代数学 I 講義ノート

安藤哲哉

注意: 校正をあまりきちんとしていないので，誤植等に注意して利用して下さい．

1. 二項演算

定義 1.1. A は空でない集合とする．写像 $f\colon A \times A \longrightarrow A$ を (**二項**) **演算**という．演算は $f(x, y)$ ($x, y \in A$) と書く代わりに，適当な特定の文字，例えば $+, \times, *$ などを用いて，$x + y$, $x \times y$, $x * y$ などと書かれる．演算を表す文字には，いろいろな歴史的由来があり，$+$ という文字で表わされる演算を**加法**とか**足し算**, $\times$ という文字で表わされる演算を**積**とか**乗法**とか**掛け算**と呼ぶことが多い．演算 $\times$ については，$x \times y$ を $x \cdot y$ とか，単に xy と表すことが多い．

この講義ではしばらくの間，説明のため，A 上に二項演算 $*$ が定義されているとして話をする．

(1) 任意の $x, y, z \in A$ に対し $(x * y) * z = x * (y * z)$, つまり $f\big(f(x, y), z\big) = f\big(f(x, f(y, z)\big)$ が成り立つとき，演算 $*$ は**結合法則**を満たすという．

(2) 任意の $x, y \in A$ に対し $y * x = x * y$, つまり $f(y, x) = f(x, y)$ が成り立つとき，演算 $*$ は**交換法則**と満たすという．

定理 1.2. 集合 A 上に二項演算 $*$ が定まっているとする．$x_1, x_2, \ldots, x_n \in A$ とする．

(1) $*$ が結合法則を満たせば，

$$((x_1 * x_2) * x_3) * x_4 = (x_1 * x_2) * (x_3 * x_4) = x_1 * ((x_2 * x_3) * x_4) = x_1 * (x_2 * (x_3 * x_4))$$

のように，演算の順序によらずに値が定まる．そこで，この演算の値を $x_1 * x_2 * x_3 * x_4$ と括弧を用いずに表す．5 個以上の A の元についての演算も同様である．

(2) 交換法則が成り立てば，σ が $1, 2, \ldots, n$ の任意の置換のとき，

$$x_{\sigma(1)} * x_{\sigma(2)} * \cdots * x_{\sigma(n)} = x_1 * x_2 * \cdots * x_n$$

が成り立つ．つまり，演算の順序に依存しない．

証明. (1), (2) ともに n に関する帰納法で証明できる． □

定義 1.3. (1) 集合 A 上に二項演算 $*$ が定義されていて，結合法則を満たすとき，集合 A は演算 $*$ について**半群**であるとか，$(A, *)$ は**半群**であるという．

(2) 集合 A 上に二項演算 $*$ が定義されていて，結合法則と交換法則を満たすとき，集合 A は演算 $*$ について**可換半群**であるとか，$(A, *)$ は**可換半群**であるという．

(3) $(A, *)$ は半群であるとする．もし，$e \in A$ が任意の $x \in A$ に対して $e * x = x$ かつ $x * e = x$ を満たすとき，e は演算 $*$ に関する A の**単位元**であるという．演算 $*$ が乗法 $\times$ の場合には，単位元 e を 1 という記号で書くことが多い．また，演算 $*$ が加法 $+$ の場合には，単位元 e を 0 という記号で書き，**零元**とか**ゼロ**ということが多い．

定理 1.4. $(A, *)$ は半群で，$e_1 \in A$ も $e_2 \in A$ も単位元であるとする．すると $e_1 = e_2$ となる．つまり，単位元は存在すれば一意的 (ただひとつ) である．

証明. e_1 は単位元なので，$e_1 * e_2 = e_2$ を満たす．e_2 は単位元なので，$e_1 * e_2 = e_1$ を満たす．よって，$e_1 = e_2$ である． □

定義 1.5. $(A, *)$ は半群で，単位元 $e \in A$ を持つとする．$x \in A$ に対し，$x * y = e$ かつ $y * x = e$ を満たす元 $y \in A$ が存在するとき，y は x の**逆元**であるという．演算 $*$ が加法 $+$ の場合には，x の逆元を $-x$ と書くことが多い．演算 $*$ が乗法 $\times$ の場合には，x の逆元を x^{-1} と書くことが多い．演算 $*$ が乗法 $\times$ で $*$ が交換法則を満たす場合には，x の逆元 x^{-1} を $1/x$ とか $\dfrac{1}{x}$ と書くこともある (乗法が定義されている A による)．

定理 1.6. $(A, *)$ は半群で，単位元 $e \in A$ を持つとする．$x \in A$ に対し，$y_1 \in A$ と $y_2 \in A$ が x の逆元ならば，$y_1 = y_2$ である．つまり，x の逆元が存在する場合，それは一意的である．

証明. $x * y_1 = e$ より $y_2 * (x * y_1) = y_2 * e = y_2$ である．結合法則と $y_2 * x = e$ より，$y_2 * (x * y_1) = (y_2 * x) * y_1 = e * y_1 = y_1$ である．よって，$y_1 = y_2$ である． □

ここで群 (Group) を定義するが，集合 A の代わりに Group の先頭の文字 G を用いて，集合 G を使うのが慣習である．

定義 1.7. $(G, *)$ は半群で，単位元 $e \in A$ を持つとする．また，任意の $x \in G$ に対してその逆元が存在すると仮定する．このとき，G は演算 $*$ について**群**であるとか，$(G, *)$ は**群**であるという．x の演算 $*$ に関する逆元は x^{-1} という記号で表すことにする．

$(G, *)$ が群で，演算 $*$ が G 上で交換法則を満たすとき，G は**アーベル群** (Abelian group) であるか**可換群** (commutative group) であるという．

$(G, *)$ が群で，G が有限集合であるとき，$(G, *)$ は**有限群**であるという．このとき，G の元の個数を $|G|$ とか $\#G$ などと書き，有限群 G の**位数**という．集合 A の元の個数 (や濃度) は $\#A$ で表すことが多いが，有限群 G の位数 (元の個数) は $|G|$ で表すことが多い．

$(G, *)$ が群で，G が無限集合であるとき，$(G, *)$ は**無限群**であるという．

例 1.8. (1) $\mathbb{Z}$ は整数全体の集合，$\mathbb{Q}$ は有理数全体の集合，$\mathbb{R}$ は実数全体の集合，$\mathbb{C}$ は複素数数全体の集合とする．$\mathbb{Z}$ も $\mathbb{Q}$ も $\mathbb{R}$ も $\mathbb{C}$ も加法 $+$ についてアーベル群である．

(2) $\mathbb{Q}^\times := \mathbb{Q} - \{0\}$ ($\mathbb{Q}$ から 0 を除いた集合), $\mathbb{R}^\times := \mathbb{R} - \{0\}$, $\mathbb{C}^\times := \mathbb{C} - \{0\}$ とする．$\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ は乗法 $\times$ についてアーベル群である．

(3) K は $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ のいずれかとして，K の元を成分とする n 次正方行列全体の集合を $M_n(K)$ とする．$M_n(K)$ は行列の和を演算としてアーベル群になる．単位元はゼロ行列である．

(4) K は同上とし，$\mathrm{GL}(n, K) = \{A \in M_n(K) \mid \det A \neq 0\}$ とおく．$\mathrm{GL}(n, K)$ は行列の積を演算として群になる．単位元は単位行列で，$A \in \mathrm{GL}(n, K)$ の逆元は A の逆行列 A^{-1} である．$n \geqq 2$ のとき $\mathrm{GL}(n, K)$ はアーベル群にはならない．$\mathrm{GL}(n, K)$ を K 上の**一般線形群**という．

(5) $n \in \mathbb{N}$ ($\mathbb{N} = \{1, 2, 3, \ldots\}$ は自然数全体の集合), $X_n := \{1, 2, \ldots, n\}$ とし，

$$\mathfrak{S}_n := \{\sigma : X_n \to X_n \mid \sigma \text{ は全単射}\}$$

とおく．$\mathfrak{S}_n$ は写像の合成 $\circ$ を演算として群になる．単位元は恒等写像で，$\sigma \in \mathfrak{S}_n$ の逆元は σ の逆写像 σ^{-1} である．$\mathfrak{S}_n$ を n 次**対称群**という．$\mathfrak{S}_n$ の元を n 次の**置換**という．$\mathfrak{S}_n$ は位数 $n!$ の有限群である．なお，$\mathfrak{S}$ という文字は S のドイツ亀の甲文字である．書きにくいので，$\mathfrak{S}_n$ を S_n と書く人も多い．ただ，S_n という記号は他にもいろな意味で使う．

定理 1.9. $(G, *)$ は群であるとし，$a \in A$ の逆元を a^{-1} と書くことにする．$a_1, \ldots, a_n \in G$ のとき，

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$$

が成り立つ．

証明. $(ab)^{-1} = b^{-1}a^{-1}$ を示せば，あとは n に関する帰納法で簡単に証明できる．$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1} \cdot e \cdot b = b^{-1}b = e$, $(ab)(b^{-1}a^{-1})(ab) = a(bb^{-1})a^{-1} = aa^{-1} = e$ より，逆元の一意性から，$(ab)^{-1} = b^{-1}a^{-1}$ となる． □

2. 部分群

定義&定理 2.1. $(G, *)$ は群であるとする．空でない部分集合 $H \subset G$ に対し．

(1) $x \in H, y \in H$ ならば $x * y \in H$

が成り立つとき，H は演算 $*$ について**閉じている**という．今，$H \subset G$ は演算 $*$ について閉じていて，

(2) $x \in H$ ならば $x^{-1} \in H$

を満たすとする．このとき H は G の**部分群**であるという．H が演算 $*$ について群になることを以下に証明しておく．また，G がアーベル群ならば H もアーベル群である．

証明. $*$ は G の元について結合法則を満たすので，H の元についても結合法則を満たす．$x \in H$ を取るとき，(2) より $x^{-1} \in H$ で，(1) より $e = x * x^{-1} \in H$ となる．(2) をあわせると，H が群であることがわかる．

また，G がアーベル群ならば，H の元についても交換法則が成り立つので，H もアーベル群である．□

定義&定理 2.2. $(G, *)$ は群で $X \subset G$ は空でない部分集合とする．

$$\mathfrak{H} := \{H \mid H \text{ は } G \text{ の部分群で } X \subset G\}$$

とおく．$G \in \mathfrak{H}$ だから $\mathfrak{H} \neq \phi$ である．

$$\langle X \rangle := \bigcap_{H \in \mathfrak{H}} H$$

とおく．すると，$\langle X \rangle$ は X を含む最小の G の部分群になる．$\langle X \rangle$ を X で**生成される** G の部分群とか，X を含む最小の G の部分群という．X を $\langle X \rangle$ の**生成系**という．

証明. (1) $\langle X \rangle$ が G の部分群であることを示す．勝手な $x, y \in \langle X \rangle$ を取る．任意の $H \in \mathfrak{H}$ に対して $x, y \in H$ である．H は G の部分群だから $xy \in H$, $x^{-1} \in H$ である．よって $xy \in \langle X \rangle$, $x^{-1} \in \langle X \rangle$ である．

(2) X を含む G の部分群 H があれば $H \in \mathfrak{H}$ であるから，$\langle X \rangle$ の定義から $\langle X \rangle \subset H$ となる．よって，$\langle X \rangle$ は H を含む G の部分群の中で最小のものである．□

今までは説明のために群 G の演算を記号 $*$ を用いて表わしていたが，ここからも $*$ を使い続けると，ちょっと面倒なこともある．そこで，ここからは G の演算は (かならずしも交換法則を満たさない) **積**であるとし，$x, y \in G$ に対する演算結果を xy とか $x \cdot y$ と書く．単位元は e の代わりに 1 と書く．また，$n \in \mathbb{N} \cup \{0\}$ と $x \in G$ に対し，帰納的に

$$x^0 = 1, \qquad x^{n+1} = x \cdot x^n$$

として，x^n を定義する．また，$n \in \mathbb{Z}$, $n < 0$ の場合には，

$$x^n = (x^{-1})^{-n}$$

と定義する．

命題 2.3. G は群で $x \in G$ とする．すると，$m, n \in \mathbb{Z}$ に対して**指数法則**

$$x^{m+n} = x^m \cdot x^n$$
$$x^{-n} = (x^{-1})^n = (x^n)^{-1}$$
$$(x^m)^n = x^{mn}$$

が成り立つ．

証明. $n \geqq 0$ の場合，$x^{m+n} = x^m \cdot x^n$ は n に関する帰納法で証明できる．$(x^n)((x^{-1})^n) = 1$ と $((x^{-1})^n)(x^n) = 1$ を n に関する帰納法で証明すると，$(x^{-1})^n = (x^n)^{-1}$ が分かる．これを利用して，$n < 0$ の場合の $x^{m+n} = x^m \cdot x^n$ と $(x^{-1})^n = (x^n)^{-1}$ を証明する．$(x^m)^n = x^{mn}$ も $n \geqq 0$ の場合に n に関する帰納法で証明して，その後に $n < 0$ の場合に証明する．□

定義 2.4. G は積に関する群で，A, B は G の部分集合とする．このとき，

$$AB := \{ab \in G \mid a \in A, b \in B\}$$
$$A^{-1} := \{a^{-1} \in G \mid a \in A\}$$

と書く．AB を $A \cdot B$ と書くこともある．$A = \{a\}$ のときは $\{a\}B$ を aB とも書き，$B\{a\}$ を Ba とも書く．aB を $a \cdot B$, Ba を $B \cdot a$ とも書く．

$C \subset G$ のとき，$(AB)C = A(BC)$ が成り立つことは，群の結合法則からすぐわかる．そこで，これを単に ABC と書く．4 個以上の場合も同様.

A と B が G の部分群でも AB は群になるとは限らない．しかし，A が G の部分群ならば $A^{-1} = A$ であり，$AA = A$ である．H が G の部分群で $a \in G$ のとき，Ha を**右剰余類**, aH を**左剰余類**という．

群 G の演算が $*$ ならば AB, aB, Ba を $A * B$, $a * B$, $B * a$ と書く．特に加法 $+$ が演算の場合は，$A + B$, $a + B$, $B + a$ と書く．

命題 2.5. G は群, H は G の部分群 $a, b \in G$ とする．このとき，以下が成り立つ．

(1) $Ha = H \iff a \in H \iff aH = H$.
(2) $Ha = Hb \iff ab^{-1} \in H$.
(2') $aH = bH \iff a^{-1}b \in H$.
(3) $Ha \neq Hb \Longrightarrow Ha \cap Hb = \phi$.
(3') $aH \neq bH \Longrightarrow aH \cap bH = \phi$.
(4) $Ha \cap Hb = \phi \iff ab^{-1} \notin H$.
(4') $aH \cap bH = \phi \iff a^{-1}b \notin H$.
(5) $(Ha)^{-1} = a^{-1}H$.
(6) $Ha = Hb \iff a^{-1}H = b^{-1}H$.

