代数学１ (群論) の授業内容 (2005 年度冬学期)

落合理[1]

Contents

1. Introduction

前期も群の定義の初歩を少しやった上で後期の授業でさらに踏み込んで群になれていきたい. 群論とは何なのだろうか.

1. 方程式のがベキ根によっていつ解けるかという問題 (一般の 5 次方程式がベキ根による方法は解けないこと, ガロアの理論)
2. 自然界の物理現象やものごとの対称性の記述を与える言葉.
3. より一般の幾何学的な代数的な不変量（多様体の基本群やホモトピー群）

授業をとる上でやってほしいこと

- 教科書をちゃんとひとつ手元におくこと
- 復習, 予習をできる限りしてください（ノートを見直す, ノートを綴じて考えてみる）
- 例を沢山理解して自分のものとすること (どれだけ例を沢山もっているかが理論をどれだけ深く理解しているかどうかのパラメーターである).

基本的には授業のノートがメインであり特定の教科書に沿って展開していくことはしない予定である. ただ数学の理論を勉強していくにはやはり本も大切である. 教科書として
森田康夫著「代数学概論」(裳華房)
を指定する. また副次的な参考書として
寺田至, 原田耕一郎共著　岩波講座現代数学の基礎「群論」(岩波書店)
を指定する.

[1]もし記述に関するミスなどありましたらお知らせください. 万が一何らかの形で本ノートを個人的に眺める以外で使う場合 (あまりないかと思いますが) はお知らせください

定義 1.1. 集合 G と 2 項演算 $*: G \times G \longrightarrow G, (s,t) \mapsto s*t$ の組 $(G,*)$ が群 (group) であるとは次の条件が満たされることをいう

(G1) $\forall s,t,u \in G$ に対して, $(s*t)*u = s*(t*u)$ が成り立つ. (結合律)
(G2) 単位元と呼ばれる元 $1_G \in G$ があって勝手な $g \in G$ に対して $g*1_G = 1_G * g = g$ が成り立つ. (単位元の存在)
(G3) $\forall s \in G$ に対して $s^{-1}*s = s^{-1}*s = 1_G$ なる元 s^{-1} が存在する. (逆元の存在)

上で導入した演算 $*$ は群の乗法と呼ばれる. 以下, 特に誤解のおそれがないときは積の演算記号は省略して $s*t = st$ と書くことにする.

例 1.2. 1. 整数 $\mathbb{Z}$, 有理数 $\mathbb{Q}$, 複素数 $\mathbb{C}$ は加法に関して群をなす. 単位元は 0, 勝手な元 x に対して逆元は $-x$ である.
2. X を集合とするとき,
$$G = \mathrm{Aut}(X) = \{f : X \longrightarrow X \mid f \text{ は全単射写像 }\}$$
は群をなす. 単位元 1_G は恒等写像, 各 $s,t \in G$ に対して積 $s*t$ は合成写像 $s \circ t$ で与える. 各 $s \in G$ に対して逆元 s^{-1} を s の逆写像によって定めることで自然に群になる.
3. n 元からなる集合 $E_n = \{e_1, \cdots, e_n\}$ を考える. このとき, 群 $\mathrm{Aut}(E_n)$ のことを置換群 (permutation group) とよび S_n と記す.
4. $\mathbb{K}$ を勝手な可換体とする. 例えば有理数体, 実数体, 有限体などが体の例である. このとき, $\mathbb{K}$ の元は足し算で群になる. また $\mathbb{K} \setminus \{0\}$ は乗法に関して群になる.
5. $\mathbb{K}$ を勝手な可換体とする. このとき,
$$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid |\det(A) \neq 0\}$$
は自然な行列の演算で群をなす.

定義 1.3. G を群とする. G が集合として有限集合のとき G を有限群 (finite group) とよぶ. G が集合として無限集合のとき G を無限群 (infinite group) とよぶ. G を有限群のときにはその集合としての位数を G の位数 (order) とよぶ. 各元 $g \in G$ に対して, $g^r = 1_G$ となる自然数 r が存在すればそのような r のうち最小のものを g の位数 (order) という. そのような r が存在しないとき g の位数は無限であるとよばれる.

例 1.4. 1. $(G,*) = (\mathbb{C} \setminus \{0\}, \times)$ は無限群である. このとき, $g \in (G,*)$ に対して, g の位数が有限であることと $g = \exp(\frac{2\pi\sqrt{-1}}{r})$ なる自然数 r があることは同値である.
2. 置換群 S_n は有限群であり, S_n の位数は $n!$ である.
3. G を群とする. ある元 g があって, 勝手な元に対してある自然数 n があって g^n とかけるとき, G は巡回群 (cyclic group) であると呼び, g を生成元と呼ぶ. 巡回群 G に対して生成元 g の位数が有限なとき G は有限巡回群 (finite cyclic group) とよばれる. このとき G の位数は g の位数と等しい. 生成元 g の位数が無限なとき G は無限巡回群 (infinite cyclic group)

とよばれる. 位数 r の有限巡回群を C_r または $\langle\sigma|\sigma^r=1\rangle$, 無限巡回群を C_∞ または $\langle\sigma\rangle$ という記号で記すことにする.

定義 1.5. $(G,*)$ を群とする. G が演算 $*$ に関して可換なとき, つまり $\forall g,h\in G$ に対して $g*h=h*g$ のとき, G は可換群またはアーベル群という. そうでないとき, G は非可換群または非アーベル群と呼ばれる.

定義 1.6. $(G,*)$ を群として部分集合 $H\subset G$ を考える. H が G の部分群であるとは G の演算 $*$ で H が群となることをいう.

補題 1.7. $(G,*)$ を群として部分集合 $H\subset G$ を考える. 次の条件は同値となる.

1. H が G の部分群である.
2. $\forall a,b\in H$ に対して G に対して定まる演算 $*$ に関して $a*b,a^{-1}\in H$ となる.
3. $\forall a,b\in H$ に対して $a^{-1}*b\in H$

Proof. 最初の 2 つの条件は同意であり, それらの条件から 3 番目の条件はただちにでる. 3 番目の条件を仮定して 2 番目の条件を導きたい. $a=b\in H$ ととると $a^{-1}*a=1_G$ である. よって $1_G\in H$ となる. 次に $\forall a\in H$ に対して, $b=1_G$ として条件を用いると a^{-1} が H に入ることがわかる. $a^{-1},b\in H$ に対して 3 番目の条件を仮定すると $(a^{-1})^{-1}*b=a*b\in H$ が導かれる. □

群の定義を弱めた概念についても少し述べておく.

定義 1.8. 集合 M と 2 項演算 $*:M\times M\longrightarrow M,(s,t)\mapsto s*t$ の組 $(M,*)$ が半群 (monoid) であるとは次の条件が満たされることをいう

(M1) $\forall s,t,u\in M$ に対して, $(s*t)*u=s*(t*u)$ が成り立つ. (結合律)
(M2) 単位元と呼ばれる元 $1_M\in M$ があって勝手な $g\in M$ に対して $g*1_M=1_M*g=g$ が成り立つ. (単位元の存在)

例 1.9. 整数 $\mathbb{Z}$ と通常の乗法 $\times$ の組 $(\mathbb{Z},\times)$ は半群になる. 同様に自然数 $\mathbb{N}$ と通常の加法 $+$ を考えるとき, $(\mathbb{N}\cup\{0\},+)$ は半群となる.

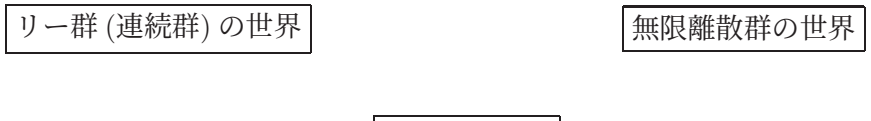
定義 1.10 (準同型と同型)**.** $(G,*)$, $(G',*')$ を群とする. これらの群の間の集合としての写像 $h:G\longrightarrow G'$ が準同型写像であるとは $h(s*t)=h(s)*'h(t)$ が任意の $s,t\in G$ で成立することをいう. 特に, 全単射な準同型写像 h のことを同型写像とよぶ.

注意 1.11. 2 つの群 G と G' の間に同型写像が存在するという関係は群同士の間の同値関係を定める. このとき, G と G' は互いに同型であるとよび, この関係を記号として $G\cong G'$ であらわす.

例 1.12.
1. $\mathbb{C}$ から $\mathbb{C}\setminus\{0\}$ への写像を $z\mapsto\exp(z)$ で定めると, $(\mathbb{C},+)$ から $(\mathbb{C}\setminus\{0\},\times)$ への群準同型を与えている. これは全射であるが, 単射ではない. 例えば, n を整数としたとき $\exp(2\pi\sqrt{-1}n)=\exp(2\pi\sqrt{-1}(n+1))=1$ である.
2. $(\mathbb{R},+)$ や $(\mathbb{R}_{>0},\times)$ といった $(\mathbb{C},+)$ や $(\mathbb{C}\setminus\{0\},\times)$ の部分群を考える. このとき上の写像 exp を $(\mathbb{R},+)$ に制限することで, $(\mathbb{R},+)$ から $(\mathbb{R}_{>0},\times)$ への準同型が得られる. これは同型になっており, 逆写像は log で与えられる.

この節の最後にこの講義の目的をいくつか述べておきたい. もちろん群の理論全般を習得することが目的なのは言うまでもない. その上でいくつか付け加えると,

1. Sylow の定理など論理的な積み重ねで群の構造を厳密に代数学におけるきっちりと論証を行う訓練をすることと代数的な論証を積み重ねることで物事の様子が明らかになる強みを実感すること.
2. ひとくちに群といってもいろんな群がある. 群論の世界の地図も大きな地方に分けられておりその地方ごとにまったく違った景色が眺められる



まずいろいろな例をあつかって群の世界に慣れて群の世界の多様性の感覚やだいたいの地図や地理感覚が頭の中にできることも目的である.

2. 群の作用について

定義 2.1. G を群, X を集合とする. G の集合への (左) 作用とは, 次の条件をみたす写像 $f : G \times X \longrightarrow X$ のことをいう.

1. 任意の $x \in X$ に対して $f(1_G, x) = x$ が成り立つ.
2. 任意の $g, h \in G, x \in X$ に対して $f(gh, x) = f(g, f(h, x))$ が成り立つ.

このとき, X は (左)G 作用をもつ集合と呼ばれる. 以後, (左) 作用 $f(g, x)$ のことを簡単に gx とも記すことにする.

