目次

群の楽しみ方

池田 岳

1　対称性を記述する代数系

「何か」(図形，方程式，行列，関数，数列，…) が対称性を持つとはどういうことでしょうか？「何か」に対して，ある操作（例えばそれを a という記号であらわすことにして）を施した結果が「もとと同じ」であるとき，その「何か」は対称性 a を持つといいます．

対称性を持つ平面図形として正 n 角形を考えてみましょう．その重心を中心として，反時計回りに角度 $2\pi/n$ の回転をする操作を a とします．a を k 回続けて行う操作を a^k と表わすのは自然ですね．もちろん，これは角度 $2\pi k/n$ の回転です．$k = n$ ならばちょうど一回転ですから，操作としては何もしないことと同じです．何もしないのも操作のうちと考えてそれを e と表わすことにすると，$a^n = e$ というわけです．回転の他に，n 本の線対称軸に関する折り返しの操作があります．そのうちのひとつをどれでもいいからひとつ選んでそれを b で表わしましょう．b^2（b を 2 回続けること）は何もしないことと同じなので $b^2 = e$ ですね．

操作の合成：一般に，何かふたつの操作 a, b があるとしましょう．操作 b を行った後に続けて操作 a を行うことを考えます．これをひとまとめにしてひとつの操作と考えて ab と表わして，これを合成といいます一般には ab と ba は異なるものになることに注意してください．

逆操作：ある操作 a の逆の操作ができるとき，それを a^{-1} で表わします．このとき

$$aa^{-1} = a^{-1}a = e$$

が成り立ちます．むしろこれが「逆」の意味です．

さて，正 n 角形の例にもどって，二つの基本的な操作 a（回転）と b（折り返し）を繰り返し合成することを考えます．すると，次のような $2n$ 個の操作が得られます：

$$e,\ a,\ a^2,\ \ldots,\ a^{n-1}, b,\ ab,\ a^2b,\ \ldots,\ a^{n-1}b.$$

実は，これらを更に合成しても，以上の $2n$ 個以外のものはもう現れないことがわかるのです．例えば ba は上記のリストのうちのどれかと一致するのですが，どれだかわかりますか？答えは

$$ba = a^{n-1}b$$

です．この関係式はとても基本的ですから丁寧に説明しましょう．まず，確認しておきたいことがあります．a^{n-1} は a と逆向きに $2\pi/n$ の回転することと同じなので $a^{n-1} = a^{-1}$ であるということです．だから，上の式を

$$ba = a^{-1}b$$

と書くことができます．このほうが意味がわかりやすいですね．回転してから折り返すことは，折り返してから逆回転することと同じですから．

話を具体的，かつ簡単にするために $n = 3$ としましょう．いま示した基本的な関係式は $ba = a^2b$ です．これを使うといろいろな合成を計算できます．たとえば $(ab)^2$ はどうなるか？

例えば次のような計算ができます：

$$(ab)^2 = abab = a(ba)b = a(a^2b)b = a^3b^2 = ee = e$$

二つめの等号で $ba = a^2b$ を使いました．２つよりも多い操作を合成する際に，文字の順序を変えない限り括弧の位置を自由に変えてかまいません．例えば

$$((xy)z)w = x((yz)w)$$

という風にです．このことは後でもう一度詳しく考えるので，いまは括弧を自由に移動してよいと気楽に考えてください．

すべての合成を表にまとめると次のようになります：

左 \ 右	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

すこし面倒なのは下の３行だけで，他の部分はほとんど計算が不要ですね．各行，各列には６個の元 e, a, a^2, b, ab, a^2b がそれぞれ一度ずつ現れていることにも注目してください．このように，２つものどうしの合成（積）の規則が与えられると，それを繰り返してもっと沢山の文字の合成も計算できます．

対称性について考えてゆくと，いくつかのモノの集まり（集合）に合成の規則が定まった構造（代数系）が現れます．それを群と呼ぶのです．

2　群の定義

対称性を持つ「何か」があったとき，対称性の操作の集まりと，それらの合成の規則を**抽象化**することによって，そこに「群」という代数系が現れます．「何か」の詳細や，操作の実際的な意味を離れて，合成の規則（つまり演算）のみに注目してゆこうという発想です．

定義 1 集合 G に演算 $G \times G \to G,\ (a, b) \mapsto ab$ が与えられているとする．以下の条件が成り立つとき，G は群であるという：

(1) すべての $a, b, c \in G$ に対して $(ab)c = a(bc)$ が成り立つ．
(2) ある元 $e \in G$ があって，すべての $a \in G$ に対して $ae = ea = a$ が成り立つ．
(3) すべての $a \in G$ に対して，ある元 b があって $ab = ba = e$ が成り立つ．

- (1) の性質を結合律という．
- (2) における e を単位元という．
- 元 a に対し $ab = ba = e$ をみたす元 b を a の逆元という．

命題 1 (単位元の一意性) G を群とし e を単位元とする．ある元 $e' \in G$ があって，すべての $a \in G$ に対して $ae' = e'a = a$ が成り立つならば $e' = e$ である．

(証明) e は単位元なので $e' = ee'$ である．e' に対する条件において $a = e$ としてみれば $ee' = e$ である．したがって $e' = e$ である．□

命題 2 (逆元の一意性) G を群とする．$a \in G$ として b が a の逆元であるとする．もしも，ある元 $c \in G$ があって，$ac = ca = e$ が成り立つならば $c = b$ である．

(証明) e が単位元であることと e を $e = ab$ と書けることをあわせて $c = ce = c(ab)$ を得る．ここで結合律を使って $c(ab) = (ca)b$ と書き換えて，更に $ca = e$ を使うと，結局 $c = (ca)b = eb = b$ となる．□

元 a の逆元はただひとつしか無いことがわかったのでそれを a^{-1} と書きます．

3　２面体群

前節で正 n 角形の対称性から抽出した構造は 2 面体群と呼ばれる群です．それを D_n で表わします．集合としては

$$D_n = \{e,\ a,\ \ldots,\ a^{n-1}, b,\ ab,\ \ldots,\ a^{n-1}b\}$$

です．演算の規則は

$$a^n = e, \quad b^2 = e, \quad ba = a^{-1}b$$

が基本的で，一般の積はこれらを用いて計算できることを $n = 3$ の場合に体験してもらいました．正 n 角形の対称性から出発して見いだした群なのですが，回転や折り返しなどの意味を離れても，抽象的な群としてはきちんとした意味を持っていることを理解して欲しいと思います．

ここで n の範囲について考えておきましょう．「正 1 角形」や「正 2 角形」というものは普通は考えないわけですが

$$D_1 = \{e, b\}, \quad D_2 = \{e, a, b, ab\}$$

は立派な群として意味があります．演算の表を書いてみます：

D_1 :

	e	b
e	e	b
b	b	e

D_2 :

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

それぞれ，次のような平面図形の対称性を記述していると考えるのが自然です．

D_1 の b は折り返しで，回転はありません（強いて言えば 360° 回転がありますが，それはつまり e です）．D_2 の a は 180° 回転です．b と ab はどちらも折り返しでそれらの対称軸は垂直になっています．

4 巡回群

次のような平面図形は，回転対称性を持ちますが，折り返しの対称性がありませんね．

D_n の部分集合

$$C_n = \{e,\ a,\ a^2,\ \ldots,\ a^{n-1}\}$$

は D_n から回転対称性の部分だけを取り出したものです．C_4 の演算を表に表わすと

C_4 :

	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

となります．このように，とても簡単な構造をした群です．これを巡回群と呼びます．

演算の計算規則は $a^n = e$ だけで

$$a^i \cdot a^j = a^{i+j}$$

とすればよいですね．a^i の肩の上の i は　$\bmod n$ で考えることにすれば，ちょうど具合がいい．肩の数字だけ書けば，

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

というすっきりとした表ができます．

正 n 角形の回転対称性から C_n という群を抽出したわけですが，代数的な構造（つまり計算の規則）は　$\bmod n$ における「和」の計算そのものだということがわかりました．C_n という群そのものは回転という意味合いを忘れても存在しているということを理解して欲しいと思います．

「何か」の対称性を抽象化した代数構造が群であるということを説明してきました．いったん群がつかまると，それはもとの「何か」を離れて一人歩きします．例えば次の平面図形はそれぞれ D_1, C_2 の対称性を持っています．

D_1 と C_2 の演算を書いてみるとわかるように，これらは本質的には同じ群だと考えるのが自然です．$b \in D_1$ は折り返し（線対称）であり $a \in C_2$ は 180° 回転（点対称）であるという解釈でしたから，a と b のもともとの図形的な意味合いは違うのですが，D_1 と C_2 の群としての構造は同じなのです．それが抽象化というものです．

群は集合に演算が備わっただけのもので，とても抽象的なものです．その抽象化を徹底して理論を展開し，それを具体的な「何か」の対称性の理解に応用しようというのが基本的な思想なのです．

5 部分群

G を群とします．G の空でない部分集合 H が G の部分群であるとは以下の 2 つの条件が成り立つことをいいます．

(1) $a, b \in H$ ならば $ab \in H$,
(2) $a \in H$ ならば $a^{-1} \in H$.

(1) により H には演算が定まります．この演算によって H は群となります．

結合律 $a, b, c \in H$ に対して $(ab)c = a(bc)$ が成り立つことは, これがすべての $a, b, c \in G$ に対して成り立つことから明らかです．

単位元の存在 空集合ではないとしたので H には少なくともひとつは元があります．$a \in H$ をそのひとつとすると，(2) により $a^{-1} \in H$ です．さらに (1) を使うと $e = aa^{-1} \in H$ であることがいえます．e は G の単位元ですが，H の単位元となります．$ae = ea = a$ はすべての $a \in G$ に対して成立するのですから，$a \in H$ であるとして，もちろん成立しているわけです．

逆元の存在 (2) により，任意の $a \in H$ の（G の元としての）逆元 a^{-1} は H に属します．$aa^{-1} = a^{-1}a = e$ は成り立ちますから a^{-1} は H の演算に関する逆元でもあります．

6 剰余類

G を群，H をその部分群であるとします．G の部分集合 C は，ある $g \in G$ を用いて $C = gH$ と表わされるとき H を法とする左剰余類であるといいます．ここで

$$gH := \{gh \mid h \in H\}$$

と定めました．$e \in H$ ですから $g \in gH$ であることに注意してください．明らかに $eH = H$ ですから，H もひとつの左剰余類です．

注意：後ほど「右剰余類」も考えるので，それと区別をするために「左剰余類」といいますが，しばらく「右」は出てこないのでサボって単に剰余類ということもあります．

例 1 $G = S_n, H = A_n$ とするします．S_n に含まれる奇置換全体の集合 X_n は，ひとつの奇置換 τ_0 を選んだとき $X_n = \tau_0 A_n$ と表わされますので A_n を法とする左剰余類です．

ここで τ_0 は奇置換でさえあればなんでもかまわず，特に何を選ぶのが自然であるというわけでもないことに注意してください．たとえば $\tau_0 = (12)$ でもよいし，$\tau_0 = (1234)$ (長さ 4 の巡回置換) などでもかまわないのです（もちろんこの場合は $n \geq 4$ としてですが）．

左剰余類 C を $g \in G$ を用いて $C = gH$ と表わしているとき g のことを C の代表であるといいます．

例 2 前の例の続き：任意の奇置換 τ_0 が剰余類 X_n の代表になる資格があります．

命題 3 G を群, H をその部分群とする．次は同値である：(1) $g_1H = g_2H$, (2) $g_2 \in g_1H$, (3) $g_1^{-1}g_2 \in H$, (4) $g_1H \cap g_2H \neq \emptyset$.

（証明）(1) $\Longrightarrow$ (2)：$g_1H = g_2H$ とすると $g_2 \in g_2H$ より $g_2 \in g_1H$ である．

(2) $\Longrightarrow$ (3)：(2) は $g_2 = g_1h$ をみたす $h \in H$ があることを言っている．このとき $g_1^{-1}g_2 = h \in H$ である．

(3) $\Longrightarrow$ (2)：$g_1^{-1}g_2 = h$ とおく．仮定より $h \in H$ である．$g_2 = g_1h$ だから $g_2 \in g_1H$ である．

(3) $\Longrightarrow$ (1)：$g_1^{-1}g_2 \in H$ を仮定して $g_2H \subset g_1H$ を示そう．g_2H の任意の元 g_2h $(h \in H)$ をとる．$g_2 = g_1g_1^{-1}g_2h$ と書く．仮定より $g_1^{-1}g_2 \in H$ であって H が部分群だから $(g_1^{-1}g_2)h \in H$ である．よって $g_2 \in g_1H$ となる．

$g_1^{-1}g_2$ の逆元 $g_2^{-1}g_1$ も H に属すから同様に $g_1H \subset g_2H$ となる．よって $g_1H = g_2H$.

(3) $\Longrightarrow$ (4)：(3) は $g_1^{-1}g_2 = h \in H$ を意味する．$x = g_2 = g_1h$ とおくと $x = g_2 \in g_2H$ であり，一方 $x = g_1h \in g_1H$ である．

(4) $\Longrightarrow$ (3)：$g_1H \cap g_2H \neq \emptyset$ とすると，少なくとも一つ元があるので，ひとつ選んで $x \in g_1H \cap g_2H$ とする．すると $x = g_1h_1 = g_2h_2$ となる $h_1, h_2 \in H$ がある．このとき $g_1^{-1}g_2 = h_1h_2^{-1} \in H$ である．H が部分群であることを使った．□.

命題の意味：C という左剰余類が g_1 という代表を用いて $C = g_1H$ と表わされているとします．C の代表になる資格があるのは g_1 だけとは限りません（$H = \{e\}$ でない限り，代表の選び方は常に複数とおりあります）．つまり $g_2 \neq g_1$ であっても $g_1H = g_2H$ が成立することがあります．そのための条件は (2) あるいは (3) という形で述べられます．更に，それが (4) の条件とも同値だといっています．(1) と (4) の同値性は，$C_1 = g_1H, C_2 = g_2H$ と代表を使わずに書いて，さらに両者を否定形にして

$$C_1 \neq C_2 \Longleftrightarrow C_1 \cap C_2 = \emptyset$$

と書いてみると意味が明瞭になるでしょう．「**異なる剰余類は共通のメンバーを持たない**」

ということを意味しています.

さて，G の任意の元 g は $C = gH$ という剰余類に属しています．だから，各 $g \in G$ に対して，それが属す剰余類「g 君の class」というものが**唯一つだけ確かに定まる**ということです．このことから次がわかります.

命題 4 G を有限群, H をその部分群とする．H を法とする有限個の左剰余類 $C_1, \ldots, C_m$ があって，G はそれらの交わらない和集合として

$$G = C_1 \sqcup C_2 \sqcup \cdots \sqcup C_m$$

と分割される.

