位数 $|m|$ の有限巡回群である。より一般に、n を自然数とするとき、$\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$, $(\mathbb{Z}/m\mathbb{Z})^n$, ... 等も加法に関しアーベル群をなす。（これらの群の演算は通常「和」の記号 $+$ で表される。）

$\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{Q} \setminus \{0\}$, ... 等は乗法に関しアーベル群をなす。（これらの群の演算は通常 $\cdot$ で表されるか、又は間に何も書かずに $(a,b) \mapsto ab$ の様に表される。）

一般に R が環であるとき、（環の定義により）R は加法に関してアーベル群をなし、$R^\times$ は乗法に関し群（R が可換環ならば可換群）をなす。前者を R の加法群 (the additive group of R)、後者を R の乗法群 (the multiplicative group of R) と呼ぶ。

(3) 可換環 R に対し、R の元を成分とする n 次正方行列 g であつて行列として可逆、即ち $\det(g) \in R^\times$, なるものの集合を $\mathrm{GL}_n(R)$ により表す。これは行列の積に関し群をなす。$n \geq 2$ ならば $\mathrm{GL}_n(R)$ は非可換である。$n = 1$ ならば $\mathrm{GL}_1(R) = R^\times$ である。

(4) 上の (1) で、例へば $X = \mathbb{Z}$ とすると、$\mathrm{Aut}(X)$ は無限非可換群である。しかし $\mathbb{Z}$ の加法群としての構造を保つ（即ち $g(x+y) = g(x)+g(y)$, $x, y \in \mathbb{Z}$, を満たす）$g \in \mathrm{Aut}(X)$ 達の集合 $\mathrm{Aut}_{群}(X)$ を考へると、その様な g は或る整数 a に対する「a 倍写像」 $x \mapsto ax$ だけであり、それが全単射であるためには $a \in \mathbb{Z}^\times = \{\pm 1\}$ が必要十分なので、$\mathrm{Aut}_{群}(X)$ は位数 2 の巡回群 $\{\pm 1\}$ と同一視される。同様に、$\mathbb{Z}^n$ の群としての構造を保つものだけ集めた $\mathrm{Aut}_{群}(\mathbb{Z}^n)$ は $\mathrm{GL}_n(\mathbb{Z})$ と同一視され、$\mathbb{Q}^n$ の $\mathbb{Q}$-ベクトル空間としての構造を保つものだけ集めた $\mathrm{Aut}_{群}(\mathbb{Q}^n)$ は $\mathrm{GL}_n(\mathbb{Q})$ と同一視される。

問 1.5. R が剰余環 $\mathbb{Z}/m\mathbb{Z}$ であるとき、$\mathrm{Aut}(R)$, $\mathrm{Aut}_{群}(R)$, $\mathrm{Aut}_{環}(R)$ をそれぞれ決定せよ。

2. 群の基本的性質

G を群とする。次の性質は容易に確かめられる：

- $g_1, \dots, g_n \in G$ の積 $g_1 \cdots g_n \in G$ は、それを計算する順序に依らない（by 結合律）。
- 単位元 $e \in G$ は唯一つ。
- 各 $g \in G$ に対し、その逆元 $g^{-1} \in G$ は唯一つ。

- $g, h \in G$ に対し
  $(gh)^{-1} = h^{-1}g^{-1}, \quad e^{-1} = e, \quad (g^{-1})^{-1} = g.$
- $g, x, y \in G$ に対し
  $gx = gy \;\Rightarrow\; x = y, \qquad xg = yg \;\Rightarrow\; x = y.$
- $g, h \in G$, と $m, n \in \mathbb{Z}$ に対し
  $g^m \cdot g^n = g^{m+n}, \quad (g^m)^n = g^{mn},$
  g と h が可換ならば $(gh)^n = g^n h^n.$

3. 部分群

定義 3.1. 群 G の部分集合 H が G の部分群 (subgroup) であるとは、G の演算（を H に制限したもの）に関して H が群を成す事である。

即ち、G の演算 $G \times G \to G$ を H に制限した $H \times H \to G$ の像が H に入り（i.e., H はこの演算に関して閉ぢてをり）、群の公理 (G1), (G2), (G3) が成り立つ事である。ここで H について (G1) が成り立つ事は自明であるから、(G2) と (G3) だけ確かめればよい。さらに、次の判定法も容易に確かめられる：

命題 3.2. 群 G の空でない部分集合 H について、次の三条件は同値である：

(1) H は G の部分群。
(2) 任意の $h, k \in H$ に対し $hk \in H$, かつ $h^{-1} \in H$.
(3) 任意の $h, k \in H$ に対し $hk^{-1} \in H$.

例 3.3. (1) X を集合、Y をその部分集合とし、

$$\begin{aligned} \mathrm{Aut}(X, Y) &:= \{g \in \mathrm{Aut}(X) |\; g(Y) = Y\}, \\ \mathrm{Aut}_Y(X) &:= \{g \in \mathrm{Aut}(X) |\; g(y) = y \quad \text{for all} \quad y \in Y\}, \end{aligned}$$

とおくと、これらは $\mathrm{Aut}(X)$ の部分群であり、$\mathrm{Aut}_Y(X)$ は $\mathrm{Aut}(X, Y)$ の部分群である。

(2) 環 R に対し、環の自己同型 $g : R \to R$ （即ち、全単射 $g : R \to R$ であつて環の構造を保つもの）全体の集合を $\mathrm{Aut}_{\text{環}}(R)$ により表す。また、R は加法に関してアーベル群をなしてゐるから、この構造を保つ $g \in \mathrm{Aut}(R)$ 全体の集合を $\mathrm{Aut}_{\text{加群}}(R)$ と書く。これらは写像の合成に関して群をなし、

$$\mathrm{Aut}_{\text{環}}(R) \;\subset\; \mathrm{Aut}_{\text{加群}}(R) \;\subset\; \mathrm{Aut}(R)$$

である（即ち $\mathrm{Aut}_{\text{環}}(R)$ は $\mathrm{Aut}_{\text{加群}}(R)$ の部分群であり $\mathrm{Aut}_{\text{加群}}(R)$ は $\mathrm{Aut}(R)$ の部分群である； cf. §3）。例へば $\mathrm{Aut}_{\text{加群}}(\mathbb{Z})$ は $\{\pm 1\}$ と同一視されるが、$\mathrm{Aut}_{\text{環}}(\mathbb{Z})$ は恒等写像のみからなる自明な群である。

(3) R を可換環とするとき、$\mathrm{SL}_n(R) := \{g \in \mathrm{GL}_n(R) |\; \det(g) = 1\}$ は $\mathrm{GL}_n(R)$ の部分群である。

(4) 偶数個の互換の積で書ける置換 $g \in S_n$ を偶置換 (even permutation) と呼ぶ。偶置換全体からなる S_n の部分集合 A_n は S_n の部分群をなす。これを n 次交代群 (nth alternating group) と呼ぶ。その位数は（$n \geq 2$ ならば） $n!/2$ である。

(5) $\mathbb{Z}$ （の加法群） は $\mathbb{Q}$ （の加法群）の部分群である。より一般に、$\mathbb{Z}^n$ は $\mathbb{Q}^n$ の部分群である。