例 2.2. 1. 有限次元の数ベクトル空間 $\mathbb{K}^n$ を考える. このとき, 行列 $GL_n(\mathbb{K})$ の左作用を次のように与える.

$$S = (s_{i,j})_{i,j} \in GL_n(\mathbb{K}), \boldsymbol{v} = \begin{pmatrix} v_1 \\ v_2 \\ \cdots \\ v_n \end{pmatrix} \in \mathbb{K}^n$$

に対して作用を $S\boldsymbol{v} = \begin{pmatrix} s_{1,1}v_1 + \cdots + s_{n,1}v_n \\ s_{1,2}v_1 + \cdots + s_{n,2}v_n \\ \cdots \\ s_{1,n}v_1 + \cdots + s_{n,n}v_n \end{pmatrix} \in \mathbb{K}^n$

で与えればよい.

2. 群の左乗法による移動作用 G を群, $H \subset G$ を部分群とするとき $f(h, g) = h * g$ ($*$ はに定まっている乗法の演算を表す) 群演算の結合律よりこれは G を集合と思ったときの群 H の作用を与えている.
3. G を群とするとき G のの上への (左) 共役作用とは, $f(s, t) = sts^{-1}$ で与えられる作用である.

次のような見方もしっかりと認識しておいてほしい.

補題 2.3. G を群, X を集合とする. G の X への左作用を与えることと群の準同型 $G \longrightarrow \mathrm{Aut}(X)$ を与えることは同値である.

Proof.

$\{f : G \times X \longrightarrow X | G \text{ の } X \text{ への左作用 }\} \longleftrightarrow \{h : G \longrightarrow \mathrm{Aut}(X) | \text{ 群準同型 }\}$

の一対一対応を与えればよい.

$\longrightarrow$ は以下のようである. 定義のような条件を満たす左作用 $f : G \times X \longrightarrow X$ がひとつ与えられたとする. このとき, g をとるごとに, $h_g : X \longrightarrow X \quad x \mapsto f(g,x)$ という X から X への写像が定まる. g の逆元 g^{-1} をとると, $h_{g^{-1}} \circ h_g$ は $x \mapsto f(g,x) \mapsto f(g^{-1}, f(g,x)) = f(g^{-1}g, x) = f(1_G, x) = x$ より, 合成写像 $h_{g^{-1}} \circ h_g$ は単射となっている. よってひとつめの写像 h_g は単射である. 逆に合成写像 $h_g \circ h_{g^{-1}}$ を考えると全射なことがいえるからふたつめの写像 h_g は全射である. かくして, 勝手な $g \in G$ で $h_g \in \mathrm{Aut}(X)$ である.

次に, この対応 $G \longrightarrow \mathrm{Aut}(X), \quad g \mapsto h_g$ で与えられる集合の写像が群準同型であること, つまり群の演算を保っていることをみたい. $\mathrm{Aut}(X)$ には写像としての合成で群演算が入っていたことを思い出すと, $h_{1_G} = \mathrm{Id}_X$, $h_{g^{-1}} = (h_g)^{-1}$, $h_{g'} \circ h_g = h_{g'g}$ を確かめればよい. 特に最後の条件のみ説明しておくと, 作用の結合則の公理から $f(g', f(g,x)) = f(g'g, x)$ であるからこれは正しい.

逆の対応 $\longleftarrow$ は以下のようである. 準同型 $h : G \longrightarrow \mathrm{Aut}(X)$ がひとつ与えられたとする. このとき, $h(g) : X \longrightarrow X$ を $h(g)$ が与える X の自己同型とすると, 左作用 $f_h : G \times X \longrightarrow X$ を $f_h(g,x) = h(g)(x)$ で定めればよい. 特に, 作用の "結合律" $f_h(g', f_h(g,x)) = f_h(g'g, x)$ を確かめるには $h(g') \circ h(g) = h(g'g)$ がいえればよい. これは h が群準同型であることおよび $\mathrm{Aut}(X)$ の群法則が写像としての合成で与えられていたことより従う. かくして f が作用であることが確かめられる. □

左作用とは逆の右作用というものも考えられる.

定義 2.4. G を群, X を集合とする. G の集合への (右) 作用とは, 次の条件をみたす写像 $f : X \times G \longrightarrow X$ のことをいう.

1. 任意の $x \in X$ に対して $f'(x, 1_G) = x$ が成り立つ.
2. 任意の $g, h \in G, x \in X$ に対して $f'(x, gh) = f'(f'(x,g), h)$ が成り立つ.

このとき, X は (右)G 作用をもつ集合と呼ばれる. 以後, (右) 作用 $f'(x,g)$ のことを簡単に xg とも記すことにする. また, 右作用の場合には x^g という指数的な書き方もしばしば用いる.

例 2.5. 1. 有限次元の数ベクトル空間 $\mathbb{K}^n$ を考える. このとき, 行列 $GL_n(\mathbb{K})$ の右作用を次のように与える.

$$S = (s_{i,j})_{i,j} \in GL_n(\mathbb{K}), \boldsymbol{v} = \begin{pmatrix} v_1, & v_2, & \cdots, & v_n \end{pmatrix} \in \mathbb{K}^n$$

に対して作用を

$$\boldsymbol{v}S = \begin{pmatrix} s_{1,1}v_1 + \cdots + s_{1,n}v_n, & s_{2,1}v_1 + \cdots + s_{2,n}v_n, & \cdots, s_{n,1}v_1 + \cdots + s_{n,n}v_n \end{pmatrix} \in \mathbb{K}^n$$

で与えればよい.

2. 群の右乗法による移動作用 G を群, $H \subset G$ を部分群とするとき $f'(g,h) = g * h$ ($*$ はに定まっている乗法の演算を表す) 群演算の結合律よりこれは G を集合と思ったときの群 H の右作用を与えている.
3. G を群とするとき G のの上への (右) 共役作用とは, $f'(t,s) = s^{-1}ts$ で与えられる作用である.

以後特にどちらかを指定しない場合は左作用であるとするが次のことが疑問になると思う.

1. 右作用と左作用との関係はあるのだろうか（あるいはどうなっているのだろうか）？
2. どうして両方の作用を考えるのか（全部左作用に統一しては駄目なのだろうか）？

まず最初の疑問に関しては例えば次のようにして左作用と右作用を互いに行き来できる (これがすべてではない).

補題 2.6. 群 G の集合 X への左作用 $f : G \times X \longrightarrow X$ が与えられているとする. このとき, $f' : X \times G \longrightarrow X$ を $f'(x, g) := f(g^{-1}, x)$ と定めることで G の集合 X への右作用 $f' : X \times G \longrightarrow X$ が定まる. 逆に, 群 G の集合 X への右作用 $f' : X \times G \longrightarrow X$ が与えられているとする. このとき, $f : G \times X \longrightarrow X$ を $f(g, x) := f(g^{-1}, x)$ と定めることで G の集合 X への左作用 $f : G \times X \longrightarrow X$ が定まる.

証明は省略するがひとつ注意をしておきたい. $G \longrightarrow G, g \mapsto g^{-1}$ のように群の掛け算の順番だけを逆転させる全単射で単位元を単位元にうつし自然に演算に関する結合律も保つもの[2]があれば右作用と左作用を入れ替えられる. 例えば, $G = GL_n(\mathbb{R})$ のときは, $GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R}),\ A \mapsto {}^tA$ がそのような写像の別の例を与えている.

さて上記の 2 番目の疑問に説明するために次のような例を考える.

例 2.7. $SL_2(\mathbb{R})$ は複素上半平面 $\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ に $g \cdot z = \dfrac{az + b}{cz + d}$ という規則で $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ が左作用する. さて, 複素上半平面 $\mathfrak{H}$ の上の正則函数 $f(z)$ たちの集合 $H(\mathfrak{H})$ に $f^g(z) = f(gz)$ と定めることで $H(\mathfrak{H})$ の上に $SL_2(\mathbb{R})$ が右作用している. [3]函数への作用は応用上大切であるが自然に入れようとするとこのように定義集合の上には左作用でも函数の上には右作用になるので (原則として左作用という方針だとしても) どちらの作用にも慣れた方がよいのである.

定義 2.8. X を G 作用をもつ集合とするとき,

$$\{x \in X \mid gx = g\ \forall g \in G\}$$

を不変部分集合とよび, X^G で記すことにする.

群は単に集合という単純な構造を持ったものではなく群, 環, 体など複雑な構造をもったものにも作用することが大事である.

定義 2.9. X を群 (resp. 環, 体) とする. X が群 G の作用をもつ集合とする. 勝手な $g \in G$ ごとに写像

$$X \longrightarrow X, \quad x \mapsto gx$$

[2] このようなものを反同型とよぶ

[3] 考え方としては, $gh \in G$ の作用が h を作用させた後に g を作用させたものであるなら左作用, g を作用させた後に h を作用させたものであるなら右作用である. このようなことに気をつけて右作用か左作用かを判断することができる

が X の演算を保つとき, G 作用をもつ群 (resp. 環, 体) という.

例 2.10. 1. X として複素数体 $\mathbb{C}$ をとる. $G = \langle\sigma\rangle$ $z \in \mathbb{C}$ を $z = x + \sqrt{-1}y$ とするとき, $\sigma \cdot z$ を複素共役 $z = x - \sqrt{-1}y$ で与える. 明らかに,

$$\sigma(z + z') = \sigma z + \sigma z', \quad \sigma(z \cdot z') = (\sigma z)\sigma(\sigma z')$$

であるから乗法や加法といった演算を保っている. このとき, X^G は実数全体に他ならない. このように体に有限群が作用する状況は後にガロア理論で発展的に論じられる.

3. 群の作用と軌道分解

定義 3.1. X を集合とする. X 上の同値関係 $\sim$ が定まっているとする. このとき, 同値なものを同一視することで商写像 $X \twoheadrightarrow X/\sim$ が考えられる. 商集合 $X/\sim$ のそれぞれの元を同値類とよぶ. 同値類 $c \in X/\sim$ に対して, $X \twoheadrightarrow X/\sim$ で c に写される $x \in X$ を (同値類 c の) 代表元とよぶ. また, $x \in X$ の $X/\sim$ における類を $[x]$ で記す. 部分集合 $\{x_\lambda\}_\Lambda \subset X$ が同値関係 $\sim$ に関する代表系もしくは完全代表系であるとは合成写像 $\{x_\lambda\}_\Lambda \hookrightarrow X \twoheadrightarrow X/\sim$ が全単射であることをいう.