（証明）G は有限集合としているので剰余類は有限個しかありません（互いに交わらない部分集合が無限個あれば無限集合になってしまうから）．なおかつ，任意の元 $g \in G$ が必ずある剰余類に属する（上の注意）のだから命題は明らかです．□.

命題 5 G を有限群，H をその部分群とする．C を H を法とする剰余類とすると

$$\#C = \#H$$

が成り立つ.

（証明）任意の剰余類 $C = gH$ と H との間に全単射を作ればよいですね．$\phi : H \to gH$ を $f(x) = gx$ $(x \in H)$ と定めましょう．（偶置換の集合から奇置換の集合への全単射を作るやり方を思い出してください）逆に $\psi : gH \to H$ を $\psi(x) = g^{-1}x$ $(x \in H)$ と定めるとき

$$\psi \circ \phi = \mathrm{id}_H, \quad \phi \circ \psi = \mathrm{id}_{gH},$$

が成り立ちます．したがって ϕ は全単射であって，ψ はその逆写像です．よって $\#C = \#H$ が成り立ちます．□.

系 1 (Lagrange) G を有限群，H をその部分群とする．$\#H$ は $\#G$ の約数である.

（証明）命題 4 より $\#G = \sum_{i=1}^{m} \#C_i$ ですが，命題 5 より $\#C_i = \#H$ なので $\#G = m \times \#H$ を得ます．□.

7 問題

難しいものも（さりげなく）あります．簡単にできなくてもあきらめないでください．挑戦している時間が楽しいと感じられれば，そのときあなたは「数学をやっている」のです．問題が解けて満足しているだけでは甘い甘い．挑戦し続けるのです！

1. (5/12：剰余類) 次の群 G とその部分群 H について G を剰余類に分割せよ．

(0) 例題：$G = S_3,\ H = \{e, (12)\}$: 剰余類は $\#G/\#H = 3!/2 = 3$ 個ある．ひとつめは H なので，H に属さない元として例えば (13) を代表とする剰余類を計算すると $(13)H = \{(13), (123)\}$ となる．H にも $(13)H$ にも含まれない元がある．例えば (23) を代表とする剰余類 $(23)H = \{(23), (132)\}$ を求めれば G の元がすべて出尽くしたからこれでおしまい．$G = H \sqcup (13)H \sqcup (23)H$ と分割された．注意：$(13)H = (123)H$ など，代表の選び方は一通りではない．

(1)：$G = S_3,\ H = \{e, (13)\}$, (2)：$G = S_3,\ H = \{e, (123), (132)\}$, (3)：$G = D_2 = \{e, a, b, ab\}$ $(a^2 = b^2 = e,\ ab = ba)$, $H = \{e, ab\}$, (4)：$G = C_6,\ H = \{e, a^3\}$ $(a^6 = e)$, (5)：$G = C_6,\ H = \{e, a^2, a^4\}$ $(a^6 = e)$, (6)：$G = D_5,\ H = C_5$, (7)：$G = D_4,\ H = \{e, a^2, a^2b, b\}$ $(a^4 = b^2 = e,\ ba = a^3b)$, (8)：$G = D_4,\ H = \{e, a^2\}$, (9)：$G = A_4,\ H = \{e, (12)(34), (13)(24), (14)(23)\}$.

2. (4/28: 部分群) 部分群であるかどうか答えよ：

(1) $G = S_3,\ H = \{e, (13), (23)\}$, (2) $G = D_3,\ H = \{e, a, b\}$, (3) $G = C_6,\ H = \{e, a^3, a^4\}$, (4) $G = D_4,\ H = \{e, a\}$, (5) $G = D_4,\ H = \{e, ab\}$, (6) $G = D_4,\ H = \{a, a^3b\}$, (7) $G = D_4,\ H = \{a, a^2, a^2b, b\}$.

3 次の群の部分群はいくつあるか答えよ：(1) $G = \{e, (12)(34), (13)(24), (14)(23)\}$, (2) $G = D_2$, (3) $G = D_3$, (4) D_4, (5) C_6, (6) C_7, (7) A_4.

4. n 次巡回群 C_n の部分群は全部でいくつあるか？ヒント：重要なことですが，難しいかも．まずは小さい n で実験してみてください．一般的には演算の数理の知識を使えばきっちりと答えられます．

5. (4/21: 置換の符号) 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$ の符号 $\mathrm{sgn}(\sigma)$ を次の二通りの方法で求めよ：(1) 互換の積として表わす．(2) 差積 $\Delta_4(x)$ に作用させて：$\sigma\Delta_4 = \mathrm{sgn}(\sigma) \cdot \Delta_4$.

6. (4/21: 置換の符号) $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} \in S_n$ とする．(1) 符号 $\mathrm{sgn}(\sigma)$ を求めよ．(2) σ をあみだくじとして実現せよ．何本の棒を使えばできるか？

7. (4/21: 行列式の交代性) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, \boldsymbol{b} \in \mathbb{R}^n$ とし，未知数 $x_1, \ldots, x_n$ に対する方程式 $x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n = \boldsymbol{b}$ を考える．$|\boldsymbol{a}_1, \ldots, \overset{i\text{列}}{\boldsymbol{b}}, \ldots, \boldsymbol{a}_n| = x_i|\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n|$ を示せ．$|\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n| \neq 0$ ならば

$$x_i = \frac{|\boldsymbol{a}_1, \ldots, \overset{i\text{列}}{\boldsymbol{b}}, \ldots, \boldsymbol{a}_n|}{|\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n|}$$

が成り立つことを示せ（クラメルの公式）．

8. (4/7：対称性, 4/28：部分群) $G = S_3, H = \{e, (12)\}$ とします．次の図 (ア) は G の対称性を持っています．図 (イ) の対称性は (ア) よりも小さくて，部分群 H によって対称性が記述されます．もうひとつの例として $G = D_4,\ H = \{e, b, a^2, a^2b\}$ を挙げておきます．

上の例にならって，以下の群の組 (G, H) の対称性を持つ平面図形の組 (ア) ,(イ) の例を与えよ．(1) $G = S_3,\ H = \{e, (13)\}$, (2) $G = D_3,\ H = C_3$, (3) $G = C_6,\ H = \{e, a^2, a^3\}$, (4) $G = D_4,\ H = \{e, a\}$, (5) $G = D_4,\ H = \{e, ab\}$, (6) $G = D_4,\ H = \{a, a^3b\}$.

9：任意の $g \in G$ に対して $gG = G$ が成り立つことを示せ.

解答例：$gG \subset G$ は明らかなので $G \subset gG$ を示す．$x \in G$ を任意の元とするとき $x = gg^{-1}x$ と書く．$g^{-1}x \in G$ なので $x \in gG$ である.

10 G を群とし $a, b \in G$ とする.

(1) $(a^{-1})^{-1} = a$ を示せ．(2) $(ab)^{-1} = b^{-1}a^{-1}$ を示せ．（ヒント：逆元の一意性）

11 次の集合とその演算の組について，それが群であるかどうか答えよ：

(1) $\mathbb{Z}$, (整数全体の集合) 演算 $(x, y) \mapsto x + y$, (1) $2\mathbb{Z}$, (偶数全体の集合) 演算 $(x, y) \mapsto x + y$, (2) $\mathbb{Z}$, 演算 $(x, y) \mapsto xy$, (4) $\mathbb{Q}$ (有理数全体の集合), 演算 $(x, y) \mapsto xy$, (5) $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ (0 以外の有理数全体の集合), 演算 $(x, y) \mapsto xy$, (3) $\mathbb{N} = \{1, 2, \ldots\}$ (自然数全体の集合), 演算 $(x, y) \mapsto x + y$, (3) $\mathbb{R}^n$, 演算 $(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{u} + \boldsymbol{v}$,

12. 実係数 n 次の正方行列であって逆行列を持つもの全体の集合を $GL_n(\mathbb{R})$ で表し, 演算 $(A, B) = AB$ (行列の積) により群と見なしたものを一般線型群と呼ぶ．次の部分集合が部分群をなすことを示せ.

(1) $SL_n(\mathbb{R}) := \{g \in GL_n(\mathbb{R}) \mid \det(g) = 1\}$, (特殊線型群 : special linear group) (2) $O_n(\mathbb{R}) := \{g \in GL_n(\mathbb{R}) \mid {}^t gg = g{}^t g = E\}$ ただし ${}^t g$ は g の転置，E は単位行列 (直交群: orthogonal group) (3) $GL_n(\mathbb{Z}) := \{g \in GL_n(\mathbb{R}) \mid \det(g) = \pm 1\}$, (4) $T_n := \{g \in GL_n(\mathbb{R}) \mid g_{ij} = 0\ (i > j)\}$ （上三角型の行列).

13. 立方体（正 6 面体）の回転対称性はいくつあるか？

14. $\boldsymbol{e}_i \in \mathbb{R}^n$ を i 行成分のみが 1 でそれ以外がゼロであるベクトルとする．次の行列式の値を求めよ：

(1) $|\boldsymbol{e}_6, \boldsymbol{e}_3, \boldsymbol{e}_4, \boldsymbol{e}_5, \boldsymbol{e}_1, \boldsymbol{e}_2|$, (2) $\begin{vmatrix} 0 & 0 & 0 & 0 & e & 0 \\ 0 & 0 & 0 & 0 & 0 & f \\ 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 \\ a & 0 & 0 & 0 & 0 & 0 \end{vmatrix}$.

15. n 文字の「括弧の付け方」の個数を C_n と表わす．Catalan 数と呼ぶ.

例えば $a((bc)d), a(b(cd)), (ab)(cd), (a(bc))d, ((ab)c)d$ だから $C_4 = 5$ である．他に $C_2 = 1, C_3 = 2, C_4 = 5, C_5 = 14$ など．$C_1 = 1$ と約束するとき，漸化式

$$C_{n+1} = \sum_{i=1}^{n-1} C_i C_{n-i}$$

が成り立つことを示せ．ヒント：「最後のかけ算」の位置に注目せよ.

16. $f : X \to Y$, $g : Y \to X$ を写像とする．次を示せ：

(1) $f \circ g = \mathrm{id}_Y$ ならば f は全射, (2) $g \circ f = \mathrm{id}_X$ ならば f は単射

ただし $\mathrm{id}_X : X \to X$ は恒等写像．つまり $\mathrm{id}_X(x) = x\ (x \in X)$ とする.

参考書：代数入門 — 群と加群 —（掘田良之著）裳華房

8　準同型写像と準同型定理

G, G' を群とします．G から G' への写像 f が準同型写像であるとは

$$f(gh) = f(g)f(h) \quad (\text{すべての } g, h \in G \text{ に対して})$$

が成り立つことをいいます．

例 3 群 G の部分群 H に対して $f : H \to G$ を包含写像とすれば準同型写像です．包含写像とは $h \in H \subset G$ を単に G の元とみなすという写像です．

例 4 群 G から，単位元だけからなる群 $\{e\}$ への写像 $f : G \to \{e\}$ $(f(g) = e)$ は準同型写像です．

例 5 置換 $\sigma \in S_n$ に対してその符号 $\mathrm{sgn}(\sigma)$ を与える写像 $\mathrm{sgn} : S_n \to \{\pm 1\}$ は準同型写像です．$\{\pm 1\}$ はかけ算により群とみなします．

命題 6 $f : G \to G'$ を準同型写像とする．

(1) $f(e) = e'$ (e' は G' の単位元)
(2) $f(g^{-1}) = f(g)^{-1}$.

(証明) (1) $f(e) = f(ee) = f(e)f(e)$ なので $f(e)^{-1}$ を両辺に掛ければ（たとえば左から）$e' = f(e)^{-1}f(e) = f(e)^{-1}f(e)f(e) = f(e)$ が得られる．

(2) f は準同型写像なので $f(g^{-1})f(g) = f(g^{-1}g) = f(e) = e'$ （最後に (1) を用いた）．同様に $f(g)f(g^{-1}) = e'$ である．よって，逆元の一意性より $f(g^{-1})$ は $f(g)$ の逆元 $f(g)^{-1}$ と一致する．□

準同型写像 f に対して，その像と核を考えることが大切です：

像　$\mathrm{Im}(f) := \{g' \in G' \mid f(g) = g' \text{ となる } g \in G \text{ がある }\}$
核　$\mathrm{Ker}(f) := \{g \in G \mid f(g) = e'\}$ ($e' \in G$ は G' の単位元)

問い：例 3, 4, 5, 8 の像と核はそれぞれどうなりますか？

次が成り立ちます：

命題 7 $f : G \to G'$ を準同型写像とする．

(1) $\mathrm{Im}(f)$ は G' の部分群である,
(2) $\mathrm{Ker}(f)$ は G の部分群である.

(証明) (1) $g', h' \in \mathrm{Im}(f)$ とし $g' = f(g)$, $h' = f(h)$ である $g, h \in G$ をとる. $g'h' = f(g)f(h)$ は f が準同型写像であることより $f(gh)$ と一致する. これは $g'h' \in \mathrm{Im}(f)$ を意味する. また $(g')^{-1} = (f(g))^{-1} = f(g^{-1})$ (命題 6 (2)) より $(g')^{-1} \in \mathrm{Im}(f)$ である.

(2) $g, h \in \mathrm{Ker}(f)$ とすると $f(g) = f(h) = e'$ である. $f(gh) = f(g)f(h) = e'e' = e'$ なので $gh \in \mathrm{Ker}(f)$ である. また $f(g^{-1}) = f(g)^{-1} = (e')^{-1} = e'$ であるから $g^{-1} \in \mathrm{Ker}(f)$ である. □

以下では, 核を $H = \mathrm{Ker}(f)$ とおきます. これが特別な役割を果たすのです.
さて $g' \in \mathrm{Im}(f)$ とします. 写像 f によって g' にうつされるもの全体がなす集合

$$f^{-1}(g') := \{g \in G \mid f(g) = g'\}$$

は写像 f の $g' \in G'$ におけるファイバー (fiber) と呼ばれます.

定義から, G' の単位元 e' のファイバー $f^{-1}(e')$ は核 $\mathrm{Ker}(f)$ に他なりません. 次の補題によると, $\mathrm{Im}(f)$ の元 $f(g)$ における f のファイバーは, 核 $\mathrm{Ker}(f)$ を法とする剰余類になっています.

補題 1 (準同型写像のファイバー) 任意の $g \in G$ に対して $f^{-1}(f(g)) = g \cdot \mathrm{Ker}(f)$.

(証明) ファイバーの定義より $x \in f^{-1}(f(g)) \Longleftrightarrow f(x) = f(g)$ ですが, f が準同型であることから, これは更に $f(g^{-1}x) = e'$ すなわち $g^{-1}x \in \mathrm{Ker}(f)$ とも同値です. §6 の命題 1 によると, この条件は $x \in g \cdot \mathrm{Ker}(f)$ と同値でした. □

剰余集合の定義： G を群, H を G の部分群とするとき

$$G/H := \{C \mid C \text{ は } H \text{ を法とする } G \text{ の左剰余類 }\}$$

とおき G の H による剰余集合と呼びます.