証明. 一般に，Ha, aH の定義と群の結合法則から，$(Ha)b = H(ab)$, $b(aH) = (ba)H$ が成り立つ．

(1) $Ha = H$ ならば $a = 1 \cdot a \in Ha = H$ である．逆に $a \in H$ とする．Ha の元は ha $(\exists h \in H)$ と書けるが，$ha \in H$ なので $Ha \subset H$ である．勝手な $h \in H$ に対し，$ha^{-1} \in H$ より $h = (ha^{-1})a \in Ha$ なので $H \subset Ha$ である．

$aH = H \iff a \in H$ の証明も同様である．よって，(1) が成り立つ．

(2) $Ha = Hb \iff H(ab^{-1}) = (Ha)b^{-1} = (Hb)b^{-1} = H(bb^{-1}) = H \cdot 1 = H \iff ab^{-1} \in H$. (2') の証明も同様である．

(3) $\exists c \in Ha \cap Hb \neq \phi$ と仮定する．すると，ある $h_1, h_2 \in H$ により $c = h_1 a = h_2 b$ と書ける．任意の $h \in H$ に対し，$ha = (hh_1^{-1}h_2)b \in Hb$ となる．よって，$Ha \subset Hb$ である．対称性から $Hb \subset Ha$ もわかるので，$Ha = Hb$ となる．(3') の証明も同様である．

(4) (2) より $ab^{-1} \notin H$ ならば $Ha \neq Hb$ である．(3) より，$Ha \cap Hb = \phi$ となる．逆に，$Ha \cap Hb = \phi$ ならば，$H(ab^{-1}) \cap H = \phi$ である．$ab^{-1} \in H(ab^{-1})$ だから $ab^{-1} \notin H$ である．(4') の証明も同様である．

(5) $(Ha)^{-1}$ の元は，$(ha)^{-1}$ $(\exists h \in H)$ と書ける．$(ha)^{-1} = a^{-1}h^{-1}$ で $h^{-1} \in H$ なので $(ha)^{-1} \in a^{-1}H$ である．よって，$(Ha)^{-1} \subset a^{-1}H$ である．

逆に，$a^{-1}H$ の元は $a^{-1}h$ $(\exists h \in H)$ と書ける．$a^{-1}h = (h^{-1}a)^{-1} \in (Ha)^{-1}$ より，$(Ha)^{-1} \supset a^{-1}H$ である．よって，$(Ha)^{-1} = a^{-1}H$ である． □

(6) は (5) からすぐわかる． □

3. 剰余類

定義 3.1. G は積に関して群であり，H は G の部分群とする．
(1) $a, b \in G$ に対し，「$a \sim b \iff aH = bH$」として G 上に関係 $\sim$ を定めると，これは同値関係である．そこで，$G/H := G/\sim$ と定義する．命題 2.5 より，$a \in G$ のこの同値関係 $\sim$ に関する同値類は aH である．よって，

$$G/H = \{aH \mid a \in G\}$$

である．
(2) 上と同様に，

$$G\backslash H = \{Ha \mid a \in G\}$$

と定義する．

G/H や $G\backslash H$ は群の構造を持つとは限らないことに注意する．

定理&定義 3.2. G, H は上の定義と同様とし，さらに G は有限群であると仮定する．すると，
(1) $\#(G/H) = \#(G\backslash H)$ が成り立つ．
そこで，$[G : H] := \#(G/H) = \#(G\backslash H)$ と定義し，$[G : H]$ を G における H の**指数**と呼ぶ．
(2) $|G| = [G : H] \cdot |H|$ が成り立つ．

証明. $h \in H$ に対して $ah \in aH$ を対応させる写像 $H \to aH$ は全単射なので，$\#(aH) = \#H = |H|$ である．$r = \#(G/H)$ として，ある $a_1, \ldots, a_r \in G$ を選ぶと，命題 2.5 より，$G = a_1H \sqcup \cdots \sqcup a_rH$ となる．よって，$|G| = \#(a_1H) + \cdots + \#(a_rH) = r \cdot |H|$ となる．

同様に，$q = \#(G\backslash H)$ とおくと $|G| = q \cdot |H|$ が証明できるので，$r = q$ である．これで，(1), (2) が証明された． □

定理&定義 3.3. G は積に関して群であり，N は G の部分群とする．このとき以下の (1), (2), (3) は同値である．(1), (2), (3) のいずれか (したがってすべて) が成り立つとき，N は G の**正規部分群** (normal subgroup) であるといい，$N \lhd G$ とか $G \rhd N$ と書く．
(1) 任意の $a \in G$ と任意の $x \in N$ に対して $axa^{-1} \in N$ が成り立つ．
(2) 任意の $a \in G$ に対して $aNa^{-1} = N$ が成り立つ．
(3) 任意の $a \in G$ に対して $aN = Na$ が成り立つ．

証明. (1) $\Longrightarrow$ (2). $a \in G$, $x \in N$ ならば $axa^{-1} \in N$ だから，$aNa^{-1} \subset N$ である．また，$b \in G$ に対して $bNb^{-1} \subset N$ なので，

$$N = 1 \cdot N \cdot 1 = (b^{-1}b)N(b^{-1}b) = b^{-1}(bNb^{-1})b \subset b^{-1}Nb$$

である．ここで，$b = a^{-1}$ とおけば，$N \subset aNa^{-1}$ となる．よって，$aNa^{-1} = N$ である．

(2) $\Longrightarrow$ (1) は自明.

(2) $\Longleftrightarrow$ (3). $aNa^{-1} = N$ ならば $aN = aN \cdot 1 = aN(a^{-1}a) = (aNa^{-1})a = Na$ である．逆に，$aN = Na$ ならば $aNa^{-1} = (aN)a^{-1} = (Na)a^{-1} = N(aa^{-1}) = N \cdot 1 = N$ である． □

定理&定義 3.4. G は積に関して群であり，N は G の正規部分群とする．すると，$G/N = G\backslash H$ も，以下のような G から誘導される自然な演算について群になる．
(演算) $a, b \in G$ に対して $(aN)(bN) = (ab)N \in G/N$. また，$(aN)^{-1} = a^{-1}N \in G$. G/N を G の N による**剰余群**という．

証明. $aN = Na$ より，

$$G/N = \{aN \mid a \in G\} = \{Ha \mid a \in G\} = G\backslash H$$

である．
$NN = N$ はすぐわかる．$(aN)(bN) = a(Nb)N = a(bN)N = (ab)(NN) = (ab)N$, $(aN)^{-1} = Na^{-1} = a^{-1}N$ である．結合法則は，$(aN)(bN)(cN) = ((ab)N)(cN) = (abc)N = (aN)((bc)N) = (aN)(bN)(cN)$ より成り立つ．$(aN)N = a(NN) = aN$, $N(aN) = N(Na) = (NN)a = Na = aN$ より，$N = 1 \cdot N$ が G/N の単位元である．$(aN)(a^{-1}N) = N$, $(a^{-1}N)(aN) = N$ より，$aN \in G/N$ の逆元は $a^{-1}N$ である． □

定理 3.5. G は積に関して群であり，N と N_1 と N_2 は G の正規部分群．H は G の部分群とする．このとき，以下が成り立つ．
(1) $HN = NH$ で HN は G の部分群である．
(2) $H \cap N$ は H の正規部分群である．
(3) N_1N_2 は G の正規部分群である．
(4) $N_1 \cap N_2$ は G の正規部分群である．
(5) G がアーベル群ならば，G の任意の部分群は正規部分群である．

証明. (1) 任意の $h \in N$ に対し $hN = Nh$ であることから，$HN = NH$ はすぐ証明できる．HN が G の部分群であることを示す．HN の勝手なの 2 元 $h_1n_1, h_2n_2 \in HN$ ($h_1, h_2 \in H$; $n_1, n_2 \in N$) を取る．$h_2N = Nh_2$ より，ある $n_3 \in N$ が存在して，$h_2n_2 = n_3h_2$ となる．$(h_1n_1)(h_2n_2) = (h_1n_1)(n_3h_2) = h_1((n_1n_3)h_2)$ である．$(n_1n_3)h_2 \in Nh_2 = h_2N$ なので，ある $n_4 \in N$ が存在して，$(n_1n_3)h_2 = h_2n_4$ となる．よって，$(h_1n_1)(h_2n_2) = h_1(h_2n_4) = (h_1h_2)n_4 \in HN$ である．$(h_1n_1)^{-1} \in HN$ も同様にして証明できる．よって，HN は G の部分群である．

(2) $a, b \in H \cap N$ ならば $ab \in H$ かつ $ab \in N$ なので，$ab \in H \cap N$ である．同様に $a^{-1} \in H \cap N$ である．よって，$H \cap N$ は G の部分群であり，H の部分群でもある．
$a \in H$ のとき，$aH = Ha$ なので $a(H \cap N) = aH \cap aN = Ha \cap Na = (H \cap N)a$ となるので，$H \cap N \lhd H$ である．

(3) (1) より N_1N_2 は G の部分群である．$a \in G$ に対し $a(N_1N_2) = (aN_1)N_2 = (N_1a)N_2 = N_1(aN_2) = N_1(N_2a) = (N_1N_2)a$ より $N_1N_2 \lhd G$ である．

(4) は (2) と同様にして証明できる．

(5) は自明. □

定義 3.6. G は積について群であるとする．$a \in G$ とする．

$$\langle a \rangle := \left\{ a^n \in G \,\middle|\, n \in \mathbb{Z} \right\}$$

を a で生成される**巡回群**という．a を $\{a\}$ の**生成元**という．もし，$\langle a \rangle = G$ ならば，G は**巡回群**であるという．

$a \in \mathbb{N}$ に対し，ある $n \in \mathbb{N}$ が存在して $a^n = 1$ を満たすとする．このとき，$a^n = 1$ を満たす最小の自然数 n を a の**位数**といい，$n = \operatorname{ord} a$ などと表す．$\operatorname{ord} a = \#\langle a \rangle$ であり，$n = \operatorname{ord} a$ とおくと，

$$\langle a \rangle := \left\{ a^i \in G \,\middle|\, i = 0, 1, 2, \ldots, n-1 \right\}$$

となる．$a^n = 1$ となる $n \in \mathbb{N}$ が存在しないとき，$\operatorname{ord} a = \infty$ と書く．

定理 3.7. G は有限群，$a \in G$ とする．
(1) a の位数 $\operatorname{ord} a$ は $|G|$ の約数である．
(2) もし $|G|$ が素数ならば，G は巡回群である．

証明. (1) a で生成される G の部分群 $\langle a \rangle$ の位数が $\operatorname{ord} a$ であった．あとは，定理 3.2(2) からわかる．

(2) $|G| = p$ (素数) とする．$1 \neq a \in G$ を取ると，$\operatorname{ord} a$ は p の約数で 1 でないので，$\operatorname{ord} a = p = |G|$ である．よって，$G = \langle a \rangle$ で，G は巡回群である． □

4. 準同型写像

定義 4.1. G は演算 $*$ に関して群で，H は演算 $\diamond$ 関して群であるとする．写像 $f\colon G \to H$ が任意の $a, b \in G$ に対し，

$$f(a * b) = f(a) \diamond f(b)$$

を満たすとき，f は (群の) **準同型** (**写像**) であるという．$f\colon G \to H$ が準同型写像で全単射であるとき，f は (群の) **同型** (**写像**) であるといい，$f\colon G \xrightarrow{\cong} H$ などと書く．群 G, H に対して，ある同型写像 $f\colon G \xrightarrow{\cong} H$ が存在する場合に G と H は (群として) **同型**であるといい，$G \cong H$ と書く．

命題 4.2. $(G, *)$ と $(H, \diamond)$ は群とし，G と H の単位元を $1_G, 1_H$ と書く．$x \in G, y \in H$ の逆元は x^{-1}, y^{-1} で表す (区別したいが適切な記号がないので)．$f\colon G \to H$ は準同型写像とする．このとき，以下が成り立つ．
(1) $f(1_G) = 1_H$.
(2) $x \in G$ に対し，$f(x^{-1}) = \big(f(x)\big)^{-1}$.
(3) f が全単射ならば，逆写像 $f^{-1}\colon H \to G$ も準同型写像である．
(4) K も群で $g\colon H \to K$ が準同型写像ならば，合成写像 $(g \circ f)\colon G \to K$ も準同型写像である．
(5) N が G の正規部分群のとき，$a \in G$ に対して $aN \in G/N$ を対応させる写像 $\pi\colon G \to G/N$ は準同型写像である．$\pi\colon G \to G/N$ を**自然な全射**という．

証明. (1) $f(1_G) = f(1_G * 1_G) = f(1_G) \diamond f(1_G)$ である．両辺に右から $\big(f(1_G)\big)^{-1}$ を掛けると，

$$\begin{aligned} 1_H = f(1_G) \diamond \big(f(1_G)\big)^{-1} &= \big(f(1_G) \diamond f(1_G)\big) \diamond \big(f(1_G)\big)^{-1} \\ &= f(1_G) \diamond \big(f(1_G) \diamond \big(f(1_G)\big)^{-1}\big) = f(1_G) \diamond 1_H = f(1_G) \end{aligned}$$

となる．

(2) $x \in G$ に対し，$f(a) \diamond f(a^{-1}) = f(a * a^{-1}) = f(1_G) = 1_H$, $f(a^{-1}) \diamond f(a) = f(a^{-1} * a) = f(1_G) = 1_H$ なので，逆元の一意性により，$f(a)^{-1} = \big(f(a)\big)^{-1}$ である．

(3) $f\colon G \to H$ が全単射だから，勝手な $y_1,\, y_2 \in H$ に対し $x_1 := f^{-1}(y_1),\, x_2 := f^{-1}(y_2)$ とおく．$f(x_1 * x_2) = f(x_1) \diamond f(x_2) = y_1 \diamond y_2$ なので，$x_1 * x_2 = f^{-1}(y_1 \diamond y_2)$ である．よって，$f^{-1}\colon H \to G$ は準同型写像である．

(4) K の演算は積 $\cdot$ で表す．$a,\, b \in G$ に対し，

$$(g \circ f)(a * b) = g(f(a * b)) = g(f(a) \diamond f(b)) = g(f(a)) \cdot g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$$

なので，$(g \circ f)\colon G \to K$ は準同型写像である．

(5) G/N の演算も $*$ で表す．$a,\, b \in G$ に対し，

$$\pi(a * b) = (a * b) * N = a * (N * b) = a * (N * N * b) = (a * N) * (N * b) = (a * N) * (b * N) = \pi(a) * \pi(b)$$

なので $\pi\colon G \to G/N$ は準同型写像である． □

準同型写像に慣れてきたところで，演算を $*$ や $\diamond$ で区別して書くのをやめて，ここからは全部積の記号で表す．

命題 4.3. G と H は積に関する群とし，$f\colon G \to H$ は準同型写像とする．$N \subset H$ は部分群とする．このとき，以下が成り立つ．
(1) K が G の部分群ならば，$f(K)$ は H の部分群である．
(2) $f^{-1}(N) := \{x \in G \mid f(x) \in N\}$ は G の部分群である．
(3) $N \lhd H$ ならば $f^{-1}(N) \lhd G$ である．

証明. (1) $y_1,\, y_2 \in f(K)$ とする．$f(x_1) = y_1,\, f(x_2) = y_2$ となる $x_1,\, x_2 \in K$ がある．$x_1x_2 \in K$, $x_1^{-1} \in K$ で，$y_1y_2 = f(x_1)f(x_2) = f(x_1x_2) \in f(K)$, $y_1^{-1} = (f(x_1))^{-1} = f(x_1^{-1}) \in f(K)$ なので，$f(K)$ は H の部分群である．

(2) $a,\, b \in f^{-1}(N)$ ならば $f(a) \in N$, $f(b) \in N$ である．N は群なので，$f(ab) = f(a)f(b) \in N$ であり，$ab \in f^{-1}(N)$ である．また，$f(a^{-1}) = f(a)^{-1} \in N$ なので，$a^{-1} \in N$ である．よって，$f^{-1}(N)$ は G の部分群である．

(3) $N \cap f(G) \lhd f(G)$ に注意する．勝手な $a \in G$ を取る．$af^{-1}(N)a^{-1}$ の元は axa^{-1} $(x \in f^{-1}(N))$ と書ける．$f(axa^{-1}) = f(a)f(x)(f(a)^{-1}) \in f(a)(N \cap f(G))(f(a))^{-1} = N \cap g(G)$ である．よって，$axa^{-1} \in f^{-1}(N)$ であり，$af^{-1}(N)a^{-1} \subset N$ となる．$af^{-1}(N)a^{-1} \supset N$ は $f^{-1}(N) \supset a^{-1}f^{-1}(N)a$ と同値で，後者は証明したので，$af^{-1}(N)a^{-1} = N$ である．よって，$f^{-1}(N) \lhd G$ である． □

定義 4.4. G と H は積に関する群とし，$f\colon G \to H$ は準同型写像とする．

$$\operatorname{Ker} f := f^{-1}(1_H) = f^{-1}(\{1_H\}) = \{x \in G \mid f(x) = 1_H\}$$
$$\operatorname{Im} f := f(G) = \{f(a) \in H \mid a \in G\}$$

と書き，$\operatorname{Ker} f$ を f の**カーネル** (kernel) とか**核**といい，$\operatorname{Im} f$ を f の**イメージ** (image) とか**像**という．前命題 (1) より $\operatorname{Im} f$ は H の部分群である．また，$\{1\}$ は H の正規部分群なので，前命題 (3) より $\operatorname{Ker} f$ は G の正規部分群である．

定理 4.6. G と H は積に関する群とし，$f\colon G \to H$ は準同型写像とする．このとき，f が単射であることと $\operatorname{Ker} f = \{1\}$ であることは同値である．

証明. f が単射のとき，$x \in \operatorname{Ker} f$ ならば $f(x) = 1 = f(1)$ であるが，f が単射なので $x = 1$ となる．よって，$\operatorname{Ker} f = \{1\}$ である．

逆に，$\operatorname{Ker} f = \{1\}$ のとき f が単射であることを示す．$x,\, y \in G$, $f(x) = f(y)$ とする．$1 = (f(x))^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y)$ なので，$x^{-1}y \in \operatorname{Ker} f = \{1\}$ となる，つまり，$x^{-1}y = 1$. よって $x = y$ となり，f は単射である． □

定理 4.6.(準同型定理) G と H は積に関する群とし，$f\colon G \to H$ は準同型写像とする．$a \operatorname{Ker} f \in G/\operatorname{Ker} f$ $(a \in G)$ に対し $f(a) \in \operatorname{Im} f$ を対応させる写像 $\overline{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f$ は矛盾なく定義できて，これは同型写像になる．つまり，

$$\overline{f}\colon G/\operatorname{Ker} f \xrightarrow{\cong} \operatorname{Im} f$$

証明. $N := \operatorname{Ker} f$ とおく.

