2004 年度蔵野ゼミ卒業論文

明治大学理工学部数学科
今泉 晃広
西 祥吾
福岡 昌伸
森野 拓矢
保村 匡亮
渡邉 将史

平成 17 年 2 月 18 日

目 次

0 序

位数が 30 以下の群の分類を行う．群論の専門書を見れば，もっとエレガントな証明法が書いてあるに違いないと思う．しかし，ここでは，基本的には学部の授業で習ったことのみを使い，自分達で考えた証明を書くことにする．

この報告を通して使われる記号を以下に定める．

特に断らない限り，n は自然数を，p は素数を表す．

e は，群の単位元を表すものとする．

C_n は，位数 n の巡回群とする．$\mathfrak{S}_n$ は n 次対称群，$\mathfrak{A}_n$ は n 次交代群を表す．k が体であるとき，

$$\mathrm{GL}(n,k) = \{A \mid A \text{ は } k\text{-係数の } n \text{ 次正則行列}\}$$

とおく．$\mathrm{GL}(n,k)$ は，掛け算で群になる．

H が群 G の部分群であるとき，$H < G$ または $G > H$ と書く．N が群 G の正規部分群であるとき，$N \triangleleft G$ または $G \triangleright N$ と書く．N, H が群，$\sigma : H \to \mathrm{Aut}(N)$ を準同型としたとき，これらによって定まる半直積を $N \underset{\sigma}{\rtimes} H$ あるいは単に $N \rtimes H$ と書く．半直積に関しては第 3 節を参照．

群 G の元 a に対して，$C_G(a) := \{x \in G \mid ax = xa\}$ とおく．$Z(G) := \{x \in G \mid \text{任意の } y \in G \text{ に対して，} xy = yx \text{ が成立}\}$ を，群 G の中心という．$C_G(a)$ や $Z(G)$ は，G の部分群である．

群 G の元 $f_1, \ldots, f_r$ に対して，$< f_1, \ldots, f_r >$ は $f_1, \ldots, f_r$ で生成された G の部分群であるとする．

集合 S に属する元の個数を $^{\#}S$ と表す．群の元 a に対して，$o(a)$ は，a の位数を表す．群 G に対して，$G(n)$ は，G の位数 n の元全体からなる集合を表すとする．

群の準同型 $f : G \to H$ において，すべての $g \in G$ に対して，$f(g) = e$ が成立するとき，f は自明な準同型であるという．

以下の表は，位数 30 以下の群のリストである．

位数	群の個数	群の同型類
1	1	C_1
2	1	C_2
3	1	C_3
4	2	$C_4,\ C_2\times C_2$
5	1	C_5
6	2	$C_2\times C_3,\ D_6$
7	1	C_7
8	5	$C_8,\ C_4\times C_2,\ C_2\times C_2\times C_2,\ D_8,\ Q_8$
9	2	$C_9,\ C_3\times C_3$
10	2	$C_2\times C_5,\ D_{10}$
11	1	C_{11}
12	5	$C_4\times C_3,\ C_2\times C_2\times C_3,\ Q_{12},\ D_{12},\ \mathfrak{A}_4$
13	1	C_{13}
14	2	$C_2\times C_7,\ D_{14}$
15	1	$C_3\times C_5$
16	14	$C_{16},\ C_8\times C_2,\ C_4\times C_4,\ C_4\times C_2\times C_2,\ C_2\times C_2\times C_2\times C_2,$ $C_8\underset{\sigma}{\rtimes} C_2,\ C_8\underset{\tau}{\rtimes} C_2,\ D_{16},\ Q_{16},\ C_4\rtimes C_4,\ Q_8\times C_2,\ (C_4\times C_2)\underset{\sigma}{\rtimes} C_2,$ $(C_4\times C_2)\underset{\tau}{\rtimes} C_2,\ D_8\times C_2$
17	1	C_{17}
18	5	$C_2\times C_9,\ C_2\times C_3\times C_3,\ D_{18},\ (C_3\times C_3)\rtimes C_2,\ C_3\times D_6$
19	1	C_{19}
20	5	$C_4\times C_5,\ C_2\times C_2\times C_5,\ C_5\rtimes C_4,\ Q_{20},\ D_{20}$
21	2	$C_3\times C_7,\ C_7\rtimes C_3$
22	2	$C_2\times C_{11},\ D_{22}$
23	1	C_{23}
24	15	$C_8\times C_3,\ C_4\times C_2\times C_3,\ C_2\times C_2\times C_2\times C_3,\ D_8\times C_3,\ Q_8\times C_3,$ $(C_2\times C_2\times C_2)\rtimes C_3,\ Q_8\rtimes C_3,\ C_3\rtimes C_8,\ D_{24},\ Q_{24},$ $C_3\rtimes (C_2\times C_2\times C_2),\ C_3\underset{\sigma}{\rtimes} D_8,\ C_3\underset{\tau}{\rtimes} D_8,\ C_3\rtimes Q_8,\ \mathfrak{S}_4$
25	2	$C_{25},\ C_5\times C_5$
26	2	$C_2\times C_{13},\ D_{26}$
27	5	$C_{27},\ C_9\times C_3,\ C_3\times C_3\times C_3,\ (C_3\times C_3)\rtimes C_3,\ C_9\rtimes C_3$
28	4	$C_4\times C_7,\ C_2\times C_2\times C_7,\ Q_{28},\ D_{28}$
29	1	C_{29}
30	4	$C_2\times C_3\times C_5,\ C_5\times D_6,\ C_3\times D_{10},\ D_{30}$

1　アーベル群の基本定理

定理 1.1 (アーベル群の基本定理) 有限生成アーベル群は，有限個の巡回群の直積と同型である．

アーベル群の基本定理より有限アーベル群 G は，

$$G \simeq C_{n_1} \times \cdots \times C_{n_k}$$

とできる．このとき $^{\#}G = n_1 \cdots n_k$ であることに注意する．直積の順番を入れ替えても，C_1 を直積しても群は同型である．

また，$n, m \in \mathbb{N}$ とすると，「$(n, m) = 1 \Longleftrightarrow C_{nm} \simeq C_n \times C_m$」であることが証明できる．

以上より有限アーベル群 G は，

$$G \simeq C_{{p_1}^{a_1}} \times \cdots \times C_{{p_s}^{a_s}}$$

としてよい．ただし，

$$\begin{cases} p_1 \leq \cdots \leq p_s \text{ は素数} \\ a_1, \ldots, a_s \text{ は自然数} \\ i = 1, \ldots, s-1 \text{ に対して，} p_i = p_{i+1} \text{ であれば，} a_i \geq a_{i+1} \end{cases} \tag{1}$$

とする．

定理 1.2 p_i, a_i $(i = 1, \ldots, s)$ と q_j, b_j $(j = 1, \ldots, t)$ は，(1) の条件を満たすものとする．

ここで，

$$C_{{p_1}^{a_1}} \times \cdots \times C_{{p_s}^{a_s}} \simeq C_{{q_1}^{b_1}} \times \cdots \times C_{{q_t}^{b_t}}$$

と仮定する．このとき，

$$\begin{cases} t = s \\ p_1 = q_1, \cdots, p_s = p_t \\ a_1 = b_1, \cdots, a_s = b_t \end{cases}$$

が成立する．

したがって，「位数 n のアーベル群の数は，$p(m_1) \cdots p(m_s)$ 個存在する．」ただし，$n = p_1^{m_1} \cdots p_s^{m_s}$ は素因数分解，$p(m)$ は m の分割数を表すとする．

例 1.3 位数 24 の可換な群は，$24 = 2^3 \times 3$ なので，$p(3)p(1) = 3$ 個であり，$C_8 \times C_3$, $C_4 \times C_2 \times C_3$, $C_2 \times C_2 \times C_2 \times C_3$ である．

2　代表的な非アーベル群

定義 2.1 n を自然数とし,

$$A_n := \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

とおく．このとき, A_n と B で生成された $\mathrm{GL}(2, \mathbb{R})$ の部分群を**二面体群**といい, D_{2n} と表す．(ただし，$\mathbb{R}$ は実数体とする．)

注意 2.2 D_{2n} では, $(A_n)^n = B^2 = E$, $A_n B = B(A_n)^{n-1}$ が成り立つ. (ただし，E は 2 次の単位行列とする．)

よって,

$$D_{2n} = \{E, A_n, (A_n)^2, \ldots, (A_n)^{n-1}, B, BA_n, B(A_n)^2, \ldots, B(A_n)^{n-1}\}$$

とあらわせる.

特に，D_{2n} の位数は $2n$ である．$n \geq 3$ のときは，D_{2n} は非アーベル群である.

定義 2.3 n を自然数とし,

$$H_{2n} := \begin{pmatrix} e^{\frac{\pi i}{n}} & 0 \\ 0 & e^{-\frac{\pi i}{n}} \end{pmatrix}, \quad F := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

とおく. このとき, H_{2n} と F で生成された $\mathrm{GL}(2, \mathbb{C})$ の部分群を**四元数型の群**といい，Q_{4n} と表す．(ただし，$\mathbb{C}$ は複素数体とする．)

注意 2.4 Q_{4n} において, $(H_{2n})^n = F^2 = -E$, $H_{2n}F = F(H_{2n})^{2n-1}$ が成り立つ.

よって,

$$Q_{4n} = \{E, H_{2n}, (H_{2n})^2, \ldots, (H_{2n})^{2n-1}, F, FH_{2n}, F(H_{2n})^2, \ldots, F(H_{2n})^{2n-1}\}$$

とあらわせる.

特に，Q_{4n} の位数は $4n$ である．$n \geq 2$ のときは，Q_{4n} は非アーベル群である.