例 6 (1) S_n の部分群 A_n を法とする剰余類は A_n と奇置換全体の集合 X_n ですから $S_n/A_n = \{A_n, X_n\}$.

(2) D_n の部分群 C_n を法とする剰余類は C_n と折り返し対称性全体の集合 $\{b, ab, \ldots, a^{n-1}b\}$ (これを R_n とおく) ですから $D_n/C_n = \{C_n, R_n\}$.

(3) C_6 の部分群 $H = \{e, a^3\}$ を法とする剰余類は H, aH, a^2H ですから $C_6/H = \{H, aH, a^2H\}$.

前の命題により写像

$$\mathrm{Im}(f) \longrightarrow G/\mathrm{Ker}(f)$$

が得られたことになります．$f(g) \in \mathrm{Im}(f)$ に対してそのファイバー $f^{-1}(f(g))$ は $\mathrm{Ker}(f)$ を法とするひとつの剰余類 $g \cdot \mathrm{Ker}(f)$，つまり $G/\mathrm{Ker}(f)$ の元であるからです．

この写像は一般に全単射です．逆写像を与えましょう．$H = \mathrm{Ker}(f)$ を法とする剰余類 C は，定義により，ある $g \in G$ を代表として $C = gH$ と表わされます．この gH **に対して** $f(g) \in \mathrm{Im}(f)$ **を対応させればよい**というのが答えです．

しかし，ここでひとつ確認しておかなければならないことがあります．剰余類の代表が一通りに定まらないということに注意を払わなければならないのです．$g_1H = g_2H$ の場合に $f(g_1) = f(g_2)$ となってくれないと具合が悪いからです．しかし，このことは

$$g_1H = g_2H \Longleftrightarrow g_1^{-1}g_2 \in H$$

という言い換え（§6 の命題 1）に基づいて説明できます．$g_1^{-1}g_2 \in H$ は，核の定義から $f(g_1^{-1}g_2) = e'$ を意味します．f は準同型写像ですから $f(g_1)^{-1}f(g_2) = e'$ となり，これから $f(g_1) = f(g_2)$ が得られます．こうして $gH \in G/\mathrm{Ker}(f)$ に対して $f(g) \in \mathrm{Im}(f)$ を対応させることができます．この写像を $\overline{f}$ と表わしましょう．$\overline{f}$ を f により定まる自然な写像と呼びます．

定理 1 (準同型定理の一歩手前) $f : G \to G'$ を準同型写像とする．f により定まる自然な写像

$$\overline{f} : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f) \quad (g\,\mathrm{Ker}(f) \mapsto f(g))$$

は全単射である．

（証明）次の二つのことを示せばよい：

(1) $H = \mathrm{Ker}(f)$ とおくとき，すべての $C \in G/H$ に対して

$$f^{-1}\left(\overline{f}(C)\right) = C.$$

(2) すべての $g' \in \mathrm{Im}(f)$ に対して

$$\overline{f}\left(f^{-1}(g')\right) = g'.$$

注意：ファイバー $f^{-1}(g')$ が $G/\mathrm{Ker}(f)$ の元であることは補題 1 で示しましたので，$\overline{f}\left(f^{-1}(g')\right)$ が意味を持ちます．

見かけは厳めしいけれど実質的にはすべて確認済みのことです．

(1) について：$C = gH$ とします．$f^{-1}\left(\overline{f}(gH)\right) = f^{-1}\left(f(g)\right)$ ですが，補題 1 からこれは gH と一致します．

(2) について：$g' = f(g)$ とするとき $f^{-1}(g') = gH$ です（これも補題 1 から）．よって $\overline{f}\left(f^{-1}(g')\right) = \overline{f}(gH) = f(g) = g'$ です．□

像 $\mathrm{Im}(f)$ は群ですから，その演算を全単射によって $G/\mathrm{Ker}(f)$ に移植することによって $G/\mathrm{Ker}(f)$ には群の構造が入ります．それはどんな演算なのでしょうか？

答えは次のように簡明なものになります：

$$gH \cdot g'H = gg'H. \tag{8.1}$$

gH は $f(g)$ に $g'H$ は $f(g')$ に対応します．よって $\mathrm{Im}(f)$ の $f(g)f(g') = f(gg')$ に対応する剰余類 $gg'H$ が求めるものです．剰余類の代表の不定性の問題はこれまでの議論ですべてクリアされていることに注意してください．

群から群への準同型写像は，それが全単射であるとき，**同型写像**であるといいます．

系 2 (準同型定理) 準同型写像 $f : G \to G'$ を準同型写像とする．$G/\mathrm{Ker}(f)$ 上の演算を (8.1) によって定めることができる．このとき $G/\mathrm{Ker}(f)$ は群となり，更に f により定まる自然な写像 $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ は群の同型写像である．

演習問題の解説（§7, **1**-(9) 剰余類への分割の例）

A_4 を４次の交代群（４文字の偶置換全体がなす群）としましょう．

$$H = \{e, (12)(34), (13)(24), (14)(23)\}$$

は A_4 の部分群をなします．これを**クラインの四元群**と呼びます．H に含まれない元として長さ３の巡回置換 (ijk)（i, j, k は異なる文字）があるので，そのようなものを書き上げてみます．4 を動かさないものとして (123) と (132) の２つがありますね．他に 1 を動かさないもの $(234), (243)$，2 を動かさないもの $(134), (143)$，3 を動かさないもの $(124), (142)$ です．このように A_4 に含まれる長さ３の巡回置換は全部で８個です．$\#H = 4$ ですから，8 を足すと 12 です．一般に交代群 A_n の位数は $n!/2$ でしたから（偶置換は置換のうちの半分）A_4 の元はこれですべて書き上げられました．$\#H = 4$ ですから H を法とする剰余類は $\#A_4/\#H = 3$ 個あります．例えば $(123)H$ を求めてみましょう．H の各元に左から (123) を掛けてゆきます．$(123)H = \{(123)e, (123)(12)(34), (123)(13)(24), (123)(14)(23)\}$．置換の合成を求めると $(123)H = \{(123), (134), (243), (142)\}$ となります．まだ登場していない４個がもうひとつの剰余類をなすはずですが，実際に例えば $(132)H$ を計算してみれば $\{(132)e, (132)(12)(34), (132)(13)(24), (132)(14)(23)\} = \{(132), (234), (124), (143)\}$ となります．これで剰余類への分割 $A_4 = H \sqcup (123)H \sqcup (132)H$ ができました．

問題

17. ２面体群 D_n から $\{\pm 1\}$ への写像 f を $f(a^i) = 1,\ f(a^i b) = -1\ (0 \leq i \leq n-1)$ と定めると f は準同型写像となることを示せ．

18. 以下の群のうちで互いに同型であるものがあります．どれとどれが同型か答えてください．(1) クラインの四元群 (2) C_4 (3) D_2 (4) A_3 (5) C_3 (6) S_3 (7) D_3.

9 群の例

$\mathbb{Z}$ に和 $(x, y) \mapsto x + y$ という演算を与える．

（結合律）$x, y, z \in \mathbb{Z}$ を任意にとるとき

$$(x + y) + z = x + (y + z)$$

が成り立つ．この事実は小学校以来慣れ親しんで来たことですが，証明する必要がないというわけではありません．きちんと証明をするためには，整数とは何かということに立ち戻らなければならないので，この講義では正面切って議論しないというだけのことです．

（単位元の存在）任意の $x \in \mathbb{Z}$ に対して

$$x + 0 = 0 + x = x$$

が成り立つから 0 が和に関する単位元である．

（逆元の存在）任意の $x \in \mathbb{Z}$ に対して，その「マイナス元」$-x$ は $\mathbb{Z}$ の元として確かに存在して

$$x + (-x) = (-x) + x = 0$$

が成り立つ．0 が単位元であることに注意しよう．これは $-x$ が x の逆元であることを示している．

群 G の演算を「和」$+$ の記号で書くとき G を加法群と呼びます．これは単に記法上の言葉使いです．よく現れる基本的な加法群としては $\mathbb{Z}$ 以外に，有理数全体の集合 $\mathbb{Q}$，実数全体の集合 $\mathbb{R}$ など「数」からなるものの他，ベクトル空間 $\mathbb{R}^n$ などがあります．

一般に群の演算は「可換性」

$$xy = yx \ (x, y \in G)$$

を持つとは限らないものを考えるのですが，加法群の場合は

$$x + y = y + x$$

が成り立つものを考えるのが普通です．これは単に慣習上の問題であって，足し算が可換でないのは「気持ち悪い」という共通感覚があるせいでしょう．

「数」の「かけ算」によって群をなす例をあげましょう．

$G = \{+1, -1\}$ を自然なかけ算で群とみなすことはこれまですでに行ってきました．

$\mathbb{Q}^\times$ を 0 を除いた有理数全体の集合とします．これはかけ算によって群となります．

（結合律）$x, y, z \in \mathbb{Q}^\times$ を任意にとるとき

$$(xy)z = x(yz)$$

が成り立つ．

（単位元の存在）任意の $x \in \mathbb{Q}^\times$ に対して

$$1 \cdot x = x \cdot 1 = x$$

が成り立つから 1 が単位元である．

（逆元の存在）任意の $x \in \mathbb{Q}^\times$ はゼロでない整数 $m, n \in \mathbb{Z}$ を用いて $x = m/n$ と表わせます（有理数の定義）．$x^{-1} = n/m$ とするとき $x^{-1} \in \mathbb{Q}^\times$（ゼロでない有理数）であって

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

が成り立ちます．つまり任意の元 x に対して逆元が存在します．

有理数全体の集合 $\mathbb{Q}$ はかけ算に関して群にはなりません．結合律と単位元の存在は成り立つのですが 0 の逆元はありません．どのような $x \in \mathbb{Q}$ に対しても $0 \cdot x = x \cdot 0 = 0$ ですから，これが 1 となることは決してないからです．

10　写像の全射性と単射性

X, Y を集合とします．f を X から Y への写像とします．X の各元 x に対して Y の元 $f(x)$ がひとつずつ定まっているということです．

（全射性）Y の任意の元 y に対して，ある $x \in X$ が存在して $y = f(x)$ が成り立つとき，f は全射であるといいます．

（単射性）$x_1, x_2 \in X$ であって $x_1 \neq x_2$ であるものに対して必ず $f(x_1) \neq f(x_2)$ が成り立つとき f は単射であるといいます．

対偶をとると，条件 $f(x_1) = f(x_2)$ から必ず $x_1 = x_2$ がしたがうような写像のことを単射と呼ぶともいえます．

f が全射かつ単射であるとします．Y の任意の元 y に対して，f の全射性より，ある $x \in X$ であって $f(x) = y$ をみたすものがあります．一般には，与えられた y に対して，このような x が複数個ある可能性があります．しかし f が単射なので，$f(x) = y$ をみた

す x は唯一つだけしかありません．$f(x') = y$ となる $x' \in X$ があったとしても $x' = x$ がしたがうからです．

次の形を覚えておくと便利です．

16.（既出） $f : X \to Y$, $g : Y \to X$ を写像とする．次を示せ：
(1) $f \circ g = \mathrm{id}_Y$ ならば f は全射, (2) $g \circ f = \mathrm{id}_X$ ならば f は単射
ただし $\mathrm{id}_X : X \to X$ は恒等写像．つまり $\mathrm{id}_X(x) = x$ $(x \in X)$ とする．

(1) について：$y \in Y$ を任意の元とする．$y = \mathrm{id}_Y(y) = (f \circ g)(y) = f(g(y))$ なので $x = g(y) \in X$ とおくとき $f(x) = y$ となる．よって f は全射．
(2) $x_1, x_2 \in X$ が $f(x_1) = f(x_2)$ をみたすとする．$x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2$ となる．よって f は単射．

11 $\mathbb{Z}$ の部分群と剰余群

加法群 $\mathbb{Z}$ の部分群にはどんなものがあるでしょうか？ $n \in \mathbb{Z}$ を正として $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ とおきます．これは $\mathbb{Z}$ の部分群です．

命題 8 加法群 $\mathbb{Z}$ の部分群は $\{0\}$ および $n\mathbb{Z}$ $(n \geq 1)$ に限る．

（証明）H を $\mathbb{Z}$ の部分群とする．$H \neq \{0\}$ とすると H にはゼロでない整数 a が含まれる．H は逆元（マイナス元）について閉じているから $-a \in H$ でもある．a か $-a$ の一方は正なので H は正の整数を含むことがわかった．H に含まれる最小の正の整数を n とする．このとき $n\mathbb{Z} \subset H$ である． [なぜなら H は和に関して閉じているから $n \in H$ より $2n = n + n \in H$ がしたがう．同様に k を自然数とすると $nk \in H$ である（k に関する帰納法）．$-n$ でもあるから $-nk \in H$ もわかる．最後に $0 = n + (-n)$ だから 0 も H に属す．] 逆の包含関係 $n\mathbb{Z} \supset H$ を示す．a を H の任意の元とする．割り算を用いて $a = qn + r$ $(0 \leq r < n)$ と書く．商 q は整数である．$n \in H$ なので $qn \in H$ であり，$a \in H$ とあわせて $r = a - qn \in H$ がしたがう．もしも $r > 0$ とすると n が H に属す最小の正の整数であることに反する．したがって $r = 0$ である．つまり $a = qn$ となり $a \in n\mathbb{Z}$ がいえた．□

$\mathbb{Z}$ とその部分群 $n\mathbb{Z}$ に関して剰余類を考えましょう．$a \in \mathbb{Z}$ を代表とする剰余類は

$$a + n\mathbb{Z} := \{a + nk \mid k \in \mathbb{Z}\}$$

ですね．これは n を法とする剰余類「$a \bmod n$」です．剰余類による分割は

$$\mathbb{Z} = n\mathbb{Z} \sqcup (1 + n\mathbb{Z}) \sqcup (2 + n\mathbb{Z}) \sqcup \cdots \sqcup ((n-1) + n\mathbb{Z})$$

となります．剰余群 $\mathbb{Z}/n\mathbb{Z}$ は整数全体 $\mathbb{Z}$ をモジュロ n で考えたものに他ならないのです．

12 生成系

G を群とします．S を G の部分集合とします．G の任意の元 g に対して S のいくつかの元 $s_1, \ldots, s_n$ があって g が s_i あるいはその逆元 s_i^{-1} を掛け合わせたものとして表わせるとき，つまり

$$g = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \quad (\epsilon_i = \pm 1)$$

となるとき，S は G を生成するといいます．

例：$D_n = \{e, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$ は $S = \{a, b\}$ によって生成される．
例：$C_n = \{e, a, \ldots, a^{n-1}\}$ は $S = \{a\}$ によって生成される．

準同型定理をどのように使うかという例をみせましょう．

命題 9 G を群とし，$g \in G$ とする．G が $\{g\}$ によって生成されるならば G は $\mathbb{Z}$ もしくは $\mathbb{Z}/n\mathbb{Z}$ のいずれかと同型である．ここに $n \geq 1$ とする．

（証明）写像 $f : \mathbb{Z} \to G$ を $f(n) = g^n$ と定めます．このとき f は準同型写像です．つまり

$$f(n+m) = f(n)f(m) \quad (n, m \in \mathbb{Z})$$

が成り立ちます．この f は全射であることに注意しましょう．G の任意の元 x は，ある整数 $n \in \mathbb{Z}$ を用いて $x = g^n$ という形に書けます（生成されるとはそういうこと）．このとき $f(n) = g^n = x$ となるからです．全射であるということは $\mathrm{Im}(f) = G$ ということです．準同型定理より $\overline{f} : \mathbb{Z}/\mathrm{Ker}(f) \cong G$ です．$\mathrm{Ker}(f)$ は $\mathbb{Z}$ の部分群ですから，命題 8 より，$\mathrm{Ker}(f) = \{0\}$ または $n\mathbb{Z}$ $(n \geq 1)$ です．$\mathrm{Ker}(f) = \{0\}$ ならば $\mathbb{Z}/\mathrm{Ker}(f) = \mathbb{Z}$ です．$\mathrm{Ker}(f) = n\mathbb{Z}$ ならば $\mathbb{Z}/n\mathbb{Z} \cong G$ となります．□

13　補充問題

19 S. $G := \mathbb{R}^2 \setminus \{\mathbf{0}\}$ とおく．$(x,y)\cdot(x',y') = (xx'-yy', xy'+x'y)$ により演算を定める．G が群をなすことを示せ.

20 S. 加法群 $\mathbb{R}$ から，乗法群 $\mathbb{R}^\times = \mathbb{R}\setminus\{0\}$ への写像 f を $f(x) = e^x$ と定める．f が準同型写像であることを示せ．$\mathrm{Im}(f)$, $\mathrm{Ker}(f)$ を求めよ.