(1) $\overline{f}\colon G/N \to \operatorname{Im} f$ が矛盾なく定義できることを示す. $b \in G$ で, G/N の元として $aN = bN$ であるとき, $a^{-1}b \in N = \operatorname{Ker} f$ なので $(f(a))^{-1}f(b) = f(a^{-1})f(b) = f(a^{-1}b) = 1_H$ である. よって, $f(a) = f(b)$ であり, $\overline{f}(aN) = \overline{f}(bN)$ である. よって, $\overline{f}$ は矛盾なく定義できる.

(2) $\overline{f}\colon G/N \to \operatorname{Im} f$ が準同型写像であることを示す. $N \lhd G$ なので, $a, b \in G$ に対し $(aN)(bN) = (ab)N$ である. よって,

$$\overline{f}((aN)(bN)) = \overline{f}((ab)N) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)$$

となるので, $\overline{f}$ は準同型写像である.

(3) $\overline{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f$ が単射であることを示す. $\overline{f}$ の定義から, $\overline{f}(a \operatorname{Ker} f) = 1$ と $f(a) = 1$ は同値ある. つまり, $a \in \operatorname{Ker} f$ と同値である. よって, $\operatorname{Ker} \overline{f} = \{\operatorname{Ker} f\} = \{1_{G/\operatorname{Ker} f}\}$ である. 前定理より, $\overline{f}$ は単射である.

(4) $\overline{f}$ の定め方から $\operatorname{Im} \overline{f} = \operatorname{Im} f$ なので, $\overline{f}$ は全射である. よって, $\overline{f}$ は同型写像である. □

5. 準同型定理の応用

定理 5.1.(第 1 同型定理) G と H は積に関する群とし, $f\colon G \to H$ は全射準同型写像とする. $N \lhd H$ のとき $f^{-1}(N) \lhd G$ で, $G/f^{-1}(N) \cong H/N$ が成り立つ.

証明. $\pi\colon H \to H/N$ を自然な全射とする. $\pi^{-1}(1_{H/N}) = \operatorname{Ker} \pi = N$ である.

$$\operatorname{Ker}(\pi \circ f) = (\pi \circ f)^{-1}(1_{H/N}) = f^{-1}(\pi^{-1}(1_{H/N})) = f^{-1}(N)$$

である. 全射 $(\pi \circ f) : G \to H/N$ に準同型定理を適用すると,

$$G/f^{-1}(N) = G/\operatorname{Ker}(\pi \circ f) \cong \operatorname{Im}(\pi \circ f) = H/N$$

である. □

定理 5.2.(第 2 同型定理) G は積に関する群とし, H は G の部分群, $N \lhd G$ とする. すると

$$H/(H \cap N) \cong (HN)/N$$

である. (注意. $HN = NH$ が G の部分群であることと, $H \cap N \lhd H$ は前回証明した.)

証明. $\pi\colon G \to G/N$ を自然な全射とし, $f := \pi|_H\colon H \to G/N$ とおく. $\operatorname{Ker} \pi = N$ なので $\operatorname{Ker} f = H \cap \operatorname{Ker} f = H \cap N$ である. 準同型定理より, $H/(H \cap N) = H/\operatorname{Ker} f \cong \operatorname{Im} f$ である.

次に $\iota\colon HN \xrightarrow{\subset} G$ を包含写像とすると, これは単射準同型写像である. $(\pi \circ \iota) : HN \to G/N$ とおくと, $\operatorname{Im}(\pi \circ \iota) \subset \operatorname{Im} f$ である. そこで, $(\pi \circ \iota)$ の終域を制限して得られる写像を, $g\colon HN \to \operatorname{Im} f$ とする.

$$\operatorname{Ker} g = \operatorname{Ker}(\pi \circ \iota) = (\pi \circ \iota)^{-1}(1) = \iota^{-1}(\pi^{-1}(1)) = \iota^{-1}(N) = N$$

であるので, 準同型定理より, $HN/N = HN/\operatorname{Ker} g \cong \operatorname{Im} g$ である. あと, g が全射であることを示せば $\operatorname{Im} g = \operatorname{Im} f$ となって証明が完了する.

勝手な $y \in \operatorname{Im} f$ を取る. $f\colon H \to G/N$ なので, ある $x \in H$ により $y = f(x)$ と書ける. このとき, $x \in HN$ なので, $g(x) = y$ であり, g は全射である. □

定理 5.3.(第 3 同型定理) G は積に関する群とし, H と N は G の正規部分群で $G \rhd H \rhd N$ であるとする. すると, 全射準同型写像 $\varphi\colon G/N \longrightarrow G/H$ が存在して, $\operatorname{Ker} \varphi = H/N \subset G/N$ であり,

$$(G/N)/(H/N) \cong G/H$$

が成立する.

証明. $a, b \in G$ が $aN = bN$ を満たせば $N \subset H$ なので, $aH = bH$ が成立する. よって, $aN \in G/N$ に対して $aH \in G/H$ を対応させる写像 $\varphi\colon G/N \to G/H$ が矛盾なく定義できる. $\varphi((aN)(bN)) = \varphi((ab)N) = (ab)H = (aH)(bH) = \varphi(aN)\varphi(bN)$ なので, φ は準同型写像である.

$\operatorname{Ker}\varphi = H/N$ を示す．$a \in H$ ならば $aH = H \in G/H$ だから $\varphi(aN) = aH = H = 1_{G/H}$ で，$H/N \subset \operatorname{Ker}\varphi$ である．逆に，$bN \in \operatorname{Ker}\varphi$ ならば $bH = \varphi(bN) = 1_{G/H} = H$ なので，$b \in H$ となる．つまり $bN \in H/N$ で，$H/N \supset \operatorname{Ker}\varphi$ である．よって，$\operatorname{Ker}\varphi = H/N$ である．

準同型定理より，$(G/N)/(H/N) = (G/N)/\operatorname{Ker}\varphi \cong G/H$ である． □

定理 5.4. G は巡回群とする．すると，$G \cong \mathbb{Z}$ であるか，または，ある $n \in \mathbb{N}$ が存在して $G \cong \mathbb{Z}/n\mathbb{Z}$ となる．

証明. 巡回群の定義から $G = \langle a \rangle$ $(a \in G)$ と書ける．$n \in \mathbb{Z}$ に対して $a^n \in G$ を対応させる写像を $f\colon \mathbb{Z} \to G$ とする．G の元は a^n と書けるから f は全射である．指数法則より f は準同型写像である．準同型定理より，$\mathbb{Z}/\operatorname{Ker} f \cong \operatorname{Im} f = G$ となる．ところで，加法群 (加法に関する群のこと) $\mathbb{Z}$ の部分群は，ある $n \in \mathbb{N} \cup \{0\}$ により $n\mathbb{Z}$ と書ける (簡単なので証明してみよ) ので，$\mathbb{Z}/n\mathbb{Z} \cong G$ である．なお，$n = 0$ のときは $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ である． □

定義&命題 5.5.(群の直積) G, H は積に関するする群とする．直積集合 $G \times H$ に次のように演算を定める．$(g_1, h_1), (g_2, h_2) \in G \times H$ $(g_1, g_2 \in G;\ h_1, h_2 \in H)$ に対し，

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

として演算 (積) を定める．すると，$G \times H$ も群になり，その単位元は $(1_G, 1_H)$ で，$(g, h) \in G \times H$ の逆元は，$(g, h)^{-1} = (g^{-1}, h^{-1})$ である．$G \times H$ を G と H の**直積**という．このとき，$(g, 1_H) \in G \times H$ と $g \in G$ を同一視して $G \subset G \times H$ と考える．また，$(1_G, h) \in G \times H$ と $h \in H$ を同一視して $H \subset G \times H$ と考える．このとき，$G \lhd G \times H$, $H \lhd G \times H$ である．また，$(G \times H)/G \cong H$, $(G \times H)/H \cong G$ である．

証明. 結合法則は G と H の結合法則からすぐ導かれる．$(1_G, 1_H)(g, h) = (1_G \cdot g, 1_H \cdot h) = (g, h)$, $(g, h)(1_G, 1_H)(g, h) = (g \cdot 1_G, h \cdot 1_H) = (g, h)$ なので，$(1_G, 1_H)$ は単位元である．同様に，$(g^{-1}, h^{-1})(g, h) = (1_G, 1_H)$, $(g, h)(g^{-1}, h^{-1}) = (1_G, 1_H)$ なので，$(g, h)^{-1} = (g^{-1}, h^{-1})$ である．よって，$G \times H$ は群になる．

$G \subset G \times H$ と考えたとき，$(g, h)G = G \times \{h\} = G(g, h)$ なので，$G \lhd G \times H$ である．$H \lhd G \times H$ も同様．

$\pi_1\colon (G \times H) \to H$ を $\pi_1(g, h) = H$ と定めると，これは全射準同型写像で $\operatorname{Ker}\pi_1 = G$ である．よって，$(G \times H)/G = (G \times H)/\operatorname{Ker}\pi_1 \cong \operatorname{Im}\pi_1 = H$. □

定理 5.6. G は積に関するする群とし，H と N は G の部分群とする．$h \in H$, $n \in N$ に対し $\varphi(h, n) = hn \in G$ で定まる写像 $\varphi : (H \times N) \longrightarrow G$ が同型写像であるための必要十分条件は，以下の (1), (2), (3) が成り立つことである．

(1) $H \lhd G$ かつ $N \lhd G$.
(2) $G = HN$.
(3) $H \cap N = \{1\}$.

このとき，$G = H \times N$ と書き，G は H と N の**直積**であるという．

証明. (必要性) $\varphi : (H \times N) \xrightarrow{\cong} G$ と仮定する．

(1) $H \lhd (H \times N)$, $N \lhd (H \times N)$ で，$\varphi(H) = H \subset G$, $\varphi(N) = N \subset G$ で，φ が同型写像だから，$H \lhd G$, $N \lhd G$ である．

(2) φ の定義から $\operatorname{Im}\varphi = HN$ であるから (2) が成り立つ．

(3) $x \in H \cap N$ とすると，$x^{-1} \in N$ なので，$(x, x^{-1}) \in H \times N$ で，$\varphi(x, x^{-1}) = xx^{-1} = 1$ となる．φ は同型写像だから単射で $\operatorname{Ker}\varphi = \{(1, 1)\}$ である．よって $(x, x^{-1}) = (1, 1)$ で $x = 1$ である．したがって，$H \cap N = \{1\}$ である．

(十分性) (1), (2), (3) が成り立つと仮定する．勝手な $g \in G$ を取る．(2) より $g = hn$ $(\exists h \in H, \exists n \in N)$ と書ける．今 $g = hn = h'n'$ $(h' \in H, n' \in N)$ とする．(3) より，$nn'^{-1} = h^{-1}h' \in H \cap N = \{1\}$ なので，$nn'^{-1} = h^{-1}h' = 1$ で $n = n'$, $h = h'$ となる．つまり，$\varphi(h, n) = \varphi(h', n')$ ならば $(h, n) = (h', n')$ となるから，φ は単射である．また，(2) より，φ は全射である．

(i) $h \in H$, $n \in N$ ならば $hn = nh$ であることを示す．(1) より $hNh^{-1} = N$ だから，$hnh^{-1}n^{-1} \in (hNh^{-1})n^{-1} = Nn^{-1} = N$ である．また，$nHn^{-1} = H$ だから，$hnh^{-1}n^{-1} \in h(nHn^{-1}) = hH = H$ である．よって，$hnh^{-1}n^{-1} \in H \cap N = \{1\}$ となり，$hnh^{-1}n^{-1} = 1$ である．したがって，$hn = nh$ である．

$h_1, h_1 \in H$; $n_1, n_2 \in N$ とする．(i) より，

$$\varphi(h_1h_2, n_1n_2) = (h_1h_2)(n_1n_2) = (h_1n_1)(h_2n_2) = \varphi(h_1, n_1)\varphi(h_2, n_2)$$

となり，φ は準同型写像である．

以上より，φ は同型写像である． □

6. 群の集合への作用

定義 6.1. G は積に関する群，X は集合とする．ある写像 $\varphi\colon (G \times X) \longrightarrow X$ が与えられているとする．$a \in G$, $x \in X$ に対し $\varphi(a, x) \in X$ を単に ax とか $a \cdot x$ と書くことにする．任意の $a, b \in G$ と任意の $x \in X$ に対し，以下の (1), (2) が成り立つとき，G は X に**作用する**といい，G をこの作用の**変換群**という．

(1) $(ab)x = a(bx)$.

(2) $1 \cdot x = x$.