(6) $n \in \mathbb{Z}$ に対し、$n\mathbb{Z} := \{nz|\ z \in \mathbb{Z}\}$ は $\mathbb{Z}$ の部分群である。逆に、$\mathbb{Z}$ の部分群はこの形のもので尽くされる。

(7) $\mathbb{N}$ は $\mathbb{Z}$ の部分群ではない。

(8) 任意の群 G に対し、

$$Z(G) \ := \ \{g \in G|\ gxg^{-1} = x \text{ for all } x \in G\}$$

は G の部分群である。これを G の 中心 (center) と呼ぶ。G がアーベル群である事と $Z(G) = G$ が成り立つ事とは同値である。

問 3.4. (1) $m \in \mathbb{Z}$ とする。加法群 $\mathbb{Z}/m\mathbb{Z}$ の部分群を全て求めよ。

(2) 対称群 S_n の部分群を（なるべく沢山）列挙せよ。

(3) 複素数体 $\mathbb{C}$ 上の一般線型群 $\mathrm{GL}_n(\mathbb{C})$ の部分群を（なるべく沢山）列挙せよ。

定義 3.5. G を群とし、S をその空でない部分集合とする。S が生成する (generate) G の部分群 $\langle S \rangle$ とは、S を含む G の部分群のうち最小のものの事である。

具体的には、

$$\langle S \rangle \ = \ \{g_1^{n_1} \cdots g_r^{n_r}|\ g_i \in S, n_i \in \mathbb{Z}, r \in \mathbb{Z}_{>0}\}$$

と書ける。

$S = \{g_1, \dots\}$ のとき $\langle S \rangle$ の代りに $\langle g_1, \dots \rangle$ とも書く。有限個の元で生成される群を 有限生成 (finitely generated) であると言ふ。特に、G が巡回群である事は一元生成、即ち、或る $g \in G$ に対し $G = \langle g \rangle$ となる事と同値である。

定義 3.6. 群 G の部分群 H に対し、$H = \langle S \rangle$ となる部分集合 S を H の（一つの）生成系 (a generating set) と呼ぶ。

例 3.7. (1) $S = \{(1\ 2), (1\ 2\ \cdots\ n)\}$ は対称群 S_n の生成系である。

(2) $S = \{\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\}$ は $\mathrm{SL}_2(\mathbb{Z})$ の生成系である。

(3) 群 G の二つの元 g, h に対し、

$$[g, h] \ := \ ghg^{-1}h^{-1}$$

と置き、g と h との 交換子 (commutator) と呼ぶ。交換子たち全体 $\{[g,h]|\ g, h \in G\}$ により生成される G の部分群を $D(G)$ または $[G, G]$ と記し、G の 交換子群 (commutator subgroup) または導来群 (derived subgroup) と呼ぶ。

問 3.8. 次の同値性を確かめよ：

(1) $[g, h] = e \iff g$ と h とは可換。

(2) $[G, G] = \{e\} \iff G$ はアーベル群。

4. 剰余類

G を群とし、H をその部分群とする。集合 G に、次により二つの関係 $\sim_{左}$ と $\sim_{右}$ を定義する：$g_1, g_2 \in G$ に対し、

- $g_1 \sim_{左} g_2 \overset{\text{def}}{\iff} g_1^{-1}g_2 \in H$,
- $g_1 \sim_{右} g_2 \overset{\text{def}}{\iff} g_2 g_1^{-1} \in H$.

これらの関係は同値関係である事が容易に確かめられる。これらの同値関係に関する同値類をそれぞれ <u>左剰余類</u> (<u>left coset</u>), <u>右剰余類</u> (<u>right coset</u>) と呼ぶ。（文献によつては「左」と「右」が逆になつてゐる事があるので要注意。）

G がアーベル群のときはこれら「左右」の概念は一致する。

各 $g \in G$ に対し、g の属する左剰余類、右剰余類はそれぞれ $gH := \{gh|\ h \in H\}$, $Hg := \{hg|\ h \in H\}$ に一致する。そこで、（先づは「左」についてだけ述べると）$\sim_{左}$ に関する完全代表系 $(g_i)_{i\in I}$ を一つ取ると、G は

$$G = \coprod_{i\in I} g_i H \tag{4.1}$$

と同値類の非交和 (disjoint union) の形に書ける。これを G の H に関する <u>左剰余類分解</u> (<u>left coset decomposition</u>) と呼ぶ。また、左剰余類たちの集合 $\{g_iH|\ i \in I\}$ を G の H に関する <u>左剰余集合</u> (the <u>set of left cosets</u>) と呼び、G/H と記す。

以上で、「左」を「右」に置き換へたものも同様。右剰余集合は $H\backslash G$ により表す。

例 4.1. $G = \mathbb{Z}$ （の加法群）、$H = m\mathbb{Z}$ $(m \in \mathbb{Z})$ のとき、剰余集合 $G/H = H\backslash G$ は剰余環 $\mathbb{Z}/m\mathbb{Z}$ の加法群に一致する。

問 4.2. G を群とし、H, K を G の二つの部分群とする。G に於ける関係 $\sim$ を

$$g_1 \sim g_2 \overset{\text{def}}{\iff} g_1 \in Hg_2K$$

により定義する。

(1) この関係 $\sim$ は同値関係である事を確かめよ。[この同値関係による各同値類 HgK を <u>両側剰余類</u> (<u>double coset</u>) と呼び、それらの集合 $H\backslash G/K := \{HgK|\ g \in G\}$ を G の H, K に関する <u>両側剰余集合</u> (the <u>set of double cosets</u>) と呼ぶ。]

(2) 自然な全射 $H\backslash G \to H\backslash G/K$ 及び $G/K \to H\backslash G/K$ が存在する事を示せ。

命題 4.3. G を群とし、H をその部分群とする。このとき、次の全単射が存在する：

(1) 各 $g \in G$ に対し

$$\begin{array}{rcl} H & \to & gH \\ h & \mapsto & gh \end{array}$$

及び

$$\begin{array}{rcl} H & \to & Hg \\ h & \mapsto & hg. \end{array}$$

(2) 左右の剰余集合の間の一対一対応

$$\begin{array}{rcl} G/H & \to & H\backslash G \\ gH & \mapsto & Hg^{-1}. \end{array}$$

5. 群の位数

集合 X に対し、その濃度を記号 $|X|$ または $\#X$ により表す。(X が無限集合のとき、この講義では（可算も非可算も区別せず）単に $|X| = \infty$ と記す)。

定義 5.1. 群 G に対し、その（集合としての）濃度を G の <u>位数</u> (<u>order</u>) と言ふ。G の部分群 H の <u>指数</u> (<u>index</u>) とは剰余集合 G/H の濃度 $|G/H|$ の事である（命題 4.3 の (2) により、これは $|H\backslash G|$ に等しい)。この値を $(G : H)$ 又は $|G : H|$ なる記号で表す。

G の位数 $|G|$ は自明な部分群 $\{e\}$ の指数 $(G : \{e\})$ に等しい。
命題 4.3 の (1) より、剰余類 gH, Hg 達の濃度は全て等しい。この事と剰余類分解 (4.1) より次が従ふ：