3　半直積

命題 3.1 N, H が群，$\sigma : H \to \mathrm{Aut}(N)$ を準同型とする．(記号の簡略化のため, $\sigma(b)$ を，σ_b と表すことが多い．)

このとき, 直積集合 $N \times H$ に次のように演算を導入する．$a_1, a_2 \in N$ と $b_1, b_2 \in H$ に対して,

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot \sigma_{b_1}(a_2), b_1 \cdot b_2)$$

と定義する．このとき，この演算により，直積集合 $N \times H$ は群になる.

証明 任意の 3 元 $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in N \times H$ に対して,

$$\begin{aligned}\{(a_1,b_1)(a_2,b_2)\}(a_3,b_3) &= (a_1\sigma_{b_1}(a_2), b_1b_2)(a_3,b_3)\\ &= (a_1\sigma_{b_1}(a_2)\sigma_{b_1b_2}(a_3), (b_1b_2)b_3)\\ (a_1,b_1)\{(a_2,b_2)(a_3,b_3)\} &= (a_1,b_1)(a_2\sigma_{b_2}(a_3), b_2b_3)\\ &= (a_1\sigma_{b_1}(a_2\sigma_{b_2}(a_3)), b_1(b_2b_3))\\ &= (a_1\sigma_{b_1}(a_2)\sigma_{b_1}\sigma_{b_2}(a_3), (b_1b_2)b_3)\end{aligned}$$

となり，$\sigma_{b_1b_2} = \sigma_{b_1}\sigma_{b_2}$ なので結合法則を充たす.

$e_N \in N, e_H \in H$ でそれぞれの単位元を表すことにすると，この群の単位元は (e_N, e_N) となる.

$(a, b) \in N \times H$ に対して，$(a^{-1}, b^{-1}) \in N \times H$ が (a, b) の逆元となることが，簡単な計算によって確かめられる.

よって，この演算によって，$N \times H$ は群になる. **証明終**

命題 3.1 によって定まる群を H と N の (σ によって定まる) 半直積といい，$N \rtimes_{\sigma} H$ あるいは単に $N \rtimes H$ と書く.

注意 3.2 群が与えられたとき，その群は，もっと小さい二つの群の半直積になることがある.

例えば，G は群，$G \triangleright N, G > H$ としよう．$i : H \to G, j : N \to G$ を包含写像，$\pi : G \to G/N$ を射影とする．$b \in H$ に対して，

$$\tau_b : N \longrightarrow N$$

を $\tau_b(a) = bab^{-1}$ によって定義する．このとき，$\tau_b \in \mathrm{Aut}(N)$ であることがわかる．ここで，

$$\tau : H \longrightarrow \mathrm{Aut}(N)$$

を，$\tau(b) := \tau_b$ によって定義する．すると，τ は準同型であることが確かめられる．よって，半直積 $N \rtimes_{\tau} H$ が定義できる.

ここで，

$$\phi : N \rtimes_{\tau} H \longrightarrow G$$

を，$\phi((a, b)) := j(a) \cdot i(b)$ によって定義する．このとき，次のことが成立する.

1. ϕ は準同型である.
2. **合成写像 πi が同型であると仮定すると，ϕ は同型である.**

よって，合成写像 πi が同型であると仮定すると，G はもっと小さな群の半直積で表せる．

実際,

$$\begin{aligned}\phi((a_1,b_1)(a_2,b_2)) &= \phi((a_1\tau_{b_1}(a_2),b_1b_2))\\ &= j(a_1b_1a_2{b_1}^{-1})i(b_1b_2)=a_1b_1a_2b_2\\ \phi((a_1,b_1))\phi((a_2,b_2)) &= j(a_1)i(b_1)j(a_2)i(b_2)=a_1b_1a_2b_2\end{aligned}$$

となり ϕ は準同型である．

ここで，合成写像 πi が同型であると仮定する．$k:=(\pi i)^{-1}$ とし，$g\in G$ に対して $a=g\cdot ik(\pi(g^{-1}))$ とおくと，

$$\pi(a)=\pi(g)\pi(ik(\pi(g^{-1})))=\pi(g)\pi(g^{-1})=e$$

なので

$$a\in \operatorname{Ker}\pi=N$$

である．ここで，$k(\pi(g^{-1}))\in H$ の逆元を $b\in H$ とすると，

$$g=ab=\phi((a,b))$$

となり ϕ は全射である．

また，$ab=a'b'$ $(a,a'\in N,\ b,b'\in H)$ を満たすと仮定する．

$$b=eb=ik\pi(a)ik(\pi i)(b)=ik\pi(ab)=ik\pi(a'b')=ik\pi(a')ik(\pi i)(b')=eb'=b'$$

であり，よって

$$a=a'$$

となる．したがって ϕ は単射である．故に同型写像となる．

注意 3.3 G を群とする．ここで，

$N\cap H=\{e\}$ かつ $^{\#}H\cdot{}^{\#}N={}^{\#}G$ を満たす $N\triangleleft G$ と $H<G$ が存在する

と仮定する．すると，注意 3.2 より $G=N\rtimes H$ となることがわかる．

例 3.4 二面体群 D_{2n} が小さい二つの群の半直積で表現できることを示す．

第 2 節の定義より $<A_n>\triangleleft D_{2n}$ となっていて，$<B>\cap<A_n>=\{e\}$ であり，さらに $^{\#}<A_n>\cdot{}^{\#}<B>={}^{\#}G$ なので，$G=<A_n>\underset{\sigma}{\rtimes}<B>$ となる．

ここで，$\sigma:<B>\to \operatorname{Aut}(<A_n>)=(\mathbb{Z}/n\mathbb{Z})^{\times}$ は，$\sigma(B)=-1$ で決まるものである．

定理 3.5 N, H を群，$\sigma, \tau : H \to \mathrm{Aut}(N)$ を，$f \in \mathrm{Aut}(N), g \in \mathrm{Aut}(H)$ とする．このとき，任意の $b \in H$ に対して，$\tau_{g(b)} f = f \sigma_b$ が成立するならば，$N \underset{\sigma}{\rtimes} H \simeq N \underset{\tau}{\rtimes} H$ が成立する．

証明 まず，

$$\begin{array}{rcl} \phi : N \underset{\sigma}{\rtimes} H & \longrightarrow & N \underset{\tau}{\rtimes} H \\ (a,b) & \longmapsto & (f(a), g(b)) \end{array}$$

とおくと ϕ は全単射となることに注意する．後は，ϕ が準同型であることを証明すればよい．

$(a_1, b_1), (a_2, b_2) \in N \underset{\sigma}{\rtimes} H$ ととると，

$$\begin{array}{rcl} \phi((a_1,b_1)(a_2,b_2)) & = & \phi((a_1\sigma_{b_1}(a_2), b_1b_2)) \\ & = & (f(a_1\sigma_{b_1}(a_2)), g(b_1b_2)) \\ & = & (f(a_1)(f(\sigma_{b_1}(a_2))), g(b_1)g(b_2)) \\ \phi((a_1,b_1))\phi((a_2,b_2)) & = & (f(a_1), g(b_1))(f(a_2), g(b_2)) \\ & = & (f(a_1)\tau_{g(b_1)}(f(a_2)), g(b_1)g(b_2)) \end{array}$$

となり，仮定の式から上の二式は一致する． **証明終**

4 群の自己同型

群を決定するには，半直積が非常に有効であり，半直積を使うためには群 N の自己同型群

$$\mathrm{Aut}(N) = \{ f : N \to N \mid f \text{ は同型写像} \}$$

を調べる必要がある．この節では，代表的な群に対してその自己同型群を決定する．

$\mathrm{Aut}(N)$ は，写像の合成により群になることに注意する．

定理 4.1

$$\mathrm{Aut}(C_n) = (\mathbb{Z}/n\mathbb{Z})^\times$$

証明 $C_n = < a >$ とする．

$f, g \in \mathrm{Aut}(C_n)$ が $f(a) = g(a)$ をみたしたとしよう．すると，任意の整数 s に対して，

$$f(a^s) = f(a)^s = g(a)^s = g(a^s)$$

が成立する．したがって，

$$f = g \Longleftrightarrow f(a) = g(a) \tag{2}$$

であることに注意する．

以下，f_s は $f_s(a) = a^s$ となる写像を表すことにする．このとき，

$$\mathrm{Aut}(C_n) = \{f_s \mid s = 0, \ldots, n-1 \text{ ただし } (s, n) = 1\}$$

であることに注意する．ここで，

$$\phi : \mathrm{Aut}(C_n) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

を，$\phi(f_s) := \bar{s}$ によって定義する．

ϕ が同型写像であることを示す．

(2) より ϕ は単射である．$\mathrm{Aut}(C_n)$ も $(\mathbb{Z}/n\mathbb{Z})^\times$ も位数は $\varphi(n)$ なので，ϕ は全射である．(ただし，φ はオイラー関数とする．) よって，ϕ は全単射である．

$\forall f_s, f_t \in \mathrm{Aut}(C_n)$ に対して，$(f_s f_t)(a) = f_s(a^t) = a^{st}$ より，$f_s f_t = f_{st}$ が成立する．したがって，ϕ は準同型写像である． **証明終**

定理 4.2

$$\mathrm{Aut}(\overbrace{C_p \times \cdots \times C_p}^{n}) = \mathrm{GL}(n, \mathbb{F}_p)$$

が成立する．

証明 $C_p = < a >$ とおく．$f \in \mathrm{Aut}(\overbrace{C_p \times \cdots \times C_p}^{n})$ に対して，

$$f((e, \ldots, e, \overset{i\text{ 番目}}{a}, e, \ldots, e)) = (a^{f_{1i}}, a^{f_{2i}}, \ldots, a^{f_{ni}})$$