例 3.2. 1. 集合 X として整数の集合 $\mathbb{Z}$ をとる.

$$x \sim x' \Longleftrightarrow x \text{ を } 3 \text{ で割った余り} = x' \text{ を } 3 \text{ で割った余り}$$

という関係とするとこれは同値関係であり, $X/\sim$ は 3 つの元からなる集合である. 整数の間のこのような同値関係をしばしば

$$x \equiv x' \mod 3$$

といった記号で表す. この場合の完全代表系は, 例えば $\{0, 1, 2\} \subset \mathbb{Z}$ で与えられる.

2. X に群 G が作用しているとする.

$$x \sim x' \Longleftrightarrow \exists g \in G,\ x = gx'$$

は同値関係である.

定義 3.3. X を集合とする. X 上に群 G が作用しているとき, 同値関係 $\sim$ が

$$x \overset{G}{\sim} x' \Longleftrightarrow \exists g \in G,\ x = gx'$$

で定まっているとする. このとき, 同値なものを同一視することで商集合 $X \twoheadrightarrow X/\overset{G}{\sim}$ が考えられる. (左) 作用 (resp. (右) 作用) による商集合 $X/\overset{G}{\sim}$ のことを特に, $G \setminus X$ (resp. X/G) と記す. $G \setminus X$ のそれぞれの元を G-軌道 (G-orbit) とよぶ. $x \in X$ に対してそれを含む G-軌道を Gx で記すことにする. $\overset{G}{\sim}$ の完全代表系 $\{x_\lambda\}_{\lambda\in\Lambda} \subset X$ をとるとき, 集合 X を G-軌道 Gx_λ の和に同値類別することができるこれを X の G-軌道分解とよぶ. 記号で

$$X = \coprod_{\lambda\in\Lambda} Gx_\lambda$$

と記すことにする.

例 3.4. 1. $X = \mathbb{Z}$ とする. 無限巡回群 $\langle\sigma\rangle$ が, $\sigma \cdot x = x + 3$ で作用しているとする. このとき

$$x \sim x' \Longleftrightarrow x \equiv x' \pmod 3$$

である. 状況を表にまとめると以下のようになる.

軌道 Gx	完全代表系	G 不変部分
$x + 3\mathbb{Z}$	$\{0, 1, 2\}$	空集合

2. $\mathbb{R}^2$ に群 $\mathbb{R}_{>0}$ を次のように作用させることができる. $\alpha \in \mathbb{R} \setminus \{0\}$, $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$ に対して $\alpha \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x \\ \alpha y \end{pmatrix}$ で与えられる.

軌道 Gx	完全代表系	G 不変部分
$\begin{pmatrix} x \\ y \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \coprod \{$ 円周 : $x^2 + y^2 = 1\}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$

3. 実数係数の 2 変数 2 次形式 $ax^2 + bxy + cy^2$ を考える.

実数係数の 2 変数 2 次形式 $\Longleftrightarrow$ 実数係数の 2×2 対称行列

$$f(x, y) = ax^2 + bxy + cy^2 \to A_f \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

$$f_A \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \leftarrow A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

という一対一対応がある. 対応する対称行列 A_f が正則であるとき $f(x, y)$ は非退化な 2 変数 2 次形式とよぶことにする. このとき, $GL_2(\mathbb{R})$ が $B \cdot f_A = f_{{}^tBAB}$ によって右作用する. この作用による完全代表系は $\{x^2 + y^2, x^2 - y^2, -x^2 - y^2\}$ である.

4. 剰余類分解と簡単な応用

さて前節でやった軌道分解の応用として剰余類分解を考えその簡単な応用を述べたい.

定義 4.1. G を群として $H \subset G$ を部分群とする. 左剰余類 (resp. 右剰余類)gH (resp. Hg) を $gH = \{gh \mid h \in H\}$ とする. つまり, 前節の言葉では, G が H に右乗法作用 (resp. 左乗法作用) するときの H 軌道ひとつひとつのことを H による左剰余類とよぶことにする. 右乗法作用 (resp. 左乗法作用) によるの商を G/H(resp. $H \setminus G$) と記すとき, H 軌道分解

$$G = \coprod_{g \in G/H} gH \quad (\text{resp.} G = \coprod_{g \in H \setminus G} Hg)$$

のことを左剰余類分解 (resp. 右剰余類分解) とよぶ.

作用に関して次の定義を付け加えたい.

定義 4.2. G が集合 X の上に作用しているとする. $\sharp(G \setminus X) = 1$ のとき (つまり勝手な $x, x' \in X$ に対してある $g \in G$ が存在して $x = gx'$ となるとき), G が集合 X の上に作用は推移的であるもしくは可移的 (transitive) であるとよばれる.

例 4.3. 1. 左剰余類集合 G/H には G が (左) 作用する. このとき, G/H 上への G の作用は推移的である.
2. $SL_2(\mathbb{R})$ は $\mathfrak{H}$ の上に一次分数変換で作用する. この作用は推移的である.
3. G が集合 X に作用しているとする. 軌道分解

$$X = \coprod_{\lambda\in\Lambda} Gx_\lambda$$

を考えたときの各 G 軌道 Gx_λ はそれ自身 G 作用をもつ集合である. さらに, Gx_λ 上への G の作用は推移的であるこのようにして一般の G 作用をもつ集合は推移的 G 作用をもつ集合の和として分解される.

定義 4.4. G が集合 X の上に作用しているとする. $x \in X$ に対して次の集合

$$G_x = \{g \in G \mid gx = x\}$$

は G の部分群となる. この部分群を x の固定化群とよぶ.

命題 4.5. G が集合 X の上に推移的に作用しているとする. このとき,
1. 勝手な $x, x' \in X$ に対して G_x と $G_{x'}$ は互いに同型な G の部分群になっている.
2. 勝手な $x \in X$ に対して G/G_x と X は G 集合として同型である (つまり集合としての全単射写像 $h : G/G_x \longrightarrow X$ があって, $h(gx) = gh(x)$ が任意の $x \in X$ と任意の $g \in G$ に対して成り立つ).

Proof. 作用が推移的であるから勝手な $x, x' \in X$ に対して $g \in G$ が存在して $x = sx' (\Leftrightarrow x' = s^{-1}x)$ となる. この s を用いて, (左) 共役作用による写像

$$G \longrightarrow G, \quad g \mapsto sgs^{-1}$$

を考える. この写像は G から G 自身への群の同型である. 今, $g \in G_{x'}$ とする. このとき,

$$(sgs^{-1})x = sg(s^{-1}x) = sgx' = s(gx') = sx' = x$$

である. したがって, $sgs^{-1} \in G_x$ となる. この対応 $G_{x'} \hookrightarrow G_x$ は群準同型であることにも注意したい.

さて一方で (右) 共役作用による写像

$$G \longrightarrow G, \quad g \mapsto s^{-1}gs$$

を考えると, 単射な群準同型 $G_x \hookrightarrow G_{x'}$ が得られて構成より上でつくった単射な群準同型 $G_{x'} \hookrightarrow G_x$ の逆写像となっている. 以上より, $G_{x'} \longrightarrow G_x, g \mapsto gsg^{-1}$ は同型写像である.

G/G_x の各軌道は $[g] = gG_x$ という形である. 今 $h : G/G_x \longrightarrow X$ を $[g] \mapsto gx$ $(g \in gG_x)$ で定める. ここで gx は代表元 $g \in gG_x$ のとり方によらないことに注意. X への G 作用が推移的であることより勝手な x' に対して $sx = x'$ なる $s \in G$ が存在する. $s \in g'G_x$ とすると $h([g']) = sx = x'$ であるから $h : G/G_x \longrightarrow X$ は全射である. さらに, 2 つの異なる剰余類 $[s], [s']$ が同じ $x' \in X$ に移ったとすると, $sx = s'x$ であるから $s(s')^{-1} \in G_x$ であり矛盾する. 作用が保たれることの議論は省略する. □

例 4.6. 先の複素上半平面 $\mathfrak{H}$ と $SL_2(\mathbb{R})$ の例を考える. このとき, $\sqrt{-1}$ の固定化群 $G_{\sqrt{-1}} \subset SL_2(\mathbb{R})$ は $SO(2,\mathbb{R}) = \{A \in SL_2(\mathbb{R}) | {}^tAA = E\}$ であった. したがって, $\mathfrak{H}$ と $SL_2(\mathbb{R})/SO(2,\mathbb{R})$ は $SL_2(\mathbb{R})$ 作用をもつ集合として同型である.

補題 4.7. G を群として $H \subset G$ を部分群とする. このとき自然な全単射 $H \setminus G \longrightarrow G/H$ がある.

Proof. G の上の写像 $G \longrightarrow G, g \mapsto g^{-1}$ を考える. このとき,

$$\begin{aligned} g, g' \in G \text{ が } G/H \text{ の同じ左剰余類に属する} &\iff gH = g'H \\ &\iff g^{-1}g' \in H \end{aligned}$$

同様に

$$\begin{aligned} g, g' \in G \text{ が } G/H \text{ の同じ右剰余類に属する} &\iff Hg = Hg' \\ &\iff g'g^{-1} \in H \end{aligned}$$

したがって G/H の完全代表系 $\{g_\lambda\}_{\lambda\in\Lambda}$ をとると $\{g_\lambda^{-1}\}_{\lambda\in\Lambda}$ が $H \setminus G$ の完全代表系となる. □

定義 4.8. G を群として $H \subset G$ を部分群とする. このとき G/H の濃度は $H \setminus G$ の濃度と等しい. $\sharp(G/H) = \sharp(H \setminus G) < \infty$ のとき, これを指数 (index) とよび $[G : H]$ で記す. $\sharp(G/H) = \sharp(H \setminus G) = \infty$ のとき指数は無限であるという.

例 4.9. 群 $G = GL_n(\mathbb{R})$ を考える. 部分群 $H = \{g \in G \mid \det(g) > 0\}$ を考えると, 指数は $[G : H] = 2$ となる. H として例えば $SL_n(\mathbb{R})$ をとると指数は無限である.

補題 4.7, 定義 4.8 からただちに次のことがしたがう.

定理 4.10 (Lagrange)**.** G を有限群, $H \subset G$ を部分群とする. このとき $\sharp H$, 指数 $[G : H]$ は $\sharp G$ の約数であり等式 $\sharp G = [G : H]\sharp H$ が成り立つ. 特に勝手な元 g の位数は $\sharp G$ の約数である.

系 4.11. 有限群 G の位数が素数であるとき, G は位数 p の巡回群と同型である.