定理 5.2 (Lagrange)**.** 有限群 G とその部分群 H に対し

$$|G| \;=\; (G : H) \cdot |H|.$$

特に G が有限のとき、H の位数は G の位数を割る。

より一般に：

定理 5.3. 群 G の二つの部分群 $H \supset K$ に対し

$$(G : K) \;=\; (G : H)(H : K).$$

定義 5.4. 群 G の元 g の <u>位数</u> (<u>order</u>) とは、$g^n = 1$ となる最小の正整数 n の事である（この様な正整数 n が存在しないときは g の位数は ∞ と解釈する)。

g の位数は、それが生成する巡回部分群 $\langle g \rangle$ の（群としての）位数に等しい。従つて Lagrange の定理より

系 5.5. 有限群 G とその元 g に対し、g の位数は G の位数の約数である。

問 5.6. g の位数 n が有限であるとき、

$$\text{整数 } m \text{ に対し、} \quad g^m = 1 \;\Leftrightarrow\; n|m$$

である事を示せ。

問 5.7 (Euler の定理（= Fermat の小定理の一般化))**.** m を 0 でない整数し、a を m と互ひに素な整数とする。このとき $a^{\varphi(m)} \equiv 1 \pmod{m}$ が成り立つ事を示せ。[ここに $\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times$ は Euler 函数である。]

6. 巡回群

巡回群とは（既に定義した様に）一つの元で生成される群である。それは或る整数 m に対する $\mathbb{Z}/m\mathbb{Z}$ と「同型」である（同型については §8 を参照)。$m=0$ のときは無限巡回群 $\mathbb{Z}$ であり、$m \neq 0$ のときは位数 $|m|$ の有限巡回群である。巡回群の部分群の分類については例 3.3 の (6) 及び問 3.4 の (1) で述べた。

例 6.1. (1) m を正整数とする。1 の m 乗根 $(\in \mathbb{C})$ 全体のなす群は m 次巡回群である。[N.B. 1 の全ての冪根 $(\in \mathbb{C})$ のなす群は巡回群ではない。]

(2) 一般に、F を可換体とするとき、その乗法群 $F^\times$ の有限部分群は巡回群である（これは後に「体論」で習ふであらう)。[非可換体や一般の可換環では同様の事は必ずしも成り立たない。]

(3) 素数 p により生成される $\mathbb{Q}^\times$ の部分群 $\langle p \rangle = \{p^n |\ n \in \mathbb{Z}\}$ は無限巡回群である。

(4) 上三角行列 $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ により生成される $\mathrm{GL}_2(\mathbb{C})$ の部分群は無限巡回群である。

問 6.2. 7 次対称群 S_7 の巡回部分群であつて、位数が 2, 3, 4, 5, 6, 7, 10, 12 のものをそれぞれ（一つずつ）作れ。また、位数が 8 の巡回部分群は存在しない事を示せ。

7. 対称群

n を整数 ≥ 1 とする。対称群 S_n の元 g は、置換の意味を考へると、次の様に巡回置換の積として書ける事が分かる；

$$g = (i_1 \dots i_{n_1})(i_{n_1+1} \dots i_{n_1+n_2}) \cdots (i_{n-n_r+1} \dots i_n),$$
$$n = n_1 + \cdots + n_r, \quad \{i_1, \dots, i_n\} = \{1, \dots, n\}.$$

ここに現れる巡回置換たちは共通の番号を有しないから、互ひに可換である。そこで

$$n_1 \geq \cdots \geq n_r \tag{7.1}$$

と仮定してよい。これらの正整数の組 $(n_1, \dots, n_r)$ を g の サイクル型 (cycle type) と呼ぶ。

問 7.1. サイクル型が $(n_1, \dots, n_r)$ の元の位数は $\mathrm{LCM}(n_1, \dots, n_r)$ である事を示せ。

正整数 n を

$$n = n_1 + \cdots + n_r$$

と書く事を n の 分割 (partition) と呼ぶ。サイクル型は n の分割とも思へる。整数の分割はしばしば ヤング図形 (Young 図形) により視覚化される。

注意 7.2. $p(n) := \#\{n \text{ の分割}\}$ とおき、これを n の函数と思つたものを 分割函数 (partition function) と呼ぶ。最初の幾つかの値は

$$p(1) = 1,\ p(2) = 2,\ p(3) = 3,\ p(4) = 5,\ p(5) = 7, \dots.$$

分割函数については様々な研究がある。数列 $p(n)$ は次の合同式を満たす：

$$\begin{aligned} p(5n+4) &\cong 0 \pmod 5, \\ p(7n+5) &\cong 0 \pmod 7, \\ p(11n+6) &\cong 0 \quad (\mathrm{mod}\ 1)1. \end{aligned}$$

また、数列 $(p(n))_{n\in\mathbb{N}}$ の母函数は無限積表示を持つ：

$$\sum_{n=1}^{\infty} p(n)q^n \ = \ \prod_{m=1}^{\infty}(1-q^m)^{-1}$$

（ここに q は変数）。この右辺の逆数を少し修正した

$$\eta(z) \ := \ q^{1/24}\prod_{m=1}^{\infty}(1-q^m), \qquad q := e^{2\pi\sqrt{-1}z},$$

は Dedekind の エータ函数 (eta function) と呼ばれる重さ 1/2 の保型形式であり、数学（や数理物理学）の色々な局面に登場する。因みに

$$\Delta(z) \ := \ \eta(z)^{24} \ = \ q\prod_{m=1}^{\infty}(1-q^m)^{24}$$

は Ramanujan の Δ と呼ばれる重さ 12 の保系形式であり、その Fourier 係数 $\tau(n)$ も幾つかの不思議な合同式を満たす。

命題 7.3. サイクル型が等しい二つの置換 $g, g' \in S_n$ は共役である、即ち、或る $h \in S_n$ に対し $hgh^{-1} = g'$ となる。

実際、$g = (i_1 \dots i_{n_1})\cdots$, $g' = (i'_1 \dots i'_{n_1})\cdots$ のとき、$h = \begin{pmatrix} i_1 & \cdots & i_n \\ i'_1 & \cdots & i'_n \end{pmatrix}$ とおけばよい。

注意 7.4. $h = \begin{pmatrix} i_1 & \cdots & i_n \\ i'_1 & \cdots & i'_n \end{pmatrix}$ のとき、$g' = hgh^{-1}$ は「g の表示に現れる i_k を i'_k で置き換へたもの」である。

「共役」については §12 でもう少し詳しく述べる。

対称群の生成系としては、次のものが有名である：

命題 7.5. n 次対称群 S_n $(n \geq 2)$ は

(1) $\{(1\ 2), (1\ 3), \dots, (1\ n)\}$ で生成される。

(2) $\{(1\ 2), (2\ 3), \dots, (n-1\ n)\}$ で生成される。

(3) $\{(1\ 2), (1\ 2\ i_3 \dots i_n)\}$ で生成される（ここに $i_3, \dots, i_n$ は任意）。

勿論「同じ型」の他の元たちによつても生成される。但し、(3) で、互換に現れる二つの数は、長さ n の巡回置換の中で隣り合つてゐなければならない。例へば、(1 2) と (1 3 2 4) とでは S_4 は生成されない。