であるとき，

$$\phi : \mathrm{Aut}(\overbrace{C_p \times \cdots \times C_p}^{n}) \longrightarrow \mathrm{GL}(n, \mathbb{F}_p)$$

を $\phi(f) = (f_{ij})$ によって定義する．このとき，この写像が群の同型写像であることが，確かめられる． **証明終**

5　位数が p または p^2 の群

この節で，位数 p または p^2 の群を決定する．

位数 p の群

G は，位数 p の群であるとする．$e \neq a \in G$ に対し，

$$<a> \, < G$$

であるので，$2 \leq {}^{\#}<a> \, \leq {}^{\#}G = p$ である．ラグランジュの定理により，${}^{\#}<a>$ は ${}^{\#}G$ の約数であるので，${}^{\#}<a> \, = p$ であり，したがって

$$<a> \, = G$$

となる．よって，G は $\underline{C_p}$ と同型である．

位数 p^2 の群

群 G の中心を $Z(G)$ とする．このとき，次が成立する．

定理 5.1 群 G の位数は p^n とする．ただし，p は素数で，n は自然数とする．このとき，$Z(G) \neq \{e\}$ である．

証明 G の共役類を $G_1, \ldots, G_t$ とおく．すると，${}^{\#}G = {}^{\#}G_1 + {}^{\#}G_2 + \cdots + {}^{\#}G_t$ が，成立する．ここで，${}^{\#}G_i$ は，${}^{\#}G$ の約数であるので，p の冪である．

また，${}^{\#}G_i = 1$ を満たす共役類の個数は，${}^{\#}Z(G)$ と一致する．よって，${}^{\#}G - {}^{\#}Z(G)$ は p の倍数であり，したがって $Z(G) \neq \{e\}$ となる．　**証明終**

以下，G は位数 p^2 の群であるとする．

ラグランジュの定理と定理 5.1 により，$Z(G)$ の位数は p または p^2 である．$G \triangleright Z(G)$ であることに注意する．このとき，$G/Z(G) = 1$ または p である．

$G/Z(G) = p$ と仮定すると，$G/Z(G)$ は巡回群．よって，$<aZ(G)> \, = G/Z(G)$ をみたす $a \in G$ が存在する．すると，G の元はいつも $a^n z$ の形に書ける ($n \in N$, $z \in Z(G)$)．よって，このとき，G はアーベル群となる．

$G/Z(G) = 1$ とすると，$G = Z(G)$ より，G はアーベル群である．

よって，位数 p^2 の群はアーベル群であることがわかった．

アーベル群の基本定理 (第 1 節参照) により，G は，$\underline{C_{p^2}}$ または $\underline{C_p \times C_p}$ と同型である．

6　位数が $2p$ の群の分類 (p は奇素数)

この節で，位数 $2p$ (p は奇素数) の群の分類を行う．

${}^{\#}G = 2p$ と仮定する．S_2, S_p は，それぞれ G の 2-シロー部分群，p-シロー部分群であるとする．すると，${}^{\#}S_2 = 2, {}^{\#}S_p = p$ である．シローの定理より，G は唯一つの p-シロー部分群をもっているので，$S_p \lhd G$ である．

また，

$$S_2 \cap S_p = \{e\}$$

であり，${}^{\#}S_2 \cdot {}^{\#}S_p = {}^{\#}G$ である．よって，注意 3.3 により，G は S_2 と S_p の半直積となる．つまり，$G \simeq S_p \rtimes_{\sigma} S_2$ と書ける．ただし，

$$\sigma : S_2 \to \mathrm{Aut}(S_p) \tag{3}$$

は準同型とする．$S_2 = \{e, a\}$ としよう．

このとき，定理 4.1 により $\mathrm{Aut}(S_p) = (\mathbb{Z}/p\mathbb{Z})^{\times} = \{1, 2, \ldots, p-1\}$ である．$(\mathbb{Z}/p\mathbb{Z})^{\times}$ の中の二乗して 1 になる元は ± 1 のみである．よって，(3) の準同型は,「$\sigma(e) = \sigma(a) = 1$」と「$\tau(e) = 1, \tau(a) = -1$」の二通りが考えられる．

σ の場合は，G は S_2 と S_p の直積と同型になり，特にアーベル群になる．

τ の場合を考える．$S_p = <b>$ とする．すると，$a^2 = b^p = e, aba^{-1} = b^{p-1}$ であり，この群は位数 $2p$ の二面体群 D_{2p} と同型である．(二面体群に関しては，第 2 節参照．)

以上により，位数が $2p$ の群 (p が奇素数) は，$\underline{C_2 \times C_p}$ と $\underline{D_{2p}}$ の二通り存在する．(D_{2p} はアーベル群ではないので，この二つの群は，同型ではありえない．)

7　シロー部分群が全て正規部分群である群

定理 7.1 G を群，${}^{\#}G = p_1^{r_1} \cdots p_n^{r_n}$ としよう．ただし，$p_1, \ldots, p_n$ は，互いに異なる素数とする．S_{p_i} を G の p_i-シロー部分群とする．全ての i に対して，$S_{p_i} \lhd G$ と仮定する．このとき，

$$G \simeq S_{p_1} \times S_{p_2} \times \cdots \times S_{p_n}$$

である．

証明 $i \neq j$ とし，$a \in S_{p_i}, b \in S_{p_j}$ とする．このとき，$aba^{-1} \in S_{p_j}$，$ba^{-1}b^{-1} \in S_{p_i}$ が成立する．よって，$aba^{-1}b^{-1} \in S_{p_i} \cap S_{p_j} = \{e\}$ となる．つまり，$ab = ba$ が成立する．よって，異なるシロー部分群の元どうしは可換であることがわかる．

次に，写像

$$\begin{array}{rccc} \phi : & S_{p_1} \times S_{p_2} \times \cdots \times S_{p_n} & \longrightarrow & G \\ & (x_1, x_2, \ldots, x_n) & \longmapsto & x_1 x_2 \cdots x_n \end{array}$$

を見てみる．すると，$(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in S_{p_1} \times S_{p_2} \times \cdots \times S_{p_n}$ に対して，

$$\begin{aligned}
\phi((x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n)) &= \phi((x_1y_1, x_2y_2, \ldots, x_ny_n)) \\
&= x_1y_1x_2y_2 \cdots x_ny_n \\
&= x_1x_2 \cdots x_ny_1y_2 \cdots y_n \\
&= \phi((x_1, x_2, \ldots, x_n))\phi((y_1, y_2, \ldots, y_n))
\end{aligned}$$

となり，ϕ は準同型写像であることがわかる．

$S_{p_i} \subset \mathrm{Im}\,\phi \subset G$ であるので，${p_i}^{r_i} \mid^{\#} \mathrm{Im}\,\phi$ となる．よって，

$$ {p_1}^{r_1}{p_2}^{r_2} \cdots {p_n}^{r_n} \mid^{\#} \mathrm{Im}\,\phi $$

が成立する．だから，$^{\#}\,\mathrm{Im}\,\phi =^{\#} G$ となる．故に，$\mathrm{Im}\,\phi = G$ となり，したがって ϕ は全射である．更に $^{\#}(S_{p_1} \times S_2 \times \cdots \times S_{p_n}) = {}^{\#}G$ より，ϕ は全単射である．

よって，

$$ G \simeq S_{p_1} \times S_{p_2} \times \cdots \times S_{p_n} $$

がわかった． **証明終**

例 7.2 位数 15 の群 G を分類する．

$15 = 3 \times 5$ より，G は，3-シロー部分群 $S_3(\simeq C_3)$ と 5-シロー部分群 $S_5(\simeq C_5)$ を持つ．n_3 は G の 3-シロー部分群の個数，n_5 は G の 5-シロー部分群の個数とする．シローの定理より，

$$ n_3 \equiv 1 \pmod 3 \text{ かつ } n_3 \mid 5 $$

$$ n_5 \equiv 1 \pmod 5 \text{ かつ } n_5 \mid 3 $$

が成立する．よって，

$$ n_3 = n_5 = 1 $$

となる．したがって，$S_3 \triangleleft G, S_5 \triangleleft G$ となり，定理 7.1 より

$$ G \simeq S_3 \times S_5 \simeq \underline{C_3 \times C_5} $$

となる．

8　位数 8 の群の分類

この節では，次の命題を証明する．

命題 8.1 位数 8 の群は，(同型を除いて) C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, Q_8 の 5 個のみである．

証明 G は位数 8 の群であるとする．

G が可換であるとき，アーベル群の基本定理 (第 1 節参照) より

$$\underline{C_8},\ \underline{C_4 \times C_2},\ \underline{C_2 \times C_2 \times C_2}$$

のどれかと同型である．

G は非可換としよう．G の元の位数は 8 の約数の 1, 2, 4, 8 のいずれかである．また，G は非可換なので位数 8 の元を持たない．一般に位数 1 の元は単位元のみなので，${}^{\#}G(2) + {}^{\#}G(4) = 7$ である．

${}^{\#}G(2)$ によって，次の三通りに場合分けして考える．

1. ${}^{\#}G(2) = 7$ のとき．このとき，$\forall x \in G$ に対して $x^2 = e$ である．すると，次の補題により，G はアーベル群となる．

   補題 8.2 G は群であるとする (位数が 8 であるとは仮定しない)．任意の $x \in G$ が $x^2 = e$ をみたせば，G はアーベル群である．

   証明 $\forall x, y \in G$ に対して，$(xy)^2 = e$ より $(xy)^{-1} = xy$ とわかる．また，$(xy)^{-1} = y^{-1}x^{-1} = yx$ なので $xy = yx$ が成立．したがって G はアーベル群となる．　**証明終**