Proof. $\sigma \in G$ を単位元 1_G とは異なる元とする. このとき, $\langle\sigma\rangle \subset G$ は自明でない部分群を与えており, $\sharp\langle\sigma\rangle | \sharp G$ である. □

自然数 n を与えたとき位数 n の有限群は (同型なものを同一視すると) 有限個しかない. このことは, 例えば乗積表を考えるとすぐわかる.

自然な発想で次のような問題が生じるのではないだろうか

問題 自然数 n を与えたとき位数が n の群はどれくらいあるだろうか? またそれらを全て決定できるだろうか?

上の命題は n が素数であるという特別な場合のこの問題の解答を与えている. この機会にそれ以外の場合にもこの問題を考えてみたい. そのためにひとつ言葉を導入しておく.

定義 4.12. G, G' を群とするとき, 直積集合 $G \times G'$ の上に 2 項演算 $*$ を

$$(s, s') * (t, t') = (st, s't') \quad s, t \in G,\ s', t' \in G'$$

で定める. このとき $G \times G'$ は単位元を $1_{G\times G'} = (1_G, 1_{G'})$, $(g, g') \in G \times G'$ の逆元を (g^{-1}, g'^{-1}) として群となる (結合法則は各自チェックのこと). この群を直積群とよび記号 $G \times G'$ で記す. 全く同様に添え字集合 Λ で添え字付けられる群の族 $\{G_\lambda\}_{\lambda\in\Lambda}$ が与えられたとき, 直積群 $\prod_{\lambda\in\Lambda} G_\lambda$ が定義される.

注意 4.13. 1. 群 G, G' が有限群のとき $G \times G'$ も有限群で $\sharp(G \times G') = \sharp G \cdot \sharp G'$ である.
2. 群 G, G' ががともにアーベル群のとき $G \times G'$ もアーベル群である.

さて先の自然数 n を与えたとき位数が n の群を分類する問題に立ち返ってみる. n が小さい順に考えていくと,

1. $n = 2, 3$ は素数より, 上のことより位数 2, 3 の群は同型を除いてそれぞれ巡回群 C_2, C_3 のみである (系 4.11 の帰結).
2. $n = 4$ のとき, C_4 と $C_2 \times C_2$ のみしか存在しない. 実際, $\sharp G = 4$ で $G \ncong C_4$ とする. このとき,
   (a) G の単位元以外の元はすべて位数が 2 である (位数 4 の元が存在した時点で $G \cong C_4$ となってしまい矛盾).
   (b) $g \neq g'$ を G の位数 2 の元とすると gg' も位数 2 である (g' の位数が 2 より $gg' = 1_G$ としたら $g = (g')^{-1} = g'$ となり矛盾, またすぐ上で述べたように $G \ncong C_4$ より位数が 4 となることはない).
   (c) gg' は g, g' たちとは異なる元である. ($gg' = g'$ とすると, g'^{-1} を右からかけて $g = 1_G$ となってしまうので矛盾する. 同様にして $gg' \neq g'$ もいえる)
   (d) gg', g, g' たちはみな互いに可換である. (例えば $(gg')(gg') = 1_G$ に右から g をかけ左から g' をかけることで $g'g = gg'$ を得る)

   $G \cong C_2 \times C_2$ を $g \mapsto (\sigma, 1), g' \mapsto (1, \sigma)$ とするとこれは同型を与えている.
3. $n = 5$ のとき, 巡回群 C_5 のみである (系 4.11 の帰結).
4. $n = 6$ のとき, (まだ証明は後回しにするが) 巡回群 C_6 と S_3 のみである. $n = 6$ が非アーベルな有限群が存在する最小の自然数である.
5. $n = 7$ のとき, 巡回群 C_7 のみである (系 4.11 の帰結).

この講義において今後もう少し色々な道具立てを発展させていく (例えば Sylow の定理など) ことでこれらの問題をもう少し考えられるようになってくる. 道具立てを整えた上で再度このような問題を考えてみたい.

5. 正規部分群と準同型定理

群論における課題とはなんだろうか? 視点を整理してみたい.

1. ある種のクラスの群の分類や数え上げ (例えば前節最後のように位数 n をもつ有限群を数えたり分類すること, 有限群すべてを適当な基準で分類したり存在性や非存在性を示すことなど)
2. 個別の群 G それぞれの内部構造（部分群の様子など）や種々の性質がわかること

定義 5.1. G を群, N を G の部分群とする. 任意の $g \in G$ に対して $gNg^{-1} = N$ となるとき (あるいは $gN = Ng$ となるとき), N は正規部分群 (normal subgroup) であるという. N が G 正規部分群であることを $N \triangleleft G$ 又は $G \triangleright N$ という記号で表す.

補題 5.2. N が G の正規部分群とする. このとき, 左剰余類分解 $G = \coprod_{\lambda\in\Lambda} g_\lambda N$ を与える左剰余類 G/N には代表元 $\{g_\lambda\}_{\lambda\in\Lambda}$ のとり方に寄らず, 2 項演算

$$* : (g_\lambda N) * (g_{\lambda'} N) = g_\lambda g_{\lambda'} N$$

が定まる.

Proof. $g_\lambda n$, $g_{\lambda'} n'$ $(n, n' \in N)$ と $g_\lambda N$, $g_{\lambda'} N$ の別の代表元をとる. このとき,

$$(g_\lambda n)(g_{\lambda'} n') = g_\lambda (g_{\lambda'} g_{\lambda'}^{-1}) n g_{\lambda'} n' = g_\lambda g_{\lambda'} (g_{\lambda'}^{-1} n g_{\lambda'}) n'$$

である (N が正規部分群より $g_{\lambda'}^{-1} n g_{\lambda'} \in N$ であることを用いている) これによって, $(g_\lambda n)(g_{\lambda'} n') \in g_\lambda g_{\lambda'} N$ が示せ, 演算 $*$ が代表元によらずに well-defined であることが得られた. □

定義 5.3. これによって G/N には群の構造が入る. また全射群準同型 $\pi : G \longrightarrow G/N,\ g \mapsto gN$ のことを標準準同型とよぶことにする.

例 5.4. 1. G をアーベル群とするとき, 任意の部分群 N は正規部分群である.

2. $G = GL_n(\mathbb{R})$ とする. このとき上半三角行列 $B = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}$ は正規部分群ではない. $g = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ とすると, gBg^{-1} は下三角行列となる.

定義 5.5. $f : G \longrightarrow G'$ を群 G から群 G' への準同型とする. このとき,

$$\mathrm{Im}(f) = \{f(g) \mid g \in G\}$$
$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1_{G'}\}$$

をそれぞれ f の像 (image), 核 (kernel) という

補題 5.6. $\mathrm{Ker}(f)$, $\mathrm{Im}(f)$ はそれぞれ G, G' の部分群である. さらに, $\mathrm{Ker}(f)$ は G の正規部分群である.

Proof. 部分群 $g\mathrm{Ker}(f)g^{-1}$ を考える. 今, $x \in \mathrm{Ker}(f)$ とするとき,

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)1_{G'}f(g)^{-1}$$

より $g\mathrm{Ker}(f)g^{-1} \subset \mathrm{Ker}(f)$ となる. 今右共役写像 $G \longrightarrow G, x \mapsto g^{-1}xg$ は全単射であるから上の包含関係から $\mathrm{Ker}(f) \subset g^{-1}\mathrm{Ker}(f)g$ が得られる. 上と同じ議論を g の代わりに g^{-1} で行うと $\mathrm{Ker}(f) \supset g^{-1}\mathrm{Ker}(f)g$ が得られる. したがって, $\mathrm{Ker}(f) = g^{-1}\mathrm{Ker}(f)g$ となる. □

定理 5.7 (準同型定理または第 1 同型定理)**.** $f : G \longrightarrow G'$ を群の準同型, $N = \mathrm{Ker}(f)$ とおくとき, $G/N \cong \mathrm{Im}(G')$ が成り立つ.

Proof. $G/\mathrm{Ker}(f)$ から $\mathrm{Im}(f)$ に対応 $\overline{f}$ を

$$gN \mapsto f(g)$$

で与える. この対応は全射であり,

$$\begin{aligned} gN = g'N &\Longleftrightarrow g^{-1}g' \in N \\ &\Longleftrightarrow f(g^{-1}g') = 1_{G'} \\ &\Longleftrightarrow f(g) = f(g') \end{aligned}$$

より単射でもある. N は正規部分群より先と同様の議論で $\overline{f}$ は群準同型でもある. よって同型 $\overline{f} : G/N \xrightarrow{\sim} \mathrm{Im}(f)$ が得られた. □

次の例に見るように第 1 同型定理によって, 由来が異なる別の群を同一視できることがある.

例 5.8. 1. $\det : GL_n(\mathbb{R}) \longrightarrow \mathrm{R}^\times$ は全射群準同型であり, 定義から $SL_n(\mathbb{R})$ がその核である. 第一同型定理より $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathrm{R}^\times$ を得る.

2. 加法群 $\mathbb{R}$ から乗法群 $\mathbb{C}^\times$ への準同型を $x \mapsto \exp(2\pi\sqrt{-1}x)$ で与える. この群準同型の核は $\mathbb{Z} \subset \mathbb{R}$ であり像は $T := \{z \in \mathbb{C} \mid |z| = 1\}$ なる $\mathbb{C}$ の部分群である. 第一同型定理より $\mathbb{R}/\mathbb{Z} \cong T$ が得られる.

補題 5.9. 1. G を群として, $H \subset G$ を (勝手な) 部分群, $N \subset G$ は正規部分群とする. このとき, $HN = \{hn \mid h \in H, n \in N\}$ は NH と等しく, また HN は G の部分群となる.

2. G を群として H_1, H_2 を G の部分群とすると $H_1 \cap H_2$ はまた G の部分群である.

Proof. N は正規部分群であるから任意の $h \in H$ に対して $hN = Nh$ が成り立つ. よって $HN = NH$ が言える. このことから $(HN)(HN) = NHHN = NHN = HNN = HN$ より HN は G の積演算 $*$ で閉じている. 今,

1. $1_G \in HN$ である.
2. $(HN)^{-1} = N^{-1}H^{-1} = NH = HN$ より逆元をとる操作でも閉じている.
3. G 全体が群であることより結合法則は明らか.

より HN は群となっている. □

定理 5.10 (第 2 同型定理)**.** G を群として, $H \subset G$ を (勝手な) 部分群, $N \subset G$ は正規部分群とする. このとき, $HN/N \cong H/H \cap N$ ば成り立つ.