ここで「二面体群」についても解説しておく。n を正整数とする（以下で $n = 1, 2$ のときは適宜解釈せよ）。正 n 角形を自分自身に移す（平面の）合同変換全体のなす群を D_n と記し、n 次二面体群 (dihedral group)

と呼ぶ。これは各 $2\pi/n$ の回転 $s = \left(\begin{smallmatrix}\cos(2\pi/n) & -\sin(2\pi/n)\\ \sin(2\pi/n) & \cos(2\pi/n)\end{smallmatrix}\right)$ と（例へば）x 軸に関する鏡映 $t = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ により生成される、位数 $2n$ の有限非可換群である。この s と t は

$$s^n = t^2 = 1, \qquad tst = s^{-1}$$

といふ関係式を満たす。そこで、集合として、

$$D_n \ = \ \{s^i t^j \mid i = 0, \ldots, n-1,\ j = 0, 1\}$$

である。D_n はまた、対称群 S_n の部分群としても実現可能である。例へば $s = (1 \cdots n)$ と $t = \begin{pmatrix}1 & \cdots & n\\ n & \cdots & 1\end{pmatrix}$ とで生成される S_n の部分群は D_n と同型である。

例 7.6. $D_1 \simeq \mathbb{Z}/2\mathbb{Z}$, $D_2 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, $D_3 \simeq S_3$.
D_4 は S_4 と同型ではない。

8. 群の準同型

G, H を群とする。

定義 8.1. G から H への <u>準同型</u>（又は <u>群準同型</u>）(<u>homomorphism</u> (of groups)) f とは、写像 $\phi : G \to H$ であつて

$$\phi(gg') \ = \ \phi(g)\phi(g') \qquad \text{for all } g, g' \in G$$

を満たすものの事である。ϕ がさらに全単射であるとき、<u>同型</u>（又は <u>群同型</u> (<u>isomorphism</u> (of groups)) であると言ふ。

定義より容易に次が確かめられる：

$$\phi(e_G) \ = \ e_H, \qquad \phi(g^{-1}) \ = \ \phi(g)^{-1} \quad \text{for all} \ \ g \in G.$$

$\phi : G \to H$ が同型であるとき、その逆写像 $\phi^{-1} : H \to G$ も同型である。従つてこのとき、G と H とは <u>互ひに同型</u> であると言ひ、$G \simeq H$ または $G \cong H$ と記す。

例 8.2. (1) $g \in G$ に対し、

$$\begin{aligned}\phi \ : G \ &\to \ G\\ x \ &\mapsto \ gxg^{-1}\end{aligned}$$

は同型である。

(2) n 次対称群 S_n の元は自然に S_{n+1} の元と思へる。即ち写像 $S_n \to S_{n+1}$ がある。これは準同型である。これは単射であるが全射ではない。

(3) 正則行列の行列式を取る写像 $\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ は準同型である。これは全射であるが、$n \geq 2$ ならば単射ではない。

置換の符号を取る写像 $\mathrm{sgn} : S_n \to \{\pm 1\}$ も同様。

(4) 写像 $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ 及びその逆写像 $\log : \mathbb{R}_{>0} \to \mathbb{R}$ は同型である。[ここに $\mathbb{R}$ は実数の加法群であり、$\mathbb{R}_{>0}$ は正の実数全体が乗法に関してなす群である。]

(5) $G = \mathbb{Z}^n$, $H = \mathbb{Z}^m$ とする。準同型 $\phi : G \to H$ は（G, H の基底を固定する毎に）行列 $A \in \mathrm{M}_{m,n}(\mathbb{Z})$ と同一視出来る。ϕ が同型である事

と $m = n$ でありかつ A が正則である事 ($\Leftrightarrow \det(A) = \pm 1$) とは同値である。

(6) M をアーベル群とする（演算を加法的に表す）。$n \in \mathbb{Z}$ に対し、M 上の n 倍写像 $x \mapsto nx$ は M から M 自身への準同型である。

命題 8.3. 位数が等しい二つの巡回群は互ひに同型である。

記号 C_m や $\mathbb{Z}/m\mathbb{Z}$ により "the" cyclic group of order m を表す事がある。

定義 8.4. 群準同型 $\phi : G \to H$ に対し

$$\mathrm{Ker}(\phi) \;:=\; \{g \in G |\ \phi(g) = e_H\}$$

を ϕ の <u>核</u> (<u>kernel</u>) と呼ぶ。

一方、任意の（即ち集合の間の）写像 $\phi : G \to H$ に対し

$$\mathrm{Im}(\phi) \;:=\; \{\phi(g) |\ g \in G\}$$

を ϕ の <u>像</u> (<u>image</u>) と呼ぶのであつた。

容易に分かる様に、$\mathrm{Ker}(\phi)$ は G の部分群であり、$\mathrm{Im}(\phi)$ は H の部分群である。さらに、$\mathrm{Ker}(\phi)$ は次の性質を持つ：

任意の $g \in G$ と $x \in \mathrm{Ker}(\phi)$ に対し $gxg^{-1} \in \mathrm{Ker}(\phi)$.

換言すると

任意の $g \in G$ に対し $g\mathrm{Ker}(\phi)g^{-1} \subset \mathrm{Ker}(\phi)$.

例 8.5. 例 8.2, (3) の準同型の核は、定義により、
$\mathrm{Ker}(\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times) = \mathrm{SL}_n(\mathbb{C})$,
$\mathrm{Ker}(\mathrm{sgn} : S_n \to \{\pm 1\}) = A_n$.

問 8.6. $\phi : G \to H$ は群準同型とする。

(1) 任意の $h \in H$ と任意の $g \in \phi^{-1}(h)$ に対し $\phi^{-1}(h) = g\mathrm{Ker}(\phi)$ である事を示せ。

(2) ϕ が単射である事と $\mathrm{Ker}(\phi) = 1$ である事とは同値である事を示せ。

9. 正規部分群、剰余群

上に述べた $\mathrm{Ker}(\phi)$ の性質を抽出したものが「正規部分群」である：

定義 9.1. 群 G の部分群 H が <u>正規</u> 部分群 (<u>normal</u> subgroup) であるとは、任意の $g \in G$ に対し $gHg^{-1} \subset H$ が成り立つ事である。.

これは次と同値である：

任意の $g \in G$ に対し $gHg^{-1} = H$ (或いは $gH = Hg$).