2. $2 \leq {}^{\#}G(2) \leq 6$ のとき．このとき，位数 4 の元 a がある．
   ${}^{\#}{<}a{>}(2) = 1$ より，$o(b) = 2$ をみたす元 $b \in G \setminus {<}a{>}$ がある．また，$G \triangleright {<}a{>}$ であり，${<}b{>} \cap {<}a{>} = \{e\}$, ${}^{\#}{<}b{>} \cdot {}^{\#}{<}a{>} = 8 = {}^{\#}G$ であるので，注意 3.3 により

   $$G \simeq {<}a{>} \rtimes_{\sigma} {<}b{>}$$

   とできる．ただし，$\sigma : {<}b{>} \to \mathrm{Aut}\,{<}a{>}$ は非自明な準同型である．第 4 節の結果により，

   $$\mathrm{Aut}\,{<}a{>} = (\mathbb{Z}/4\mathbb{Z})^{\times} = \{\pm 1\}$$

   であるので，$\sigma(b) = -1$ としてよい．これによって，非自明な準同型 $\sigma : {<}b{>} \to \mathrm{Aut}\,{<}a{>}$ はただ一通り定まる．このとき，例 3.4 より $\underline{D_8}$ と同型である．

3. ${}^{\#}G(2) = 1$ のとき．このとき，

$$o(a) = o(b) = 4, \quad a \notin <b> \tag{4}$$

を満たす $a, b \in G$ が存在する．
$4 < {}^{\#}<a, b> \leq 8$ より，$<a, b> = G$ である．位数 2 の元は 1 つのみなので，

$$a^2 = b^2 \tag{5}$$

である．
また，$G \rhd <a>$ であり，a の位数を考えると $bab^{-1} = a$ または a^3 である．
もし $bab^{-1} = a$ ならば， $ba = ab$ となり G の生成元が交換可能となり G がアーベル群になってしまう．よって，

$$bab^{-1} = a^3 \tag{6}$$

としてよい．
(4), (5), (6) により G の演算は一通りに決まり，$G \simeq \underline{Q_8}$ とわかる (Q_8 に関しては，第 2 節参照)．

証明終

9　位数 12 の群の分類

命題 9.1 位数 12 の群は，同型を除いて 5 個存在する．

証明 G を位数 12 の群とする．$12 = 2^2 \times 3$ より，G は 2-シロー部分群 (C_4 または $C_2 \times C_2$ に同型) と 3-シロー部分群 (C_3 に同型) を持つ．
　G がアーベル群のとき．アーベル群の基本定理 (第 1 節参照) より，G は

$$\underline{C_4 \times C_3}, \quad \underline{C_2 \times C_2 \times C_3}$$

のどちらかに同型である．
　G が非アーベル群のとき．G の 2-シロー部分群の個数を n_2，G の 3-シロー部分群の個数を n_3 とする．シローの定理より，

$$n_2 \equiv 1 \pmod 2 \ \text{かつ} \ n_2 \mid 3$$

$$n_3 \equiv 1 \pmod 3 \ \text{かつ} \ n_3 \mid 4$$

である．よって，

$$n_2 = 1 \ \text{または} \ 3$$

$$n_3 = 1 \ \text{または} \ 4$$

である．ここで，3-シロー部分群の個数 n_3 によって場合分けをする．

(1) $n_3 = 1$ のとき．$S_3 \triangleleft G$ かつ，$S_3 \cap S_2 = \{e\}$, ${}^{\#}S_3 \cdot {}^{\#}S_2 = 12$ であるので，注意 3.3 より，$G = S_3 \underset{\sigma}{\rtimes} S_2$ としてよい．次に S_2 の構造によって場合分けを行う．

(1-1) $S_2 \simeq C_2 \times C_2$ のとき．このとき，$G = C_3 \underset{\sigma}{\rtimes} (C_2 \times C_2)$ である．ただし，$\sigma : C_2 \times C_2 \to \operatorname{Aut} C_3$ である．$C_2 \times C_2$ の生成元 (b_1, e), (e, b_2) に対して，$(\sigma_{(b_1,e)})^2 = (\sigma_{(e,b_2)})^2 = \mathrm{id}$ である．さらに，定理 4.1 より，$\operatorname{Aut} C_3 = (\mathbb{Z}/3\mathbb{Z})^{\times} = \{\pm 1\}$ である．このとき，σ は非自明な準同型であるとすれば，$C_2 \times C_2$ の生成元を取り替えれば，$\sigma_{(b_1,e)} = 1, \sigma_{(e,b_2)} = -1$ としてよい．このとき，群が一つ定まるが，この群は $\underline{D_{12}}$ と同型である．

(1-2) $S_2 \simeq C_4$ のとき．このとき，$G = C_3 \underset{\sigma}{\rtimes} C_4$ である．ただし，$\sigma : C_4 \to \operatorname{Aut} C_3$ である．C_4 の生成元 b に対して，$(\sigma_b)^4 = \mathrm{id}$ である．また，定理 4.1 より，$\operatorname{Aut} C_3 = (\mathbb{Z}/3\mathbb{Z})^{\times} \simeq \{\pm 1\}$ であるから，

$$\sigma_b = 1 \quad \text{または} \quad -1$$

である．$\sigma_b = 1$ のときは G がアーベル群になってしまうため不適．よって，$\sigma_b = -1$ としてよい．このとき，

$$G \simeq C_3 \underset{\sigma}{\rtimes} C_4 \simeq \underline{Q_{12}}$$

となる．

(2) $n_3 = 4$ のとき．3-シロー部分群を A_1, A_2, A_3, A_4 とおく．

$$\begin{array}{rcl} \phi : G & \longrightarrow & \mathfrak{S}_4 \\ g & \longmapsto & \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ gA_1g^{-1} & gA_2g^{-1} & gA_3g^{-1} & gA_4g^{-1} \end{pmatrix} \end{array}$$

という写像を考えると，これは準同型になる．3-シロー部分群はすべて互いに共役なので，$\operatorname{Im}\phi$ は可移である．よって，${}^{\#}\operatorname{Im}\phi$ は 4 の倍数である．したがって，${}^{\#}\ker\phi$ は，1 または 3 となる．しかし，G の位数 3 の部分群は正規部分群ではないので，したがって $\ker\phi = \{e\}$ である．よって，$G \simeq \operatorname{Im}\phi$ である．$\mathfrak{S}_4$ の位数 12 の部分群は $\mathfrak{A}_4$ のみであるので，このケースでは $G \simeq \underline{\mathfrak{A}_4}$ である．

証明終

10　位数 18 の群の分類

命題 10.1 位数 18 の群は，同型を除いて 5 個存在する．

証明 位数 18 のアーベル群は，$\underline{C_2 \times C_9}$ と $\underline{C_2 \times C_3 \times C_3}$ の二種類ある．

G を位数 18 の非アーベル群とする．シローの定理より 3-シロー部分群は一つのみ．注意 3.3 より，$G = S_3 \underset{\sigma}{\rtimes} S_2$ とあらわせる．ただし， $\sigma : S_2 \to \mathrm{Aut}\, S_3$ は非自明な準同型写像である．

S_3 の構造によって，次の二つに場合分けして考える．

(1) $S_3 \simeq C_9$ のとき．第 4 節の結果により，$\mathrm{Aut}\, C_9 = (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$ である．この中の位数 2 の元は，8 のみ．これにより一つの群が決まる．これは，$\underline{D_{18}}$ である．

(2) $S_3 \simeq C_3 \times C_3$ のとき．定理 4.2 より，$\mathrm{Aut}\,(C_3 \times C_3) = \mathrm{GL}(2, \mathbb{F}_3)$．また，$S_2 = C_2 := <a>$．$(\sigma_a)^2 = E$ より，σ_a の最小多項式は $x^2 - 1$ を割り切る．よって，$x-1, x+1, x^2-1$ のいずれかである．

(2-1) $x - 1$ なら $\sigma_a = E$ よりアーベル群となる．

(2-2) $x + 1$ なら $\sigma_a = -E$ ．この写像で一つ半直積の群 $\underline{(C_3 \times C_3) \rtimes C_2}$ が定まる．

(2-2) $x^2 - 1$ なら，2 次式なのでこれが固有多項式となり，固有値は $1, -1$ である．基底を取り替えることにより，

$$\sigma_a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{7}$$

としてもよい．これから一つ半直積の群が定まる．これは，$\underline{C_3 \times D_6}$ と同型である．

前者の群の中心には位数 3 の元はないが，後者には群の中心に位数 3 の元があるので二つは同型でない．

証明終

11 位数 20 の群の分類

命題 11.1 位数 20 の群は，同型を除いて 5 個存在する．

証明 アーベル群の基本定理により，位数 20 のアーベル群は $\underline{C_4 \times C_5}, \underline{C_2 \times C_2 \times C_5}$ の二つである．

G を位数 20 の非アーベル群とする．G の 5-シロー部分群の数 n_5 は，シローの定理より

$$n_5 | 20 \quad \text{かつ} \quad n_5 \equiv 1 (mod 5)$$

をみたす．したがって，$n_5 = 1$ なので，G の 5-シロー部分群 S_5 は正規部分群である．

すると，注意 3.3 より，G は S_2 と S_5 の半直積であらわせる．

$$\sigma : S_2 \longrightarrow \operatorname{Aut} S_5 = (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$$