21 A. $S := \{(\cos\theta, \sin\theta) \mid \theta \in \mathbb{R}\}$ とおく.
(1) S は $\mathbb{R}^2\setminus\{\mathbf{0}\}$ （**19** の群）の部分群であることを示せ.
(2) 写像 $f : \mathbb{R} \to S$ を $f(\theta) = (\cos\theta, \sin\theta)$ により定める．f が準同型写像であることを示し，同型 $S \cong \mathbb{R}/2\pi\mathbb{Z}$ を導け.

22 A. $G := \mathbb{R}^2\setminus\{\mathbf{0}\}$ を **19** の演算により群とみなす．$\mathbb{R}_{>0} = \{x\in\mathbb{R} \mid x>0\}$ を乗法により群とする．同型 $G \cong \mathbb{R}_{>0}\times S$ を示せ.

14　演習の解答例

5. ：(1) $\sigma = (1243) = (12)(24)(43)$ と書けるから $\mathrm{sgn}(\sigma) = -1$. (2) 差積の定義は $\Delta_4(x) = \prod_{1\le i<j\le 4}(x_i - x_j) = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$ です．$\sigma\Delta_4(x)$ は $\Delta_4(x)$ において変数を $x_1\mapsto x_2$, $x_2\mapsto x_4$, $x_3\mapsto x_1$, $x_4\mapsto x_3$ と置き換えるということなので $(x_2-x_4)(x_2-x_1)(x_2-x_3)(x_4-x_1)(x_4-x_3)(x_1-x_3) = (-1)^3\Delta_4(x) = -\Delta_4(x)$ となる．したがって $\mathrm{sgn}(\sigma) = -1$ である.

10. ：(1) x が a^{-1} の逆元であるということは $a^{-1}x = xa^{-1} = e$ が成り立つということである．$x = a$ はこれをみたす．したがって $a = (a^{-1})^{-1}$ である．(2) x が ab の逆元であるとは $xab = abx = e$ が成り立つということである．$x = b^{-1}a^{-1}$ とおくと $xab = b^{-1}a^{-1}ab = b^{-1}b = e$ となる．同様に $abx = e$ である．よって $b^{-1}a^{-1} = (ab)^{-1}$ である.

15　なぜ代数学を，あるいは群論を学ぶのか

もともと，代数学は方程式を解くための理論だったはずです．方程式には未知数 x が含まれますね．数の代わりに文字 x を用いて足し算やかけ算をはじめるときに，原始的

な代数学が生まれたと考えられます．古来は整数のみたす方程式に主な興味があったでしょう．演算の数理では，整数の理論に関して１９世紀までによくわかっていた主要な結果を紹介しました．

抽象代数学は２０世紀の前半に一気に整備されました．抽象代数学の動機のひとつは間違いなく整数論にあったと思われます．素因数分解の一意性が成り立たないような「整数」の世界が膨大にあるということがはっきりしてきたのです．そこでデデキント環の理論が生まれました．もうひとつの動機は代数幾何学への応用です．代数幾何学とは，代数方程式の解の集合を幾何学的な概念を用いて研究する学問です．代数幾何学の現代的な発展のために，可換環の理論を深化させる必要がありました（今も大いにあります）．「環」とは足し算とかけ算の２種類の演算を持つ代数系です．

一方，群という概念は代数方程式の対称性を議論する目的でガロワによって発見されました（代数学 II ではその話を聞くことができますよ）．その後，広く対称性を記述する構造として注目されて自然科学にも広く応用されています．有限群の理論と，無限群の理論は発展の道筋がかなり違います．ガロワの理論で活躍するのは有限群です．有限群に関しては，単純群を分類するという大問題がありましたが，１９８０年代の後半に解決されました．無限群をすべて分類するなどということはとうてい不可能だと思われますが，非常に性質のよい無限群の種類があります．リー群と呼ばれるものです．$GL_n(\mathbb{R})$ がその典型です．リー群は幾何学や解析学にも応用のひろい大切な群の仲間です．とはいえ，群に関しては，まずは，有限群の理論を勉強するのが標準コースです．

繰り返しになりますが，群という代数系はとても自然で，応用の広いものです．それだけでなく，抽象的な代数の議論に慣れるためにも，まずは群論を勉強するというのがよいだろうという考えで，標準コースの題材に選ばれているのです．標準コースであるといっても，有限群というのは，初学者にとってはなかなか難しいものです．実は，有限群の専門家にとっても（おそらく）大変難しいものなのです．

みなさんは，解き方のはっきりわかっている問題を覚えて解くという段階を卒業して，専門的で本格的な数学の研究にすでに踏み込みはじめているのです．一歩踏み込んだだけでとてつもなく難しい問題がいくらでもある一方で，非常に見事な理論というものがいくつも建設されている途中です．それが現在発展中の生きた数学です．代数学の講義のなかに生きた数学の縮図が有るような感じがします．群論を学ぶ過程では，目の覚めるような鮮やかな結果がある一方で，薮の中に頭を突っ込むような印象を受ける複雑な現象にも出くわすでしょう．どうしても一筋縄ではゆかないのです．すっきりと説明できる部分と，混沌としてはいるが豊かな現実世界とを行ったり来たりしながら，すこしづつ理解が深まってゆくのではないでしょうか．

16 復習の要点

1. 図形の対称性（下記の問題 **23**）
   - 家紋の対称性
   - ２面体群 D_n，巡回群 C_n
   - 正四面体の対称性
2. 群の定義とその帰結を理解すること.
   - 問題 **11**, **12** ((3),(4) を除く), **19**（群の定義の確認）
   - 逆元の一意性，問題 **10**（定義の帰結）
3. 対称群 S_n と置換の符号
   - 問題 **5**（符号の意味）
4. 部分群と剰余類について
   - 問題 **2**（部分群）
   - 問題 **1**（剰余類への分割）
   - §6 剰余類, p.7, **命題 1**（剰余類の基本的な性質）
5. 準同型写像の例を知ること．核と像の意味を理解すること.
   - 問題 **17**, **20**（準同型写像の例）
   - §8 準同型写像と準同型定理, p.13, **命題 1**（準同型写像の基本的な性質）
6. 写像の全射性と単射性
   - 問題 **16**

復習用の補充問題

23S. (1) 次の図形の対称性を表わす群を以下の選択肢から選べ.

選択肢 $C_3, C_4, C_5, C_6, D_2, D_3, D_4, D_6$

(2) 2 面体群 D_6 において図の対称軸をあらわす元は何か？

(3) 正四面体の回転対称性は全部でいくつあるか？そのうちで $g^2 = e$ をみたすものをすべて答えよ（図示せよ）．図のように a, b を定める ab および ba を図示せよ．

24S. 以下の写像のうち準同型写像であるものを選べ．また全射であるもの，単射であるものを選べ：(イ) $f : \mathbb{Z} \to \mathbb{Q}^\times$, $f(n) = 2^n$, (ロ) $f : \mathbb{Z} \to \mathbb{Q}^\times$, $f(n) = n^2$, (ハ) $f : \mathbb{Q}^\times \to \mathbb{Q}^\times$, $f(x) = x^2$, (ニ) $f : \mathbb{R}_{>0} \to \mathbb{R}$, $f(x) = \log_e(x)$, (ホ) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$, (ヘ)$f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 1$.

質問可能時間：
10 日（09:00-13:00, 15:30-18:30）
11 日（16:30-18:30）
12 日（要予約 11:45-13:00, 16:45-18:00）
なお 14 日, 15 日は出張です.

17　正規部分群

定理 2 G, G' を群とし，f を G から G' への準同型写像とするとき，群の自然な同型

$$\overline{f}:\ G/\mathrm{Ker}(f) \xrightarrow{\cong} \mathrm{Im}(f)$$

が存在する．

左辺の $G/\mathrm{Ker}(f)$ は剰余群です．見やすくするために $H := \mathrm{Ker}(f)$ とおきましょう．H を法とする剰余類 gH 全体がなす集合 G/H に演算を

$$g_1H \cdot g_2H = g_1g_2H$$

と定めることにより群の構造を与えたものです．

この演算の定め方は，次のことが成り立つことを前提としています：

$$(\star)\ :\ g_1H = g_1'H,\ g_2H = g_2'H \Longrightarrow g_1g_2H = g_1'g_2'H.$$

準同型写像の核 $H = \mathrm{Ker}(f)$ がこの性質をみたしていることを後で再度確認します．

実は $(\star)$ という条件はどんな部分群に対しても成り立つわけではないのです．このことを示すため次の例を考えてみましょう．

例. $G = S_3,\ H = \{e, (12)\}$ とすると，$G/H = \{H, (13)H, (23)H\}$ ですね．例えば $eH = (12)H,\ (13)H = (123)H$ であることに注意しましょう．つまり $g_1 = e,\ g_1' = (12),\ g_2 = (13),\ g_2' = (123)$ とすると $g_1H = g_1'H,\ g_2H = g_2'H$ が成立しています．このとき $g_1g_2 = (13),\ g_1'g_2' = (12)(123) = (23)$ です．この例では $g_1g_2H \neq g_1'g_2'H$ となっています．剰余類の代表を変更するとき，代表どうしの積 g_1g_2 と $g_1'g_2'$ が別な剰余類に属してしまうのです．

$(\star)$ が成り立つための十分条件として次が重要です：

$$gHg^{-1} = H \quad (\text{すべての } g \in G \text{ に対して})$$

ここで $gHg^{-1} := \{ghg^{-1} \mid h \in H\}$ としました．G の部分群 H がこの条件をみたすとき H は**正規部分群**であるといいます．

定理 3 群 G の正規部分群 H に対して $(\star)$ が成立する．

（証明）$g_1H = g_1'H$, $g_2H = g_2'H$ としましょう．これは $h_1 := g_1^{-1}g_1'$, $h_2 := g_2^{-1}g_2' \in H$ を意味します．$(g_1g_2)^{-1}(g_1'g_2') \in H$ を示せばよいわけです．そこで

$$(g_1g_2)^{-1}(g_1'g_2') = g_2^{-1}g_1^{-1}g_1'g_2' = g_2^{-1}h_1g_2' = g_2^{-1}h_1g_2g_2^{-1}g_2' = g_2^{-1}h_1g_2 \cdot h_2$$

と書き直してみます．H が正規部分群であることから $g_2^{-1}h_1g_2 \in H$ がしたがいます．$h_2 \in H$ であることと H が積で閉じていることから $g_2^{-1}h_1g_2 \cdot h_2 \in H$ が得られます．□

命題 10 準同型写像の核 $\mathrm{Ker}(f)$ は正規部分群である．

（証明）$h \in \mathrm{Ker}(f)$ とする．任意の $g \in G$ に対し $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e'$ である．つまり $ghg^{-1} \in \mathrm{Ker}(f)$ である．□

命題 11 群 G の部分群 H が次をみたせば，正規部分群である：

$$gHg^{-1} \subset H \quad (\text{すべての } g \in G \text{ に対して}).$$

（証明）示すべきことは，任意の $g \in G$ に対して $H \subset gHg^{-1}$ となることである．命題の条件より $g^{-1}Hg \subset H$ がしたがう（g として g^{-1} を考えればよい）．だから $h \in H$ を任意にとるとき $g^{-1}hg \in H$ である．$h = g(g^{-1}hg)g^{-1}$ と書いてみれば $g^{-1}hg \in H$ とあわせて $h \in gHg^{-1}$ がしたがう．つまり $H \subset gHg^{-1}$ が示された．□

これまで扱った例のうち，基本的な正規部分群としては次がある．
例：$C_n \subset D_n$ は正規部分群である．
例：$A_n \subset S_n$ は正規部分群である．

25B. 次の群 G とその部分群 H について，H が G の正規部分群であるかどうか調べよ．(1) $G = S_3$, $H = \{e, (13)\}$, (2) $G = S_3$, $H = \{e, (123), (132)\}$, (3) $G = D_4$, $H = \{e, a\}$, (4) $G = D_4$, $H = \{e, a^2\}$, (5) $G = D_4$, $H = \{e, a^2, b, a^2b\}$.