以下，G が X に作用しているとする．$A \subset X$ に対し，

$$G \cdot A = \{gx \in G \mid g \in G, x \in A\}$$
$$G_A = \{g \in G \mid gA = A\}$$

と書き，$G \cdot A$ を A の G-**軌道** (G-orbit), G_A を x における G の**安定部分群** (stabilizer) とか**等方部分群** (isotropy group) とか x の**固定部分群**という．$G \cdot A$ は GA とも書く．$A = \{x\}$ のとき，$G \cdot A$ を $G \cdot x$ または Gx, G_A を G_x と書く．

$x, y \in X$ に対して，ある $g \in G$ が存在して $y = gx$ ($x = g^{-1}y$) となるとき $x \sim y$ と定めると，$\sim$ は X 上の同値関係になる．このとき，$X/\sim$ を X/G とも書き，X の G による**商集合**という．

$$X/G = X/\sim = \{G_x \mid x \in X\}$$

である．また，

$$X^G := \{x \in X \mid \text{任意の } g \in G \text{ に対し } gx = x\}$$

を X の G による**不変部分集合**という．

ある元 $x \in X$ に対し $G \cdot x = X$ となるとき，G は X に**推移的** (transitive) に作用するという．このとき，$X/G = \{1 \text{ 点 }\}$ である．

命題 6.2. 群 G は集合 X に作用しているとする．また，$x \in X$ とする．このとき，以下が成り立つ．

(1) G_x は G の部分群である．

(2) $a \in G$, $y = ax \in X$ のとき，$G_y = aG_xa^{-1}$ である．

(3) G が有限群ならば，

$$\#(G \cdot x) = [G : G_x]$$

が成り立つ．

証明. (1) $a, b \in G_x$ ならば $ax = x$, $bx = x$ なので，$(ab)x = a(bx) = ax = x$ であり，$ab \in G_x$ である．また，$x = 1 \cdot x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$ より，$a^{-1} \in G_x$ である．よって，G_x は G の部分群である．

(2) aG_xa^{-1} の元は，ある $b \in G_x$ により aba^{-1} と書ける．$bx = x$, $y = ax$ なので，$x = a^{-1}y$ であり，$x = bx = ba^{-1}y$ となる．よって，$y = ax = abx = aba^{-1}y$ となり，$aba^{-1} \in G_y$ がわかる．したがって，$aG_xa^{-1} \subset G_y$ である．$x = a^{-1}y$ より，対称性から $a^{-1}G_ya \subset G_x$ となる．これより，$G_y \subset aG_xa^{-1}$ なので，$G_y = aG_xa^{-1}$ となる．

(3) $a, b \in G$ で，$ax = bx$ が成り立つとき，$(a^{-1}b)x = x$ だから $a^{-1}b \in G_x$ である．よって，$a^{-1}bG_x = G_x$ であり，$bG_x = aG_x$ となる．逆に，$aG_x = bG_x$ のとき，$a^{-1}b \in G_x$ より $ax = bx$ が得られる．したがって，「$ax = bx \iff aG_x = bG_x$」である．

これより，$aG_x \in G/G_x$ に対し $ax \in G\cdot x$ を対応させる写像 $\psi\colon G/G_x \longrightarrow G\cdot x$ が矛盾なく定義できる．定義から ψ は全射である．また $ax = bx$ ならば $aG_x = bG_x$ だから，ψ は単射である．よって，ψ は全単射で，$[G : G_x] = \#(G/G_x) = \#(G\cdot x)$ となる． □

定義&命題 6.3. G は積に関するする群とする．そのとき，

$$Z(G) := \left\{a \in G \;\middle|\; \text{任意の } x \in G \text{ に対し } ax = xa\right\}$$

を G の**中心** (center) という．$Z(G)$ は G の正規部分群である．

証明. $Z(G)$ は G の部分群であることを示す．$a, b \in Z(G)$ ならば，$x \in G$ に対し $ax = xa$, $bx = xb$ が成り立つので，$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ となり，$ab \in Z(G)$ である．また，$ax = xa$ より $xa^{-1} = a^{-1}x$ となるので，$a^{-1} \in Z(G)$ である．よって，$Z(G)$ は G の部分群である．
また，$xax^{-1} = axx^{-1} = a \in Z(G)$ なので，$Z(G) \lhd G$ である． □

定理 6.4.(類等式) G は積に関するする有限群とする．$x \in G$ に対し，

$$Cx := \left\{axa^{-1} \in G \;\middle|\; a \in G\right\}$$

と書くことにする．このとき，以下が成り立つ．
(1) 有限個の $x_1, x_2, \ldots, x_r \in G$ が存在して，

$$G = Cx_1 \sqcup Cx_2 \sqcup \cdots \sqcup Cx_r$$

が成り立つ．
(2) $|G| = |Z(G)| + \displaystyle\sum_{|Cx_i| \geqq 2} |Cx_i|$ が成り立つ．
(2) を**類等式**という．Cx を (x の) **共役類**といい，r を G の**類数**という．

証明. (1) $x \in G$ に対して $x \in Cx \subset G$ だから，$G = \displaystyle\bigcup_{x\in G} Cx$ である．(1) を示すには，

(∗)「$x, y \in G$, $Cx \cap Cy \neq \phi$ ならば $Cx = Cy$」

を示せばよい．$z \in Cx \cap Cy \neq \phi$ とする．ある $a, b \in G$ により，$z = axa^{-1} = byb^{-1}$ と書ける．Cx の元は cxc^{-1} ($c \in G$) という形に書ける．$x = a^{-1}byb^{-1}a$ より，$cxc^{-1} = ca^{-1}byb^{-1}ac^{-1} = (ca^{-1}b)y(ca^{-1}b)^{-1} \in Cy$ なので．$Cx \subset Cy$ である．対称性から $Cy \subset Cx$ なので $Cx = Cy$ である．

(2) (1) より，$|G| = \displaystyle\sum_{i=1}^{r} |Cx_i|$ である．$|Gx_i| = 1$ と $x_i \in Z(G)$ が同値であることを示せば，(2) が得られる．
$|Cx_i| = 1$ ならば $Cx_i = \{x_i\}$ で，任意の $a \in G$ に対して $ax_ia^{-1} \in Cx_i = \{x_i\}$ より，$ax_ia^{-1} = x_i$ となる．よって，$ax_i = x_ia$ で $x_i \in Z(G)$ となる．
逆に，$x_i \in Z(G)$ ならば，任意の $a \in G$ に対して $ax_i = x_ia$ だから，$ax_ia^{-1} = x_i$ で，$Cx_i = \{x_i\}$ となる．よって，$|Cx_i| = 1$ である． □

G は演算 $*$ に関する群，$X = G$ とし，$a \in G$ は $x \in X = G$ に $a\cdot x = a * x * a^{-1}$ として作用しているとする．作用のほうを $\cdot$, 群の演算を $*$ と書いて区別することにする．軌道も Gx ではなく $G\cdot x$ と書く．上の定理における Cx は軌道 $G\cdot x$ と一致する．Cx を $O_G(x)$ と書くことも多い．また，安定部部群 G_x を

$$C_G(x) := \left\{g \in G \;\middle|; g * x = x * g\right\}$$

と書き，x における G の**中心化群**という．$A \subset G$ に対し，安定部分群 G_A を

$$N_G(A) := \left\{g \in G \;\middle|\; g * A * g^{-1} = A\right\}$$

と書き，A の**正規化群**と呼ぶ $C_G(A) \subset N_G(A)$ である．

定理 6.5. G は有限群，$x \in G$ とすると，$N_G(x) \lhd G$ であって，

$$|Cx| = |O_G(x)| = |G/N_G(x)| = [G : N_G(x)], \quad |Cx| \cdot |N_G(x)| = |G|$$

である．

証明. $N_G(x) \lhd G$ は $N_G(A)$ の定義と正規部分群の定義からすぐわかる．
命題 6.2 の記号で，$G_x = N_G(x)$, $G \cdot x = O_G(x) = Cx$ なので，命題 6.2(3) より $|Cx| = |O_G(x)| = |G/N_G(x)| = [G : N_G(x)]$ である． □

命題 6.6. G は群，H は G の部分群とする．このとき，$H \lhd G$ と $N_G(H) = H$ は同値である．

証明. $N_G(H)$ の定義から明らか． □

7. シローの定理

定義 7.1. G は積に関する群，H_1 と H_1 は G の部分群とする．ある $a \in G$ が存在して，$aH_1a^{-1} = H_2$ (つまり $aH_1 = H_2a$) となるとき，H_1 と H_2 は**共役**であるという．

定義 7.2. G は有限群，p は素数とする．もし，ある $n \in \mathbb{N}$ が存在して $|G| = p^n$ であるとき，G は p-**群**であるという．今，$|G| = p^nm$ (m は p と互いに素な自然数) であると仮定する．G の部分群 H が $|H| = p^n$ を満たすとき，H は G の p-**シロー** (**部分**) **群** (p-Sylow group) であるとか**シロー** p-**群** (Sylow p-group) であるという．また，一般に $k = p^nm$ ($\mathrm{GCD}(m, p) = 1$) のとき，$\mathrm{ord}_p\, k = n$ と定める．つまり，$\mathrm{ord}_p\, k$ は p^n が k の約数になるような最大の n の値である．

定理 7.3.(シローの定理 1) $|G| = p^nm$ (p は素数で $\mathrm{GCD}(p, m) = 1$) とすると，p-シロー群 $P \subset G$ ($|P| = p^n$) が存在する．

証明. $X := \{A \subset G \mid |A| = p^n\}$ とおく．$gA = \{gs \mid s \in A\}$ とおくと，$|gA| = |A| = p^n$ なので $gA \in X$ である．そこで，$g \in G$ の $A \in X$ への作用を $g(A) = gA$ で定める．ここでは，作用のほうを $g(A)$ と書いて，群の演算 gA と区別する．

$$\#X = \binom{p^nm}{p^n} = \frac{(p^nm)!}{(p^n(m-1))!(p^n)!} = \frac{\displaystyle\prod_{i=0}^{p^n-1}(p^nm-i)}{\displaystyle\prod_{i=0}^{p^n-1}(p^n-i)}$$

であるが，$0 \leqq i < p^n$ のとき，$\mathrm{ord}_p(p^nm - i) = \mathrm{ord}_p\, i = \mathrm{ord}_p(p^n - i)$ なので，$\mathrm{ord}_p\, |X| = 0$ である．よって，$A \in X$ の軌道 $GA := \{gA \mid g \in G\} \subset X$ の中で，$\mathrm{ord}_p\, |GA| = 0$ であるものが存在する．
安定部分群 $G_A := \{g \in G \mid gA = A\}$ を考えると，$|GA| = |G/G_A|$ より $|GA| \cdot |G_A| = |G| = p^nm$ であるが，$\mathrm{GCD}(p, |GA|) = 1$ より $|G_A|$ は p^n の倍数である．
$s_0 \in A$ を固定するとき，$g \in G_A$ に対し $f(g) = gs_0 \in A$ で定まる写像 $f\colon G_A \to A$ は単射だから，$|G_A| \leqq |A| = p^n$ なので，結局 $|G_A| = p^n$ となり，これが 1 つの p-シロー群である． □

定理 7.4.(シローの定理 2) G は有限群，$|G| = p^nm$ (p は素数で $\mathrm{GCD}(p, m) = 1$) とし，N は G のひとつの p-部分群 (つまり $|N| = p^r$) であると仮定する．
(1) N を含む p-シロー群 P が存在する．
(2) G の 2 つの p-シローは互いに共役である．
(3) G の p-シロー部分群の個数を s とすると，$s \equiv 1 \pmod p$ を満たす．また，p-シロー群の安定化群を $N_G(P)$ とするとき，$s = [G : N_G(P)]$ である．特に，s は $|G|$ の約数である．

証明. (1) H は G の一般の部分群とし，G の p-シロー部分群 $P_0 \in S$ を 1 つ固定する．

$$Y := \{P \subset G \mid P \text{ は } P_0 \text{ と共役}\}$$

とおく．$h \in H$ と $P \in Y$ に対し，$h(P) = hPh^{-1} \in Y$ として H の Y への作用を定める．$P \in Y$ の軌道と固定群を，

$$O_H(P) := \{hPh^{-1} \mid h \in H\} \subset Y, \quad N_H(P) := \{h \in H \mid hPh^{-1} = P\} \subset H$$

で表す．$s = |O_G(P)|$ で，$|O_H(P)| \cdot |N_H(P)| = |H|$ である．

特に，$H = G$ の場合を考えると，$Y = O_G(P_0)$ で，$|Y| \cdot |N_G(P_0)| = |G| = p^n m$ である．P_0 は $N_G(P_0)$ の部分群だから，$|N_G(P_0)|$ は $|P_0| = p^n$ の倍数で，$|Y|$ は m の約数となる．つまり，$|Y|$ は p と互いに素である．

$H = N$ の場合を考える．$|O_N(P)| \cdot |N_N(P)| = |N| = p^r$ より，$|O_N(P)| = p^k$ $(k \in \mathbb{N} \cup \{0\})$ と書ける．$P_i, P_j \in Y$ が $O_N(P_i) \cap O_N(P_j) \neq \phi$ を満たせば $O_N(P_i) = O_N(P_j)$ であるから，ある P_1,…, $P_t \in Y$ を選んで，$Y = O_N(P_1) \sqcup \cdots \sqcup O_N(P_t)$ と書ける．$\mathrm{ord}_p |O_N(P_i)| = 0$ を満たす $P_i \in Y$ が存在し，$|O_N(P_i)| = p^0 = 1$ となる．つまり，$O_N(P_i) = \{P_i\}$. この P_i を改めて P と書くことにする．

$hPh^{-1} = P$ $(\forall h \in N)$ だから $hP = Ph$ であり，$NP = PN$ がわかる．NP は G の部分群である．また，任意の $g \in NP$ に対し $gPg^{-1} = P$ もすぐわかるので，P は NP の正規部分群である．

$(NP)/P \cong N/(N \cap P)$ なので，$|NP|$ は $|N| \cdot |P| = p^{r+n}$ の約数である．$P \subset NP \subset G$ だから，$|NP| = p^n$ である．特に，$NP = P$ がわかった．よって，$P = NP$ が N を含む p-シロー群である．

(2) P_0, P_1 を勝手な p-シロー群とし，$N = P_1$ とおいて (1) の証明を適用すると，N を含む Y の元 P が存在し，$P = P_1$ となる．P_1 は P_0 と共役である．

(3) 1 つの p-シロー部分群 P_0 を固定して，$N = P_0$ として (1) の証明を適用する．G の任意の p-シロー部分群は Y の要素である．Y は $O_N(P_i)$ 達の直和集合であり，$|O_N(P_i)| = p^{k_i}$ $(k_i \in \mathbb{N} \cup \{0\})$ であった．もし，$k_i = 0$ ならば，$O_N(P_i) = \{P_0\}$ となってしまうのであった．逆に言うと，$O_N(P_i) = \{P_0\}$ 以外の軌道 $O_N(P_j)$ は $\mathrm{ord}_p |O_N(P_j)| \geqq 1$ を満たす．よって，(3) が成り立つ． □

シローの定理は応用が広く役に立つが，以下に 1 つの応用例を示す．

定理 7.5. p, q は相異なる素数で $p > q$ であるとする．また，G は有限有限群で $|G| = pq$ を満たすとする．P は G の p-シロー部分群，Q は G の q-シロー部分群とする．このとき，以下が成り立つ．
(1) $P \lhd G$, $G = PQ$, $P \cap Q = \{1\}$ である．
(2) もし q が $p - 1$ の約数でないならば，$G = P \times Q$ で，G は巡回群である．

証明. (1) $|G| = pq$ だから $|P| = p$, $|Q| = q$ である．$P \subset N_G(P) \subset G$ であるが，$[G : P] = q$ (素数) なので，$N_G(P) = P$ または $N_G(P) = G$ のいずれかである．$[G : N_G(P)] \equiv 1 \pmod{p}$ で $q < p$ なので，$[G : N_G(P)] = q$ となることはなく，$[G : N_G(P)] = 1$ で $G = N_G(P)$ となる．$N_G(P)$ の定義から，任意の $g \in N_G(P) = G$ に対して $gPg^{-1} = P$ が成り立つので，$P \lhd G$ である．よって，$PQ = QP$ で PQ は G の部分群になる．PQ には位数 p の元と位数 q の元が存在するので，$|PQ| \geqq pq$ で，$PQ = G$ となる．$x \in P \cap Q$ ならば $x^p = 1$, $x^q = 1$ であるが，$pk + ql = 1$ を満たす整数 k, l を取れば，$x = x^{pk+ql} = (x^p)^k \cdot (x^q)^l = 1$ となる．よって，$P \cap Q = \{1\}$ である．

(2) $x \in P \cong \mathbb{Z}/p\mathbb{Z}$, $y \in Q \cong \mathbb{Z}/q\mathbb{Z}$ を取り，$f_y(x) := yxy^{-1}$ とおく．$f_y : P \to P$ は同型写像である．以下，f_y が恒等写像でないと仮定して矛盾を導く．

一般に $g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ が加法群の同型写像ならば，ある整数 $1 \leqq k \leqq p - 1$ が存在して $g(z) = kz$ $(z \in \mathbb{Z}/p\mathbb{Z})$ と書ける．f_y は恒等写像でないので $k \not\equiv 1 \pmod{p}$ である．g を r 回合成した写像は $g^r(z) = k^r z \in \mathbb{Z}/p\mathbb{Z}$ である．フェルマーの小定理より，$\mathbb{Z}/p\mathbb{Z}$ 内では $k^{p-1} = 1$ なので，g^{p-1} は恒等写像になる．よって，$f_y^{p-1} : P \to P$ も恒等写像である．

他方，$f_y^i(x) = y^i x y^{-i} = f_{y^i}(x)$ である．f_y は恒等写像でないので，$H := \left\{ f_y^i \,\middle|\, 0 \leqq i < q \right\}$ は Q と同型な群である．$f_y^{p-1} = 1_H$ なので，$p - 1$ は $q = |H|$ の倍数である．これは仮定に反する．よって，f_y は恒等写像で，$yxy^{-1} = x$ である．言い換えると，任意の $x \in P, y \in Q$ に対し，$xy = yx$ が成り立つ．