を，半直積を定める非自明な準同型としよう．

S_2 の構造によって，次の二つに場合分けして考える．

1. $S_2 \simeq C_4$ であると仮定する．
   $S_2 = <b>$ としよう．$\sigma(b) = 2,\ 2^2,\ 2^3$ のいずれかである．それぞれの写像を $\sigma,\ \tau,\ \nu$ とおく．
   σ と ν が作る半直積を見てみる．$f := \mathrm{Id}_{C_5}$, $g : C_4 \to C_4$ を $g(b) = b^{-1}$ で定まるものとすれば，任意の $c \in S_2$ に対して，
   $$f\sigma_c = \nu_{g(c)} f$$
   が成立する．よって，定理 3.5 によって，$C_5 \underset{\sigma}{\rtimes} C_4$ と $C_5 \underset{\nu}{\rtimes} C_4$ は同型である．また，$C_5 \underset{\tau}{\rtimes} C_4$ の中心には位数 2 の元があるが，$\underline{C_5 \underset{\sigma}{\rtimes} C_4}$ にはないのでこの二つは同型ではないことに注意．(中心に位数 2 の元があれば，シローの定理により，その元は任意の 2-シロー部分群に含まれることに注意．) また，$C_5 \underset{\tau}{\rtimes} C_4 \simeq \underline{Q_{20}}$ に注意する．
2. $S_2 \simeq C_2 \times C_2$ のとき．
   ${}^{\#}\operatorname{Ker}\sigma = 1, 2, 4$ のいずれかである．${}^{\#}\operatorname{Ker}\sigma = 1$ なら σ が同型写像となり矛盾する．また，${}^{\#}\operatorname{Ker}\sigma = 4$ なら σ は自明な写像となる．よって，${}^{\#}\operatorname{Ker}\sigma = 2$ である．
   基底を取り替えることにより，σ は
   $$\begin{array}{cccc} \sigma : & C_2 \times C_2 & \longrightarrow & (\mathbb{Z}/5\mathbb{Z})^\times \\ & (c, e) & \longmapsto & 2^2 \\ & (e, d) & \longmapsto & 1 \end{array} \tag{8}$$
   としてよい (定理 3.5 を使う)．ただし，$C_2 \times C_2$ において，左の C_2 は $\{e, c\}$，右の C_2 は $\{e, d\}$ とした．このとき G はただ一つ定まる．それは，$\underline{D_{20}}$ である．

証明終

12　位数 21 の群の分類

定理 12.1 位数 21 の群は，同型を除いて 2 個存在する．

証明 G を位数 21 の群とする．$21 = 3 \times 7$ より，G は，3-シロー部分群 $S_3(\simeq C_3)$ と 7-シロー部分群 $S_7(\simeq C_7)$ を持つ．

G がアーベル群のとき．アーベル群の基本定理 (第 1 節参照) より，$G \simeq \underline{C_3 \times C_7}$ となる．

G が非アーベル群のとき．G の 3-シロー部分群の個数を n_3，G の 7-シロー部分群の個数を n_7 としよう．このとき，シローの定理より，

$$n_3 \equiv 1 \pmod 3 \text{ かつ } n_3 \mid 7$$

$$n_7 \equiv 1 \pmod 7 \text{ かつ } n_7 \mid 3$$

である．よって，

$$n_3 = 1 \text{ または } 7,\quad n_7 = 1$$

となる．したがって，$S_7 \triangleleft G$ かつ，$S_3 \cap S_7 = \{e\}$, ${}^{\#}S_3 \cdot {}^{\#}S_7 = {}^{\#}G$ だから，注意 3.3 より，準同型写像 $\sigma : C_3 \longrightarrow \operatorname{Aut} C_7$ が存在して

$$G \simeq C_7 \underset{\sigma}{\rtimes} C_3$$

となる．

σ を具体的に定める．C_3 の生成元 a に対し $(\sigma_a)^3 = e$ となることに注意．更に定理 4.1 より，$\operatorname{Aut} C_7 = (\mathbb{Z}/7\mathbb{Z})^\times \simeq C_6$ である．$\sigma_a \in \operatorname{Aut} C_7 = (\mathbb{Z}/7\mathbb{Z})^\times$ と考える．

- $\sigma_a = 1$ のとき．C_7 の生成元 b に対し $aba^{-1} = \sigma_a(b) = b$ となり，G がアーベル群になってしまう．

- $\sigma_a = 2$ のとき．このときは，一つの群が定まる．ここでの半直積で用いる準同型を $\tau : C_3 \to \operatorname{Aut} C_7 = (\mathbb{Z}/7\mathbb{Z})^\times$ としよう．

- $\sigma_a = 4$ のとき．このときは，一つの群が定まる．ここでの半直積で用いる準同型を $\nu : C_3 \to \operatorname{Aut} C_7 = (\mathbb{Z}/7\mathbb{Z})^\times$ としよう．

ここで，$g \in \operatorname{Aut} C_3$ を $g(\alpha) = \alpha^{-1}$ $(\alpha \in C_3)$ で定めると，$\nu_{g(a)} = \tau_a$ であるので，定理 3.5 により

$$C_7 \underset{\tau}{\rtimes} C_3 \simeq C_7 \underset{\nu}{\rtimes} C_3$$

となり，非アーベル群 $\underline{C_7 \rtimes C_3}$ が一つだけ定まる． **証明終**

13 位数 27 の群の分類

命題 13.1 位数 27 の群は，同型を除いて 5 個存在する．

証明 G を位数 27 の群とする．

G がアーベル群のとき．アーベル群の基本定理 (第 1 節参照) より，

$$\underline{C_{27}},\quad \underline{C_3 \times C_9},\quad \underline{C_3 \times C_3 \times C_3}$$

の三通りの群が定まる．

G が非アーベル群のとき．$G(9)$ について場合分けする．$g \in G(9)$ とすると，$<g> \setminus \{e, g^3, g^6\} \subset G(9)$ だから，

$$6 \mid^{\#} G(9)$$

であることに注意する．

(1) ${}^{\#}G(9) \leq 12$ と仮定する．このとき，${}^{\#}G(3) \geq 14$ となる．

$Z(G) \neq \{e\}$ だから，ある $a \in Z(G)$ が $o(a) = 3$ を満たす．$<a> \triangleleft G$ より，${}^{\#}G/<a> = 9$ であり，第 5 節より，$G/<a>$ はアーベル群である．したがって $b \in G(3) \setminus <a>$ ととると，

$$<a, b> \triangleleft G$$

となる．ここで，$<a, b>$ はアーベル群であるので $<a, b> \neq G$ である．よって，${}^{\#}<a, b> = 9$ に注意する．仮定より $c \in G(3) \setminus <a, b>$ が存在する．$<a, b> \cap <c> = \{e\}$ かつ ${}^{\#}<c> \cdot {}^{\#}<a, b> = {}^{\#}G$ なので，注意 3.3 より，準同型写像 $\sigma : <c> \longrightarrow \mathrm{Aut}<a, b>$ が存在して，

$$G = <a, b> \rtimes_{\sigma} <c>$$

となる．ここで $<a, b>$ はアーベル群で，位数 9 の元を含まないので $<a, b> \simeq C_3 \times C_3$ である．また，$<c> \simeq C_3$ より，準同型写像 $\sigma : C_3 \longrightarrow \mathrm{Aut}(C_3 \times C_3)$ とおきなおすと，

$$G \simeq (C_3 \times C_3) \rtimes_{\sigma} C_3$$

となる．

σ を具体的に定める．定理 4.2 より，$\mathrm{Aut}\,(C_3 \times C_3) = \mathrm{GL}(2, \mathbb{F}_3)$ である．$\sigma_c \in \mathrm{Aut}\,(C_3 \times C_3) = \mathrm{GL}(2, \mathbb{F}_3)$ とみなすと，$\sigma_c^3 = E$ である．よって，

$$\sigma_c \text{ の最小多項式} \mid X^3 - 1$$

となる．ここで，$\mathbb{F}_3$ において $X^3 - 1 = (X - 1)^3$ なので，σ_c の固有値は 1 のみである．このとき，$C_3 \times C_3$ の生成元を取替えると σ_c は互いに相似な行列となる．

$$\sigma_c \text{ のジョルダン標準形} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ または } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

である．よって，定理 3.5 により，σ_c は，上の二つの行列のどちらかであるとしてよい．

$\sigma_c = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ のとき．このときは，G がアーベル群になってしまうため矛盾．

$\sigma_c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ のとき．このときは，$\underline{(C_3 \times C_3) \rtimes C_3}$ が定まる．