26S. クラインの 4 元群 $H = \{e, (12)(34), (13)(24), (14)(23)\}$ が S_4 の正規部分群であることを示せ．

ヒント：$(a_1a_2\cdots a_r)$ を巡回置換とするとき $\sigma(a_1a_2\cdots a_r)\sigma^{-1}$ はどのようになるのだっかか？

27A. G を有限群とし，H をその部分群であって $\#G = 2 \cdot \#H$ が成り立つとき H は G の正規部分群である．これを示せ．

18　$\mathbb{Z}^r$ の部分群 — 単因子論 —

$\mathbb{Z}^r$ と同型な群 F を自由アーベル群と呼びます．その定義から，同型写像 $f : \mathbb{Z}^r \xrightarrow{\cong} F$ があります．f は全射ですから F の任意の元 x に対して $\boldsymbol{m} \in \mathbb{Z}^r$ があって $f(\boldsymbol{m}) = x$ となります．$\boldsymbol{e}_1 \ldots, \boldsymbol{e}_r$ を $\mathbb{Z}^r$ の標準基底とすると $\boldsymbol{m} = {}^t(m_1, \ldots, m_r) = \sum_{i=1}^r m_i \boldsymbol{e}_i$ と書けるわけですが，f は準同型写像なので $f(\boldsymbol{m}) = f\left(\sum_{i=1}^r m_i \boldsymbol{e}_i\right) = \sum_{i=1}^r m_i f(\boldsymbol{e}_i)$ となります．ここで $a_i := f(\boldsymbol{e}_i)$ とおくことにします． 結局，

(i) 任意の $x \in F$ に対して $x = \sum_{i=1}^r m_i a_i$ をみたす整数 $m_1, \ldots, m_r$ が存在する

ことがわかったのです．このことを「F は $a_1, \ldots, a_r$ で生成される」といいます．

さて，f は単射でもありますから $f(\boldsymbol{m}) = f(\boldsymbol{m}')$ から $\boldsymbol{m} = \boldsymbol{m}'$ がしたがいます．これは，つまり

$$m_1 a_1 + \cdots + m_r a_r = m_1' a_1 + \cdots + m_r' a_r$$

ならば $m_i = m_i'$ $(1 \leq i \leq r)$ となることを意味します．特に

(ii) $m_1 a_1 + \cdots + m_r a_r = 0$ ならば $m_1 = \cdots = m_r = 0$

です．このことを「$a_1, \ldots, a_r$ は $\mathbb{Z}$ 上一次独立である」といいます．

$a_1, \ldots, a_r \in F$ が (i), (ii) をみたすとき，$a_1, \ldots, a_r$ は F の $\mathbb{Z}$ 上の基底であるといいます．F の基底は何通りも（無限に）存在するのですが，基底をなす元の個数 r は F のみによって決まる数であることが次の命題からわかります．いいかえると，どのような基底も r 個の元からなるのです．この r を F の階数と呼んで $r = \mathrm{rank}(F)$ と書きます．

命題 12 $F \cong \mathbb{Z}^r$ かつ $F \cong \mathbb{Z}^s$ ならば $s = r$ が成り立つ．

(証明) $F \cong \mathbb{Z}^r$ とする．$n \geq 2$ を自然数とし（なんでもよい），$nF := \{nx \mid x \in F\}$ は F の部分群である．$a_1, \ldots, a_r$ を F の基底とする．F の元 $x = \sum_{i=1}^r m_i a_i$ が nF に属すための条件は $i = 1, \ldots, r$ に対して $m_i \equiv 0 \pmod{n}$ が成り立つことである．だから F/nF の元を与えることは，各 $i = 1, \ldots, r$ について $\overline{m_i} = m_i \pmod{n} \in \mathbb{Z}/n\mathbb{Z}$ を与えることと同じである．したがって

$$\#(F/nF) = n^r$$

が成り立つ．右辺の n^r は基底を用いて計算したが，左辺は基底によらずに決まる数である．このことは，r という数が基底の選び方にはよらずに決まっていることを示してい

る．実際 $n^r = n^s$ ならば $r = s$ だから，命題の主張がしたがう．□

自由アーベル群 F の階数 $\mathrm{rank}(F)$ はベクトル空間 V の次元 $\dim_{\mathbb{R}}(V)$ と類似しています．ベクトル空間 V が基底 $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ を持つとします．V の基底はいくらでもあるのですが，必ず r 個の元からなります．r という自然数は V の基底の選び方によらずに決まります（だから，それを V の次元 $\dim_{\mathbb{R}}(V)$ と定めることに意味があります）．この事実は，線型代数の重要事項ですが，初学者が理解するのはなかなか難しいことです．３年生の皆さんは再挑戦して理解しておいて欲しいものです．

定理 4 F を階数 r の自由アーベル群とする．F の部分群 H に対して F の基底 $a_1, \ldots, a_r$ であって $e_1a_1, \ldots, e_sa_s$ が H の基底となるものが存在する．ここで $e_1, \ldots, e_s$ $(s \leq r)$ は自然数であって $e_i | e_{i+1}$ $(1 \leq i \leq r-1)$ をみたす．このような $(e_1, \ldots, e_s)$ は H に対して一意的に定まる．

補題 2 $a_1, \ldots, a_r$ を F の基底とする．$b_1 = a_1 + \sum_{i=2}^{r} n_i a_i$ $(n_i \in \mathbb{Z})$ とおくとき $b_1, a_2, \ldots, a_r$ は F の基底をなす．

（証明）$a_1 = b_1 - \sum_{i=2}^{r} n_i a_i$ と書けるので $b_1, a_2, \ldots, a_r$ は F を生成する．念のため，もう少し詳しくいう．F の任意の元 x をとるとき $x = \sum_{i=1}^{r} m_i a_i$ と書ける．$x = m_1 a_1 + \sum_{i=2}^{r} m_i a_i = m_1(b_1 - \sum_{i=2}^{r} n_i a_i) + \sum_{i=2}^{r} m_i a_i = m_1 b_1 + \sum_{i=2}^{r} (m_i - m_1 n_i) a_i$ となる．

１次独立性：$m_1 b_1 + \sum_{i=2}^{r} m_i a_i = 0$ とする．$0 = m_1(a_1 + \sum_{i=2}^{r} n_i a_i) + \sum_{i=2}^{r} m_i a_i = m_1 a_1 + \sum_{i=2}^{r} (m_1 n_i + m_i) a_i$ となる．$a_1, \ldots, a_r$ が１次独立なので，まず $m_1 = 0$ がわかる．このとき $0 = \sum_{i=2}^{r} m_i a_i$ となるから $m_i = 0$ $(2 \leq i \leq r)$ もしたがう．□

（定理の証明）$\mathrm{rank}(F) = r$ に関する帰納法を用いる．$r = 1$ のときは $F = \mathbb{Z}$ と考えてよい．$\mathbb{Z}$ の任意の部分群 H がある $m \geq 0$ によって $H = m\mathbb{Z}$ と表わされることは既に示した．$a_1 = 1$ は $\mathbb{Z}$ の基底である．$m > 0$ の場合は $s = 1$, $e_1 = m$ とすればよい．$m = 0$ なら $s = 0$ でよい．

$r \geq 2$ として階数が $r-1$ の自由アーベル群に対しては定理が成り立つと仮定する．F には基底があるので，そのひとつを $b_1, \ldots, b_r$ とする．H の元 x を $x = \sum_{i=1} m_i b_i$ と表わす．x を H 全体にわたって動かしたときに $|m_1|, \ldots, |m_r|$ の最小値が h であるとき，H の基底 $b_1, \ldots, b_r$ に関する高さが $h = h(H, \{b_1, \ldots, b_r\})$ であるという．すべての基底を動かして，そのうちで高さ $h = h(H, \{b_1, \ldots, b_r\})$ が最小値をとる基底 $b_1, \ldots, b_r$ を

選ぶ（沢山ある）．$H \neq 0$ である限り $h > 0$ である．$x_0 \in H$ を，その基底で展開して $x_0 = m_1 b_1 + \cdots + m_r b_r$ としたときに $m_1 = h$ となるとしてよい．

主張：$m_2, \ldots, m_r$ は m_1 で割り切れる．

証明：$m_i = q_i m_1 + r_i$ $(0 \leq r_i < m_1,\ 2 \leq i \leq r)$ とする．

$$x_0 = m_1 b_1 + m_2 b_2 + \cdots + m_r b_r = m_1 b_1 + (q_2 m_1 + r_2) b_2 + \cdots + (q_r m_1 + r_r) b_r$$

$$= m_1 (b_1 + q_2 b_2 + \cdots + q_r b_r) + r_2 b_2 + \cdots + r_r b_r$$

と書き直す．$a_1 = b_1 + q_2 b_2 + \cdots + q_r b_r$ とおくと補題より $a_1, b_2, \ldots, b_r$ は F の基底である．さて，H の元を任意の基底で展開するときに，0 でない係数の絶対値は $h = m_1$ 以上である．よって $r_2 = \cdots = r_r = 0$ となる．（主張の証明終わり）

ここまでわかったことをまとめると $a_1, b_2, \ldots, b_r$ は F の基底であって $m_1 a_1 \in H$ である．実際 $m_i = q_i m_1 (2 \leq i \leq r)$ なので $x_0 = m_1 b_1 + m_2 b_2 + \cdots + m_r b_r = m_1 (b_1 + q_2 b_2 + \cdots + q_r b_r) = m_1 a_1$ である．

さて，H の任意の元 x を $x = n_1 a_1 + n_2 b_2 + \cdots + n_r b_r$ と展開してみよう．このとき n_1 は m_1 で割り切れる．なぜなら $n_1 = q m_1 + s$ $(0 \leq s < m_1)$ とするとき $H \ni x - q m_1 a_1 = s a_1 + n_2 b_2 + \cdots + n_r b_r$ となるから，これから $s = 0$ がしたがう．

ここで $b_2, \ldots, b_r$ が生成する F の部分群を F' とする． $b_2, \ldots, b_r$ は $\mathbb{Z}$ 上一次独立なので F' は階数 $r-1$ の自由アーベル群である．ここで $e_1 = m_1$ とおこう．前段落でみたことは，H の任意の元 x が $x = x_1 + y$ $(x_1 \in e_1 a_1 \mathbb{Z},\ y \in H \cap F')$ の形に（一意的に）書けることである．

$F' \cong \mathbb{Z}^{r-1}$ の部分群 $H \cap F'$ に帰納法の仮定を適用して F' の基底 $a_2, \ldots, a_r$ であって $e_2 a_2, \ldots e_s a_s$ が $H \cap F'$ の基底となるものが存在する．更に，このとき $e_i | e_{i+1}$ $(2 \leq i \leq r-1)$ が成り立っている．ここまでくれば $a_1, a_2, \ldots, a_r$ が F の基底をなし，$e_1 a_1, \ldots, e_s a_s$ が H の基底をなすことは明らかである．

$e_1 | e_2$ を示そう．$e_2 = u e_1 + t$ $(0 \leq t < e_1)$ とする．このとき $H \ni e_1 a_1 + e_2 a_2 = e_1 a_1 + (u e_1 + t) a_2 = e_1 (a_1 + u a_2) + t a_2$ となる．$a_1 + u a_2, a_2, \ldots, a_r$ は F の基底なので $t = 0$ がしたがう．

以上で $(e_1, \ldots, e_r)$ の一意性を除いて証明が終わった．一意性を示すためには更に準備が必要なので，節を改めて説明しよう．□

19　アーベル群の基本定理

群 G は $xy = yx$ がすべての $x, y \in G$ に対して成り立つときアーベル群であるといいます．可換群であるともいいます．以下では，特に断らない限り，アーベル群の演算を和の記号 $x + y$ により表記します．

例：$\mathbb{Z}$ はアーベル群です．他にも，演算を加法により表記する群は（慣習上）すべてアーベル群です．乗法群 $\mathbb{Q}^\times$ などもアーベル群です．巡回群 C_n もアーベル群です．アーベル群の部分群や剰余群はアーベル群です．D_n $(n \geq 2)$ や S_n $(n \geq 3)$ はアーベル群ではありません．アーベル群でない群は非可換群であるといいます．

ここで，群の直積について説明しておきます．$G_1, \ldots, G_r$ を群とします（アーベル群とは限らない．演算は積の形で書く）． $g_1 \in G_1, \ldots, g_r \in G_r$ をならべて r 個の組 $(g_1, \ldots, g_r)$ を考えます．このようなもの全体がなす集合を $G_1 \times \cdots \times G_r$ で表わします．この集合の演算を

$$(g_1, \ldots, g_r) \cdot (g_1', \ldots, g_r') = (g_1 g_1', \ldots, g_r g_r')$$

と定めると，群の条件をみたします．これを群の直積といいます．

定理 5 (アーベル群の基本定理) G を有限生成アーベル群であるとする．自然数の列 $e_1, e_2, \ldots, e_r$ で $e_i \geq 2$, $e_i | e_{i+1}$ $(1 \leq i \leq r-1)$ をみたすもの，および非負の整数 l が存在して群の同型

$$G \cong (\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_r\mathbb{Z}) \times \mathbb{Z}^l$$

が成立する．更に，このとき $(e_1, \ldots, e_r)$ および l は G によって一意的に定まる．

$(e_1, \ldots, e_r)$ を G の単因子型，l を G の階数と呼びます．

明らかに G が有限集合であることと $l = 0$ は同値です．この定理は有限アーベル群の完全な分類を含んでいるわけです．

例：位数が 4 の任意のアーベル群は $\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ののいずれか一方と同型です．それぞれ，単因子型が $(4), (2, 2)$ のアーベル群です．

例：p を素数とするとき，位数が p^2 のアーベル群の単因子型は $(p^2), (p, p)$ です．

位数が p^3 のアーベル群の単因子型は $(p^3), (p, p^2), (p, p, p)$ の 3 通りです.

自然数の列 $1 \leq a_1 \leq a_2 \leq \cdots \leq a_r$ $(r \leq n)$ で $a_1 + a_2 + \cdots + a_r = n$ をみたすものに対して，単因子型 $(p^{a_1}, \ldots, p^{a_r})$ を対応させることができます.

$n = 4$ ならば $1+1+1+1$, $1+1+2$, $1+3$, $2+2$, 4 の 5 通りがあるので，位数 p^4 のアーベル群としては

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z},$$

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z}, \quad \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}, \quad \mathbb{Z}/p^4\mathbb{Z}$$

という 5 通りの互いに同型でないものがあるのです.