$G = PQ$ の 2 元は x_1y_1, x_2y_2 $(x_1, x_2 \in P; y_1, y_2 \in Q)$ と書けるが，$x_iy_j = y_jx_i$ より $(x_2y_2)(x_1y_1) = (x_1y_1)(x_2y_2)$ となり，G はアーベル群である．

x を巡回群 P の生成元，y を巡回群 Q の生成元とすれば，xy は位数 pq の元になるから，G は xy で生成される巡回群になる． □

8. 有限アーベル群

G がアーベル群の場合，演算は積でなく和 $+$ で表すほうが便利である．単位元も 1 でなく 0 と書く．1 は別の用途に用いる．このように表すとき，アーベル群のことを**加群**ともいう．さらに，このとき，G は単なる群構造だけでなく，$\mathbb{Z}$-加群の構造を持つ．その定義を述べておく．

定義 8.1. 一般に集合 R に和 $+$ と積 ($x \times y$, $x \cdot y$, xy と書く) が定義されていて，以下の (1) 〜 (3) を満たすとする．
(1) R は $+$ について 0 を単位元とするアーベル群である．$x \in R$ の $+$ についての逆元は $-x$ と書く．
(2) R は $\times$ については半群であって，単位元 1 を持つ．
(3) 分配法則 $a(b+c) = ab + ac$ $(a, b, c \in R)$ を満たす．
このとき，R は**環**であるという．さらに，交換法則 $ba = ab$ $(a, b \in R)$ と満たすとき，R は**可換環**であるという．

以下，R は環とする．上の 0, 1 を区別するため 0_R, 1_R と書く．M は加法 $+$ についてアーベル群で，単元は 0_M とする．さらに，R は M に作用していて，$a \in R$ の $x \in M$ への作用を ax と書く．この作用は，以下の (4) 〜 (6) を満たすとする．ただし，$a, b \in R$; $x, y \in M$ とする．
(4) (結合法則) $(ab)x = a(bx)$. (作用の定義に含まれてはいるが)
(5) $1_R \cdot x = x$, $0_R \cdot x = 0_M$. ($0_R \cdot x = 0_M$ は次の (6) から導かれるので書かなくてもよい.)
(6) (分配法則) $(a+b)x = ax + bx$, $a(x+y) = ax + by$.
このとき，M は R-加群であるという．

例えば，$\mathbb{Z}$ は可換環である．G がアーベル群で演算を $+$ で表すとき，$n \in \mathbb{Z}$ が $n > 0$ を満たすときは，$x \in G$ に対して，

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ 個}}$$

として nx を定める，$n = 0_{\mathbb{Z}}$ のときは $0_{\mathbb{Z}}x = 0_G$ と定める．$n < 0$ のときは $-n > 0$ なので，$nx = -(-n)x$ と定める．容易にわかるように，この作用で G は $\mathbb{Z}$-加群になる．特に，有限アーベル群 G を考察するときは，この $\mathbb{Z}$ の作用を利用して考察すると，$\mathbb{Z}$ の性質を利用して議論できるので，話が簡明になる．有限アーベル群の構造定理を証明したいが，証明が長くなるので，定理を 2 段階に分けて証明する．

補題 8.2. p は素数，$e \in \mathbb{N}$，G はアーベル群で $|G| = p^e$ を満たすとする．すると，ある $r \in \mathbb{N}$ と自然数 $e_1 \geqq e_2 \geqq \cdots \geqq e_r$ が存在して，

$$G \cong (\mathbb{Z}/p^{e_1}\mathbb{Z}) \times (\mathbb{Z}/p^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{e_r}\mathbb{Z})$$

となる．しかも，この r と e_1,..., e_r は G から一意的に定まる．

証明. G の演算は $+$ で表す．G の中の位数最大の元のひとつを h とし，$\operatorname{ord} h = p^{e_1}$, $H = \langle h \rangle$ とする．
(1) $G \cong H \times (\mathbb{Z}/p^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{e_r}\mathbb{Z})$ と表せることを $|G|$ に関する帰納法で証明する．
もし $H = G$ ならば $G = H \cong \mathbb{Z}/p^e\mathbb{Z}$ である．
$H \subsetneqq G$ の場合を考える．$|H| = p^{e_1}$, $e_1 < e$ であり，H は巡回群なので $H \cong \mathbb{Z}/p^{e_1}\mathbb{Z}$ である，$g \in G$ を $g \notin H$ となるように取る．$p^e g = 0 \in P$ だから，$p^k g \in P$ となるような最小の自然数 k が存在する．$g' := p^{k-1}g$ とすれば，$g' \notin P$, $pg' \in P$ である．g の代わりに g' を選び，最初から $pg \in P$ と仮定しておく．$pg = mh$ を満たす $m \in \mathbb{Z}$, $0 \leqq m < p^{e_1}$ が一意的に存在する．もし，$\mathrm{GCD}(p, m) = 1$ なら $H = \langle mh \rangle$ だから，$\operatorname{ord} g = p \operatorname{ord} h > \operatorname{ord} h$ となって $\operatorname{ord} h$ の最大性に矛盾する．よって，m は p の倍数で，$m = pm'$ と書ける．$x := g - m'h$ とおく．$px = pg - mh = 0$ である．また，$x = g - m'h \notin H$ だから $x \neq 0$ である．$N := \langle x \rangle \lhd G$ とおく．$G' := G/N$ とおき，$\pi\colon G \to G'$ を自然な全射とする．$h \notin N$ だから $\pi(h) \neq 0$ で，$\operatorname{ord} \pi(h) = \operatorname{ord} h$ である．よって，$H' = \pi(H) = \langle \pi(h) \rangle \lhd G$ とおくと，$H \cong H'$ である．帰納法の仮定から，

$$G' \cong H' \times (\mathbb{Z}/p^{f_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{f_s}\mathbb{Z})$$

と書ける．$Q' := (\mathbb{Z}/p^{f_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{f_s}\mathbb{Z})$ とおき，$Q := \pi^{-1}(Q')$ とする．$N \subset Q$ だから，準同型定理より $H + Q = G$ が成り立つ．また，$H \cap Q \subset \pi^{-1}(H' \cap Q') = \pi^{-1}(0) = N = \langle x \rangle \lhd G$ である．ところが $x \notin H$ だから $H \cap Q = \{0\}$ である．したがって，$G = H \times Q$ である．再び帰納法の仮定から，

$$Q \cong (\mathbb{Z}/p^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{e_r}\mathbb{Z})$$

と書ける．よって，(1) が証明された．

(2) (r, e_1,..., e_r の一意的の証明)
一般に $\iota\colon \mathbb{Z}/p^i\mathbb{Z} \longrightarrow \mathbb{Z}/p^{i+1}\mathbb{Z}$ を $\iota(x) = px$ で定めると単射準同型写像になるので，この ι を通して $\mathbb{Z}/p^i\mathbb{Z} \lhd \mathbb{Z}/p^{i+1}\mathbb{Z}$ と考えることができる．$\mathbb{Z}/p^i\mathbb{Z} = \left\{ x \in \mathbb{Z}/p^{i+1}\mathbb{Z} \;\middle|\; \operatorname{ord} x \leqq p^i \right\}$ である．

$G \cong (\mathbb{Z}/p^{f_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{f_s}\mathbb{Z})$, $f_1 \geqq \cdots \geqq f_s$ とも表わせたとして，$r = s$, $e_i = f_i$ を示す．e_1, f_1 は G 内の位数最大の元の位数なので，$e_1 = f_1$ である．$e_1 = e_2 = \cdots = e_k > e_{k+1}$, $e_1 = f_1 = f_2 = \cdots = f_l > f_{l+1}$ と仮定する．改めて，

$$H := \left\{ x \in G \;\middle|\; \operatorname{ord} x \leqq p^{e_1-1} \right\}$$

とおく．上の考察から，H に対応する $(\mathbb{Z}/p^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{e_r}\mathbb{Z})$ の部分群は

$$H_1 := (\mathbb{Z}/p^{e_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{e_k-1}\mathbb{Z}) \times (\mathbb{Z}/p^{e_{k+1}}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{e_r}\mathbb{Z})$$

であり，H に対応する $(\mathbb{Z}/p^{f_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{f_s}\mathbb{Z})$ の部分群は

$$H_2 := (\mathbb{Z}/p^{f_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{f_l-1}\mathbb{Z}) \times (\mathbb{Z}/p^{f_{l+1}}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{f_s}\mathbb{Z})$$

である．$H_1 \cong H \cong H_2$ だから，帰納法の仮定から，$r = s$ で $e_1 - 1 = f_1 - 1$,..., $e_r = f_l$ となる．$k < l$ と仮定すると $e_k - 1 = f_k - 1$, $e_{k+1} = f_{k+1} - 1$ となるが，そうすると $|H_1| < |H_2|$ となって矛盾する．$k > l$ だと $|H_1| > |H_2|$ となるので $k = l$ である．結局すべての $1 \leqq i \leqq r = s$ に対して $e_i = f_i$ となる． □

注意 8.3. p を素数とし，$G = (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ とする．$\iota\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z}$ を $\iota(x) = px$ で定まる単射準同型写像とし，$\pi\colon \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ を $\pi(n + p^2\mathbb{Z}) = n + p\mathbb{Z}$ でで定まる自然な全射準同型写像とする．$\iota(\pi(x)) = px$, $\pi(\iota(x)) = 0$ に注意する．

$x \in \mathbb{Z}/p^2\mathbb{Z}$, $y \in \mathbb{Z}/p\mathbb{Z}$ に対し，$f_1\colon G \to G$ と $g_1\colon G \to G$ を

$$f_1(x, y) = \big(x,\, y + \pi(x)\big), \quad g_1(x, y) = \big(x,\, y - \pi(x)\big)$$

で定めると f_1, g_1 は準同型写像になる．

$$g_1(f_1(x, y)) = g_1\big(x,\, y + \pi(x)\big) = \big(x,\, y + \pi(x) - \pi(x)\big) = (x, y)$$
$$f_1(g_1(x, y)) = f_1\big(x,\, y - \pi(x)\big) = \big(x,\, y - \pi(x) + \pi(x)\big) = (x, y)$$

なので，$g_1 = f_1^{-1}$ で f_1, g_1 は同型写像になる．このとき，$f_1(\mathbb{Z}/p^2\mathbb{Z}) \not\subset \mathbb{Z}/p^2\mathbb{Z}$ である．

同様に $f_2\colon G \to G$ と $g_2\colon G \to G$ を

$$f_2(x, y) = \big(x + \iota(y),\, y\big), \quad g_2(x, y) = \big(x - \iota(y),\, y\big)$$

で定めると，$g_2 = f_2^{-1}$ で f_2, g_2 も準同型写像になる．このとき，$f_2(\mathbb{Z}/p\mathbb{Z}) \not\subset \mathbb{Z}/p\mathbb{Z}$ である．

このように，同型写像 $f : \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ によって，直積因子 $\mathbb{Z}/p^2\mathbb{Z}$ と $\mathbb{Z}/p\mathbb{Z}$ が $\mathbb{Z}/p^2\mathbb{Z}$ と $\mathbb{Z}/p\mathbb{Z}$ に写るとは限らず，上の f_1, f_2 のように斜めに入ることがある．ただし，次のように位数が互いに素な群の直積の場合はこういう現象は起きない．

定理 8.4. G と H は積に関する有限群とし，$|G|$ と $|H|$ は互いに素であると仮定する．もし，$f\colon G \times H \longrightarrow G \times H$ が同型写像ならば，$f(G) = G$, $f(H) = H$ が成り立つ．

証明. $|G| = g$, $|H| = h$ とする．$1_G \neq x \in G$ を取り，$f(x,\, 1_H) = (a,\, b)$ $(a \in G,\, b \in H)$ とおく．$x^g = 1_G$ だから $(1_G,\, 1_H) = f(x^g,\, 1_H) = (a^g,\, b^g)$ で，$b^g = 1_H$ となる．$\mathrm{GCD}(g,\, h) = 1$ なので $gm + hn = 1$ を満たす $m,\, n \in \mathbb{Z}$ が存在する．$b \in H$ なので $b^h = 1_H$ である．よって，$b = b^1 = b^{gm+hn} = (b^g)^m (b^h)^n = 1_H^m \cdot 1_H^n = 1_H$ となる．つまり，$f(x,\, 1_H) \subset G$ で，$f(G) \subset G$ となる．f は単射で G は有限集合だから $f(G) = G$ でなければならない．

同様に $f(H) = H$ である． □

長くなるので，ここからは次回に説明する．

9. 有限アーベル群の構造定理

定理 9.1.(有限アーベル群の構造定理) G が $\{0\}$ 以外の有限アーベル群ならば，ある自然数 r と，(相異なるとは限らない) 素数 p_1,..., p_r と，自然数 e_1,..., e_r が存在して，

$$G \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})$$

と書ける．この r や p_i, e_i の値は，並べる順番を無視すれば，G から一意的に定まる．例えば，$(p_i,\, e_i)$ を (逆) 辞書式順序で並べておけば，一意的である．

なお加群については，直積の記号 $\times$ を $\oplus$ と書く場合が多い (無限個の加群については直積 $\times$ と直和 $\oplus$ は同じでないが，有限個の場合は同じ)．その記号で書けば，

$$G \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \oplus (\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_r^{e_r}\mathbb{Z}).$$

証明. $(p_i,\, e_i)$ $(i = 1,\ldots,\, r)$ を逆辞書式順序で大きいほうから順に並べておき，$p = p_1$ とする．

(1) $n = |G| \geqq 2$ とし，$G \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})$ と書けることを n に関する帰納法で証明する．

$n = p^e$ の場合は，補題 8.2 より定理が成り立つ．

$n = p^e m$ $(\mathrm{GCD}(p,\, m) = 1)$ は合成数であるとする．

$$P := \left\{x \in G \;\middle|\; \operatorname{ord} x \text{ は } p^e \text{ の約数}\right\}, \quad H := \left\{x \in G \;\middle|\; \operatorname{ord} x \text{ は } m \text{ の約数}\right\}$$

とおく．P, H は G の正規部分群である．$\mathrm{GCD}(p^e,\, m) = 1$ だから $P \cap H = \{0\}$ である．また，$P + H$ は $p^e \times m = n$ 個の元を持つから $P + H = G$ である ($P + H$ は演算を積で書いた場合の PH のこと)．よって，$G = P \times H$ である．帰納法の仮定から H は $\mathbb{Z}/p_i^{e_i}$ という形の群の直積に書ける．補題 8.2 より P も $\mathbb{Z}/p_i^{e_i}$ という形の群の直積に書けるので，(1) が証明された．

(2) 一意性を $|G|$ に関する帰納法で示す．$|G| = p$ のときは上に述べた通りである．(1) の証明の中で，P と H は G から一意的に定まる部分群である．$p_1 = \cdots = p_k = p$ で，$p > p_{k+1} \geqq \cdots \geqq p_r$ となるような k を取る．

$$P' := (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z}), \quad H' := (\mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})$$

とおく．$G \cong P' \times H'$ で，定義から $P \cong P'$, $H \cong H'$ である．定理 8.4 から，任意の同型写像 $\varphi : P \times H \longrightarrow P' \times H'$ は $\varphi(P) = P'$, $\varphi(H) = H'$ を満たす．よって，P, H について帰納法の仮定を適用すれば，r, p_i, e_i は G から一意的に定まることがわかる． □

上の定理と，以下の中国剰余定理を組み合わせて使うと，有限アーベル群は，かなり楽に扱える．ただ，アーベル群 $\mathbb{Z}/n\mathbb{Z}$ は $+$ についての群の構造以外に，$(x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z}$ $(x,\, y \in \mathbb{Z})$ で定まる積 (乗法) を持っていて，定義 8.1 で説明した可換環になる．R_1, R_2 が環で，$f\colon R_1 \longrightarrow R_2$ が $+$ についてのアーベル群としての準同型写像であって，さらに

(1) 任意の $x,\, y \in R_1$ に対して $f(xy) = f(x)f(y)$ が成り立つ．

(2) $f(1_{R_1}) = 1_{R_2}$.