(2) ${}^{\#}G(9) = 18$ のとき．このとき，${}^{\#}G(3) = 8$ となる．

$Z(G) \neq \{e\}$ だから，ある $a \in Z(G)$ が $o(a) = 3$ を満たす．$<a> \triangleleft G$ より，${}^{\#}G/<a> = 9$ だから第 5 節より，$G/<a>$ はアーベル群である．したがって $b \in G(9)$ ととると，

$$<a, b> \triangleleft G$$

となる．ここで $<a, b>$ はアーベル群であるので，$G \neq <a, b>$ である．b の位数は 9 なので，

$$<a, b> = <b>$$

となる．仮定より $c \in G(3) \setminus <b>$ が存在する．$<b> \cap <c> = \{e\}$ かつ ${}^{\#}<c> \cdot {}^{\#}<b> = {}^{\#}G$ なので，注意 3.3 より，準同型写像 $\sigma : <c> \longrightarrow \mathrm{Aut}<b>$ が存在して，

$$G \simeq <b> \underset{\sigma}{\rtimes} <c>$$

となる．

σ を具体的に定める．${\sigma_c}^3 = \mathrm{id}_{<b>}$ より，

$$\sigma_c(b) = b, \quad b^4, \text{ または } b^7$$

である．

(2-1) $\sigma_c(b) = b$ のとき．このときは，G がアーベル群になってしまうため矛盾．

(2-2) $\sigma_c(b) = b^4$ のとき．記号を代え，この σ を τ と書く．このとき，

$$<b> \underset{\tau}{\rtimes} <c>$$

が決まる．

(2-3) $\sigma_c(b) = b^7$ のとき．記号を代え，この σ を ν と書く．このとき，

$$<b> \underset{\nu}{\rtimes} <c>$$

が決まる．

ここで，$g \in \mathrm{Aut}\, C_3$ を $g(\alpha) = \alpha^2$ $(\alpha \in C_3)$ としたとき，$\nu_{g(a)} = \tau_a$ が成立するので，定理 3.5 より，

$$<b> \underset{\tau}{\rtimes} <c> \simeq <b> \underset{\nu}{\rtimes} <c>$$

となり，$\underline{C_9 \rtimes C_3}$ が一つに定まる．

(3) $G(9) = 24$ のとき．このとき，$G(3) = 2$ となる．

すると，$Z(G) \supset G(3)$ だから，ある $a \in Z(G)$ が $o(a) = 3$ を満たす．$<a> \triangleleft G$ より，$^{\#}G/<a> = 9$ だから第 5 節より，$G/<a>$ はアーベル群である．したがって $b \in G(9) \setminus Z(G)$ ととると，

$$<a, b> \triangleleft G$$

となる．ここで $<a, b>$ はアーベル群であるので，

$$<a, b> = <b>$$

となる．仮定より，$c \in G(9) \setminus <b>$ が存在する．更に $cbc^{-1} = b^n$ とおけ，$c^3 \in Z(G)$，$b = c^3bc^{-3} = b^{n^3}$ なので，$n^3 \equiv 1 \pmod 9$ となる．よって，

$$cbc^{-1} = b^4 \text{ または } b^7$$

となる．また，$<b^3> = <c^3>$ だから，

$$b^3 = c^3 \text{ または } c^6$$

が成立する．次の 4 つに場合わけする．

(3-1) $cbc^{-1} = b^4$ かつ $b^3 = c^3$ のとき．このとき，$(cb^2)^3 = e$ なので

$$cb^2 = e,\ \ b^3,\ \text{または } b^6$$

である．

(3-1-1) $cb^2 = e$ のとき．$c = b^{-2}$ となり矛盾する．

(3-1-2) $cb^2 = b^3$ のとき．$c = b$ となり矛盾する．

(3-1-3) $cb^2 = b^6$ のとき．$c = b^4$ となり矛盾する．

(3-2) $cbc^{-1} = b^4$ かつ $b^3 = c^6$ のとき．このとき，$(cb)^3 = e$ なので

$$cb = e,\ \ b^3,\ \text{または } b^6$$

である．

(3-2-1) $cb = e$ のとき．$c = b^{-1}$ となり矛盾する．

(3-2-2) $cb = b^3$ のとき．$c = b^2$ となり矛盾する．

(3-2-3) $cb = b^6$ のとき．$c = b^5$ となり矛盾する．

(3-3) $cbc^{-1} = b^7$ かつ $b^3 = c^3$ のとき．このとき，$(cb^2)^3 = e$ なので

$$cb^2 = e,\quad b^3,\ \text{または}\ b^6$$

である．

(3-3-1) $cb^2 = e$ のとき．$c = b^{-2}$ となり矛盾する．

(3-3-2) $cb^2 = b^3$ のとき．$c = b$ となり矛盾する．

(3-3-3) $cb^2 = b^6$ のとき．$c = b^4$ となり矛盾する．

(3-4) $cbc^{-1} = b^7$ かつ $b^3 = c^6$ のとき．このとき，$(cb)^3 = e$ なので

$$cb = e,\quad b^3,\ \text{または}\ b^6$$

である．

(3-4-1) $cb = e$ のとき．$c = b^{-1}$ となり矛盾する．

(3-4-2) $cb = b^3$ のとき．$c = b^2$ となり矛盾する．

(3-4-3) $cb = b^6$ のとき．$c = b^5$ となり矛盾する．

したがって，このような場合は起こらない．

証明終

14 位数 28 の群の分類

位数 28 のアーベル群は，$\underline{C_4 \times C_7}$ か $\underline{C_2 \times C_2 \times C_7}$ のどちらかである．

G は位数 28 の非アーベル群と仮定する．7-シロー部分群を S_7 とすると，シローの定理により，G は唯一つの 7-シロー部分群をもつ．よって，$S_7 \triangleleft G$ である．

S_2 は，G の 2-シロー部分群としよう．すると，注意 3.3 によって，$G \simeq S_7 \rtimes S_2$ である．

S_2 の位数は 4 であるので，S_2 は C_4 か $C_2 \times C_2$ のどちらかと同型である．よって，G は，$C_7 \rtimes_\sigma C_4$ かまたは $C_7 \rtimes_\tau (C_2 \times C_2)$ と同型になる．

ただし，$\sigma : C_4 \to \mathrm{Aut}(C_7)$，$\tau : C_2 \times C_2 \to \mathrm{Aut}(C_7)$ は準同型である．

まず，$S_2 \simeq C_4$ と仮定しよう．$C_4 =< a >$ とする．定理 4.1 より，$\mathrm{Aut}(C_7) = (\mathbb{Z}/7\mathbb{Z})^\times$ である．$\sigma(a) = 1$ または -1 である．$\sigma_1(a) = 1$ の場合は，G は C_4 と C_7 との直積と同型になり，特にアーベル群になる．$\sigma(a) = -1$ の場合は，非アーベル群 $C_7 \rtimes_\sigma C_4$ が一つ決まる．この群は，$\underline{Q_{28}}$ と同型である．

次に，$S_2 \simeq C_2 \times C_2$ と仮定しよう．$C_6 =< b >, C_2 \times C_2 = \{(e,e),(e,a),(a,e),(a,a)\}$ とする．すると，定理 3.5 により，$\tau((e,e)) = \tau((e,a)) = 1$，$\tau((a,e)) = \tau((a,a)) = -1$ であるとしてよい．これによって，一つの群ができるが，これは $\underline{D_{28}}$ と同型である．

15　位数 30 の群の分類

位数 30 のアーベル群は，$\underline{C_2 \times C_3 \times C_5}$ である．

以下，G は位数 30 の非アーベル群であるとする．

まず，G は位数 15 の部分群を持つことを証明する．

G の 5-シロー部分群または 3-シロー部分群は，正規部分群であることに注意．(5-シロー部分群が正規部分群でないなら，5-シロー部分群は 6 個あり，したがって位数 5 の元は 24 個あることになる．3-シロー部分群が正規部分群でないなら，3-シロー部分群は 10 個あり，したがって位数 3 の元は 20 個あることになる．今，群の位数は 30 であるので，5-シロー部分群または 3-シロー部分群は，正規部分群である．)

5-シロー部分群 (以下 S_5) が正規部分群としよう．$f : G \to G/S_5$ を全射準同型とすると，

$$G/S_5 \rhd C_3$$

である．(第 7 節により，位数 15 の群はアーベル群であることに注意．) このとき，$f^{-1}(C_3) \lhd G$ で，${}^{\#}f^{-1}(C_3) = 15$ である．つまり，G は，位数 15 の部分群をもつ．

3-シロー部分群 (以下 S_3) が正規部分群と仮定しよう．$g : G \to G/S_3$ を全射準同型とすると，

$$G/S_3 \rhd C_5$$

である．(第 6 節により，位数 10 の群は巡回群 C_{10} か二面体群 D_{10} であり，両方とも位数 5 の部分群を持つ．) すると，$g^{-1}(C_5) \lhd G$ で，${}^{\#}g^{-1}(C_5) = 15$ である．

よって，G 内に位数 15 の正規部分群が存在することがわかった．

したがって，注意 3.3 により，G は C_{15} と C_2 の半直積になることがわかる．つまり，$G \simeq C_{15} \underset{\sigma}{\rtimes} C_2$ とできる．ただし，$\sigma : C_2 \to \mathrm{Aut}(C_{15})$ は準同型である．

ここで，定理 4.1 により，$\mathrm{Aut}(C_{15}) \simeq (\mathbb{Z}/15\mathbb{Z})^{\times}$ に注意．

中国剰余定理より，

$$(\mathbb{Z}/15\mathbb{Z})^{\times} = (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})^{\times} = (\mathbb{Z}/5\mathbb{Z})^{\times} \times (\mathbb{Z}/3\mathbb{Z})^{\times} \simeq C_4 \times C_2$$

である．よって，$\sigma : C_2 \to C_4 \times C_2$ と考えてよい．

$C_2 = <a>$，$C_4 \times C_2 = \{(e,e),(b,e),(b^2,e),(b^3,e),(e,c),(b,c),(b^2,c),(b^3,c)\}$ とする．$C_4 \times C_2$ の中で位数 2 の元は，(e,e), (b^2,e)，(e,c)，(b^2,c) の 4 つである．

$\sigma_a = (e,e)$ のとき．このときは，アーベル群である．

$\sigma_a = (e,c)$ のとき．このときは，

$$G \simeq (C_5 \times C_3) \underset{\sigma}{\rtimes} C_2 \simeq \underline{C_5 \times D_6}$$

である．

$\sigma_a = (b^2, e)$ のとき．このときは，

$$G \simeq (C_5 \times C_3) \underset{\sigma}{\rtimes} C_2 \simeq \underline{C_3 \times D_{10}}$$