（証明）$x_1, \ldots, x_n$ が G を生成するとします．写像 $f : \mathbb{Z}^n \to G$ を $(m_1, \ldots, m_n) \mapsto \sum_{i=1}^n m_i x_i$ により定めると，f は準同型写像であって全射です．準同型定理より群の同型

$$\overline{f} : \mathbb{Z}^n/\mathrm{Ker}(f) \xrightarrow{\cong} G$$

が得られます．前節の定理より $\mathbb{Z}^n$ の基底 $a_1, \ldots, a_n$ であって $e_1 a_1, \ldots, e_m a_m$ が $\mathrm{Ker}(f)$ の基底をなすようなものが存在します．ここに $m \leq n$ であって $e_1, \ldots, e_m$ は自然数の列で $e_i | e_{i+1}$ $(1 \leq i \leq m-1)$ をみたすものです．$\mathbb{Z}^n$ の元 x は

$$x = m_1 a_1 + \cdots + m_n a_n \quad (m_1, \ldots, m_n \in \mathbb{Z})$$

の形に一意的に表わされます．$x = \sum_{i=1}^n m_i a_i$, $x' = \sum_{i=1}^n m_i' a_i \in \mathbb{Z}^n$ が部分群 $\mathrm{Ker}(f)$ に関して同じ剰余類に属すことを $x \equiv x' \bmod \mathrm{Ker}(f)$ と表わすことにします．これは差 $x - x'$ が $\mathrm{Ker}(f)$ に属すことと同値です．$\mathrm{Ker}(f)$ が $e_1 a_1, \ldots, e_m a_m$ を基底としているので

$$x - x' = \sum_{i=1}^m (m_i - m_i') a_i + \sum_{j=m+1}^n (m_j - m_j') a_j \in \mathrm{Ker}(f)$$

は

$$m_i \equiv m_i' \mod e_i \ (1 \leq i \leq m), \quad m_j = m_j' \ (m+1 \leq j \leq n)$$

と同値です．最初の r 個の成分についてそれぞれが法 e_i で合同であって，残りの $n - m$ 個の成分が一致するときに限り x と x' は同一の剰余類に属すのです．剰余類をひとつ決めることは $\mathbb{Z}/e_1\mathbb{Z}, \ldots, \mathbb{Z}/e_m\mathbb{Z}$ の元をひとつづつ選んで更に，整数の組 $(m_{m+1}, \ldots, m_n) \in \mathbb{Z}^{n-m}$ を選ぶことと同等です．以上より全単射

$$\mathbb{Z}/\mathrm{Ker}(f) \cong \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_m\mathbb{Z} \times \mathbb{Z}^{n-m}$$

が得られました．これは群の同型です．$e_1, \ldots, e_m$ のうち，はじめのいくつかが 1 であるかもしれないのでそれを捨てて，残りを改めて $e_1, \ldots, e_r$ とすると定理の同型が得られます．

一意性について：$(e_1, \ldots, e_r)$, l および $(e'_1, \ldots, e'_{r'})$, l' が定理の条件をみたすものとして

$$G \cong (\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_r\mathbb{Z}) \times \mathbb{Z}^l \cong (\mathbb{Z}/e'_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e'_{r'}\mathbb{Z}) \times \mathbb{Z}^{l'}$$

から $r' = r$, $e_i = e'_i$ $(1 \leq i \leq r)$, $l = l'$ を導きます．

アーベル群 G の元 x であって，ある $n \geq 1$ に対して $nx = 0$ をみたすもの全体の集合を $T(G)$ で表わします．$T(G)$ は G の部分群です．上記のふたつの表示から

$$T(G) \cong (\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_r\mathbb{Z}) \cong (\mathbb{Z}/e'_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e'_{r'}\mathbb{Z}) \tag{19.2}$$

が得られます．これより $G/T(G) \cong \mathbb{Z}^l \cong \mathbb{Z}^{l'}$ となりますから階数の不変性より $l = l'$ がしたがいます．

あとは (19.2) より $r' = r$, $e_i = e'_i$ $(1 \leq i \leq r)$ を示します．次の補題を用います．

補題 3 $G \cong \mathbb{Z}/n\mathbb{Z}$ とする．$mG = \{mx \mid x \in G\}$ とおく．

m が n の倍数ならば $mG \cong \{0\}$

m が n の約数ならば $mG \cong \mathbb{Z}/(n/m)\mathbb{Z}$

ふたつの数列 $e_1, \ldots, e_r$ と $e'_1, \ldots, e'_{r'}$ を後ろからみていって k 個が等しくて $k+1$ 番目が異なるとします．つまり $e_r = e'_{r'}, \ldots, e_{r-k+1} = e'_{r'-k+1}$ かつ $e_{r-k} \neq e'_{r'-k}$ とします．$e_{r-k} < e'_{r'-k}$ としてかまいません．補題 1 を用いると

$$\begin{aligned} e_{r-k} \cdot T(G) &\cong (e_{r-k}\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (e_{r-k}\mathbb{Z}/e_{r-k}\mathbb{Z}) \times (e_{r-k}\mathbb{Z}/e_{r-k+1}\mathbb{Z}) \times \cdots \times (e_{r-k}\mathbb{Z}/e_r\mathbb{Z}) \\ &\cong (\mathbb{Z}/(e_{r-k+1}/e_{r-k})\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(e_r/e_{r-k})\mathbb{Z}) \end{aligned}$$

となる一方，同じ $e_{r-k} \cdot T(G)$ は補題 1 と $e_r = e'_{r'}, \ldots, e_{r-k+1} = e'_{r'-k+1}$ を用いると

$$\begin{aligned} &(e_{r-k}\mathbb{Z}/e'_1\mathbb{Z}) \times \cdots \times (e_{r-k}\mathbb{Z}/e'_{r-k}\mathbb{Z}) \times (e_{r-k}\mathbb{Z}/e'_{r'-k+1}\mathbb{Z}) \times \cdots \times (e_{r-k}\mathbb{Z}/e'_{r'}\mathbb{Z}) \\ \cong\ &(e_{r-k}\mathbb{Z}/e'_1\mathbb{Z}) \times \cdots \times (e_{r-k}\mathbb{Z}/e'_{r-k}\mathbb{Z}) \times (\mathbb{Z}/(e_{r-k+1}/e_{r-k})\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(e_r/e_{r-k})\mathbb{Z}) \end{aligned}$$

とも同型になることがわかります．さて，ここで $e_{r-k} < e'_{r'-k'}$ だから $e_{r-k} \not\equiv 0 \mod e'_{r'-k'}$ です．特に $(e_{r-k}\mathbb{Z}/e'_{r'-k}\mathbb{Z})$ は自明でない群なので位数を比較すると矛盾が生じます．□

20 Sylow の定理

G を有限群とします．Lagrange の定理によると G の部分群 H の位数は G の位数 $\#G$ の約数です．逆に，$\#G$ の約数 m に対して，m を位数に持つ部分群が存在するかどうか？存在するとしたら，そのような部分群の個数について何を知ることができるかという問題を考えます．特に m が素数 p のべき p^s の場合に，見事な定理があります．

20.1 用語の確認

G を有限群とするとき G に含まれる元の総数を $\#G$ で表わし G の位数と呼びます．

H を G の部分群とします．H を法とする左剰余類（左 H 剰余類）とは gH $(g \in G)$ と表わされる G の部分集合のことでした．同様に Hg $(g \in G)$ の形の部分集合を右 H 剰余類と呼びます．本によって右と左が逆のものもあるので注意が必要です．

左 H 剰余類全体の集合を G/H で表わします．左 H 剰余類の個数を H の指数と呼び $[G : H]$ で表わします．Lagrange の定理により $\#G = \#H \times [G : H]$ が成り立ちます．指数 $[G : H]$ は右 H 剰余類の個数とも一致[*1]します．

$g \in G$ を用いて $gHg^{-1} := \{ghg^{-1} \mid h \in H\}$ と定まる部分集合は G の部分群をなします．これを H と共役な部分群であるといいます．

すべての $g \in G$ に対して $gHg^{-1} = H$ が成り立つとき H は正規部分群であるといいます．言い換えると，共役な部分群が自分自身以外に無いということです．このとき $gH = Hg$ が成り立ち[*2]，左剰余類と右剰余類の区別をする必要がなくなります．H が正規剰余類ならば G/H に群の構造が自然に定まります．これを剰余群と呼びます．このとき，写像 $f : G \longrightarrow G/H$ $(g \mapsto gH)$ は全射準同型です．これを自然な射影と呼びます．核 $\mathrm{Ker}(f)$ は H と一致します．

一般に位数が p のべきの群を p-群といいます．G の部分群であって p-群であるものを p-部分群といいます．

[*1] Lagrange の定理の証明は右 H 剰余類についても全く同様に適用できます．

[*2] 演習問題．

20.2 p-部分群の存在

定理 6 (p-部分群の存在) G の位数が素数 p のべき p^s $(s \geq 1)$ で割り切れるならば，G には位数 p^s の部分群が存在する．

この定理の証明のために，次の補題を用います．$Z(G) := \{g \in G \mid gx = xg\}$ として G の中心と呼びます．$Z(G)$ は G の部分群です．定義から $Z(G)$ は可換群（アーベル群）です．

補題 4 $\#G$ が素数 p で割り切れるとする．$H \neq G$ なるすべての部分群に対して指数 $[G : H]$ が p で割り切れるならば，$Z(G)$ の位数は p で割り切れる．

この補題 1 の証明は「類等式」と呼ばれる等式の応用として得られます．次の節にまわしましょう．

（定理の証明）$\#G$ に関する帰納法を用います．$\#G = p$ のときは明らかです．$\#G > p$ として $\#G$ よりも小さい位数を持つ群に対して定理が成立すると仮定します．

(i) 位数が p^s で割り切れる部分群 $H(\neq G)$ が存在する場合．

$\#H < \#G$ であって $\#H$ が p^s で割り切れるのですから帰納法の仮定より H には位数 p^s の部分群が存在します．それは G の部分群でもありますから，この場合は OK です．

(ii) $H \neq G$ なるすべての部分群 H の位数が p^s で割り切れない場合．

補題 1 により G の中心の位数 $\#Z(G)$ が p で割り切れます．さて，次がわかります：

- $Z(G)$ には位数 p の部分群 P が存在する．（アーベル群の基本定理を用いる）
- P は G の正規部分群である．（中心 $Z(G)$ の部分群は正規部分群）

したがって剰余群 G/P が考えられるわけですが，その位数[*3]は p^{s-1} で割り切れます．帰納法の仮定により G/P の部分群 $\overline{H}$ で位数が p^{s-1} のものが存在します．$f : G \longrightarrow G/P$ を自然な射影（準同型写像）とすると f は p 対 1 の写像[*4]なので $\overline{H}$ の逆像 $f^{-1}(\overline{H}) \subset G$ は位数が $p^{s-1} \times p = p^s$ の部分群です．□

[*3] $\#(G/P) = \#G/p$ だから．

[*4] ファイバーは $\mathrm{Ker}(f) = P$ の剰余類です．

20.3 Sylow の定理

さて G の位数が p で割り切れるとして $\#G = p^r q$（q は p で割れない）とします．定理 1 より，位数が p^r の部分群が存在します．このような部分群を Sylow p-部分群と呼びます．S が G の Sylow p-部分群であるということは，S が G の部分群であって p-群であるもの（p-部分群）のうち極大なものといっても同じことです．

H_1 と H_2 が共役であるとは $H_2 = gH_1g^{-1}$ となる $g \in G$ が存在することをいいます（用語の確認）．

定理 7 (Sylow の定理)

(1) P を G の p-部分群であるとする．P を含む Sylow p-部分群が存在する．

(2) H_1, H_2 が Sylow p-部分群であるとする．H_1 と H_2 は共役である．

(3) Sylow p-部分群の個数を n_p とすると $n_p \equiv 1 \mod p$ である．

系 3 H が Sylow p-部分群であって正規部分群であるとする．H はこのとき，唯一の Sylow p-部分群である．

（証明）H が正規部分群であるということは H 自身以外には共役な部分群が無いということである．したがって (2) より系は明らか．□

20.4 両側分解

Sylow の定理を証明するために両側剰余類という概念を用います．

H, K を G の部分群とします．$x \in G$ として次の部分集合

$$HxK := \{hxk \mid h \in H,\ k \in K\}$$

を考えます．これを両側剰余類と呼びます．代表 $x_1, \ldots, x_n \in G$ を選ぶと分割

$$G = Hx_1K \sqcup \cdots \sqcup Hx_nK$$

ができるのは左剰余類のときと同様です．

ひとつの両側剰余類 HxK を更に分割することを考えます．定義から $HxK = \bigcup_{k \in K} Hxk$ ですから，HxK は「右 H 剰余類」Hxk たちの和集合です．異なる (右) 剰余類は共通元を持たないので，いくつかの K の元 $k_1, \ldots, k_r$ を選び出すことで右 H 剰余類への分割

$$HxK = Hxk_1 \sqcup \cdots \sqcup Hxk_r \tag{20.3}$$

ができます．個数 r（x に対して決まるので $r = r_x$ と書く）について調べるために $k, k' \in K$ に対して $Hxk = Hxk'$ が成り立つ条件を調べましょう．

$$Hxk = Hxk' \Longleftrightarrow (xk)(xk')^{-1} = xk(k')^{-1}x^{-1} \in H \Longleftrightarrow k(k')^{-1} \in x^{-1}Hx.$$

これは k と k' が K の部分群 $K \cap x^{-1}Hx$ を法とする同一の右剰余類に属すること[*5]と同値です．したがって $r_x = [K : K \cap x^{-1}Hx]$ がわかりました．

さて，分割 (20.3) に戻ります．各 Hx_iK が r_{x_i} 個の右 H 剰余類に分割されるのですから

$$[G : H] = r_{x_1} + \cdots + r_{x_n}, \quad r_{x_i} = [K : K \cap x_i^{-1}Hx_i] \tag{20.4}$$

が成立します．

20.5 Sylow の定理の証明

(1), (2) の証明：

H をひとつの Sylow p-部分群とします（存在は定理 1 により保証されています）．H の共役であって与えられた p-部分群 P を含むものが存在することを示します．両側分解

$$G = Hx_1P \sqcup \cdots \sqcup Hx_nP$$

を考えます．$r_{x_i} = [P : P \cap x_i^{-1}Hx_i]$ は p-群 P の指数なので $r_{x_i} = p^{e_i}$ $(e_1 \geq 0)$ と書けます．このとき

$$q = [G : H] = p^{e_1} + \cdots + p^{e_n}$$

で q は p で割れませんから，ある e_i がゼロです．すると $r_{x_i} = 1 = [P : P \cap x_i^{-1}Hx_i]$ だから $P \subset x_i^{-1}Hx_i$ がしたがいます．ここでもしも P が p-Sylow 部分群ならば $P = x_i^{-1}Hx_i$ となります．□

(3) の証明の前にすこし準備をします．H を G の部分群とするとき

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

とおいて H の正規化群といいます．定義から $N_G(H)$ は H を正規部分群として含みます．

(3) の証明.

[*5] H を G の部分群とするとき $Hg_1 = Hg_2 \Longleftrightarrow g_1g_2^{-1} \in H$. 証明は左剰余類のときと同様.