従つて特に、H が正規部分群であるとき、G の H に関する左剰余類分解と右剰余類分解とは一致する。

例 9.2. (0) 群準同型 ϕ の核 $\mathrm{Ker}(\phi)$ は正規部分群である。

(1) 群 G に対し、その中心 $Z(G)$ は G の正規部分群である。

(2) 群 G の対し、その交換子群 $D(G) = [G, G]$ は G の正規部分群である。

(3) 交代群 A_n は対称群 S_n の正規部分群である。$n \geq 5$ のとき、A_n は非自明な正規部分群を持たない。

(4) R を可換環とするとき、$\mathrm{SL}_n(R)$ は $\mathrm{GL}_n(R)$ の正規部分群である。また、I を R のイデアルとするとき、

$$\Gamma_n(R, I) := \{g \in \mathrm{GL}_n(R) |\ g \equiv 1_n \pmod{I}\}$$

とおく[1] と、これも $\mathrm{GL}_n(R)$ の正規部分群である。

定義 9.3. H が群 G の正規部分群であるとき、剰余集合 G/H に二項演算

$$G/H \times G/H \ \to \ G/H$$

を

$$(g_1 H, g_2 H) \ \mapsto \ g_1 g_2 H$$

により定めると、（これは well-defined で）G/H はこの演算に関し群の公理を満たす。この群 G/H を G の H による <u>剰余群</u>（または <u>商群</u>）(<u>residue class group</u> or <u>quotient group</u> or <u>factor group</u>) と言ふ。

注意 9.4. G の二つの部分集合 A, B に対し、それらの積 $A \cdot B$（または AB）を

$$A \cdot B \ = \ \{ab |\ a \in A, b \in B\}$$

と定義すると、H が正規部分群であるとき、等式

$$(g_1 H) \cdot (g_2 H) \ = \ g_1 g_2 H$$

が成り立つ。従つて上の定義は、G/H の演算を

$$(g_1 H, g_2 H) \ \mapsto \ (g_1 H) \cdot (g_2 H)$$

により定める、と言つても同じ事である。

命題 9.5. 自然な写像

$$\begin{aligned} \pi : \ G \ &\to \ G/H \\ g \ &\mapsto \ gH \end{aligned}$$

は全射準同型であり、その核は H に等しい。

定義 9.6. 群 G とその部分群 H に対し

$$N_G(H) \ := \ \{g \in G |\ gHg^{-1} = H\}$$

を H の G に於ける <u>正規化群</u> (<u>normalizer</u>) と呼ぶ。

$N_G(H)$ は G の部分群であり、H は $N_G(H)$ の正規部分群である。しかも $N_G(H)$ はこの様な G の部分群の中で最大のものである。

[1] 二つの行列 $g, h \in \mathrm{GL}_n(R)$ に対し、$g \equiv h \pmod{I}$ とは、g, h の対応する成分同士が mod I で合同、といふ意味である。

10. 準同型定理

群準同型 $\phi : G \to G'$ が与へられたとき、それが誘導する写像

$$\begin{array}{rcl} \bar{\phi}:\ G/\mathrm{Ker}(\phi) & \to & \mathrm{Im}(\phi) \\ g\mathrm{Ker}(\phi) & \mapsto & \phi(g) \end{array}$$

が考へられる。

問 10.1. この写像が well-defined である事を確かめよ。

定理 10.2 (準同型定理)**.** 上の写像 $\bar{\phi} : G/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$ は同型である。

問 10.3. $\phi : G \to G'$ を群準同型とする。
(1) G の正規部分群 H が $H \subset \mathrm{Ker}(\phi)$ を満たすならば、群準同型 $\varphi : G/H \to G'$ であつて $\phi = \varphi \circ \pi$ を満たすものが唯一つ存在する事を示せ。[ここに $\pi : G \to G/H$ は自然な全射群準同型である。]
(2) H' を $\mathrm{Im}(\phi)$ の正規部分群とし、$K := \phi^{-1}(H')$ とおく。このとき自然な同型

$$\begin{array}{rcl} \bar{\phi}:\ G/K & \to & \mathrm{Im}(\phi)/H' \\ gK & \mapsto & \phi(g)H' \end{array}$$

が存在する事を示せ。[$H' = \{e_{G'}\}$ の場合が上の準同型定理である。]

例 10.4. (1) R を可換環とする。$\det : \mathrm{GL}_n(R) \to R^\times$ は全射群準同型で、その核は（定義により）$\mathrm{SL}_n(R) = \{g \in \mathrm{GL}_n(R) |\ \det(g) = 1\}$ に等しい。故に $\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \simeq R^\times$.
(2) $\mathrm{sgn} : S_n \to \{\pm 1\}$ は全射群準同型で、その核は（定義により）$A_n = \{g \in S_n |\ \mathrm{sgn}(g) = 1\}$ に等しい。故に $S_n/A_n \simeq \{\pm 1\}$.

この様に $(\mathrm{GL}_n, \mathrm{SL}_n, \det)$ と (S_n, A_n, sgn) とは「似た者同士」になつてゐるが、実際次の関係がある：

問 10.5. $g \in S_n$ に対し置換行列 $P(g) = (a_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$ を $a_{ij} := \delta_{i,g(j)}$（ここに δ_{ij} は Kronecker's δ）により定義すると、$P : S_n \to \mathrm{GL}_n(\mathbb{Z})$ は単射群準同型で、$\det(P(g)) = \mathrm{sgn}(g)$ が成り立つ事を示せ。

例 10.6. 整数 $N \geq 1$ に対し、「行列の各成分を mod N する」といふ写像

$$\pi_N :\ \mathrm{GL}_n(\mathbb{Z}) \ \to \ \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$$

は群準同型であり、その核は

$$\Gamma_n(N) := \{g \in \mathrm{GL}_n(\mathbb{Z}) |\ g \equiv 1_n \pmod{N}\}$$

に等しい。π_N は一般には全射ではなく、その像は

$$\{\bar{g} \in \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z}) |\ \det(\bar{g}) = \pm\bar{1}\}$$

に等しい。[2] 従つて $\mathrm{GL}_n(\mathbb{Z})/\Gamma_n(N)$ はこの群と同型である。

[2] $(\mathbb{Z}/N\mathbb{Z})^\times = \{\pm\bar{1}\}$ となるのは $N = 1, 2, 3, 4, 6$ の時だから、これらの場合に限り π_N は全射となる。

また、π_N を $\mathrm{GL}_n(\mathbb{Z})$ の部分群 $\mathrm{SL}_n(\mathbb{Z})$ に制限したもの $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ の像は $\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ に等しい。従つて準同型定理により $\mathrm{SL}_n(\mathbb{Z})/\Gamma_n(N) \simeq \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ である。

上の準同型定理 10.2 を第一同型定理と呼び、次の二つの定理をそれぞれ第二、第三同型定理と呼ぶ事がある：

定理 10.7. N が G の正規部分群であるとき、次の一対一対応がある：

$$\begin{array}{rcl} \{G \text{ の部分群で } N \text{ を含むもの}\} & \xrightarrow{1:1} & \{G/N \text{ の部分群}\} \\ H & \mapsto & H/N \end{array}$$

この対応において、正規部分群同士は対応する。

問 10.8. N が G の正規部分群であり、H が G の部分群であるとき、$H \cap N$ は H の正規部分群である事、及び HN は G の部分群である事を確かめよ。

定理 10.9. N が G の正規部分群であり、H が G の部分群であるとき、自然な写像

$$\begin{array}{rcl} H/(H \cap N) & \to & HN/N \\ h(H \cap N) & \mapsto & hN \end{array}$$

は同型である。

11. 部分群の生成

部分群の生成については既に §3 で説明してしまつた。代りに群の直積について説明しよう。

二つの群 G_1, G_2 に対し、その直積集合

$$G_1 \times G_2 \;=\; \{(g_1, g_2) |\ g_i \in G_i\}$$

に演算を

$$(g_1, g_2) \cdot (g_1', g_2') \;:=\; (g_1 g_1', g_2 g_2')$$

により定義すると、$G_1 \times G_2$ はこの演算に関して群を成す。これを G_1 と G_2 の <u>直積</u> (<u>direct product</u>) と呼ぶ。その単位元は (e_1, e_2) であり、$(g_1, g_2) \in G_1 \times G_2$ の逆元は (g_1^{-1}, g_2^{-1}) である。