である．

$\sigma_a = (b^2, c)$ のとき．このとき，

$$G \simeq C_{15} \underset{\sigma}{\rtimes} C_2 \simeq \underline{D_{30}}$$

である．

$C_5 \times D_6$，$C_3 \times D_{10}$, D_{30} が互いに同型ではないことを示そう．シローの定理により，次のことがわかる．$C_5 \times D_6$ では，中心に位数 5 の元があるが，位数 3 の元はない．$C_3 \times D_{10}$ では，中心に位数 3 の元があるが，位数 5 の元はない．D_{30} では，中心に位数 3 の元も位数 5 の元もない．

以上によって，どれも同型ではない．

16　位数 16 の群の分類

次を証明する．

命題 16.1 位数 16 の群は，同型を除いて 14 個存在する．

G を位数 16 の群とする．

G がアーベル群のとき．アーベル群の基本定理 (第 1 節参照) より，G は，

$$\underline{C_{16}},\ \underline{C_8 \times C_2},\ \underline{C_4 \times C_4},\ \underline{C_4 \times C_2 \times C_2},\ \underline{C_2 \times C_2 \times C_2 \times C_2}$$

のどれかと同型である．

G が非アーベル群としよう．$G(8)$ について場合分けする．$g \in G(8)$ とすると，$< g > \setminus \{e, g^2, g^4, g^6\} \subset G(8)$ だから，

$$4 \mid {}^{\#}G(8)$$

であることに注意する．

(1) ${}^{\#}G(8) > 0$ のとき．$G(2)$ について再び場合分けをする．

(1-1) $G(2) \geq 2$ のとき．$a \in G(8)$ をとると仮定より $b \in G(2) \setminus < a >$ が存在する．$< a > \rtimes G$, $< a > \cap < b > = \{e\}$ かつ ${}^{\#} < b > \cdot {}^{\#} < a > = {}^{\#}G$ なので，注意 3.3 より，準同型写像 $\sigma : < b > \to \mathrm{Aut} < a >$ が存在して，

$$G \simeq < a > \underset{\sigma}{\rtimes} < b >$$

となる．

σ を具体的に定める．${\sigma_b}^2 = \mathrm{id}_{<a>}$ だから，

$$\sigma_b(a) = bab^{-1} = a,\ a^3,\ a^5, \text{または}\, a^7$$

である．

(1-1-1) $\sigma_b(a) = a$ のとき．G がアーベル群になってしまうため不適．

(1-1-2) $\sigma_b(a) = a^3$ のとき．

$$G = \underline{C_8 \rtimes_{\sigma} C_2}$$

が一つ定まる．

(1-1-3) $\sigma_b(a) = a^5$ のとき．$\tau := \sigma$ とおきかえると，

$$G = \underline{C_8 \rtimes_{\tau} C_2}$$

が一つ定まる．

(1-1-4) $\sigma_b(a) = a^7$ のとき．$\nu := \sigma$ とおきかえると，

$$G = C_8 \rtimes_{\nu} C_2 \simeq \underline{D_{16}}$$

となる．

(1-1-2), (1-1-3), (1-1-4) のどのケースでも $G = \{e, a, \ldots, a^7, b, ab, \ldots, a^7b\}$ である．$Z(C_8 \rtimes_{\sigma} C_2) = <a^4>$, $Z(C_8 \rtimes_{\tau} C_2) = <a^2>$, $Z(D_{16}) = <a^4>$ に注意する．また，${}^{\#}(C_8 \rtimes_{\sigma} C_2)(2) = 5$, ${}^{\#}D_{16} = 9$ であるので，$C_8 \rtimes_{\sigma} C_2$, $C_8 \rtimes_{\tau} C_2$, D_{16} は，互いに同型ではない．

(1-2) $G(2) = 1$ のとき．$g \in G(4)$ とすると，$<g> \backslash \{e, g^2\} \subset G(4)$ だから，

$$2 \mid^{\#} G(4)$$

に注意する．

(1-2-1) $G(4) = 2$ のとき．$G(8) = 12$ となる．$a, b \in G(8)$ が $b \notin <a>$ を満たすとする．このとき，$<a> \triangleleft G$ となる．$<a> \cup <b> \subset <a, b>$ なので，$<a, b> = G$ である．$<a^2> = <b^2>$ であるので，必要ならば b を b^{-1} で取り替えて，$a^2 = b^2$ としてよい．ここで，G はアーベル群ではないので，

$$bab^{-1} = a^3,\quad a^5 \quad \text{または} \quad a^7$$

である．G は位数 4 の部分群 $<a^2>$ を唯一つ含み，それは $<a>$ にも $<b>$ にも含まれる．よって，$a^2 \in Z(G)$ である．このことより，$bab^{-1} = a^5$ でないといけない．しかし，このとき $(ab)^2 = e$ であるので $o(ab) = 2$ であり，$ab \in <a>$ となり，$b \in <a>$ となって矛盾する．

(1-2-2) ${}^{\#}G(4) \geq 4$ のとき．$a \in G(8), b \in G(4)$ が $b \notin <a>$ を満たすとすると $<a> \triangleleft G$ かつ $<a, b> = G$ である．ここで，G はアーベル群ではないので，

$$bab^{-1} = a^3, \quad a^5 \quad \text{または} \quad a^7$$

である．このとき，$G = \{e, a, \ldots, a^7, b, ab, \ldots, a^7b\}$ に注意する．

- $bab^{-1} = a^3$ のとき．$(ab)^2 = e$ となり ${}^{\#}G(2) = 2$ に矛盾する．
- $bab^{-1} = a^5$ のとき．$(a^2b)^2 = e$ となり ${}^{\#}G(2) = 2$ に矛盾する．
- $bab^{-1} = a^7$ のとき．$ba = a^7b$ である．$a^4 = b^2$ に注意する．このとき，

$$G = <a, b> \simeq \underline{Q_{16}}$$

となる．

(2) $G(8) = 0$ と仮定する．もし任意の $g \in G$ が $o(g) = 2$ となれば，G がアーベル群である (補題 8.2 参照)．よって，

$$G(4) > 0$$

としてよい．${}^{\#}G(2) + {}^{\#}G(4) = 15$ であり，${}^{\#}G(4)$ は偶数であることに注意．${}^{\#}G(2)$ が $1, 3, \geq 5$ の三つに場合分けする．

(2-1) $G(2) = 1$ のとき．$G(4) = 14$ である．$a \in G(4)$ ととる．

ここで，$a \in Z(G)$ と仮定する．$b \notin <a>$ を満たす $b \in G(4)$ に対して $<a, b>$ はアーベル群であり $C_4 \times C_2$ と同型である．しかし，$C_4 \times C_2$ は位数 2 の元を三つ含むので矛盾．

よって，

$$G(4) \cap Z(G) = \phi$$

である．$a \in G(4)$ ととると $<a> \subset C_G(a) \neq G$ である．${}^{\#}C_G(a) = 4$ とすると，a と共役な元の数は ${}^{\#}G/{}^{\#}C_G(a) = 4$ である．$Z(G) = <a^2> \subset <a>$ かつ $G/Z(G)$ がアーベル群なので $<a> \triangleleft G$ となる．ここで，$\forall g \in G$ に対して $gag^{-1} \in <a>$ なので，$gag^{-1} = a$ または a^{-3} となりこれは矛盾である．したがって，$a \in G(4)$ は ${}^{\#}C_G(a) = 8$ を満たす．このとき，$C_G(a)$ はアーベル群になることに注意．すると，アーベル群の基本定理より，

$$C_G(a) \simeq C_4 \times C_2$$

となり，位数 2 の元が三つあることになり矛盾する．

(2-2) $G(2) = 3$ のとき．このとき，$G(4) = 12$ である．まず，次を示す．

主張 16.2 ある元 $a_0 \in G(4)$ が $<a_0> \triangleleft G$ を満たす．

証明 $C_G(a) \supset <a>$ より，$a \in G(4)$ ならば ${}^{\#}C_G(a) \geq 4$ となる．${}^{\#}C_G(a)$ について場合分けする．

(A) $\forall a \in G(4)$ に対して ${}^{\#}C_G(a) = 4$ のとき．a と共役な元の数は ${}^{\#}G/{}^{\#}C_G(a) = 4$ である．
$C_G(a) \supset Z(G) \neq \{e\}$ より，${}^{\#}Z(G) = 2$ であり $Z(G) = <a^2>$ となる．$G/Z(G)$ では，任意の元の二乗が e なので，これはアーベル群である．よって，$<a> \triangleleft G$ となる．

(B) $\exists a \in G(4)$ に対して ${}^{\#}C_G(a) = 8$ のとき．$C_G(a) \triangleleft G$ である．$C_G(a)$ はアーベル群で，位数 4 の元を含むから $C_G(a) \simeq C_4 \times C_2$ である．だから，$\exists b \in G(2)$ が，$C_G(a) = <a, b>$ を満たす．$c \in G \setminus C_G(a)$ をとると，$G = <a, b, c>$ となる．
$<a> \ntriangleleft G$ と仮定すると $cac^{-1} = ab$ または a^3b である．必要なら b と a^2b とを取り替えることにより，$cac^{-1} = ab$ とできる．$c^2 \in C_G(a)$ であるので $cabc^{-1} = a$ である．よって $cbc^{-1} = b$ となるから $b \in Z(G)$ である．ここで，$c^2 = a^2, b$ または a^2b である．
   - $c^2 = a^2$ のとき．このとき，$(ab)^2 = e$ となる．$G/<b>$ はアーベル群なので，$<ab>$ が正規部分群になり，$a_0 = ac$ が求めるものである．
   - $c^2 = b$ のとき．$a^{-1}ca = cb$ だから，$<c> \triangleleft G$ となり，$a_0 = c$ とすればよい．
   - $c^2 = a^2b$ のとき．$Z(G) \geq 4$ かつ $(ac)^2 = e$ である．$G(2) = \{a^2, b, a^2b\}$ なので，ac は，a^2, b または a^2b となり，どの場合も $c \in C_G(a)$ となり不適．