Proof. 第一同型定理で得られた準同型 $h : G \longrightarrow G/N$ を H に制限するとその核は $H \cap N$ である. $h|_H$ に対して第一同型定理を用いると

$$H/H \cap N \cong \mathrm{Im}(h|_H)$$

が得られる. 一方で準同型 $h : G \longrightarrow G/N$ を HN に制限するとその核は H である. $h|_H$ に対して第一同型定理を用いると

$$HN/N \cong \mathrm{Im}(h|_{HN})$$

が得られる. $\mathrm{Im}(h|_{HN}) = \mathrm{Im}(h|_H)$ であるから $HN/N \cong H/H \cap N$ が得られる. □

補題 5.11. *N を群 G の正規部分群として標準準同型 $\pi : G \twoheadrightarrow G/N$ を考える. このとき, 次のような一対一対応がある:*

$$\{N \subset H \text{ なる } G \text{ の部分群 } H \text{ たち }\} \longleftrightarrow \{G/N \text{ の部分群 } \overline{H} \text{ たち }\}$$
$$H \to \pi(H)$$
$$\pi^{-1}(\overline{H}) \leftarrow \overline{H}$$

定理 5.12 (第 3 同型定理)**.** *G を群として, N_1, N_2 は G の正規部分群で $N_2 \subset N_1$ とする. このとき, $(G/N_2)/(N_1/N_2) \cong G/N_1$*

Proof. 次のような合成写像を考える. $G \overset{\pi_1}{\twoheadrightarrow} G/N_2 \overset{\pi_2}{\twoheadrightarrow} (G/N_2)/(N_1/N_2)$ を考える. $\mathrm{Ker}(\pi_2) \subset G/N_2$ は N_1/N_2 であることに注意したい. また, 上の補題より $\mathrm{Ker}(\pi_2 \circ \pi_1) = \pi_1^{-1}(N_1/N_2) = N_1$ である. 合成写像 $\pi_1 \circ \pi_2$ に対して第一同型定理を適用すると証明が終わる. □

この節の最後に少し正規部分群や同型定理に関係する抽象概念や抽象的結果をいくつか述べておきたい.

補題 5.13. *G を群, $H \subset G$ を指数 2 の部分群とする. このとき, H はの正規部分群となる.*

Proof. $g \in G - H$ とすると, $gH \neq H$ であるから左剰余類分解 $G = H \coprod gH$ が得られる. 一方で $Hg \neq H$ であるから右剰余類分解 $G = H \coprod Hg$ が得られる. よって, $gH = Hg$ であるから H は正規部分群でなければならない. □

定義 5.14. *G を群とする. $[a, b] = a^{-1}b^{-1}ab$ とするとき*

$$\{[a, b] \mid a, b \in G\}$$

を含む最小の G の部分群を交換子群とよび記号 $D(G)$ で記す.

命題 5.15. *$D(G)$ は正規部分群であり, 剰余群 $G/D(G)$ はアーベル群である. また逆に N をがアーベル群となるような正規部分群とすると必ず $D(G) \subset N$ である.*

Proof. $g \in G$ とする. 勝手な $a, b \in G$ に対して $g[a, b]g^{-1} = [g^{-1}ag, g^{-1}bg]$ である. よって集合として

$$g\{[a, b] \mid a, b \in G\}g^{-1} = \{[a, b] \mid a, b \in G\}$$

である. $gD(G)g^{-1}$ はやはり $\{[a, b] \mid a, b \in G\}$ を含む最小の G の部分群であるから $D(G)$ に等しく, $D(G)$ は G の正規部分群でなければならない. 今, N を勝手な正規部分群とする. $a, b \in G$ に対して G/N における像を $\overline{a}, \overline{b}$ で記す.

$$\overline{a}\overline{b} = \overline{b}\overline{a} \Longleftrightarrow \overline{a}^{-1}\overline{b}^{-1}\overline{a}\overline{b} = 1_{G/N}$$
$$\Longleftrightarrow [a, b] \in N$$

より他の性質がしたがう. □

$G/D(G)$ はアーベル群であるような G の剰余群のうち “最大” のものである.

定義 5.16. G を群とするとき, $G/D(G)$ をアーベル化 (abelianization) とよぶ.

定義 5.17. G を群とするとき, $\mathrm{Isom}(G)$ を G の自己同型全体の集合とする. $\mathrm{Isom}(G)$ は自然に写像としての合成を積演算として群をなす. 言い換えると, $\mathrm{Isom}(G)$ は $\mathrm{Aut}(G)$ の元のうち群演算を保つものからなる部分群である.

例 5.18. 素数 $p \geq 3$ を位数にもつ巡回群 $C_p = \langle \sigma \rangle$ を考える. $\tau \in \mathrm{Isom}(C_p)$ とするとき, $\tau(1_{C_p}) = 1_{C_p}$ でなければならない. $\tau(\sigma) \neq 1_{C_p}$ よりある $i \in (\mathbb{Z}/(p)\mathbb{Z})^\times$ があって, $\tau(\sigma) \neq \sigma^i$ とかける. また, $\tau(\sigma) = \sigma^i$ ならば他の元 σ^j $(j = 1, \cdots, p-1)$ の行き先は $\tau(\sigma^j) = \tau(\sigma)^j = (\sigma^i)^j = \sigma^{ij}$ として決まってしまう. これは群同型であることも確かめられる. 以上より, $\mathrm{Isom}(C_p) \cong (\mathbb{Z}/(p)\mathbb{Z})^\times$ がわかる.

一般には G に対して $\mathrm{Isom}(G)$ を決めるのは難しい問題である.

定義 5.19. G を群とする. ある $s \in G$ によって与えられる写像

$$i_s : G \longrightarrow G, \quad g \mapsto sgs^{-1}$$

は G の自己同型である. このように共役によって与えられる G の自己同型を内部自己同型 (inner automorphism) とよぶ. 内部自己同型全体からなる $\mathrm{Isom}(G)$ の部分群を $\mathrm{Inn}(G)$

定義 5.20. G を群とする.

$$Z(G) = \{g \in G \mid g \text{ は } G \text{ の全ての群と可換 }\}$$

という部分集合は G の正規部分群となる. $Z(G)$ のことを G の中心 (center) とよぶ.

例 5.21. $\mathbb{K}$ を可換体とする. $G = GL_n(\mathbb{K})$ とするとき, $Z(G)$ はスカラー行列のなす部分群 $\{\lambda E_n \mid \lambda \in \mathbb{K}^\times\}$ である.

命題 5.22. G を群とする.

1. $\mathrm{Inn}(G)$ は $\mathrm{Isom}(G)$ の正規部分群である.
2. 自然な写像 $G \longrightarrow \mathrm{Inn}(G), s \mapsto i_s$ の核は $Z(G)$ と一致する. 特に G がアーベル群ならば $\mathrm{Inn}(G) = \{1\}$ である.

定義 5.23. G を群とする. $\mathrm{Isom}(G)/\mathrm{Inn}(G)$ のことを外部自己同型群とよび $\mathrm{Out}(G)$ と記す.

この節ででてきた概念の例や重要性については今後機会があるごとに触れていきたい.

6. 群の表示と簡単な群の例について

ここでもう少し今までにでていない群のうち特に主要な有限群をいくつかみてみたい. そのためにまず群の構造に関する情報を決める要素について考えてみたい. 群が定まるには次のような乗積表を考えるのがひとつの方法である.

	$\mathbf{1}_2 \times \mathbf{1}_2$	$\sigma \times \mathbf{1}_2$	$\mathbf{1}_2 \times \sigma$	$\sigma \times \sigma$
$\mathbf{1}_2 \times \mathbf{1}_2$	$\mathbf{1}_2 \times \mathbf{1}_2$	$\sigma \times \mathbf{1}_2$	$\mathbf{1}_2 \times \sigma$	$\sigma \times \sigma$
$\sigma \times \mathbf{1}_2$	$\sigma \times \mathbf{1}_2$	$\mathbf{1}_2 \times \mathbf{1}_2$	$\sigma \times \sigma$	$\mathbf{1}_2 \times \sigma$
$\mathbf{1}_2 \times \sigma$	$\mathbf{1}_2 \times \sigma$	$\sigma \times \sigma$	$\mathbf{1}_2 \times \mathbf{1}_2$	$\sigma \times \mathbf{1}_2$
$\sigma \times \sigma$	$\sigma \times \sigma$	$\mathbf{1}_2 \times \sigma$	$\sigma \times \mathbf{1}_2$	$\mathbf{1}_2 \times \mathbf{1}_2$

実際, $C_2 = \langle \sigma \rangle$ の直積 $C_2 \times C_2$ の乗積表は上のようになる. この表はの演算のパターンすべてを表しているのである意味で群としての情報を全て含んでいるといえる. 例えば, $C_2 \times C_2$ が C_4 と同型でないことは乗積表を書いて比べればわかるわけである. 一方で, 群の位数が大きくなれば書くのは大変である. また群が無限であれば乗積表はかくことができない. 以下で群を規定する別の表示として「生成元と関係式」について触れていきたい. そのためにまず必要な自由群を導入する.

定義 6.1. $S = \{s_\lambda\}_{\lambda \in \Lambda}$ を集合とする (Λ は添え字集合). このとき, 同じ添え字集合を持つ $\overline{S}$ を $\overline{S} = \{s_\lambda^{-1}\}_{\lambda \in \Lambda}$ と記し, また空語として記号的に $\{\mathbf{1}\}$ で導入する. 合併集合 $\widetilde{S} = S \cup \overline{S} \cup \{\mathbf{1}\}$ の各元をアルファベットとよび,

$$\widetilde{F}(S) = \{\widetilde{S} \text{ の有限個のアルファベットの配列すべて }\}$$

とおく. $\widetilde{G}$ に次のような同値関係を入れる.

1. $\forall s \in \widetilde{S}$ に対して $\mathbf{1}s \sim s\mathbf{1} \sim s$.
2. $\forall \lambda \in \Lambda$ に対して $s_\lambda s_\lambda^{-1} \sim s_\lambda^{-1} s_\lambda \sim \mathbf{1}$.

$F(S) = \widetilde{F}(S)/\sim$ とおく. $F(S)$ の元 g, h の積 gh を次のように入れる. g, h の $\widetilde{F}(S)$ における代表元を $g_1 \cdots g_m$, $h_1 \cdots h_n$ としたとき (ここで, $g_1, \cdots, h_n$ は $\widetilde{S}$ の中のアルファベット), gh は $g_1 \cdots g_m h_1 \cdots h_n \in \widetilde{F}(S)$ を代表元にもつ元である. $F(S)$ は単位元を $\mathbf{1}$ として群をなす. $F(S)$ を S で生成される自由群 (free group) とよぶ. 特に S が位数 n の有限集合であるとき, $F(S)$ を F_n で記して階数 n の自由群とよぶ.