より一般に、（二つの群に限らず）群の族 $(G_i)_{i \in I}$ が与へらえたとき、直積集合 $\prod_{i \in I} G_i := \{(g_i)_{i \in I} |\ g_i \in G_i\}$ には上と同様にして群構造が定義出来る。これを $(G_i)_{i \in I}$ の <u>直積群</u> または単に <u>直積</u> (<u>direct product</u>) と呼ぶ。

$G = \prod_{i \in I} G_i$ とおく。$(g_i)_{i \in I} \in G$ に対し、その第 j 成分を取る写像

$$\begin{array}{rcl} \pi_j :\ G & \to & G_j \\ (g_i)_{i \in I} & \mapsto & g_j \end{array}$$

を <u>第 j 射影</u> (<u>j-th projection</u>) と呼ぶ。これは全射群準同型であり、その核 $G^{(j)} := \{(g_i)_{i \in I} |\ g_j = e_j\}$（ここに e_j は G_j の単位元）は $\prod_{i \in I \setminus \{j\}} G_i$ と同一視出来る。

各 $j \in I$ に対し

$$G'_j \ := \ \{(g_i)_{i\in I} |\ g_i = e_i \text{ for all } i \neq j\}$$

とおく。これは G の正規部分群であり、「G_j を G の第 j 成分に埋め込む」といふ自然な写像

$$\iota_j:\ G_j \ \to \ G$$

（これは単射群準同型）の像になつてゐる。相異なる $j, k \in I$ に対し、G'_j の元と G'_k の元とは互ひに可換である。

問 11.1. G を群とし、H_1, H_2 をその二つの部分群とする。写像

$$\begin{aligned} \phi:\ H_1 \times H_2 \ &\to \ G \\ (h_1, h_2) \ &\mapsto \ h_1 h_1 \end{aligned}$$

を考へる。

(1) ϕ が群準同型であるためには H_1 と H_2 とが可換（即ち H_1 の任意の元と H_2 の任意の元とが可換）である事が必要十分である事を示せ。

(2) ϕ が単射であるためには $H_1 \cap H_2 = \{e\}$ である事が必要十分である事を示せ。

(3) ϕ が全射であるためには $H_1 H_2 = G$ である事が必要十分である事を示せ。

(註) 以上より、ϕ が群の同型であるためには、H_1 と H_2 とが可換であり、$H_1 \cap H_2 = \{e\}$ かつ $H_1 H_2 = G$ である事が必要十分である。

(4) ϕ が同型であるためには、H_1 と H_2 が可換であり、かつ G の任意の元 g が $g = h_1 h_2$ $(h_i \in H_i)$ と一意的に書ける事が必要十分である事を示せ。また、このとき H_1, H_2 は G の正規部分群である事を示せ。

(5) 上の (1)〜(4) を、n 個の部分群 $H_1, \ldots, H_n$ の場合に一般化せよ。

一般に、群 G に対し、その部分群 $H_1, \ldots, H_n$ を用ゐて

$$G \ = \ H_1 \times \cdots \times H_n$$

と表示する[3] 事を、G の <u>直積分解</u> (<u>direct-product decomposition</u>) と言ふ。

12. 共役、中心化群

群 G に於いて、関係 $\sim$ を

$$x \sim y \ \overset{\text{def}}{\iff} \ y = gxg^{-1} \ \text{ for some } \ g \in G$$

により定義すると、これは同値関係である。この関係があるとき、x と y とは <u>共役</u> である (<u>conjugate</u>) と言ふ。また、x の属する同値類を x の <u>共役類</u> (<u>conjugacy class</u>) と言ひ、（ここでは） $C(x)$ なる記号で表す。単に G の（一つの）<u>共役類</u> と言つたら、或る元 x の共役類の事である。

[3]正確には、ここの等号「=」 は「自然な群準同型 $H_1 \times \cdots \times H_n \to G$ が同型」の意味である。

例 12.1. 対称群 S_n に於いて、サイクル型 の等しい二つの元は共役である (§7)。従つて、S_n の共役類は n の分割と一対一に対応する。

$x \in G$ に対し、

$$Z_G(x) \ := \ \{g \in G | \ gxg^{-1} = x\}$$

を x の 中心化群 (centralizer) と呼ぶ（実際これは G の部分群であり、巡回部分群 $\langle x \rangle$ を含む)。より一般に、G の任意の部分集合 S に対し、S の G に於ける中心化群

$$Z_G(S) \ := \ \{g \in G | \ gxg^{-1} = x \ \text{ for all } \ x \in S\} \ = \ \bigcap_{x \in S} Z_G(x)$$

も考へられる。この記号法によれば、G の G に於ける中心化群 $Z_G(G)$ は G の中心 $Z(G)$ に一致する。

13. 類等式

G を有限群とし、その共役類を $C_1, \ldots, C_k$ とすると、G はそれらの非交和

$$G \ = \ C_1 \sqcup \cdots \sqcup C_k$$

であるから、等式

$$|G| \ = \ |C_1| + \cdots + |C_k|$$

が成り立つ。これを有限群 G の 類等式 (class equation) と言ふ。

例 13.1. n 次対称群 S_n の共役類は n の分割と一対一に対応するのであつた。分割 $n = n_1 + \cdots + n_r$ に対応する共役類の元（即ち、サイクル型が $(i_1, \ldots, i_{n_1}) \cdots (i_{n-n_r+1}, \ldots, i_n)$ の元）の個数は $n_1, \ldots, n_r$ が全て異なれば

$$\binom{n}{n_1}(n_1-1)!\binom{n-n_1}{n_2}(n_2-1)!\binom{n-(n_1+n_2)}{n_3}(n_3-1)! \cdots \binom{n_r}{n_r}(n_r-1)!$$

$$= \ \frac{n!}{n_1 \cdots n_r}.$$

（n_i 達の中に等しいものがあれば要修正。）そこで、例へば $n = 5$ なら、5 の分割 $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$ に応じて、S_5 の類等式は

$$5! \ = \ 4! + 5 \cdot 3! + \binom{5}{3}2! + \binom{5}{3}2! + \binom{5}{3}\binom{3}{2}/2 + \binom{5}{2} + 1.$$

14. 群の作用

群 G が集合 X に作用するとは、各 $g \in G$ と $x \in X$ に対し $gx \in X$ なる元が定まり、一定の規則を満たす事である。即ち：

定義 14.1. 群 G の集合 X への 作用 (action) とは、写像

$$\begin{aligned} G \times X \ &\to \ X \\ (g, x) \ &\mapsto \ gx \end{aligned}$$

であつて

(A1) 任意の $g, h \in G$ と $x \in X$ に対し $(gh)x = g(hx)$,
(A2) 任意の $x \in X$ に対し $ex = x$,
を満たすものの事である。