を満たすとき，$f\colon R_1 \to R_2$ は環としての**準同型**写像であるという．さらに，f が全単射のとき，f は環としての**同型**写像であるといい，同型写像 f が存在するとき R_1 と R_2 は環として同型であるという．

$$(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})$$

も，単にアーベル群であるだけでなく，各直積因子毎の積 (乗法) によって全体の積 (乗法) を定めることによって，可換環になる．単位元 1 は各直積因子の 1 を並べたものである．以下の中国剰余定理は，アーベル群としての同型より強く，可換環としての同型を主張している．

定理 9.2.(中国剰余定理) 2 以上の自然数 n が $n = p_1^{e_1} \cdots p_r^{e_r}$ $(p_1,\ldots,\, p_r$ は相異なる素数) と素因数分解できたとする．写像 $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_r^{e_r}\mathbb{Z})$ を

$$f(x + n\mathbb{Z}) = \left(x + p_1^{e_1}\mathbb{Z},\, \ldots,\, x + p_r^{e_r}\mathbb{Z}\right)$$

で定める．この写像 f は可換環としての同型写像である．

証明. f が環の準同型写像であることは，$f(xy) = f(x)f(y)$ を確認すればよく，すぐわかる．あと，f が全単射であることを示せばよいが，元の個数が等しい有限集合の間の写像なので，f が単射であることを示せば，f が全単射であることがわかる．f は (少なくとも群の) 準同型写像なので，$\mathrm{Ker}\, f = f^{-1}(0) = \{0\}$ を示せば f が単射であることがわかる．

勝手な $x + n\mathbb{Z} \in \mathrm{Ker}\, f \subset \mathbb{Z}/n\mathbb{Z}$ $(x \in \mathbb{Z})$ を取る．$0 \leqq x < n$ と仮定してよい．$f(x + n\mathbb{Z}) = 0$ なので，$x + p_i^{e_i}\mathbb{Z} = 0 \in \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ $(1 \leqq \forall i \leqq r)$ である．これは，x が $p_i^{e_1}$ の倍数であることを意味している．$p_1^{e_1},\ldots,\, p_r^{e_r}$ は互いに素なので，x は $p_1^{e_1} \cdots p_r^{e_r} = n$ の倍数である．$0 \leqq x < n$ であったので $x = 0$ となる．よって，$\mathrm{Ker}\, f = \{0\}$ で f は単射であり，同型写像である． □

上の定理から，p, q が相異なる素数のときは，$\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}\cong\mathbb{Z}/pq\mathbb{Z}$ となり，巡回群になるが，$\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ と $\mathbb{Z}/p^2\mathbb{Z}$ は同型ではない．実際 $\mathbb{Z}/p^2\mathbb{Z}$ には位数 p^2 の元 (例えば $1+p^2\mathbb{Z}$) が存在するが，$\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ の元の位数は p か 1 のいずれか (0 のみ位数 1 で，それ以外の元の位数はすべて p) であるので，$\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ と $\mathbb{Z}/p^2\mathbb{Z}$ は同型になり得ない．また，$\mathbb{Z}/p^2\mathbb{Z}$ は巡回群であるが，$\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ は巡回群ではない．なお，定理 7.5 で証明したように，$p>q$ で $p-1$ が q の倍数でないときは，位数 pq の群 G は $\mathbb{Z}/pq\mathbb{Z}$ と同型であった．しかし，$p-1$ が q の倍数だと $\mathbb{Z}/pq\mathbb{Z}$ 以外に位数 pq の群が存在し得る．例えば $p=3$, $q=2$ の場合，3 次対称群 $\mathfrak{S}_3$ は位数 6 であるがアーベル群でない群である．

10. 組成列

ここからの話はまた可換とは限らない群に戻るので，演算は積の記号で表す．単位元は 1 である．

G は群，$N\lhd G$, $A\subset G$ (部分集合) とし，$\pi\colon G\to G/N$ を自然な全射とする．ものもとの定義は $G/N:=\{gN\mid g\in G\}$ であるので，$\pi(A)=\{aN\mid a\in A\}$ である．$\pi(g)=gN$ だから $\pi(A)=AN$ と書いてもいいが，そうすると，$AN\in G/N$ と考えているのか $AN\subset G$ と考えているのか区別がつかない．そこで，AN の代わりに $\pi(A)=AN/N\subset G/N$ と書くことにする．その流儀で書くと，$\pi(g)=gN/N$ ということになる．定義に戻れば gN/N は gN のことなのであるが，gN のほうは $gN\in G/N$ と $gN\subset G$ の 2 つの見方が可能であるが，gN/N という書き方だと $gN/N\in G/N$ と解釈するしかない．分母の N は N から定まる同値関係で割っている (類別している) んだよ，という気持ちを表わしている．また，$A=AN$ の場合は，AN/N を単に A/N と書く．

さて，先に，ちょっと記号がごちゃごちゃして分かりにくい補題を 1 つ証明しておく．証明の中に上の記号の使い方が登場する．

定理 10.1.(ツァッセンハウスの補題) G は積に関する群，H と K は G の部分群，$H'\lhd H$, $K'\lhd K$ とする．このとき，以下が成り立つ．
(1) $H'(H\cap K')\lhd H'(H\cap K)$, $K'(H'\cap K)\lhd K'(H\cap K)$.
(2) $H'(H\cap K)/H'(H\cap K')\cong K'(H\cap K)/K'(H'\cap K)$.

証明. $H\cap K\subset H'(H\cap K)\subset H$ である．定理 3.5(1) より，$H'(H\cap K)$ と $H'(H\cap K')$ は H の部分群である．また，$H'\lhd H$ より，$H'\lhd H'(H\cap K)$ である．これに $\cap K$ を行うと，

$$H'\cap K\lhd H'(H\cap K)\cap K=(H'\cap K)(H\cap K)=H\cap K$$

が得られる．第 2 同型定理 $H_0/(H_0\cap N)\cong(H_0N)/N$ を $N:=H'\lhd H_0:=H\cap K$ として適用すると，同型写像

$$f:(H\cap K)/(H'\cap K)\xrightarrow{\cong}H'(H\cap K)/H' \qquad ①$$

が得られる．対称性から，(H,H') と (K,K') を交換した式も成立し，$K'(H\cap K)$ と $K'(H'\cap K)$ は K の部分群，$H\cap K'\lhd H\cap K$ である．$H'\cap K\lhd H\cap K$ の $H\cap K'$ を法とする同値類を $(H'\cap K)(H\cap K')/(H\cap K)\lhd(H\cap K)/(H'\cap K)$ — ② とみなすとき，

$$f\big((H'\cap K)(H\cap K')/(H'\cap K)\big)=H'(H\cap K')/H'\subset H'(H\cap K)/H'$$

となる．ここで，② より $H'(H\cap K')/H'\lhd H'(H\cap K)/H'$ となる．これより，$H'(H\cap K')\lhd H'(H\cap K)$ となり，(1) の最初の式が得られた．(1) のもう 1 つの式は，(H,H') と (K,K') の対称性から得られる．

さて，第 3 同型定理より ① の両辺をこれらで割って，f から同型写像

$$\overline{f}:(H\cap K)/(H'\cap K)(H\cap K')\xrightarrow{\cong}H'(H\cap K)/H'(H\cap K') \qquad ③$$

が得られる．(H,H') と (K,K') の対称性から，同型写像

$$\overline{g}:(H\cap K)/(H'\cap K)(H\cap K')\xrightarrow{\cong}K'(H\cap K)/K'(H'\cap K) \qquad ④$$

も存在する．③ と ④ から，同型写像

$$\overline{g}\circ\overline{f}^{-1}:H'(H\cap K)/H'(H\cap K')\xrightarrow{\cong}K'(H\cap K)/K'(H'\cap K)$$

が得られ，(2) がわかる． □

定義 10.2.(正規列・組成列) G は積に関する群とする．部分群の列

$$G=G_0\rhd G_1\rhd G_2\rhd\cdots\rhd G_r=\{1\} \qquad ①$$

(各 $i = 1,\ldots, r$ に対して G_i は G_{i-1} の正規部分群である，という意味．G_i は必ずしも G の正規部分群ではない) を，G の**正規列**という．

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_l = \{1\} \qquad ②$$

も正規列であるとする．

(1) 正規列 ① において，$G_i = G_{i-1}$ となるような $i \in \{1,\ldots, r\}$ が存在しないとき，① は**固有**の正規列であるという．
(2) ある単射 $\varphi : \{1,\ldots, r\} \longrightarrow \{1,\ldots, l\}$ で $i < j$ ならば $\varphi(i) < \varphi(j)$ を満たすものが存在し，$G_i = H_{\varphi(i)}$ $(1 \leqq \forall i \leqq r)$ を満たすとき，正規列 ② は正規列 ① の**細分**であるという．さらに，ある $1 \leqq j \leqq r$ を選ぶと H_j がどの G_i とも一致しないとき，正規列 ② は正規列 ① の**真の細分**であるという．
(3) 正規列 ① が固有の正規列であって，真の細分を持たないとき，① は**組成列**であるという．
(4) $r = l$ であって，ある全単射 $\sigma : \{1,\ldots, r\} \longrightarrow \{1,\ldots, r\}$ が存在し，$H_{\sigma(i)-1}/H_{\sigma(i)} \cong G_{i-1}/G_i$ を満たすとき，① と ② は**同値**であるという．

定理 10.3.(シュライアーの細分定理) G は積に関する群とし，上の定義の ① と ② のような正規列を持つとする．すると，① の細分であるようなある正規列 (S_1) と，② の細分であるようなある正規列 (S_2) で，(S_1) と (S_2) が同値になるようなものが存在する．

証明. $1 \leqq i \leqq r$, $1 \leqq j \leqq l$ に対して，

$$K_{l(i-1)+j} = G_i(G_{i-1} \cap H_j), \quad L_{r(j-1)+i} = H_j(H_{j-1} \cap G_i)$$

とおく．また，$K_0 = L_0 = G$ とおく．$1 \leqq j < l$ のときは $H_j \rhd H_{j+1}$ なので定理 10.1(1) より，$K_{l(i-1)+j} \rhd K_{l(i-1)+j+1}$ である．また，$j = l$ のときは，

$$K_{l(i-1)+l} = K_{li} = G_i(G_{i-1} \cap H_l) = G_i = G_{i+1}(G_i \cap H_0) \rhd G_{i+1}(G_i \cap H_1) = K_{li+1}$$

とうまくつながっている．$L_{r(j-1)+i}$ のほうも同様である．よって，2 つの正規列

$$(S_1) \quad G = K_0 \rhd K_1 \rhd \cdots \rhd K_{lr} = \{1\}, \quad (S_2) \quad G = L_0 \rhd L_1 \rhd \cdots \rhd L_{lr} = \{1\}$$

が得られる．定理 10.1(2) を $H = G_{i-1}$, $H' = G_i$, $K = H_{j-1}$, $K' = K_j$ として用いると，

$$\begin{aligned} K_{l(i-1)+j-1}/K_{l(i-1)+j} &= G_i(G_{i-1} \cap H_{j-1})/G_i(G_{i-1} \cap H_j) \\ &\cong H_j(H_{j-1} \cap G_{i-1})/H_j(H_{j-1} \cap G_i) = L_{r(j-1)+i-1}/L_{r(j-1)+i} \end{aligned}$$

が得られる．よって，(S_1) と (S_2) は同値である． □

一般には，群 G が組成列を持つとは限らないが，もし組成列を持てば，次の定理の意味で同値を除いて一意的である．

定理 10.4.(ジョルダン・ヘルダーの定理) G は積に関する群とし，定義 10.2 の正規列 ①，② はいずれも組成列であると仮定する．すると，① と ② は同値である．

証明. シュライアーの細分定理より，① の細分 $(S_1) : G = K_0 \rhd \cdots \rhd K_n = \{1\}$ と，② の細分 $(S_2) : G = L_0 \rhd \cdots \rhd L_n = \{1\}$ で，(S_1) と (S_2) が同値になるようなものが存在する．ところで，① は真の細分を持たないから，$\mathfrak{K} := \{K_{i-1}/K_i \mid 1 \leqq i \leqq n\}$ は $\mathfrak{G} := \{G_{i-1}/G_i \mid 1 \leqq i \leqq r\}$ に何個かの $\{1\}$ を付け加えただけのものである．だから集合としては $\mathfrak{K} = \mathfrak{G} \cup \{\{1\}\}$ である．同様に，$\mathfrak{L} := \{L_{i-1}/L_i \mid 1 \leqq i \leqq n\}$ は $\mathfrak{H} := \{H_{i-1}/H_i \mid 1 \leqq i \leqq r\}$ に何個かの $\{1\}$ を付け加えただけのもので，$\mathfrak{L} = \mathfrak{H} \cup \{\{1\}\}$ である．シュライアーの細分定理より $\mathfrak{K} = \mathfrak{L}$ であったから，$\mathfrak{G} = \mathfrak{H}$ である． □

11. 交換子と可解群

定義 11.1. G は積の関する群とする．$a, b \in G$ に対し，

$$[a, b] := a^{-1}b^{-1}ab$$

を a と b の**交換子**という．H と K が G の部分群のとき，集合 $\{[a, b] \mid a \in H, b \in K\}$ を含む G の最小の部分群を H と K の**交換子群**といい $[H, K]$ で表す．$H = K$ のときは $[H, H]$ を H の交換子群という．$[H, H]$ を $D(G)$ と書くこともある．

$[a,\, b] := aba^{-1}b^{-1}$ と定義する流儀もあるが，その場合，$a^{-1}b^{-1}ab = [a^{-1},\, b^{-1}]$ であるので，どちらの定義を採用しても $[H,\, K]$ は同じ群になるので，以下の理論は同じものになる．この講義では，$[a,\, b] := a^{-1}b^{-1}ab$ としておく．

上の交換子 $[a,\, b] := a^{-1}b^{-1}ab$ と，正方行列 $A,\, B$ の交換子 $[A,\, B] = AB - BA$ と混同しないこと．ただ，用途は結構似ている．

定理 11.2. G は積に関する群とし，$a,\, b,\, c \in G$ とする．
(1) $[a,\, b] = 1 \iff ba = ab$.
(2) $c^{-1}[a,\, b]c = [c^{-1}ac,\, c^{-1}bc]$.