命題 6.2. 1. G を勝手な群, S を勝手な集合とする. このとき勝手な集合としての写像 $h : S \longrightarrow G$ は群の準同型 $\overline{h} : F(S) \longrightarrow G$ で $h = \overline{h} \circ i$ (但し, i は合成写像 $S \hookrightarrow \widetilde{S} \twoheadrightarrow F(S)$) をひきおこす. 一方で合成写像 i は単射であることに注意すると
2. 勝手な群 G に対して集合が存在して G は自由群 $F(S)$ の剰余群となる.

Proof. 最初の記述について説明する. 次のようにして $h :\longrightarrow G$ は写像 $\widetilde{h} : \widetilde{F}(S) \longrightarrow G$ へと拡張される.

1. 与えられた $h : S \longrightarrow G$ を写像 $\widetilde{h} : \widetilde{S} \longrightarrow G$ に $\widetilde{h}(\mathbf{1}) = 1_G$, $\widetilde{h}(s^{-1}) = h(s)^{-1}$ で拡張する.
2. また G での群演算を $*$ としたとき, $\widetilde{h}(ss') = \widetilde{h}(s) * \widetilde{h}(s')$ で定める.

このように $\widetilde{h}$ を与えると.

$$\widetilde{h}(ss^{-1}) = \widetilde{h}(s)\widetilde{h}(s)^{-1} = 1_G$$
$$\widetilde{h}(s^{-1}s) = \widetilde{h}(s)^{-1}\widetilde{h}(s) = 1_G$$
$$\widetilde{h}(s\mathbf{1}) = \widetilde{h}(s)1_G = \widetilde{h}(s)$$
$$\widetilde{h}(\mathbf{1}s) = 1_G\widetilde{h}(s) = \widetilde{h}(s)$$

が成り立つ. よって同値関係でわったところの準同型 $\overline{h} : F(S) \longrightarrow G$ を自然に引き起こす.

2 番目の記述は最初のものを用いてとくに自由群 $F(G)$ を考え, 集合の恒等写像 $G \longrightarrow G$ が引き起こす群準同型 $F(G) \longrightarrow G$ を考えればよい. この写像は全射より G は自由群 $F(G)$ の剰余群となる. □

定義 6.3. 集合 $S = \{s_\lambda\}_{\lambda\in\Lambda}$ で生成される自由群 $F(S)$ を $\{t_\mu\}_{\mu\in M} \subset F(S)$ を含む最小の正規部分群による剰余群を

$$\langle s_\lambda(\lambda \in \Lambda) \mid t_\mu(\mu \in M)\rangle$$

であらわすことにする. 上述の命題により勝手な群はこのような形の群で表されるので

$$G \cong \langle s_\lambda(\lambda \in \Lambda) \mid t_\mu(\mu \in M)\rangle$$

とあらわすこと (もしくは表し方) を G の表示 (presentation) とよび, s_λ たちを生成系, t_μ たちを関係式とよぶ.

注意 6.4.
1. F(S) がアーベル群であるのは $\sharp S = 1$ のときのみである. $S = \{s\}$ のとき, $F(S)$ は, $s\cdots s$(s の n 個の積) を $n \in \mathbb{Z}$ へうつし, $s^{-1}\cdots s^{-1}$(s^{-1} の n 個の積) を $-n \in \mathbb{Z}$ へうつす対応で与えられる群の同型 $F(S) \cong \mathbb{Z}$ がある.
2. $F_n/D(F_n)$ は n 個の直積群 $\mathbb{Z}\times\cdots\times\mathbb{Z}$ と同型である.
3. 自由群の部分群は常に自由群である. 有限な階数をもつ自由群 F_n の指数有限な部分群はまた有限な階数をもつ自由群であるが階数は n より大きくなり得る.

定義 6.5. 自然数 $n > 1$ に対してオイラー数 $\varphi(n)$ を環 $\mathbb{Z}/(n)\mathbb{Z}$ の可逆元 $(\mathbb{Z}/(n)\mathbb{Z})^\times$ のなす群の位数として定義する. 同値な定義として $\varphi(n)$ は $1 \leq i \leq n$ なる自然数のうちで $(i, n) = 1$ なるものの個数である.

補題 6.6. $n > 1$ が自然数とするとき, $n = \sum_{1\leq r|n} \varphi(r)$ が成り立つ (ここで, $r = 1, n$ も含んでいることに注意).

巡回群の特徴づけとして次のようなことが成り立つ.

命題 6.7. *G を位数 n の有限群とするとき, 次の条件は同値である:*
1. 勝手な約数 $r|n$ に対して部分集合 $o_r(G) = \{\sigma \in G \mid \sigma^r = 1_G\}$ の位数は r 以下である.
2. G は有限巡回群である.
3. G は次のような表示 $\langle\sigma|\sigma^n = \mathbf{1}\rangle$ をもつ.
4. G は加法群 $\mathbb{Z}/(n)\mathbb{Z}$ と同型.

証明の前にこの命題の (最初のステートメントの)「意味」を理解するために次の簡単な例には注意しておきたい.

注意 6.8. 位数 n の有限群 G が巡回群でなければ $\sharp o_r(G) > r$ なる n の約数 r があるはずである.

1. $G = C_2 \times C_2$ のとき, $n = 4$, $o_2(G) = G$ である.
2. $G = S_3$ のとき, $n = 4$, $\sharp o_2(S_3) = 4 > 2$ である.

Proof. 同値性 $1 \iff 2 \iff 3$ は明らか. 2 から 1 を導くのも容易であるから, 1 から 2 を導くことのみ行う. したがって以後 1 を仮定する. 位数が丁度の n 元が存在することをいえば証明が終わる. 勝手な元 $g \in G$ の位数は n の約数である. g の位数は r であったとする. g^i $(i = 1, \cdots, r)$ は全て異なる. 一方で, 勝手な i で $(g^i)^r = 1_G$ より $S_r = \{g, g^2, \cdots, g^r\}$ となる. この中で位数が r になるものは $(i, r) = 1$ である g^i のみでありかつ位数が r の元はそれで尽くされる. よって次がいえる.

(1) 位数 r の元の個数は (もし存在すれば)$\varphi(r)$ 個である.

また Lagrange の定理から次も成り立つ.

$$\sharp G = \sum_{1 \le r \le n} \text{位数が丁度 } r \text{ の元たちの個数} \tag{2}$$

である. 補題 6.6 の式と合わせると位数たちの勘定から必ず位数 n の元が存在しなければならないことが導かれた. □

系 6.9. K を可換体とする. G を乗法群 $K^\times = K - \{0\}$ の有限部分群とするときは巡回群である. 特に $\sharp K$ が有限な体 K に対しては $K^\times = K - \{0\}$ は巡回群である.

巡回群と関連して次の大切な定理は思い出しておきたい:

定理 6.10 (有限アーベル群の構造定理)**.** G を位数有限のアーベル群とするとき有限個の自然数 $n_1, \cdots, n_r$ が存在して G は $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ と同型になる.

次のような群を考える

定義 6.11. $n \ge 2$ を自然数とする. 次のような表示で与えられる群:

$$D_n = \langle \sigma, \tau \mid \sigma^2 = \mathbf{1}, \tau^n = \mathbf{1}, \sigma\tau\sigma = \tau^{-1} \rangle$$

を n 次 2 面体群 (dihedral group) とよぶ.

注意 6.12. n 次 2 面体群はユークリッド空間 $\mathbb{R}^2$ の合同変換群[4]のの中で正 n 角形をそれ自身にうつすような部分群としての意味をもつ.

命題 6.13. 各自然数 $n \ge 2$ に対して n 次 2 面体群 D_n の位数は $2n$ である. また, $n \ge 3$ なら D_n は非アーベル群である.

[4]一般に n 次元ユークリッド空間 $\mathbb{R}^n$ の合同変換群とは勝手な 2 点の間の距離を変えない $\mathbb{R}^n$ から $\mathbb{R}^n$ への写像のなす群ことをいう. 例えば, 回転写像や平行移動, 超平面に関する鏡映変換などが合同変換である. 定義より合同変換は全単射であることが導かれる. また $\mathbb{R}^n$ の勝手な合同変換は高々$n + 1$ 個の鏡映の合成で表せる

Proof. $n=2$ のとき $D_2 \cong C_2 \times C_2$ である. よって $n \geq 3$ とする. $N = \langle \tau \rangle \subset D_n$ は N は位数 n の部分群である.

$$\sigma\tau = (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1} = \tau^{n-1}\sigma \tag{3}$$

に注意しよう. $n \geq 3$ より特に $\sigma\tau \neq \tau\sigma$ であるから D_n は非アーベル群である. また $\sigma N = N\sigma$ より N は正規部分群である. 剰余群 D_n/N は $(\sigma N)(\sigma N) = (N\sigma)(\sigma N) = NN = N$ より位数 2 の巡回群である. よって D_n の位数は $2n$ である. □

以前定義したように $\sharp X = n$ の有限集合の自己同型群 $\mathrm{Aut}(X)$ が n 次対称群 S_n であった.

命題 6.14. *G を位数 n の有限群とする. G は対称群 S_n のある部分群と同型になる.*

Proof. $\sharp(G) = n$ に注意したい. S_n を $\mathrm{Aut}(G)$ と同一視するとき, $G \longrightarrow \mathrm{Aut}(G) \cong S_n$ を $s \in G$ に対して $f_s \in \mathrm{Aut}(G), g \mapsto sg$ を与える写像とするとこれは準同型である. $s \neq s'$ とすると $f_s(\mathbf{1}) = s \neq s' = f_{s'}(\mathbf{1})$ よりこの写像 $G \longrightarrow S_n$ は単射である. よって証明を終える. □

集合の同型 $X \cong X'$ は自己同型群の同型 $\mathrm{Aut}(X) \cong \mathrm{Aut}(X')$ を引き起こす. 以後特に $S_n = \mathrm{Aut}(\{1, 2, \cdots, n\})$ とみなすことにする.