H をひとつの Sylow p-部分群とします．すべての Sylow p 部分群は (2) によると gHg^{-1} の形で得られます．$g_1Hg_1^{-1} = g_2Hg_2^{-1}$ が成り立つ条件は $g_1^{-1}g_2 \in N_G(H)$ と同値なので $n_p = [G : N_G(H)]$ という等式が得られます．

さて，$N := H_G(H)$ とおいて両側分解

$$G = Nx_1H \sqcup \cdots \sqcup Nx_nH$$

を考えましょう．$r_{x_i} = [H : H \cap x_i^{-1}Nx_i]$ とおくと $r_{x_i} = p^{e_i}$ $(e_i \geq 0)$ と書けます．等式

$$n_p = [G : N] = p^{e_1} + p^{e_2} + \cdots + p^{e_n}$$

を用います．$x_1 = e$（単位元）とし $Nx_iH \neq NH$ $(2 \leq i \leq n)$ としておきます．まず $r_{x_1} = [H : H \cap N] = 1$ に注意しましょう（$N \supset H$ だから $H \cap N = H$ である）．したがって $e_1 = 0$ で

$$n_p = 1 + p^{e_2} + \cdots + p^{e_n}$$

となるから $e_i \geq 1$ $(i \geq 2)$ を示せばよいことがわかります．

さて，ある $i \geq 2$ に対して $e_i = 0$ だとします．$[H : H \cap x_i^{-1}Nx_i] = 1$ つまり $H = H \cap x_i^{-1}Nx_i$ だから $H \subset x_i^{-1}Nx_i$ となります．これは $x_iHx_i^{-1} \subset N$ と同じことです．

さて H も $x_iHx_i^{-1}$ も，ともに N の p-Sylow 部分群[*6]です．H は $N = N_G(H)$ の正規部分群なので系 1 より $H = x_i^{-1}Hx_i$ がしたがいます．これは $x_i \in N = N_G(H)$ を意味します．このとき $Nx_i = N$ だから $Nx_iH = NH$ となり矛盾します．□

21 共役類と類等式

$x \in G$ に対して $C(x) = \{gxg^{-1} \mid g \in G\}$ を x の共役類といいます．G は有限個の共役類の和に分割されます：

$$G = C(x_1) \sqcup \cdots \sqcup C(x_n)$$

定義から $\#C(x) = 1$ は $x \in Z(G)$ と同値です．だから上の分割をあらためて

$$G = Z(g) \sqcup C(x_1) \sqcup \cdots \sqcup C(x_r) \quad (\#C(x_i) \geq 2)$$

[*6] 共役な部分群の位数は同じ．

と書き直します．$\#C(x_i) = 1$ となる共役類を $Z(G)$ にまとめたのです．これから類等式と呼ばれる有用な等式

$$\#G = \#Z(G) + \sum_{i=1}^{r} \#C(x_i)$$

が得られます．

$x \in G$ に対して $Z_G(x) := \{g \in G \mid gxg^{-1} = x\}$ を x の中心化群と呼びます．

命題 13 $\#C(x) = [G : Z_G(x)]$.

（証明）G から $C(x)$ への写像 f を $g \mapsto gxg^{-1}$ と定めます．定義から f は全射です．$y \in C(x)$ の f によるファイバー $f^{-1}(y)$ を考えましょう．$y = g_0 x g_0^{-1}$ としておきます．

$$g \in f^{-1}(y) \Longleftrightarrow gxg^{-1} = y \Longleftrightarrow gxg^{-1} = g_0 x g_0^{-1} \Longleftrightarrow g_0^{-1} g x (g_0^{-1} g)^{-1} = x$$

となるので，これは $g_0^{-1} g \in Z_G(x)$ と同値です．これは更に $g \in g_0 Z_G(x)$ とも同値です．つまり $f^{-1}(y) = g_0 Z_G(x)$ がわかりました．以上により $G/Z_G(x)$（左 $Z_G(x)$ 剰余類の集合）が $C(x)$ と全単射になっていることがわかりました．したがって $\#C(x) = [G : Z_G(x)]$ が成立します．□

（補題 1 の証明）類等式 $\#G = \#Z(G) + \sum_{i=1}^{r} \#C(x_i)$ を用います．命題 13 より $\#C(x_i) = [G : Z_G(x_i)]$ が成り立ちますが，$\#C(x_i) \geq 2$ なので $Z_G(x_i) \neq G$ です．補題の仮定[*7]より $\#C(x_i) = [G : Z_G(x_i)]$ はすべて p で割り切れます．$\#G$ も p で割り切れるので $\#Z(G)$ で割り切れることがしたがいます．□

[*7] 真部分群の指数は p で割り切れる．

22 Sylow の定理の応用

22.1 有限群論でよく使われること

Sylow の定理の応用を述べる前に，有限群論でよく用いられる命題を列挙しておきます．

命題 14 G の位数が素数 p ならば G は巡回群 C_p と同型である．

（証明）$a \neq e$ である元 a を選ぶ．$f : \mathbb{Z} \to G$ を $n \mapsto a^n$ により定める．G の部分群 $\mathrm{Im}(f)$ は a を含むから $\{e\}$ ではない．位数 $\#\mathrm{Im}(f)$ は Lagrange の定理より p の約数だが $\#\mathrm{Im}(f) \neq 1$ なので，p が素数であることから $\#\mathrm{Im}(f) = p$ である．したがって $\mathrm{Im}(f) = G$ である（つまり f は全射）．準同型定理より $\mathbb{Z}/\mathrm{Ker}(f) \cong G$ となる．$\mathrm{Ker}(f)$ は $\mathbb{Z}$ の部分群なので $\{0\}$ もしくは $m\mathbb{Z}\ (m > 0)$ [*8]である．$\mathrm{Ker}(f) = \{0\}$ ならば $\mathbb{Z} \cong G$ となっておかしい（G の位数は有限）．$\mathrm{Ker}(f) = m\mathbb{Z}\ (m > 0)$ となるが，位数の比較により $m = p$ である．よって $G \cong \mathbb{Z}/p\mathbb{Z} \cong C_p$ が示された．□

命題 15 指数 2 の部分群は正規部分群である．

（証明）H に属さない $g \in G$ を任意に選ぶとき，左剰余類への分割 $G = H \sqcup gH$ ができる．一方，右剰余類への分割 $G = H \sqcup Hg$ ができる．これは $gH = Hg$ を意味する．両辺に右から g^{-1} をかけて $gHg^{-1} = H$ がしたがう．□

Sylow の定理を使うときに次の事実にも気をつけると便利です．

命題 16 $\#G = p^r \cdot q$（$r \geq 1$, q は p で割れない）とする．Sylow p-部分群の個数 n_p は q の約数である．

（証明）ある Sylow p-部分群 H を選ぶと $n_p = [G : N_G(H)]$ と与えられます．$N_G(H) \subset H$ なので

$$[G : H] = \frac{\#G}{\#H} = \frac{\#G}{\#N_G(H)} \cdot \frac{\#N_G(H)}{\#H} = [G : N_G(H)][N_G(H) : H]$$

である．よって $n_p = [G : N_G(H)]$ は $q = [G : H]$ の約数である．□

[*8] §11. $\mathbb{Z}$ の部分群と剰余群，命題.

類等式の応用として示される次の事実は p-群を扱うときの基本事項です．次の 2 つの命題を読み飛ばしても §22.2 Sylow の定理の応用例を読むには差し支えありません．

命題 17 p を素数とする．p-群 G の中心 $Z(G)$ は自明群 $\{e\}$ ではない．

（証明）類等式 $\#G = \#Z(G) + \sum_{i=1}^{r} \#C(x_i)$ を用います．ここで $C(x_1), \ldots, C(x_r)$ は $\#C(x_i) \geq 2$ である共役類です．共役類の元の個数は $\#G$ の約数[*9] なので $C(x_i)$ は p で割り切れます．類等式により $\#Z(G)$ が p で割り切れることがわかります．だから $Z(G)$ は $\{e\}$ ではありません．□

次のことは前命題の簡単な応用で，群論を学んだひとの常識のひとつです．

命題 18 p を素数とする．位数が p^2 の群はアーベル群である．

（証明）命題 17 より $\#Z(G)$ は p または p^2 である．$\#Z(G) = p^2$ なら $G = Z(G)$ であるから G はアーベル群である．$\#Z(G) = p$ の場合は $Z(G) \cong C_p$ となる．$Z(G)$ は正規部分群である．剰余群 $G/Z(G)$ の位数は p だから $G/Z(G) \cong C_p$ である．$G/Z(G)$ の生成元 $aZ(G)$ $(a \in G)$ を選ぶ．$G = Z(G) \sqcup aZ(G) \sqcup \cdots \sqcup a^{p-1}Z(G)$ （$a^p \in Z(G)$） と剰余類分割できる．特に G は $Z(G) \cup \{a\}$ で生成される．$Z(G)$ の任意の元は a と可換なので G はアーベル群である．□

22.2 Sylow の定理の応用例

Sylow の定理の応用例をふたつ挙げます．

命題 19 位数が 15 の群 G は C_{15} と同型である．

（証明）$\#G = 3 \cdot 5$ と素因数分解する．Sylow の定理より Sylow 3-部分群 H と Sylow 5-部分群 K が存在する．H, K はともに素数位数なので巡回群と同型[*10]である．つまり $H \cong C_3$, $K \cong C_5$ である．Sylow 3-部分群の個数 n_3 は $[G : H] = 5$ の約数[*11]であって，Sylow の定理より法 3 で 1 と合同なので $n_3 = 1$ である．よって H は正規部分群である．同様に，Sylow 5-部分群の個数 n_5 は $[G : K] = 3$ の約数[*12]であって，Sylow の定理より法 5 で 1 と合同なので $n_5 = 1$ である．よって K は正規部分群である．

[*9] §21. 共役類と類等式, 命題 $\#C(x) = [G : Z_G(x)]$
[*10] 命題 14
[*11] 命題 16
[*12] 命題 16

G に位数が 15 の元が存在することを示す．G の元の位数は 15 の約数なので $1, 3, 5, 15$ のいずれかである．H は位数 3 の元を 2 つふくむ．H は唯一の Sylow 3-部分群なので，G に含まれる位数 3 の元はこれですべてである．K は位数 5 の元を 4 つ含む．K は唯一の Sylow 5-部分群なので，G に含まれる位数 5 の元はこれですべてである．つまり位数 $1, 3, 5$ の元がそれぞれ $1, 2, 4$ 個である．$1 + 2 + 4 = 7$ は $\#G$ よりも少ないので G には位数 15 の元が少なくともひとつ存在する（実際には $15 - 7 = 8$ 個）．したがって G は巡回群 C_{15} と同型である．□

命題 20 位数が 6 の群 G は C_6 もしくは S_3 と同型である．

（証明）$\#G = 2 \cdot 3$ と素因数分解する．Sylow の定理より Sylow 2-部分群 H と Sylow 3-部分群 K が存在する．H, K はともに素数位数なので巡回群と同型[*13]である．つまり $H \cong C_2$, $K \cong C_3$ である．K は指数 2 なので G の正規部分群[*14]である．K のひとつの生成元を a として $K = \{e, a, a^2\}$ $(a^3 = e)$ とする．G を K に関して剰余類分割して $G = K \sqcup bK$ とする．特に G は a, b で生成される．$b \notin K$ であって $b \neq e$ だから $H = \{e, b\}$ $(b^2 = e)$ であることがわかる．

さて K は正規部分群なので $bab^{-1} \in K$ である．もしも $bab^{-1} = e$ ならば $a = e$ となる．だから $bab^{-1} = a$ または $bab^{-1} = a^2$ である．もしも $bab^{-1} = a$ ならば $ab = ba$ なので，G はアーベル群である（G は a, b で生成される）．このとき ab の位数は $2 \cdot 3 = 6$ である[*15]．これより $x = ab$ とおくと $G = \{e, x, x^2, \ldots, x^5\}$ $(x^6 = e)$ つまり $G \cong C_6$ である．もしも $bab^{-1} = a^2$ ならば a, b のみたす関係式は D_3 を定める関係式と同じなので $G \cong D_3 \cong S_3$ である．□

23 復習の要点

代数学 I の定期試験は以下の問題とほぼ同じ形式で出題します（ただし Standard は選択問題）．終了直後に試験の解答例を配布しますので復習に役立ててください．代数学演習 I の定期試験は代数学 I と同じ形式で（ただし Basic のみ）出題します．

[*13] 命題 14

[*14] 命題 15

[*15] $(ab)^k = a^k b^k$ に注意して計算すればわかる．$(ab)^2 = a^2b^2 = a^2$, $(ab)^3 = a^3b^3 = b$, $(ab)^4 = a^4b^4 = a$, $(ab)^5 = a^5b^5 = a^2b, (ab)^6 = a^3b^3 = e$. 一般に $ab = ba$ であって a, b の位数を m, n とするとき，m と n が互いに素ならば ab の位数は mn である．

Basic（7/21 の講義で解説するので各自で解いて来てください）

1. S_4 の部分群 $H = \{e, (123), (132)\}$ が正規部分群でないことを示せ.

2. 位数 24 のアーベル群の単因子型を列挙せよ.
ヒント：$24 = e_1 \cdots e_r$ であって $e_i \geq 2,\ e_i | e_{i+1}\ (i = 1, \ldots, r-1)$ となるような $(e_1, \ldots, e_r)$ をすべて求める.

3. 次の整数行列の単因子を求めよ.

$$\begin{pmatrix} 7 & -3 & 6 \\ 12 & 3 & 12 \\ 13 & -3 & 12 \end{pmatrix}.$$

4. D_6 の次の部分集合について（ア）正規部分群であるもの（イ）部分群であるが正規部分群でないもの（ウ）部分群でないもののいずれにあてはまるか答えよ.
(1) $\{e, b\}$, (2) $\{e, a^3, b, a^3b\}$, (3) $\{a, b\}$, (4) $\{e, a^2, b, a^4b\}$, (5) $\{e, ab\}$, (6) $\{e, b, ab\}$, (7) $\{e, a^2, a^4\}$, (8) $\{e, a^2, a^4, b, a^2b, a^4b\}$, (9) $\{e, a^2, a^3, b, ab\}$, (10) $\{e, a^3\}$.

5. 以下をすべて求めよ．(1) D_5 の Sylow 5-部分群, (2) D_5 の Sylow 2-部分群, (3) A_4 の Sylow 3-部分群, (4) A_4 の Sylow 2-部分群, (5) S_4 の Sylow 3-部分群.

6. 位数が 33 の Sylow 部分群はすべて正規部分群であることを示せ.

Standard

1. H が正規部分群であるとする．$g_1H = g_1'H,\ g_2H = g_2'H$ ならば $g_1g_2H = g_1'g_2'H$ が成り立つことを示せ.

2. $f : G \to G'$ を準同型写像とする．$\mathrm{Ker}(f)$ が G の正規部分群であることを示せ.

3. H を G の部分群とする．$g \in G$ に対して $H' := gHg^{-1}$ とおく．H' が G の部分群であることを示せ.

4. 素数を位数に持つ有限群は巡回群であることを示せ.