証明. 簡単なので省略. □

定義 11.3. G は積に関する群とする．$G_0 := G,\, G_{i+1} := [G_i,\, G_i]$ $(i \geqq 0)$ で $G_0 \supset G_1 \supset \cdots$ を定義するとき，ある $r \in \mathbb{N}$ が存在して $G_r = \{1\}$ となるばらば，G は**可解群**であるという．$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$ を G の**可解列**という．

定理 11.4. G は群とする．
(1) $[G,\, G] \lhd G$ である．
(2) $G/[G,\, G]$ はアーベル群である．
(3) 正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ で，各 $i = 1,\ldots,\, r$ に対して G_{i-1}/G_i がアーベル群になるものが存在すれば，G は可解群である．
(4) $N \lhd G$ で，G/N と N が可解群ならば，G も可解群である．
(5) G が有限可解群ならば，正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ で，各 $i = 1,\ldots,\, r$ に対して G_{i-1}/G_i が位数が素数の巡回群になるものが存在する．

証明. (1) $a,\, b,\, c \in G$ のとき，$a' = c^{-1}ac,\, b' = c^{-1}bc$ とおくと，$c^{-1}[a,b]c = [a',b']$ だから．

(2) $ba = abb^{-1}a^{-1}ba = ab[b,a] \in ab[G,\, G]$ である．よって，$ba[G,\, G] = ab[G,\, G]$ で，$G/[G,\, G]$ はアーベル群である．

(3) $\pi_i \colon G_{i-1} \longrightarrow G_{i-1}/G_i$ を自然な全射とする．$\pi_i([G_{i-1},\, G_{i-1}]) \neq \{1\}$ とすると，ある $a,\, b \in G_{i-1}$ で $[a,b] \notin G_i$ となるものが存在する．つまり，$\pi_i(a^{-1}b^{-1}ab) \neq 1$ なので，$\pi_i(a)\pi_i(b) \neq \pi_i(b)\pi_i(a)$ となる．これは G_{i-1}/G_i がアーベル群であることに矛盾する．よって，$[G_{i-1},\, G_{i-1}] \lhd G_i$ である．

$N_0 := G,\, N_i := [N_{i-1},\, N_{i-1}]$ $(i \geqq 1)$ で正規列 $G = N_0 \rhd N_1 \rhd \cdots$ を定める．$N_{i-1} \subset G_{i-1}$ ならば，$N_i = [N_{i-1},\, N_{i-1}] \subset [G_{i-1},\, G_{i-1}] = G_i$ なので，i に関する帰納法で，$N_i \subset G_i$ が証明できる．よって，$N_r = \{1\}$ で，G は可解群である．

(4) $\pi \colon G \to G/N$ を自然な全射とする．$H_0 := G/N,\, H_{i+1} = [H_i,\, H_i]$ $(i \geqq 0)$ とするとき，ある $m \in \mathbb{N}$ で $H_m = \{1\}$ となる．$N_i := \pi^{-1}(H_i)$ とおくと，$G = N_0 \rhd N_1 \rhd \cdots \rhd N_m = N$ で，各 $i = 1,\ldots,\, m$ に対して N_{i-1}/N_i がアーベル群になる．これに N の可解列をつなげば，(3) を満たす G の正規列が得られる．

(5) 有限アーベル群の構造定理からわかる． □

定理 11.5. G が可解群ならば，G の部分群 H も可解群である．

証明. $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ を G の可解列とする．$H_i := H \cap G_i$ とおく．各 $1 \leqq i \leqq r$ に対して．$G_i \lhd G_{i-1}$ より $H_i \lhd H_{i-1}$ である．同型定理より，

$$H_{i-1}/H_i = H_{i-1}/(G_i \cap H_{i-1}) \cong H_{i-1}G_i/G_i \subset G_{i-1}/G_i$$

で，G_{i-1}/G_i がアーベル群なので H_{i-1}/H_i もアーベル群である．よって，H も可解群である． □

定義 11.6. 群 G が $\{1\}$ と G 以内に正規部分群を持たないとき，G は**単純群**であるという．

命題 11.7. G は積に関する群とする．
(1) G が単純群でアーベル群でないならば，G は可解群でない．

(2) $[G, G] = G$ ならば G は単純群である．

証明. (1) $[G, G] \lhd G$ であるが，G が単純群だと，G の正規部分群は G と $\{1\}$ しかないので，$[G, G] = G$ または $[G, G] = \{1\}$ である．$[G, G] = \{1\}$ だと，任意の $a, b \in G$ に対して $[a, b] \in [G, G] = \{1\}$ となり，$a^{-1}b^{-1}ab = [a, b]$ となる．よって，$ab = ba$ となり，G はアーベル群になってしまう．したがって，$[G, G] = G$ である．これが G は可解群でないことを意味する． □

自然数 n に対し $X_n := \{1, 2, \ldots, n\}$ とし，

$$\mathfrak{S}_n := \{\sigma \mid \sigma: X_n \to X_n \text{ は全単射}\}$$
$$\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \mid \mathrm{sign}(\sigma) = 1\}$$

とおく．ここで，$\mathrm{sign}(\sigma)$ は置換 σ の符号である．$\mathfrak{S}_n$ を n 次**対称群**, $\mathfrak{A}_n$ を n 次**交代群**といった．

定理 11.8.
(1) $n \geqq 2$ のとき $\mathfrak{A}_n$ は $\mathfrak{S}_n$ の正規部分群で，$\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ である．
(2) $n \geqq 5$ のとき $\mathfrak{A}_n$ は単純群である．

証明. (1) 偶置換の合成や逆置換は偶置換であるので，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の部分群である．$\mathfrak{B}_n$ は $\mathfrak{S}_n$ の部分群である．$\tau \in \mathfrak{S}_n$ が互換のとき，$\tau\mathfrak{A}_n$ は $\mathfrak{S}_n$ 内の奇置換全体の集合である．$\mathfrak{A}_n\tau$ も $\mathfrak{S}_n$ 内の奇置換全体の集合でなので，$\tau\mathfrak{A}_n = \mathfrak{A}_n\tau$ である．よって，$\mathfrak{A}_n \lhd \mathfrak{S}_n$ である．また，$\mathfrak{S}_n = \mathfrak{A}_n \sqcup \tau\mathfrak{A}_n$ なので，$\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ である．

(2) 一般に，(i, j) は i と j の互換とする．$2 \leqq i < j \leqq n$ に対し，$(i, j) = (1, i)(1, j)(1, i) \in \mathfrak{S}_n$ で，$\mathfrak{A}_n$ の元は偶数個の互換の積で表せるから，$\mathfrak{A}_n$ の元は $(1, i)$ $(2 \leqq i \leqq n)$ という形の互換偶数個の積で表せる．

$1 \leqq i < j < k \leqq n$ に対し，$(i, j, k) \in \mathfrak{A}_n$ は i, j, k の巡回置換 $(i \to j, j \to k, k \to i.$ これは偶置換である) を表すとする．$(1, 2)(1, j) = (1, 2, j)^2$, $(1, i)(1, j) = (1, 2, i)(1, 2, j)^2$ だから，$\mathfrak{A}_n$ は $\{(1, 2, i) \mid 3 \leqq i \leqq n\}$ で生成される．

今，i, j, k は 3 以上 n 以下の相異なる整数とする．巡回置換は偶置換だから，$\sigma := (k, i, i) \in \mathfrak{A}_n$, $\tau := (j, 2, k) \in \mathfrak{A}_n$ である．ところが，

$$[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau = (1, i, k)(k, 2, j)(k, i, 1)(j, 2, k) = (1, 2, k)$$

である．したがって，$[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$ である．よって，$\mathfrak{A}_n$ は単純群である． □

次の定理は将来ガロア理論で大切になる．

定理 11.9.
(1) $n \leqq 4$ のとき，$\mathfrak{S}_n$, $\mathfrak{A}_n$ は可解群である．
(2) $n \geqq 5$ のとき，$\mathfrak{S}_n$, $\mathfrak{A}_n$ は可解群でない．

証明. (1) $n \leqq 4$ のとき $\mathfrak{S}_n$ と $\mathfrak{A}_n$ は $\mathfrak{S}_4$ の部分群であるので，$\mathfrak{S}_4$ が可解群であることを示せばよい．
$1 \leqq i < j \leqq 4$ に対して $(i, j) \in \mathfrak{S}_4$ は i と j の互換を表すとし，

$$V_4 := \{\mathrm{id}_{X_4}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

とすると，$\mathfrak{S}_4 \rhd \mathfrak{A}_4 \rhd V_4 \rhd \{1\}$ で，$\mathfrak{S}_4/\mathfrak{A}_4 \cong \mathbb{Z}/2\mathbb{Z}$, $\mathfrak{A}_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$, $V_4/\{1\} = V_4 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ である．よって，$\mathfrak{S}_4$ は可解群である．

(2) $n \geqq 5$ のとき，$\mathfrak{A}_5$ は単純群なので可解群でない． □

12. 巾零群

定理 12.1. G は有限群，$P \subset G$ は p-シロー群，$N \lhd G$ で，$P \subset N$ であると仮定する．すると，$G = N \cdot N_G(P)$ が成り立つ．

証明. P は N の p-シロー群でもある．$a \in G$ とすると，$aPa^{-1} \subset aNa^{-1} = N$ であるから，aPa^{-1} は N の p-シロー群にもなる．よって，ある $b \in N$ により，$aPa^{-1} = bPb^{-1}$ と書ける．$(b^{-1}a)P(b^{-1}a)^{-1} = P$ だから $b^{-1}a \in N_G(P)$ である．$(N_G(P) = \{c \in G \mid cPc^{-1} = P\}$ であった.)

よって，$a \in bN_G(P) \subset N \cdot N_G(P)$ であり，$G \subset N \cdot N_G(P)$ である．$\supset$ は自明だから，$G = N \cdot N_G(P)$ が成り立つ． □

定義 12.2. G は群とする．部分群の列

$$(*) : G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

で，各 $i = 1, 2, \ldots, n$ に対して，

$$G_i \lhd G, \quad G_{i-1}/G_i \subset Z(G/G_i)$$

を満たすものを G の**中心列**という．G がこのような中心列をもつとき，G は**巾零群**であるという．

$G_i \lhd G$ ならば $G_i \lhd G_{i-1}$ であるから，中心列は正規列である．

$H \subsetneqq G$ が部分群で，$H \subsetneqq K \subsetneqq G$ を満たす部分群 K が存在しないとき，H は G の**極大部分群**であるという．

命題 12.3. 巾零群は可解群である．

証明. 中心列は，定理 11.4(3) の条件を満たしている． □

命題 12.3.
(1) G が巾零群で，H が G の部分群ならば，H も巾零群である．
(2) G が巾零群で，$N \lhd G$ ならば，G/N も巾零群である．
(3) $G_1, \ldots, G_m$ が巾零群ならば，$G_1 \times \cdots \times G_m$ も巾零群である．

証明. (1) $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ を中心列とする．$H_i := G_i \cap H$ とおく．$G_i \lhd G$ より $H_i = G_i \cap H \lhd H$ である．$f\colon H_{i-1} \xrightarrow{\subset} G_{i-1} \to G_{i-1}/G_i$ を包含写像と自然な全射の合成写像とする．$\operatorname{Ker} f = G_i \cap H_{i-1} = G_i \cap (G_{i-1} \cap H) = G_i \cap H = H_i$ なので，準同型定理から，単射準同型写像 $\overline{f}\colon H_{i-1}/H_i \longrightarrow G_{i-1}/G_i$ が誘導される．$G_{i-1}/G_i \subset Z(G/G_i)$ だから，$H_{i-1}/H_i \subset Z(H/H_i)$ である．よって，H は巾零群である．

(2) $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ を中心列とし，$\pi\colon G \to G/N$ を自然な全射とする．$K_i := \pi(G_i) = G_iN/N$ とする．$G_iN \lhd G$ より $K_i \lhd G/N$ である．第 3 同型定理より，$K_{i-1}/K_i \cong G_{i-1}N/G_iN$ である．

$G_{i-1}/G_i \subset Z(G/G_i)$ だから，任意の $a \in G_{i-1}$ と $g \in G$ に対して $agG_i = gaG_i$ が成り立つ．したがって，$agG_iN = gaG_iN$ である．これより，$G_{i-1}N/G_iN \subset Z(GN/G_iN)$ であり，(2) がわかる．

(3) $m = 2$ の場合に証明すれば，あとは m に関する帰納法ですぐわかる．G_1, G_2 を改めて G, H と書き，古い G_i の記号は捨てて，改めて，$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ と $H = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}$ を中心列とする．$0 \leqq i \leqq n$ に対し $K_i := G_i \times H$ とし，$1 \leqq j \leqq m$ に $K_{n+j} := G_n \times H_j$ とおく．$H_n = G_n \times H = G_n \times H_0$ である．$1 \leqq i \leqq n$ のとき，$G_i \lhd G$ より $G_i \times H \lhd G \times H$ である．また，同型定理から

$$K_{i-1}/K_i = (G_{i-1} \times H)/(G_i \times H) \cong G_{i-1}/G_i \subset Z(G/G_i) \cong Z(K_0/K_i)$$

である．$1 \leqq j \leqq m$ のときは，$K_{n+j-1} = G_n \times H_{j-1} \lhd G_n \times H$ だっから，$K_{n+j-1} \lhd G \times H$ もわかる．また，

$$K_{n+j-1}/K_{n+j} = (G_n \times H_{j-1})/(G_n \times H_j) \cong H_{j-1}/J_i \subset Z(G/H_j) \cong Z(K_n/K_{n+j}) \subset Z(K_0/K_{n+j})$$

である．よって，$G \times H = K_0$ も巾零群である． □

定理 12.4. G は巾零群とする．
(1) $H \subsetneqq G$ が部分群ならば，$H \subsetneqq N_G(H)$ が成り立つ．
(2) H が G の極大部分群ならば，$H \lhd G$ である．

証明. (1) $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ を中心列とする．$H \supset G_i$, $H \not\supset G_{i-1}$ となる $1 \leqq i \leqq n$ がある．$G_{i-1}/G_i \subset Z(G/G_i)$ だから，任意の $a \in G_{i-1}$ と $h \in H \subset G$ に対して $ahG_i = haG_i$, つま

り，$aha^{-1}h^{-1} = [a^{-1}, h^{-1}] \in G_i \subset H$ となる．$h \in H$ だから $aha^{-1} \in H$ であり，$a \in N_G(H)$ となる．よって，$G_{i-1} \subset N_G(H)$ である．

$H \subset N_G(H)$ であるが，もし $H = N_G(H)$ とすると，$G_{i-1} \subset H$ となって矛盾する．よって，$H \subsetneqq N_G(H)$ である．

(2) H が G の極大部分群ならば，(1) より $N_G(H) = G$ である．したがって，$H \lhd G$ である． □

命題 12.5. p は素数，G は p-群 ($|G| = p^n$) とする．すると，ある $1 \leqq k \leqq n$ により $|Z(G)| = p^k$ となる．

証明. 類等式 $|G| = |Z(G)| + \sum_{|Cx_i| \geqq 2} |Cx_i|$ において，$1 \in Z(G) \lhd G$ で，定理 6.5 より $|Cx_i| = [G : N_G(x_i)]$ なので，$|Cx_i| \geqq 2$ ならば $|Cx_i|$ は p の倍数である．よって，類等式より $|Z(G)|$ は p の倍数である．$|Z(G)|$ は $|G| = p^n$ の約数だから，ある $1 \leqq k \leqq n$ により $|Z(G)| = p^k$ とかける． □

定理 12.6. G を有限群とするとき，次の (1) 〜 (4) は同値である．
(1) G は巾零群である．
(2) G の任意の極大部分群は正規部分群である．
(3) G の任意の p-シロー群は正規部分群である．
(4) G は何個かの p-シロー群の直積である．

証明. (1) $\Longrightarrow$ (2). 定理 12.4(2) で示した．

(2) $\Longrightarrow$ (3). (2) を仮定し，$P \subset G$ は p-シロー群とする．P が G の正規部分群でないと仮定すると，$N_G(P) \subsetneqq G$ である．$N_G(P)$ を含む H の極大部分群 $H \subsetneqq G$ が存在する (G が有限群だから Zorn の補題など使わなくてもすぐ証明できる)．(2) より $H \lhd G$ である．定理 12.1 より $G = H \cdot N_G(P)$ が成り立つ．$N_G(P) \subset H$ なので $H \cdot N_G(P) = H$ であり，$G = H$ となって矛盾する．

(3) $\Longrightarrow$ (4). $G = p_1^{e_1} \cdots p_r^{e_r}$ ($p_1, \ldots, p_r$ は相異なる素数) とし，G の p_i-シロー群を P_i とする．$G = P_1 \cdots P_r$ である．(4) を r に関する帰納法で証明する．$r = 1$ なら自明．

$r \geqq 2$ とし，$N := P_1 \cdots P_{r-1}$ とおく．N も (3) を満たし，帰納法の仮定から $N = P_1 \times \cdots \times P_{r-1}$ である．$G = NP_r$ である．$|N|$ と $|P_r|$ は互いに素だから，$N \cap P_r = \{1\}$ である．(3) より $P_r \lhd G$ である．また，$P_i \lhd G$ $(1 \leqq i < r)$ より，$N \lhd G$ である．よって，定理 5.6 より $G \cong N \times P_r = P_1 \times \cdots \times P_r$ となる．

(4) $\Longrightarrow$ (1). 命題 12.3(3) より，G が p-群の場合に証明すれば十分である．$|G| = p^e$ とし，e に関する帰納法で証明する．$e = 1$ なら $G \cong \mathbb{Z}/p\mathbb{Z} \supset \{1\}$ が中心列で，G は巾零群である．