定義 6.15. *$r \leq n$ なる自然数があったとき長さ r の巡回置換 (cyclic permutation) とは r 個の異なる数 $\{i_1, \cdots, i_r\} \subset \{1, \cdots, n\}$ に対して, $i_1 \mapsto i_2, i_2 \mapsto i_3, \cdots, i_{r-1} \mapsto i_r, i_r \mapsto i_1$ と入れ替えて, $\{1, \cdots, n\} - \{i_1, \cdots, i_r\}$ の上では恒等置換であるような変換のことをいう. この巡回置換を記号として $(i_1, \cdots, i_r)$ で表す. $r = 2$ の巡回置換のことを特に互換とよぶ.*

命題 6.16.
1. *一般に $(i_1, \cdots, i_q, \cdots, i_r) = (i_1, \cdots, i_q) \circ (i_q, \cdots, i_r)$ が成り立つ.*
2. *特に S_n に含まれる勝手な長さ $r \leq n$ の勝手な巡回置換 $(i_1, \cdots i_r)$ は互換の積で表される. 例えば, $(i_1, \cdots i_r) = (i_1, i_r) \circ (i_1, i_{r-1}) \circ \cdots \circ (i_1, i_3) \circ (i_1, i_2)$ である.*
3. *$\{i_1, \cdots i_q\}$, $\{i_r, \cdots i_s\}$ がともに $\{1, \cdots, n\}$ の部分集合で, $\{i_1, \cdots i_q\} \cap \{i_r, \cdots i_s\} = \emptyset$ とするとき, $(i_1, \cdots, i_q) \circ (i_r, \cdots, i_s) = (i_r, \cdots, i_s) \circ (i_1, \cdots, i_q)$ が成り立つ.*
4. *S_n の勝手な元は $r \leq n$ の勝手な巡回置換 $(i_1, \cdots i_r)$ のいくつかの積で表される.*

命題 6.17. *S_n は次のような表示をもつ:*

$$\left\langle \sigma_i (i = 1, \cdots, n-1) \;\middle|\; \sigma_i^2 = \mathbf{1}, [\sigma_i, \sigma_j] = \mathbf{1} (i < j, j - i \geq 2), (\sigma_i \sigma_{i+1})^3 = \mathbf{1} \right\rangle$$

Proof. 上の表示で定義される群を G_n とする. $G_n \longrightarrow S_n$ を $\sigma_i \mapsto (i, i+1)$ で定めることにより全射群準同型になる. $\sharp S_n = n!$ より $\sharp G_n \leq n!$ を言えば証明が終わる. 帰納法によって証明をしていけばよいがこのことの証明は省略する. □

定義 6.18. $g \in S_n$ を考える. このとき,

$$g = (i_1, \cdots, i_{r_1})(i_{r_1+1}, \cdots, i_{r_1+r_2}) \cdots (i_{r_+r_2+\cdots r_{l-1}}, \cdots, i_n)$$

という形に書ける. ここで $i_j \in \{1, \cdots, n\}$ が g で動かないとき, (i_j) で恒等写像をあらわすことにする. $(i_1, \cdots, i_{r_1}), (i_{r_1+1}, \cdots, i_{r_1+r_2}), \cdots, (i_{r_1+r_2+\cdots r_{l-1}}, \cdots, i_n)$ はすべて可換より $r_1 \geq r_2 \geq \cdots \geq r_{l-1} \geq r_l$ $(r_l = n - (r_1 + \cdots + r_{l-1}))$ と仮定してよい.

1. $r_1 \geq r_2 \geq \cdots \geq r_{l-1} \geq r_l \geq 1$
2. $r_1 + \cdots + r_{l-1} + r_l = n$

を満たす組 $(r_1, r_2, \cdots, r_{l-1}, r_l)$ のことを g の巡回型 (cycle type) とよぶ.

命題 6.19. 1. 上の定義で現れた 2 条件を満たす自然数の組 $(r_1, r_2, \cdots r_l)$ に対して, この組を巡回置換型にもつ $g \in S_n$ が存在する.
2. $g, g' \in S_n$ が共役であるための必要十分条件はその巡回型が等しいことである.

Proof. 最初の記述はよい. 2 番目の記述については g, g' が共役つまり $g' = \sigma g \sigma^{-1}$ なる $\sigma \in S_n$ が存在するとき,

$$g = (i_1, \cdots, i_{r_1})(i_{r_1+1}, \cdots, i_{r_1+r_2}) \cdots (i_{r_+r_2+\cdots r_{l-1}}, \cdots, i_n)$$

ならば

$$g' = (i'_1, \cdots, i'_{r_1})(i'_{r_1+1}, \cdots, i'_{r_1+r_2}) \cdots (i'_{r_+r_2+\cdots r_{l-1}}, \cdots, i'_n)$$

とかける (但し, $i'_j = \sigma(i_j)$ とする). □

例 6.20. S_3 を考える. 巡回置換型の可能性は $(1,1,1), (2,1), (3)$ の通りである. $(1,1,1)$ を持つ元は単位元 $\mathbf{1}$ のみ, $(2,1)$ を持つ元は $(1,2), (2,3), (3,1)$ のつ, (3) をもつ元は巡回置換 $(1,2,3)$ と $(1,2,3)^2 = (1,2,3)^{-1}$ の 2 つである. G を共役作用で剰余類分解すると $6 = 1 + 3 + 2$ という足し算が現れる. 次節でやる類等式の一例のなっている.

補題 6.21. g を幾つかの互換の積に表したときに現れる互換の個数の偶奇はあらわし方によらず一定である.

定義 6.22. 1. 偶数個の互換の積で表される置換 $\sigma \in S_n$ を偶置換, 奇数個の互換の積で表される置換 $\sigma \in S_n$ を奇置換とよぶ.
2. $\sigma \in S_n$ が r 個の置換で表されているとき $\mathrm{sgn}(\sigma) = (-1)^r$ を σ の符号とよぶ.
3. 交代群 A_n を

$$A_n = \{g \in S_n \mid g \text{ は偶置換 }\}$$

で定まる部分群とする.

補題 6.23. A_n は S_n の指数 2 の部分群であり次の準同型

$$\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$$

の核と一致する. また, S_n の指数 2 の部分群は A_n のみである.

7. 有限群と Sylow の定理

有限群 G の構造を調べるひとつの手がかりとなる Sylow の定理について論じたい. そのためのキーとなる手法が類等式である. 類等式は

1. 有限群 G にある部分群があることを保証する存在定理 (シローの定理など)
2. 有限群 G にある部分群がないことを示す非存在定理 (ある群 G 単純であることなど)

という両方の面で有限群の内部構造を調べることに役立つ. 少しずつ準備をしていきたい.

定義 7.1. G を勝手な群とする. $x \in G$ に対して $\{g \in G \mid gx = xg\}$ は群をなす. これを x の中心化群とよび $\mathrm{Cent}(x)$ で記す.

補題 7.2. 1. どの二つも互いに共役でないような元たち $\{x_\lambda\}_{\lambda\in\Lambda} \subset G$ が存在して $G = \coprod_{\lambda\in\Lambda} C_{x_\lambda}$ となる. 但し, $C_x = \{gxg^{-1} \mid g \in G\} \subset G$ とする.
2. $\sharp C_x = 1$ であることと $x \in Z(G)$ であることは同値である.
3. 勝手な $x \in G$ に対して $\sharp C_x = \sharp G/\sharp \mathrm{Cent}(x)$ である.

Proof. 最初の記述は群の作用による軌道分解そのものである (群 G が $X = G$ 自分自身に作用している). 2 番目の記述もほぼ定義に他ならない. さて剰余類分解のときにやったように剰余類分解 $G = \coprod_{\lambda\in\Lambda} C_{x_\lambda}$ の各成分 C_{x_λ} は G が推移的に作用する集合である. よって固定化群 $G_{x_\lambda} = \{g \in G \mid g \cdot x_\lambda = x_\lambda\}$ によって G-作用をもつ集合としての同型 $C_{x_\lambda} \cong G_{x_\lambda} \setminus G$ がある. さて, 以上の以前に準備した一般論をこの場合に適用するにあたり今考えている作用が共役作用 $g \cdot x = gxg^{-1}$ であったことに注意したい. この場合 $G_x = \mathrm{Cent}(x)$ に他ならないので証明が終わる. □

定義 7.3. G が有限群のとき等式が成り立つ.

$$\sharp G = \sharp Z(G) + \sum_{[x]\in G/\sim, x\notin Z(G)} \sharp C_x$$

但し, $G/\sim$ は共役作用による同値類を表す. この式を群 G の類等式とよぶ.

例 7.4. 1. $\mathrm{Cent}(S_3) = \{1\}$ である. また類等式は,

$$\begin{aligned}\sharp G &= \sharp Z(G) + \sharp C_{(1,2)} + \sharp C_{(1,2,3)} \\ &= 1 + 3 + 2\end{aligned}$$

である.

2. 例として n 次 2 面体群 D_n を考える. $D_n = \langle \sigma, \tau | \sigma^2 = \mathbf{1}, \tau^n = \mathbf{1}\rangle$, $\sharp D_n = 2n$ であることを思い出そう. n が偶数ならば $\sharp Z(D_n) = \{\mathbf{1}, \tau^{n/2}\}$, n が奇数ならば $Z(D_n) = \{1\}$ である. 例えば, n が奇数ならば, $C_{\tau^i} = \{\tau^i, \tau^{-i}\}$ $(i = 1, \cdots, (n-1)/2)$, $C_\sigma = \{\sigma, \sigma\tau, \cdots, \sigma\tau^{n-1}\}$ であるから類等式は,

$$\begin{aligned}\sharp D_n &= \sharp Z(G) + \sum_{1\le i\le (n-1)/2} \sharp C_{\tau^i} + \sharp C_\sigma \\ &= 1 + 2 \times \frac{n-1}{2} + n\end{aligned}$$

である.

定理 7.5 (Cauchy)**.** 素数 p が有限群 G の位数を割るとき必ず位数 p の元が存在する (つまり位数 p の部分群が存在する).

注意 7.6. 証明する前にひとつだけこの定理の意味について注意したい. 上の素数 p の代わりに勝手な $\sharp G$ の約数 n をとったときには位数の部分群は存在するとは限らない. 例えば, A_4 は位数 12 の群であり

$$A_4 = \{\mathbf{1}, (12)(34), (13)(24), (14)(23), \\ (123), (123)^2, (234), (234)^2, (341), (341)^2, (412), (412)^2\}$$

という形の元からなる. A_4 が位数 6 の部分群をもつか考える. 位数 6 の群は巡回群 C_6 か対称群 S_3 である. 位数 6 の元は A_4 の中には存在しないので C_6 が部分群になることはない. A_4 の上の元から位数 $2, 3$ の元 $\sigma, \tau \in A_4$ を選ぶと σ, τ の積によって他も全ても元があらわされてしまうので, S_3 が A_4 の部分群と同型になることもありえないことがわかる.