上の「積」の様な記号 gx の代りに、$g \cdot x$ や $g.x$ 等の記号を用ゐる事もある。また、G が X に作用してゐる事を

$$G \curvearrowright X$$

なる記号で表す事がある。

例 14.2. (1) G を群とし、$X = G$ とすると、G の演算 $G \times G \to G$ 即ち $G \times X \to X$ は G の X への作用になつてゐる。この作用を <u>左移動</u> と呼ぶ。

(2) G を群とし、$X = G$ とすると、「共役作用」

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & gxg^{-1} \end{array}$$

は G の X への作用になつてゐる。

(3) H は群 G の正規 <u>アーベル</u> 部分群であるとし、$\overline{G} = G/H$ とおく。$\bar{g} \in \overline{G}$ と $x \in H$ に対し、$\bar{g}$ の代表元 $g \in G$ を取り、$\bar{g}h := ghg^{-1}$ と定めると、これは well-defined で、これにより $\overline{G}$ は H に作用する。

(4) $G = S_n$, $X = \{1, \ldots, n\}$ とする。このとき $(g, x) \in G \times X$ に対し $g(x) \in X$ を対応させる写像は G の X への作用になつてゐる。

一般に、X が集合で $G = \mathrm{Aut}(X)$ のとき、$(g, x) \in G \times X$ に対し $g(x) \in X$ を対応させる写像は G の X への作用になつてゐる。

(5) 群 G が集合 X に作用してゐるとき、G の部分群 H も X 自然に作用する（G の作用の H への制限）。例へば：

f を有理数係数の多項式とし、$X = \{x_1, \ldots, x_n\}$ をその根 $(\in \mathbb{C})$ 全体の集合とする。上で見た様に、対称群 $G = \mathrm{Aut}(X) \simeq S_n$ は X に作用してゐる。G_f を、G の部分集合であつて次の条件 (Gal) をみたす元 g 全体の集合とする：

(Gal) 任意の有理数係数 n 変数多項式 $F(X_1, \ldots, X_n)$ に対し、
$F(x_1, \ldots, x_n) = 0$ ならば $F(g(x_1), \ldots, g(x_n)) = 0$.

この G_f は G の部分群をなし、多項式 f の（$\mathbb{Q}$ 上の）<u>ガロア群</u> (<u>Galois group</u>) と呼ばれる。

(6) R を可換環とし、$G = \mathrm{GL}_n(R)$, $X = R^n$ とおく。このとき、行列 $g \in \mathrm{GL}_n(R)$ を縦ベクトル $x \in X$ に左から掛ける事により写像 $G \times X \to X$ が得られるが、これは G の X への作用になつてゐる。

注意 14.3. 上の例の様に、多くの場合、「その文脈に於いて考へられる最も自然な作用」があり、これを <u>自然な作用</u> と呼ぶ（が、「自然な」の厳密な定義がある訳ではない）。

問 14.4. 群 G が集合 X に作用してゐるとき、各 $g \in G$ に対し、写像

$$\begin{array}{rccc} \rho_g\colon & X & \to & X \\ & x & \mapsto & gx \end{array}$$

が考へられる。

(1) ρ_g は全単射（従つて $\mathrm{Aut}(X)$ の元）である事を示せ。

(2) 写像

$$\begin{array}{rccc} \rho : & G & \to & \mathrm{Aut}(X) \\ & g & \mapsto & \rho_g \end{array}$$

は群準同型である事を示せ。

(3) 逆に、群準同型 $\rho : G \to \mathrm{Aut}(X)$ を与へると、G の X への作用が定まる事を示せ。

この問の状況で、しばしば X が何らか（例へばアーベル群）の構造を持つてゐて、G はその構造を保つ様に作用してゐる、といふ事がある。その場合、上の $\mathrm{Aut}(X)$ はその構造を込みにした Aut で置き換へられる。

例 14.5. X は体 F 上のベクトル空間とする。群 G が X に作用してゐて、その作用が X の F-ベクトル空間の構造を保つ、即ち

$$g(x+y) = gx + gy, \quad g(cx) = c(gx) \qquad (g \in G, x, y \in X, c \in F)$$

が成り立つとき、準同型 $\rho : G \to \mathrm{Aut}(X)$ の像は

$$\mathrm{GL}_F(X) := \{ \text{全単射 } F\text{-線型写像 } f : X \to X \}$$

に含まれる。従つて準同型

$$\rho : G \to \mathrm{GL}_F(X)$$

が得られる。この群 $\mathrm{GL}_F(X)$ は $n = \dim_F(X)$ が有限ならば（X の基底を固定する毎に）正則な F-係数 n 次正方行列全体のなす群 $\mathrm{GL}_n(F)$ と同一視出来る事に注意せよ。

定義 14.6. 群 G が集合 X に作用してゐるとする。

(1) $x \in X$ がこの作用の固定点 (fixed point) であるとは、任意の $g \in G$ に対し $gx = x$ である事である。固定点全体の集合をしばしば X^G なる記号で表す。固定点を持たない作用を fixed-point free な作用と言ふ。

(2) G の X への作用が忠実 (faithful) であるとは、$gx = x$ for all $x \in X$ となる $g \in G$ は e のみである事である。（作用 $G \curvearrowright X$ と群準同型 $\rho : G \to \mathrm{Aut}(X)$ の対応を使つて言ひ換えると、これは「ρ が単射」といふ事である。$\mathrm{Ker}(\rho)$ をこの作用 $G \curvearrowright X$ の核と呼ぶ事がある。）

(3) G の X への作用が推移的 (transitive) であるとは、任意の $x, y \in X$ に対し或る $g \in G$ が存在して $y = gx$ となる事である。

例 14.2 (1) の作用は fixed-point free かつ忠実かつ推移的である。

例 14.2 (2) の作用の固定点全体の集合は G の中心 $Z(G)$ に一致する。また、この作用の核も $Z(G)$ に一致する。この作用は $G \neq \{e\}$ ならば推移的ではない。

例 14.2 (1) と問 14.4 より、

命題 14.7. 任意の有限群 G は或る次数の対称群に埋込める、即ち、或る整数 $n \geq 1$ と単射群準同型 $G \to S_n$ が存在する。

定義 14.8. 群 G が集合 X に作用してゐるとき、各 $x \in X$ に対し、

$$O_G(x) \ := \ \{gx|\ g \in G\}$$

を x の G-軌道 (G-orbit) または単に 軌道 (orbit) と呼ぶ（単に $O(x)$ とも、或いは Gx とも記す)。

二つの軌道 $O_G(x)$ と $O_G(y)$ とは、交はらないか一致するかのどちらかである。即ち、X の二つの元について、「同じ軌道に属する」といふ関係は同値関係であり、X は軌道たちの非交和

$$X \ = \ \coprod_{x \in X} O_G(x) \ = \ \coprod_{i \in I} O_G(x_i)$$

に分割出来る（ここに $(x_i)_{i \in I}$ はこの同値関係に関する一つの完全代表系)。これを X の G-軌道分解 (G-orbit decomposition) と呼ぶ。

$X = G$ で $G \curvearrowright X$ が共役作用 ($x \mapsto gxg^{-1}$) であるとき、G-軌道分解は共役類分解 (§12, §13) と一致する。

定義より、次の三条件は同値である：

- $G \curvearrowright X$ は推移的。
- $X = O_G(x)$ for some $x \in X$.
- $X = O_G(x)$ for all $x \in X$.