$e \geqq 2$ とする．前命題より $|Z(G)|$ は p の倍数である．$Z(G) \lhd G$ だから，$H := G/Z(G)$ とおくと，帰納法の仮定により H は巾零群である．$\pi: G \longrightarrow G/Z(G) = H$ を自然な全射とし，$H = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}$ を中心列とする．$G_i := \pi^{-1}(H_i)$ $(0 \leqq i \leqq m)$ とし，$G_{m+1} := \{1\}$ とする．$1 \leqq i \leqq m$ のとき，$H_i \lhd H$ より $G_i \lhd G$ である．また，$H_{m+1} = \{1\} \lhd G$ である．第 3 同型定理より $H_{i-1}/H_i \cong G_{i-1}/G_i$，$H/H_i \cong G/G_i$ である．よって，$Z(H/H_i) \cong Z(G/G_i)$ である．よって，$H_{i-1}/H_i \subset Z(H/H_i)$ から $G_{i-1}/G_i \subset Z(G/G_i)$ がわかる．また，$G_{m-1}/G_m = Z(G) = Z(G/G_m)$ である．したがって，$G = G_0 \supset G_1 \supset \cdots \supset G_{m+1} = \{1\}$ は中心列であり，G は巾零群である． □

13. 位数の 12 以下の有限群 (1)

命題 13.1. G は積に関する非アーベル群とする．すると $G/Z(G)$ は巡回群ではない．

証明. $\{1\} \neq G/Z(G)$ が巡回群であるとする．$m := |G/Z(G)|$ とおくと $G/Z(G) \cong \mathbb{Z}/m\mathbb{Z}$ で，ある $g \in G$ を選ぶと同値類 $gZ(G)$ が $G/Z(G)$ を生成する．勝手な $a \in G$ を取ると，ある $i \in \mathbb{Z}$ によって $a \in g^i Z(G)$ となり，ある $z_1 \in Z(G)$ によって $a = g^i z_1$ と書ける．別の $b \in G$ も $b = g^j z_2$ $(z_2 \in Z(G))$ と書ける．ところが，$gz_i = z_i g$ だから，$ba = g^{i+j} z_1 z_2 = ab$ となり，G はアーベル群になり，矛盾する． □

定理 13.2. p は素数，G は有限群で，$|G| = p^2$ ならば，G はアーベル群である．よって，$G \cong \mathbb{Z}/p^2\mathbb{Z}$ または $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ である．

証明. 命題 12.5 より，$|Z(G)| = p^2$ または $|Z(G)| = p$ である．もし，$|Z(G)| = p^2$ なら $Z(G)$ の定義から G はアーベル群である．もし，$|Z(G)| = p$ ならば，$G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ は巡回群になるので，前定理より G はアーベル群である．(この場合は $Z(G) = G$ となり矛盾する.)
最後の分類は有限アーベル群の構造定理からわかる． □

定義 13.3. X_n は平面上の正 n 角形とする．平面上の合同変換 $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ で $f(X_n) = X_n$ を満たすもの全体の集合を D_n とする．D_n は写像の合成に関して群になる．D_n を**二面体群**という．

X_n はその中心が原点 O で，単位円に内接し，ひとつの頂点が $(1, 0)$ であると仮定しても一般性を失わない．R は原点を中心とする角度 $2\pi/n$ の回転，S を x 軸に関する対称移動とすれば，D_n は R_n と S で生成される群である．$C_n := \left\{R^i \in D_n \;\middle|\; i \in \mathbb{Z}\right\}$ は D_n の正規部分群で，$D_n = C_n \sqcup C_n \cdot S$ である．また，$R^n = 1$, $S^2 = 1$, $SRS = R^{-1}$ という関係式を満たす．
逆に群 G が $r, s \in G$ で生成され，$r^n = s^2 = 1$, $srs = r^{-1}$ を満たすとき，$\varphi\colon D_n \to G$ を $\varphi(R^i S^j) = r^i s^j$ で定めると全射順同型写像になる．$s \neq 1$ で，$r^i = 1$, $1 \leqq i < n$ を満たす i が存在しなければ，$\varphi\colon D_n \to G$ は同型写像になる．

定理 13.4. p は 3 以上の素数とし，G は積に関する群で $|G| = 2p$ と仮定する．すると，$G \cong \mathbb{Z}/2p\mathbb{Z}$ または $G \cong D_{2p}$ である．

証明. G がアーベル群ならば，有限アーベル群の構造定理より，$G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$ である．
以下，G が非アーベル群の場合を考える．G は巡回群でないから，位数 $2p$ の元を持たない．P を G の p-シロー群，Q を 2-シロー群とする．定理 7.5(1) より，$P \lhd G$, $G = PQ$, $P \cap Q = \{1\}$ である．巡回群 P の生成群を r, Q の生成元を s とする．$r^p = s^2 = 1$ である．$P \lhd G$ より $srs = srs^{-1} \in P$ だから，ある $1 \leqq k \leqq p-1$ により $srs = r^k$ と書ける．

$$r = s^2 r s^2 = s(srs)s = sr^k s^{-1} = (srs^{-1})^k = (r^k)^2 = r^{k^2}$$

なので，$r^{k^2-1} = 1$ であり，$(k-1)(k+1) = k^2 - 1 \equiv 0 \pmod{p}$ である．p は素数なので，$k-1$ または $k+1$ は p の倍数で，$1 \leqq k \leqq p-1$ により $k = 1$ または $k = p-1$ である．
もし，$k = 1$ だと，$srs = r$, $s = s^{-1}$ より $sr = rs$ となって，G はアーベル群になる．よって，$srs = r^{p-1}$ である．この定理の直前の考察から，$G \cong D_p$ となる． □

$p = 3$ のとき $|\mathfrak{S}_3| = 6 = 2p$ で $\mathfrak{S}_3$ はアーベル群でないから $\mathfrak{S}_3 \cong D_3$. である．(直接同型写像を構成してもよい.)

位数 12 以下の有限群 G を考える．今までの諸定理から，以下が分かる．

定理 13.5.
(1) $|G| = 1$ ならば $G = \{1\}$ である．
(2) $|G| = 2$ ならば $G \cong \mathbb{Z}/2\mathbb{Z}$ である．
(3) $|G| = 3$ ならば $G \cong \mathbb{Z}/3\mathbb{Z}$ である．
(4) $|G| = 4$ ならば $G \cong \mathbb{Z}/4\mathbb{Z}$ または $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．
(5) $|G| = 5$ ならば $G \cong \mathbb{Z}/5\mathbb{Z}$ である．
(6) $|G| = 6$ ならば $G \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ または $G \cong D_3 \cong \mathfrak{S}_3$ である．
(7) $|G| = 7$ ならば $G \cong \mathbb{Z}/7\mathbb{Z}$ である．
(8) $|G| = 9$ ならば $G \cong \mathbb{Z}/9\mathbb{Z}$ または $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ である．
(9) $|G| = 10$ ならば $G \cong \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ または $G \cong D_5$ である．
(10) $|G| = 11$ ならば $G \cong \mathbb{Z}/11\mathbb{Z}$ である．
残っているのは，$|G| = 8, 12$ の場合である．簡単なものから片付けていく．

定義 13.6.(四元数群) $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$ を満たす元 i, j, k と，実数 $a_1, \ldots, a_4 \in \mathbb{R}$ を用いて，$x = a_1 + a_2 i + a_3 j + a_4 k$ という形に表せる数を**四元数**

といい，四元数全体の集合を $\mathbb{H}$ と書く．$\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ と考えられる．$\mathbb{H}$ には上の規則から乗法を定めることができ，自然に和も定義できる．このとき，$\mathbb{H}$ は環になる．ただし，乗法についての交換法則は成立しない．しかも，$x \neq 0$ のとき，

$$x^{-1} = \frac{a_1 - a_2 i - a_3 j - a_4 k}{a_1^2 + a_2^2 + a_3^2 + a_4^2}$$

が $xx^{-1} = x^{-1}x = 1$ を満たして x の逆元になる．$\mathbb{H}$ を**四元数体**という．(これは代数学 I の範囲外.) このとき，

$$Q_8 := \{1, -1, i, -i, j, -j, k, -k\}$$

は積に関して群になる．Q_8 を**四元数群**という．

定理 13.7. $|G| = 8$ ならば，$G \cong \mathbb{Z}/8\mathbb{Z}$ または $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ または $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ または $G \cong D_4$（二面体群) または $G \cong Q_8$(四元数群) または $G \cong \mathfrak{A}_4$ である．

証明. G がアーベル群の場合は，有限アーベル群の構造定理により結論が得られる．

G が位数 8 の元を持てば $G \cong \mathbb{Z}/8\mathbb{Z}$ である．

また，G のすべての元の位数が 2 以下であるとすると，$x \in G$ ならば $x^2 = 1$ より $x^{-1} = x$ だから，$x, y \in G$ のとき，$x^{-1}y^{-1}xy = xyxy = (xy)^2 = 1$ となり，$xy = yx$ となる．よって，G はアーベル群で，$G = (\mathbb{Z}/2\mathbb{Z})^3$ である．

以下, G は非アーベル群で, G の元の位数は, 4 以下で, 位数 4 の元 h を持つと仮定する．$H := \langle h \rangle \subset G$ とおく．$g \notin H$ となる $g \in G$ を取る．$G/H = \{H, gH\}$, $H\backslash G = \{H, Hg\}$ で，$H \sqcup gH = G = H \sqcup Hg$ なので $gH = Hg$ となる．よって，$H \lhd G$ で，$ghg^{-1} \in H$ である．$ghg^{-1} = h^m$, $0 \leqq m \leqq 3$ を満たす m が一意的に存在する．$m = 0$ だと $h = 1$ となってしまう．$m = 1$ だと $gh = hg$ だから G はアーベル群になってしまう．$m = 2$ だと，$h^2 = (g^{-1}h^2g) = g^{-1}h^4g = 1$ となって，$\operatorname{ord} h = 4$ と矛盾する．よって，$m = 3$ で，

$$ghg^{-1} = h^3 = h^{-1}, \quad gh = h^3 g$$

である．$G/H \cong \mathbb{Z}/2\mathbb{Z}$ であったので $g^2 \in H$ であるから，$g^2 = h^n$ $(0 \leqq n \leqq 3)$ と書ける．$g^2 = h$ または $g = h^3$ だと $\operatorname{ord} g = 8$ となって矛盾するので，$n = 0$ または 2 である．

(1) $n = 0$ の場合，つまり $g^2 = 1$ の場合.

$ghg = ghg^{-1} \in H$ なので，$ghg = h^k$ $(0 \leqq k \leqq 3)$ と書ける．

$$h = g^2hg^2 = g(ghg)g = gh^k g^{-1} = (ghg^{-1})^k = (h^k)^2 = h^{k^2}$$

なので，$h^{k^2-1} = 1$ であり，$k^2 - 1$ は 4 の倍数である．よって，$k = 1, 3$ である．$k = 1$ だと $gh = hg$ より G はアーベル群になるので，$k = 3$ である．すると，$g^4 = h^2 = 1$, $ghg = h^{-1}$ より $G \cong D_4$ となる．

(2) $n = 2$ の場合，つまり $g^2 = h^2$ の場合.

$p := g^2 = h^2 \in G$, $f := gh = h^3 g$ とする．$p^2 = 1$ である．$ghg^{-1} = h^3 = h^{-1}$ より $f = gh = h^3 g = phg$ である．$hf = h(h^3 g) = g$, $fh = (gh)h = gh^2 = g^3 = pg$ である．$fg = (h^3 g)g = h(h^2)(g^2) = hp^2 = h$, $gf = g(gh) = (g^2)h = ph$ である．また，$f^2 = (gh)(h^3 g) = gh^4 g = g^2 = p$ である．よって，$f \in G$ に $i \in Q_8$, $g \in G$ に $j \in Q_8$, $h \in G$ に $k \in Q_8$, $p \in G$ に $-1 \in Q_8$ を対応させる写像は同型写像であり，$G \cong Q_8$ になる． □

位数 12 の群は次回に回す.

14. 位数の 12 以下の有限群 (2)

定義 14.1. n は 2 以上の整数とする． 2 つの元 a, b で生成される位数 $4n$ の有限群 G で，a, b が

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

を満たすとき，G を Q_{4n} と書き，**一般四元数群**という．Q_8 は四元数群である．これは，$\mathrm{GL}_2(\mathbb{C})$ の中で，2 つの元

$$a = \begin{pmatrix} e^{\pi\sqrt{-1}/n} & 0 \\ 0 & e^{-\pi\sqrt{-1}/n} \end{pmatrix}. \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

で生成される群と同一視できる.

定理 14.2. $|G| = 12$ ならば，$G \cong \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ または $G \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}2\mathbb{Z}$ または $G \cong D_6$（二面体群）または $G \cong Q_{12}$(一般四元数群) である．

証明. G がアーベル群の場合は，有限アーベル群の構造定理により結論が得られる．以下 G は非アーベル群とする．G が位数 12 の元を持てば $G \cong \mathbb{Z}/12\mathbb{Z}$ なので，G は位数 6 以下の元しか持たない．

定理 7.4(3) より，G の 3-シロー部分群の個数を s_3 とすると，$s_3 \equiv 1 \pmod 3$ を満たす．また s_3 は $|G| = 12$ の約数である．よって，$s_3 = 1$ または $s_3 = 4$ である．

(1) $s_3 = 1$ の場合．G の 2-シロー群を P_2, 唯一の 3-シロー群を P_3 とする．$s_3 = 1$ より $P \lhd G$ である．P_3 の生成元 x を取る．G の 3-シロー群は P_3 しかないから，G 内の位数 3 の元は x と x^2 のみである．定理 6.5 の記号で $Cx = \{x, x^2\}$ で，$|Cx| \cdot |N_G(x)| = |G| = 12$ だから，$|N_G(x)| = 6$ である．$N_G(x)$ の位数 2 の元 y を取る．$xy = yx$ である．$a := xy$ とおく．$\operatorname{ord} a = 6$ である．$N := \langle a \rangle$ は G の正規部分群なので，$b \in G, b \notin N$ とすると，$bab^{-1} \in N$ なので，ある $0 \leqq i \leqq 5$ により $bab^{-1} = a^i$ と書ける．$\operatorname{ord} a^i = \operatorname{ord} bab^{-1} = \operatorname{ord} a = 6$ だから，$i = 1$ または $i = 5$ であるが，$i = 1$ だと $ab = ba$ で G がアーベル群になってしまう．よって，$bab^{-1} = a^5 = a^{-1}$ である．ところで，$P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ または $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ である．

(1-1) $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ の場合．$y \in P_2$ であるが，上の b を $b \in P_2$ となるように選ぶことができる．すると，$b^2 = 1$ である．a に定義 13.3 の R を，b に S を対応させると，同型写像 $G \to D_6$ が得られる．

(1-2) $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ の場合．この場合は，b を $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ の生成元として選ぶことができる．$b^2 \in N$ で $\operatorname{ord} b^2 = 2$ であるが，$N \cong \mathbb{Z}/6\mathbb{Z}$ 内の位数 2 の元は a^3 のみなので，$b^2 = a^3$ である．この b を上の定義の b^{-1} と考えれば，$G \cong Q_{12}$ である．

(2) $s_3 = 4$ の場合は，$G \cong \mathfrak{A}_4$ であることを示す．G の 4 個の 3-シロー群を，記号を改めて P_1, P_2, P_3, P_4 とし，$X_4 := \{P_1, P_2, P_3, P_4\}$ とおく．$g \in G$ を取る．$gP_ig^{-1} \in X_4$ で，$i \neq j$ ならば $gP_ig^{-1} \neq gP_jg^{-1}$ である．よって，g は X_4 上の置換 σ_g を引きおこす．$g \in G$ に $\sigma_g \in \mathfrak{S}_4$ を対応させる写像 $\varphi: G \to \mathfrak{S}_4$ は準同型写像である．任意の $1 \leqq i < j \leqq 4$ に対して $\sigma_g(P_i) = P_i$ を満たす $g \in G$ が存在するので，$|\operatorname{Im}\varphi|$ は 4 の倍数である．$|\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi| = 12$ より，$|\operatorname{Ker}\varphi| = 1$ または 3 である．$\operatorname{Ker}\varphi \lhd G$ で G は位数 3 の正規部分群を持たないので，$|\operatorname{Ker}\varphi| = 1$ である．よって，φ は単射である．

$|\operatorname{Im}\varphi| = |G| = 12$ であるから，$\operatorname{Im}\varphi \lhd \mathfrak{S}_4$ である．よって，$G \cong \operatorname{Im}\varphi = \mathfrak{A}_4$ である． □