Proof. $\sharp G$ に関する帰納法で証明する. $\sharp G$ が素数のときにはは巡回群であるから明らかに定理は正しい. 特に, $\sharp G = 2$ のとき定理は正しいので帰納法の出発点は正しい. 帰納法の仮定の下で, 一般の場合に示したい.

ここで, 類等式を用いる.

$$\sharp G = \sharp Z(G) + \sum_{[x_i] \in G/\sim, x_i \notin Z(G)} \sharp C_{x_i}$$

とする. さて各 x において $\sharp C_{x_i} = \sharp G / \sharp \mathrm{Cent}(x_i)$ に注意したい. 今, ある i において中心化群 $\mathrm{Cent}(x_i) \subset G$ が G 全体になったとする. 中心化群の定義から G はアーベル群である (このとき全ての i で $\mathrm{Cent}(x_i) = G$ である). 有限アーベル群の構造定理からこの場合は定理は正しい. 従って以下では全ての i で $\mathrm{Cent}(x_i) \subsetneq G$ とする. また, $p | \sharp Z(G)$ ならば有限アーベル群の構造定理によって $Z(G)$ は位数 p の部分群をもつ. 以下では, $Z(G)$ の位数は p で割れないと仮定する.

今仮に上の類等式における全ての $x_i \neq \mathbf{1}_G$ において素数 $p \nmid \sharp \mathrm{Cent}(x_i)$ とする. 補題 7.2 より上の類等式における全ての x_i に対して $p | \sharp C_{x_i}$ である. よって $p | (\sharp G - \sharp Z(G))$ でなければならない. これは $p | \sharp G$ に矛盾する. したがって, 上の類等式におけるある $x_i \neq 1_G$ において素数 p が $\sharp \mathrm{Cent}(x_i)$ を割り切らねばならない. $\sharp \mathrm{Cent}(x_i) < \sharp G$ であるから群の位数に関する帰納法によって $\mathrm{Cent}(x_i)$ には位数 p の元が存在する. $\mathrm{Cent}(x_i)$ はの部分群より G にも位数 p の元が存在する. 証明を終える. □

同様の方法によって次の存在定理も示されるがここでは証明を省略して結果をみとめて先へすすむことにする.

命題 7.7. $\sharp G$ を割りきる任意の素数ベキ p^s に対して必ず $\sharp H = p^s$ の G の部分群が存在する.

定義 7.8. G を有限群とする. p は $\sharp G$ を割る素数として $\sharp G = p^r m$ $(m, p) = 1$ とする. このとき, $\sharp H = p^r$ なる部分群 $H \subset G$ をの p-Sylow 部分群とよぶ.

定理 7.9 (Sylow の定理)**.** G を有限群とする．p は $\sharp G$ を割る素数とする．このとき次が成り立つ．

1. p-*Sylow* 部分群は必ず存在する．
2. G を有限群とする．G の-*Sylow* 部分群の個数を t とすると $t \equiv 1 \ (mod\ p)$ である．
3. G の p-*Sylow* 部分群たちは互いに共役である．
4. $\sharp G = p^r m$ $(m, p) = 1$ とするとき G の-*Sylow* 部分群の個数は m の約数である．特に, G の-*Sylow* 部分群の個数は $\sharp G$ の約数である．

Proof. 最初の記述は時間の都合と証明の基本が先の Cauchy の定理と同じであることから認めることにする．

2 番目の記述を証明する．

$$S_p = \{H_1, H_2, \cdots, H_t\}$$

を G の p-Sylow 部分群全体のなす集合とする．勝手な元 $g \in G$ と $H_i \in S_p$ に対して共役 gH_ig^{-1} はまた部分群であり $\sharp(gH_ig^{-1}) = \sharp H_i$ なので gH_ig^{-1} もまた S_p に入る．よって G 及び勝手な部分群 $H \subset G$ が有限集合 S_p に共役作用する．H_1 を S_p に作用させるとき, $h \in H_1$ に対して $hH_1h^{-1} = H_1$ より, $H_1 \in S_p$ を含む軌道は H_1 だけからなる．

Claim 7.10. $i \neq 1$ に対して H_1 の共役作用による $H_i \in S_p$ の軌道は位数が p ベキである．

仮にある $i \neq 1$ H_i を含む軌道が H_i 自身だけであったとする．このとき, $H_1H_i = H_iH_1$ であるから集合 H_1H_i は G の部分群となる．

$$\sharp(H_1H_i) = \sharp H_1 \cdot \sharp H_i / \sharp(H_1 \cap H_i)$$

は p ベキであり, 同時に $\sharp H_1 < \sharp(H_1H_i)$ である．これは H_1 が p-Sylow 部分群であることに反する．よって H_1 は $H_i \in S_p$ $(i \neq 1)$ に非自明に共役作用する．

$$\sharp C_x = \frac{\sharp H}{\sharp H_x} \text{ (有限群 } H \text{ が有限集合 } X \text{ に作用, } x \in X)$$

という一般論により $H_i \in S_p$ $(i \neq 1)$ の軌道に含まれる元の数は p ベキとなる．

S_p を H_1 の作用で軌道分解すると H_1 はそれ自身からなる軌道をもち, 他の軌道はすべて p ベキ個の元をもつ軌道である．よって $t \equiv 1 \pmod p$ が得られる．これで 2 番目の記述が得られた．

3 番目の記述を示す．背理法で示すこととして, 全ての p-Sylow 部分群が互いに共役とはならないとする．違う言い方をするとこれは G の S_p への共役作用が推移的ではないということに他ならない．必要ならば順番を並べ替えて

$$S_p = S \cup S', \quad S = \{H_1, \cdots, H_s\} \text{ かつ } S' = \{H_{s+1}, \cdots H_t\}$$

で $H_1, \cdots, H_s$ は互いに共役で, S の元と S' の元は全て互いに共役でないとする．H_1 を S に作用させて軌道分解すると, $\sharp S = s \equiv 1 \bmod p$ が得られる．一方で, H_{s+1} を S に作用させて軌道分解すると $\sharp S = s \equiv 0 \bmod p$ が得られ二つの結論は矛盾する．よって, 3 番目の記述が示された．

4 番目の記述の証明は, 3 番目で示された G の S_p への共役作用が推移的であることを用いる．例えば G_1 を $H_1 \in S_p$ の固定化群とすると S_p は G-作用を

もつ集合として G/G_1 と同型である. 今, $G_1 \supset H_1$ より $\sharp S_p = \sharp(G/G_1)|m$ が得られ, 証明が終わる. □

8. 可解群と巾零群

群 G はアーベル群に近い方がいろいろと取り扱いやすい面が多い. アーベル群に近い群のクラスとして可解群や巾零群を導入しておく.

命題 8.1. 群 G に対して次の二つの条件は同値である:

1. G の交換子群 $D(G) = [G, G]$ に対して, ある n で $D^n(G) = \{1\}$ となる (但し, $D^1(G) = D(G) = [G, G]$, $D^{i+1}(G) = D(D^i(G))$).
2. 正規部分群の列 $G_0 := G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{1\}$ があって各剰余群 G_i/G_{i+1} $(i = 0, \cdots, n-1)$ はアーベル群

Proof. $1 \Rightarrow 2$ は $G_i = D^i(G)$ とおくことで明らかである. $2 \Rightarrow 1$ を示す. G/G_1 がアーベル群であるから $G_1 \supset D(G)$ が成り立つ. 今, $G_i \supset D^i(G)$ が成り立っているとする. 包含関係から $D(G_i) \supset D^{i+1}(G)$ が成り立ちまた, G_i/G_{i+1} がアーベル群より $G_{i+1} \supset D(G_i)$ が成り立つ. よってすべての i で $G_{i+1} \supset D^{i+1}(G)$ が成り立つ. よって $D^n(G) \subset G_n = \{1\}$ となり 1 が導かれる. □

定義 8.2. G を群とする. このとき, 上の命題で考察された同値な条件が成り立てば G は可解群とよぶ.

注意 8.3. 1. G が非可換な単純群だとすると G は可解ではない.
2. $G = A_4$ は可解群. 実際,

$$G = G_0 \triangleright G_1 = \{\mathbf{1}, (12)(34), (13)(24), (14)(23)\} \triangleright G_2 = \{1\}$$

という正規部分群の列があり, $G_0/G_1 \cong_3$, $G_1 \cong C_2 \times C_2$ である.

可解群よりさらにアーベル群に近い群として次に説明する巾零群がある.

命題 8.4. 群 G に対して, $\Gamma_0(G) = G$, $\Gamma(G) = \Gamma^1(G) = [G, G]$, $\Gamma^{i+1}(G) = [G, \Gamma^i(G)]$ とする. 次の二つの条件は同値である:

1. ある n で $\Gamma^n(G) = \{1\}$ となる.
2. 正規部分群の列 $G_0 := G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{1\}$ があって各剰余群 G_i/G_{i+1} が G/G_{i+1} の中心に含まれる.

Proof. $1 \Rightarrow 2$ は $G_i = \Gamma^i(G)$ とおくことで明らかである. $2 \Rightarrow 1$ を示す. 先と同様に帰納法で $G_i \supset D^i(G)$ を示せば $\Gamma^n(G) \subset G_n = \{1\}$ となり 1 が導かれる. $G_i \supset \Gamma^i(G)$ を認めたとき, 包含関係から $\Gamma(G_i) \supset \Gamma^{i+1}(G)$ が成り立ちまた, G_i/G_{i+1} が G/G_{i+1} の中心に含まれるから $G_{i+1} \supset \Gamma(G_i)$ が成り立つ. よってすべての i で $G_{i+1} \supset \Gamma^{i+1}(G)$ が成り立つ. □

注意 8.5. 1. G がアーベル群ならば G は巾零群である. G が巾零群ならば G は可解群である.
2. $G = A_4$ は可解群であるが巾零群ではない. 実際, $G_0 = A_4$ の非自明でない正規部分群は $G_1 = \{\mathbf{1}, (12)(34), (13)(24), (14)(23)\}$ のみであるが, G_1 は G_0 の中心ではない.

3. p を素数とする. G は有限群で $\sharp G$ は p の巾であるとする. このとき G は巾零群である.
4. $G \subset GL_2(\mathbb{C})$ を

$$G = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \pm \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \right\}$$

で定めたとき $\sharp G = 8 = 2^3$ であり, 非可換な巾零群の例を与える.