5. G を有限群，H をその部分群とする．$[G : H] = 2$ ならば H は正規部分群である．これを示せ.

質問可能時間（予定）: 7/20（月）: 10:00-18:00, 7/21（火）: 10:00-12:00, 7/22（水）: 10:00-14:00, 7/23（木）: 10:00-12:00, 7/26（月）: 10:00-18:00

急な用ができる場合もあります．確認は ike@xmath.ous.ac.jp まで．

24 参考文献

代数学一般の入門書としては「代数入門」堀田良之（裳華房）あるいは「入門代数学」三宅敏恒（培風館）をすすめます．今回の講義でこの他に特に参考にしたのは「群論の基礎」永尾汎（朝倉書店）です．

代数幾何学の入門書としては「代数幾何学講義」D. マンフォード (シュプリンガー数学クラシックス) をすすめます．整数論は「数論序説」小野孝（裳華房）がとても良いですが難しいです（私もまだはじめのほうしか読んでいない）．もうすこし敷居の低い本として「数論入門」山本芳彦（岩波書店）を挙げておきます．必ずしも代数学とは言い切れないのですが群の表現論と呼ばれる分野への入門として「加群十話」堀田良之（朝倉書店）も手にとってみて欲しい本です．

代数幾何学，整数論ともに環論の知識は欠かせません．環論の入門書としては「可換代数入門」M.F. Atiyah, L.G. MacDonald（共立出版）が最善です．

演算の数理のような内容が好きな人には「なっとくするオイラーとフェルマー」小林昭七（講談社）をすすめます．読み物としては「素数の音楽」マーカス・デュ・ソートイ（新潮クレストブックス）や「フェルマーの最終定理」サイモン・シン（新潮文庫）が面白いです．もっと教科書的なものがよければ「初等整数論入門」楫元（培風館）がいいです．「はじめての数論」ジョセフ・H. シルヴァーマン（ピアソンエデュケーション）も素晴らしい本です．

「怠け数学者の記」小平邦彦 (岩波現代文庫) は一流の数学者の生き方や思想がわかって面白いです．私は学生の頃から何度読み返したかわからない．

本格的な数学の本は一年かけて通読できればよいほうです．なかなか読めなくてもあせらないでいいですよ．仲間を集めて一緒に読むのもいいです．しかし，やはりある程度以上のレベルの本は先生に指導してもらいながら読むものです．

代数学 I 定期試験 2010 年 7 月 28 日実施

1. S_4 の部分群 $H = \{e, (123), (132)\}$ が正規部分群でないことを示せ.

2. 以下の位数のアーベル群の単因子型を列挙せよ.
(1) 24　　(2) 225　　(3) 243

3. 次の整数行列の単因子を求めよ.

$$\begin{pmatrix} 38 & -4 & 36 \\ -12 & 2 & -12 \\ 25 & -2 & 24 \end{pmatrix}.$$

4. D_6 の次の部分集合について（ア）正規部分群であるもの（イ）部分群であるが正規部分群でないもの（ウ）部分群でないもののいずれにあてはまるか答えよ．**解答は答えだけでよい．** (1) $\{e, b\}$ (2) $\{e, a^3\}$ (3) $\{a, b\}$ (4) $\{e, ab\}$ (5) $\{e, a^2, a^4\}$ (6) $\{e, a^2, a^4, b, a^2b, a^4b\}$ (7) $\{e, a^2, a^3, b, ab\}$ (8) $\{e, a^3, b, a^3b\}$

5. 以下をすべて求めよ．**答えだけでなく，必要な説明を書いてください．**
(1) D_5 の Sylow 5-部分群 (2) D_5 の Sylow 2-部分群 (3) A_4 の Sylow 3-部分群 (4) A_4 の Sylow 2-部分群 (5) S_4 の Sylow 3-部分群 (6) D_6 の Sylow 2-部分群 (7) D_6 の Sylow 3-部分群

6. 位数が 33 の Sylow 部分群はすべて正規部分群であることを示せ.

以下の問題から 3 題以上を選んで解答せよ.

A. H は群 G の正規部分群であるとする．$g_1H = g_1'H$, $g_2H = g_2'H$ ならば $g_1g_2H = g_1'g_2'H$ が成り立つことを示せ.

B. $f : G \to G'$ を準同型写像とする．$\mathrm{Ker}(f)$ が G の正規部分群であることを示せ.

C. H を G の部分群とする．$g \in G$ に対して $H' := gHg^{-1}$ とおく．H' が G の部分群であることを示せ.

D. 素数を位数に持つ有限群は巡回群であることを示せ.

E. G を有限群，H をその部分群とする．$[G : H] = 2$ ならば H は正規部分群である．これを示せ.

1. $(14)(123)(14)^{-1} = (423) \notin H$ なので正規部分群ではない.

2. **(1)** $(2^3 \cdot 3),\ (2, 2^2 \cdot 3),\ (2, 2, 2 \cdot 3)$ **(2)** $(3^2 \cdot 5^2),\ (3, 3 \cdot 5^2),\ (5, 3^2 \cdot 5),\ (3 \cdot 5, 3 \cdot 5)$ **(3)** $(3^5),\ (3^4, 3),\ (3^3, 3, 3),\ (3^3, 3^2),\ (3^2, 3^2, 3),\ (3^2, 3, 3, 3),\ (3, 3, 3, 3, 3)$.

3. $(1, 2, 12)$

4. (1) イ (2) ア (3) ウ (4) イ (5) ア (6) ア (7) ウ (8) イ

5. (1) D_5 の Sylow 5-部分群：C_5 は位数が 5 だから Sylow 5-部分群．これは正規部分群なので Sylow 5-部分群はこのひとつ．(2) D_5 の Sylow 2-部分群：位数 2 の部分群として $\{e, a^i b\}$ $(i = 0, 1, 2, 3, 4)$ が見つかる．$n_2 \equiv 1 \pmod 2$ で $n_2 | 5$ なので $n_2 = 1, 5$ だが，5 個見つかっているわけだから $n_2 = 5$ である．つまりこれらがすべての Sylow 2-部分群である．(3) A_4 の Sylow 3-部分群：位数が 3 の部分群として $\{e, (123), (132)\}$ など 1 文字を動かさないものからなる部分群（正四面体のひとつの頂点を通る軸の回転）が全部で 4 つある．つまり上記の他に $\{e, (134), (143)\}, \{e, (124), (142)\}, \{e, (234), (243)\}$ がある．$n_3 \equiv 1 \pmod 3$ および $n_3 | 4$ より $n_3 = 1, 4$ だが 4 個見つかったので $n_3 = 4$ である．つまりこれらがすべての Sylow 3-部分群である．(4) A_4 の Sylow 2-部分群：位数が 2^2 の部分群として $\{e, (12)(34), (13)(24), (14)(23)\}$ がある．これは正規部分群である．任意の $\sigma \in A_4$ に対して $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$ となることからわかる．だから，これがただ一つの Sylow 2-部分群である．(5) S_4 の Sylow 3-部分群：問題 (3) で見つけた 4 個の部分群は S_4 の Sylow 3-部分群でもある．$n_3 \equiv 1 \pmod 3$ と $n_3 | 8$ より $n_3 = 1, 4$ にしぼられる．4 個見つかっているから $n_3 = 4$ である．つまりすでに見つけた 4 個がすべての Sylow 3-部分群である．(6) D_6 の Sylow 2-部分群：$n_2 \equiv 1 \pmod 2$ であって n_2 は 3 の約数なので Sylow 2-部分群は 1 個もしくは 3 個．位数が 2^2 の部分群として前問に登場した $H = \{e, a^3, b, a^3 b\}$ がある．これは正規部分群ではない．$aba^{-1} = a^2 b$ などより計算して $aHa^{-1} = \{e, a^3, a^2 b, a^5 b\}$, $a^2 H a^{-2} = \{e, a^3, a^4 b, ab\}$ がわかる．これら 3 個が Sylow 2-部分群である．(7) D_6 の Sylow 3-部分群：位数 3 の部分群として $\{e, a^2, a^4\}$ がある．$ba^2 b = a^4$ などから，これは正規部分群であることがわかる．Sylow 3-部分群はこれひとつだけ.

6. $33 = 3 \cdot 11$ と素因数分解する．Sylow p-部分群がひとつだけならば正規部分群である（H が Sylow p-部分群ならば，その共役 gHg^{-1} も同じ位数だから Sylow p-部分群である．Sylow p-部分群がひとつしかなければ $gHg^{-1} = H$ となる）．Sylow 3-部分群について：$n_3 \equiv 1 \pmod 3$ および $n_3 | 11$ より $n_3 = 1$ となる．つまり Sylow 3-部分群はただひとつ．および Sylow 11 部分群について：$n_{11} \equiv 1 \pmod{11}$ および $n_{11} | 3$ より $n_{11} = 1$ となる．つまり Sylow 11-部分群はただひとつ.

代数学演習 I 定期試験 2010 年 8 月 4 日実施

1. 以下の位数を持つアーベル群の単因子型を列挙せよ.
(1) 64　　(2) 36

2. 次の整数行列の単因子を求めよ.

$$\begin{pmatrix} 11 & 8 & -18 \\ 14 & 17 & -30 \\ 8 & 8 & -15 \end{pmatrix}$$

3. D_{12} の次の部分集合について（ア）正規部分群であるもの（イ）部分群であるが正規部分群でないもの（ウ）部分群でないもののいずれにあてはまるか答えよ．**解答は答えだけでよい．** (1) $\{e, a^3, a^6, a^9\}$ (2) $\{e, a^3, a^6, a^9, b, a^3b, a^6b, a^9b\}$ (3) $\{e, a^4, a^8\}$ (4) $\{e, a^6\}$ (5) $\{e, ab, a^7b, a^6\}$ (6) $\{e, a^2, b, a^4b\}$

4. S_4 の部分集合 $H = \{e, (12)(34), (13)(24), (14)(23), (1234), (1432), (13), (24)\}$ は部分群である（示さなくてよい）．正規部分群であるかどうか調べよ.

5. 以下をすべて求めよ．**答えだけでなく，必要な説明を書いてください．**
(1) D_7 の Sylow 7-部分群
(2) D_7 の Sylow 2-部分群
(3) A_4 の Sylow 3-部分群
(4) A_4 の Sylow 2-部分群
(5) D_6 の Sylow 2-部分群
(6) D_6 の Sylow 3-部分群
(7) D_{10} の Sylow 5-部分群
(8) D_{12} の Sylow 2-部分群
(9) D_{12} の Sylow 3-部分群
(10) S_4 の Sylow 2-部分群

6. G は位数が 15 の群であるとする．G の Sylow 3-部分群は何個存在するか？

1. **(1)** $64 = 2^6$ なので $(2^6), (2^5, 2), (2^4, 2^2), (2^4, 2, 2), (2^3, 2^3), (2^3, 2^2, 2), (2^3, 2, 2, 2), (2^2, 2^2, 2^2), (2^2, 2^2, 2, 2), (2^2, 2, 2, 2, 2), (2, 2, 2, 2, 2, 2)$ の 11 通り．**(2)** $36 = 2^2 \cdot 3^2$ なので $(2^2 \cdot 3^2), (2, 2 \cdot 3^2), (2 \cdot 3, 2 \cdot 3), (3, 2^2 \cdot 3)$ の 4 通り．

2. $(1, 3, 9)$.

3. (1) ア $\{e, a^3, a^6, a^9\}$：部分群である．$ba^3b = a^9$, $ba^6b = a^3$, $ba^9b = a^3$ などから正規部分群であることがわかる．(2) イ $\{e, a^3, a^6, a^9, b, a^3b, a^6b, a^9b\}$：部分群である．例えば $aba^{-1} = a^2b$ はこの部分群に属さないから正規部分群ではない．(3) ア $\{e, a^4, a^8\}$：部分群である．$ba^4b = a^8$, $ba^8b = a^4$ などから正規部分群であることがわかる．(4) ア $\{e, a^6\}$：$(a^6)^2 = e$ から部分群であることがわかる．$ba^6b = a^6$ から正規部分群であることがわかる．(5) イ $\{e, ab, a^7b, a^6\}$：部分群である．例えば $b(ab)b = a^{11}b$ だから正規部分群ではない．(6) ウ $\{e, a^2, b, a^4b\}$：部分群ではない．例えば a^2 と b の積 a^2b はこの集合に属さない．

4. 正規部分群ではない．例えば $(12)(13)(12) = (23) \notin H$ などからわかる．

5. (1) $\#D_7 = 2 \cdot 7$ なので Sylow 7 部分群とは位数 7 の部分群のこと．C_7 がある．これは正規部分群（指数が 2）なのでこれでおしまい．(2) Sylow 2-部分群とは位数が 2 の部分群のこと．$\{e, a^ib\}$ $(0 \leq i \leq 6)$ の 7 個がある．n_2 は 7 の約数であって，2 で割ると 1 余る数なので 1 あるいは 7 である．7 個あるので，これ以上はなくて Sylow 2-部分群がすべて求まった．(3)〜(6) は代数学 I の試験と同じ．(7) $\#D_{10} = 20 = 2^2 \cdot 5$ だから Sylow 5-部分群とは位数が 5 の部分群である．n_5 は 2^2 の約数であって，5 で割ると 1 余る数だから $n_5 = 1$ である．ひとつ見つければよい．$\{e, a^2, a^4, a^6, a^8\}$ に気がつくでしょう．ちなみにこれが正規部分群であることはすぐに確認できる．(8) D_{12} の Sylow 2-部分群：$\#D_{12} = 24 = 2^3 \cdot 3$ だから Sylow 2-部分群とは位数が 2^3 の部分群である．n_2 は 3 の約数で 2 で割って 1 余るから 1 または 3 である．問題 **3** (2) より $H = \{e, a^3, a^6, a^9, b, a^3b, a^6b, a^9b\}$ という Sylow 2-部分群がひとつあることがわかる．上で調べたように正規部分群ではないので，H と共役な部分群を求めればよい．$aHa^{-1} = \{e, a^3, a^6, a^9, a^2b, a^5b, a^8b, a^{11}b\}$, $a^2Ha^{-2} = \{e, a^3, a^6, a^9, a^4b, a^7b, a^{10}b, ab\}$ (9) D_{12} の Sylow 3-部分群：問題 **3** (3) より位数 3 の正規部分群 $\{e, a^4, a^8\}$ がある．これが Sylow 3-部分群．(10) 問題 **4** の群 H は位数が $8 = 2^3$ なので Sylow 2-部分群である．すでに調べたように，これは正規部分群ではない．n_2 は 3 の約数で奇数だから 1 または 3 である．H が正規でないということは $n_2 = 3$ である．H の共役が H 以外に 2 つあるはず．実際 $H' = \{e, (12)(34), (13)(24), (14)(23), (1243), (1342), (14), (23)\} = (34)H(34)$ と $H'' = \{e, (12)(34), (13)(24), (14)(23), (1324), (1423), (12), (34)\} = (23)H(23)$ が見つかる．

6. $\#G = 3 \cdot 5$ なので Sylow 3-部分群の個数 n_3 は 5 の約数（つまり 1 か 5）で 3 で割って 1 余るから，$n_3 = 1$ である．つまり 1 個.

“I do not know what I may appear to the world, but to myself I seem to have been only like a boy playing on the sea-shore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me.” (Isaac Newton)