例 14.9. F を体とし、$X = F^n$, $G = \mathrm{GL}_n(F)$ とおく。G は X に自然に作用する (cf. 例 14.2 (5)).

(1) X の G-軌道分解は

$$X \ = \ \{0\} \sqcup (X \setminus \{0\}).$$

(2) $B = \{$ 上三角行列 $\in G\}$ とおく。X の B-軌道分解は

$$X \ = \ X_0 \sqcup (X_1 \setminus X_0) \sqcup \cdots \sqcup (X_n \setminus X_{n-1}).$$

ここに

$$X_j \ := \ \{(x_i) \in X|\ x_{j+1} = \cdots = x_n = 0\}$$

と置いた (但し $X_n := X$).

(3) $C = \{$ 対角行列 $\in G\}$ とおく。X の C-軌道分解は

$$X \ = \ \coprod_{J \subset \{1,\ldots,n\}} X_J.$$

ここに J は $\{1, \ldots, n\}$ の部分集合を全て動き、各 J に対し

$$X_J \ := \ \{(x_i) \in X|\ x_i = 0 \text{ for } i \notin J \text{ かつ } x_j \neq 0 \text{ for } j \in J\}$$

と置いた。

(4) N により C 及び置換行列たち全体で生成される G の部分群を表す。X の N-軌道分解は

$$X \ = \ \coprod_{k=0}^{n} Y_k.$$

ここに

$$Y_k \ := \ \{(x_i) \in X|\ x_i = 0 \text{ なる } i \text{ は丁度 } k \text{ 個 }\}$$

と置いた。

定義 14.10. 群 G が集合 X に作用してゐるとする。$x \in X$ に対し、

$$\mathrm{Stab}_G(x) \ := \ \{g \in G|\ gx = x\}$$

を x の <u>固定化群</u> または <u>安定化群</u> (<u>stabilizer</u>)

例 14.11. G を群とする。
(1) $X = G$ とし、G を X に共役 $(x \mapsto gxg^{-1})$ により作用させると、$x \in X$ の固定化群 $\mathrm{Stab}_G(x)$ は x の中心化群 $Z_G(x)$ (cf. §12) に等しい。
(2) X を G の部分群全体の集合とする。G を X に共役 $(H \mapsto gHg^{-1})$ により作用させると、$H \in X$ の固定化群 $\mathrm{Stab}_G(H)$ は H の正規化群 $N_G(H)$ に等しい。

命題 14.12. 上の状況で、次の自然な全単射がある：

$$\begin{aligned} G/\mathrm{Stab}_G(x) \ &\to \ O_G(x) \\ g\mathrm{Stab}_G(x) \ &\mapsto \ gx. \end{aligned}$$

系 14.13. $|O_G(x)| = (G : \mathrm{Stab}_G(x))$. 特に、$G$ が有限のとき $|O_G(x)|$ は $|G|$ の約数である。

問 14.14. p は素数とする。
(1) p 群の中心は非自明である事を示せ。
(2) 位数 p^2 の群はアーベル群である事を示せ。

15. Sylow の定理

群の作用の応用として、Sylow の定理を証明する。以下で、p は素数とする。

定義 15.1. 有限群が <u>p-群</u> (<u>p-group</u>) であるとは、その位数が p 冪である事である。有限群 G の部分群 S が <u>p-Sylow 部分群</u> (<u>p-Sylow subgroup</u>) であるとは、$|G| = p^r q$ $(p \nmid q)$ とするとき、$|S| = p^r$ である事である。

定理 15.2. G を有限群とする。
(1) 任意の素数 p に対し、G は p-Sylow 部分群を持つ。
(2) G の任意の p-部分群は或る p-Sylow 部分群に含まれる。
(3) G の p-Sylow 部分群たちは互ひに共役である。
(4) 任意の p-Sylow 部分群 S に対し $\{G$ の p-Sylow 部分群$\} \simeq G/N_G(S)$.
(5) (G の p-Sylow 部分群の個数) $\equiv 1 \pmod p$.

<u>証明の概略</u>： $|G| = p^r q$ $(p \nmid q)$ とする。$\mathscr{X}$ により、G の部分集合 S であつて $|S| = p^r$ なるもの全体の集合を表す。これに G を左移動 $(S \mapsto gS)$ により作用させる。
(1) $\mathscr{X}$ を G-軌道分解すると、$|\mathscr{X}| = \binom{p^r q}{p^r} \equiv q \pmod p$ だから、軌道の濃度 $|O_G(S)|$ が p で割れない様な $S \in \mathscr{X}$ が存在する。この S の固定化群 $\mathrm{Stab}_G(S)$ が p-Sylow 部分群である事が分かる。
(2), (3), (4) p-Sylow 部分群 S を一つ固定し $\mathscr{S} := \{gSg^{-1}|\ g \in G\}$ とおく。G の任意の p-部分群 H は或る $S' \in \mathscr{S}$ に含まれる事を示す。G を $\mathscr{S}$ に共役 $(S' \mapsto gS'g^{-1})$ で作用させる。$S \in \mathscr{S}$ の固定化群 $\mathrm{Stab}_G(S)$ は S の正規化群 $N_G(S)$ に等しく、特に S 自身を含む。$\mathscr{S} \simeq G/N_G(S)$ だから $|\mathscr{S}|$ は p で割れない。この作用を H に制限して、$\mathscr{S}$ の H-軌道分解を考へると、各軌道の濃度は $|H|$ の約数、即ち p 冪だか

ら、或る $S_i \in \mathscr{S}$ であつて $|O_H(S_i)| = 1$ なるものが存在する。 これは $H \subset N_G(S_i)$ を意味する。すると、HS_i は G の p-部分群である事が分かり、従つて $H \subset S_i$ が分かる。以上より $\mathscr{S} = \{G$ の p-Sylow 部分群 $\} \simeq G/N_G(S)$ である。
(5) $S \in \mathscr{S}$ を固定し、$\mathscr{S}$ を S の共役作用に関して S-軌道分解すると $|\mathscr{S}| = \sum_i |O_S(S_i)|$. ここで各 $|O_S(S_i)|$ は p 冪であり、

$$|O_S(S_i)| = 1 \;\Leftrightarrow\; S_i = S.$$

故に $|\mathscr{S}| \cong 1 \pmod{p}$.

例 15.3. $G = \mathrm{GL}_n(\mathbb{F}_p)$ の位数は $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\cdots(p-1)$. よつて G の p-Sylow 部分群の位数は $p^{n(n-1)/2}$. 上三角行列 $\in G$ であつて対角成分が全て 1 であるもの全体のなす部分群 $S \subset G$ の位数は丁度 $p^{n(n-1)/2}$ であるから、これが一つの p-Sylow 部分群である。その正規化群は $B = \{$ 上三角行列 $\in G\}$ であり、その位数は $p^{n(n-1)/2}(p-1)^n$. よつて G の p-Sylow 部分群の個数は

$$\begin{aligned} \frac{p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\cdots(p-1)}{p^{n(n-1)/2}(p-1)^n} &= \prod_{i=1}^{n-1}(p^{n-i}+\cdots+p+1) \\ &\equiv 1 \pmod{p}. \end{aligned}$$