(C) $\exists a \in G(4)$ に対して ${}^{\#}C_G(a) = 16$ のとき．$a \in Z(G)$ なので，$a_0 := a$ とすればよい．

証明終

上の主張により，$o(a) = 4, <a> \triangleleft G$ をみたす a があるとしてよい．$G/<a>$ は C_4 または $C_2 \times C_2$ に同型である．

(2-2-1) $G/<a> \simeq C_4$ のとき．ある元 $b \in G(4)$ が $<a> \cap <b> = \{e\}$ を満たすので

$$G = <a> \rtimes_{\sigma} <b>$$

となる．σ を具体的に求める．$\mathrm{Aut}\, C_4 = (\mathbb{Z}/4\mathbb{Z})^{\times} = \{\pm 1\}$ だから，$\sigma_{(b)} = -1$ となり，群 $\underline{C_4 \rtimes C_4}$ が一つ定まる．

(2-2-2) $G/<a_0> \simeq C_2 \times C_2$ のとき．${}^{\#}G(2) = 3$ であるので，G の位数 8 の部分群 N と，N に含まれていない位数 2 の元があって，G は N と $<c>$ の半直積となる．$N(2)$ の個数は 2 以下である

ので，$N \simeq Q_8$ である．$N = <a,b>$, $a^4 = b^4 = e$, $a^2 = b^2$. $bab^{-1} = a^3$ とする．$G = <a,b> \underset{\sigma}{\rtimes} <c>$ とおく．σ を具体的に求める．$\sigma : <c> \longrightarrow \mathrm{Aut}\, N$ かつ $(\sigma_c)^2 = \mathrm{id}$ だから，$\sigma_c(a) = a$ または a^3 である．

(2-2-2-1) $\sigma_c(a) = a$ のとき．$\sigma_c(b) = b, ab, a^2b$ または a^3b である．
$\sigma_c(b) = b$ のとき．このとき，$\sigma_c = \mathrm{id}_{Q_8}$ であるので，

$$G \simeq \underline{Q_8 \times C_2}$$

となる．
$\sigma_c(b) = ab$ のとき．このときは，$\sigma_c^2(b) = a^2b$ となり矛盾する．
$\sigma_c(b) = a^2b$ のとき．$(a^tbc)^2 = e$ より，位数 2 の元が 4 つ以上になり矛盾する．
$\sigma_c(b) = a^3b$ のとき．$\sigma_c^2(b) = a^2b$ となり矛盾する．

(2-2-2-2) $\sigma_c(a) = a^3$ のとき．a の共役類は $\{a, a^3\}$ なので ${}^{\#}C_G(a) = 8$ である．$C_(a)$ はアーベル群であり，$C_G(a) \simeq C_4 \times C_2$ である．d を $C_G(a) \setminus <a>$ に入る位数 2 の元とする．すると，$d \notin N$ であるので，c の代わりに d を用いれば $\sigma_d(a) = a$ となり，(2-2-2-1) のケースになる．

(2-3) $4 \leq G(2) < 15$ のとき．このとき，$0 < G(4) \leq 11$ である．まず，次を示す．

主張 16.3 ある $H < G$ が $H \simeq C_4 \times C_2$ を満たす．

証明 次のように場合分けして考える．

(A) $\forall a \in G(4)$ に対して $C_G(a) = 4$ のとき．つまり，$C_G(a) = <a>$ である．$Z(G) \neq \{e\}$ より $Z(G) = <a^2>$ である．よって，$\forall \alpha \in G/<a^2>$ に対して $o(\alpha) = 2$ となる．したがって，$G/<a^2>$ はアーベル群となり $<a> \triangleleft G$ となる．ここで，a と共役な元の数は ${}^{\#}G/{}^{\#}C_G(a) = 4$ である．しかし実際は $\{a, a^3\}$ のため矛盾．

(B) $\exists a \in G(4)$ に対して $C_G(a) = 8$ のとき．$C_G(a)$ は，アーベル群で位数 4 の元を含むから $C_G(a) \simeq C_4 \times C_2$ である．

(C) $\exists a \in G(4)$ に対して $C_G(a) = 16$ のとき．ある $b \in G(2)$ が $<a>$ には含まれていないので，$<a,b> \simeq C_4 \times C_2$ である．

証明終

主張 16.3 の H をとる．このとき，$a \in G(4)$, $b \in G(2)$ で $H = <a,b>$ を満たすものがある．また，$H \triangleleft G$ であり，$c \in G(2) \setminus H$ で $H \cap <c> = \{e\}$ と ${}^{\#}H \cdot {}^{\#}<c> = {}^{\#}G$ を満すものがあるので，

$$G \simeq <a,b> \underset{\sigma}{\rtimes} <c>$$

となる．σ を具体的に定める．$(\sigma_c)^2 = \mathrm{id}$ なので，以下の 6 通りに場合分けする．

(2-3-1) $\sigma_c(a) = a$ かつ $\sigma_c(b) = b$ のとき．

$$G \simeq <a, b> \times <c> \simeq C_4 \times C_2 \times C_2$$

となり，アーベル群になる．

(2-3-2) $\sigma_c(a) = a$ かつ $\sigma_c(b) = a^2 b$ のとき．このとき，

$$\underline{(C_4 \times C_2) \rtimes_{\sigma} C_2}$$

が一つ定まる．

(2-3-3) $\sigma_c(a) = a^3$ かつ $\sigma_c(b) = a^2 b$ のとき．a と ab とを取り替えれば，この群は，(2-3-2) と同型な群となる．

(2-3-4) $\sigma_c(a) = a^3$ かつ $\sigma_c(b) = b$ のとき．このときは，

$$G \simeq \underline{C_2 \times D_8}$$

となる．

(2-3-6) $\sigma_c(a) = ab$ かつ $\sigma_c(b) = b$ のとき．このときは，記号を代え τ をすると，

$$G \simeq \underline{(C_4 \times C_2) \rtimes_{\tau} C_2}$$

ができる．

(2-3-6) $\sigma_c(a) = a^3 b$ かつ $\sigma_c(b) = b$ のとき．b と $a^2 b$ とを取り替えれば，この群は，(2-3-5) のものと同型となる．

$(C_4 \times C_2) \rtimes_{\sigma} C_2$, $C_2 \times D_8$, $(C_4 \times C_2) \rtimes_{\tau} C_2$ の三つの群が同型ではないことを示そう．$Z((C_4 \times C_2) \rtimes_{\sigma} C_2)$ は，位数 4 の元を含む．しかし，$C_2 \times D_8$, $(C_4 \times C_2) \rtimes_{\tau} C_2$ の中心には位数 4 の元はない．$C_2 \times D_8$ には，位数 4 の元が四つある．しかし，$(C_4 \times C_2) \rtimes_{\tau} C_2$ には $(ac)^2 = a^2 b$ であるので，位数 4 の元は五つ以上ある．よって，この三つの群は，同型ではない．

17　位数 24 の群の分類

この節の目的は，次を証明することである．

命題 17.1 位数 24 の群は，同型を除いて 15 個存在する．

証明 $24 = 2^3 \times 3$ であるので，位数 24 のアーベル群は，$\underline{C_8 \times C_3}$, $\underline{C_4 \times C_2 \times C_3}$, $\underline{C_2 \times C_2 \times C_2 \times C_3}$ の三通りである．

以下，G は位数 24 の非アーベル群とする．

S_2, S_3 が正規部分群かどうかにより，次の四通りに場合分けして考える．

(1) $S_2, S_3 \triangleleft G$ のとき．第 7 節より，G は直積 $S_2 \times S_3$ と同型になる．よって，このとき，$\underline{D_8 \times C_3}$, $\underline{Q_8 \times C_3}$ が出てくる．

(2) $S_2 \triangleleft G$, $S_3 \not\triangleleft G$ のとき．このとき，注意 3.3 により $G \simeq S_2 \underset{\sigma}{\rtimes} S_3$ と書ける．ただし，$\sigma : S_3 \to \mathrm{Aut}\, S_2$ は非自明な準同型写像である．よって，$S_3 := <a>(\simeq C_3)$ としたとき，

$$o(\sigma_a) = 3 \tag{9}$$

である．

ここで，S_2 の構造によって，次の五通りに場合分けする．

(2-1) $S_2 \simeq C_8$ のとき．第 4 節の結果により，$\mathrm{Aut}\, C_8 = (\mathbb{Z}/8\mathbb{Z})^\times \simeq C_2 \times C_2$ である．これには位数 3 の元がないので，(9) に矛盾．

(2-2) $S_2 \simeq C_4 \times C_2$ のとき．$C_4 \times C_2 := <b> \times <c>$ とし，σ_a を考える．位数を考慮すると

$$\begin{array}{rcl} \sigma_a((b,e)) & = & (b,e),\ (b^3,e),\ (b,c) \text{ または } (b^3,c) \\ \sigma_a((e,c)) & = & (e,c),\ (b^2,e) \text{ または } (b^2,c) \end{array}$$

である．

もし $\sigma_a((e,c)) = (b^2,e)$ なら，$(e,c) = \sigma_a^{-1}((b^2,e)) = \{\sigma_a^{-1}((b,e))\}^2$ だが，この式を満たす元はないので矛盾．(この議論から，$\sigma_a((b^2,e)) = (b^2,e)$ がわかる．)

もし $\sigma_a((e,c)) = (b^2,c)$ なら，$\sigma_a^2((e,c)) = (e,c)$ より (9) に矛盾．

したがって，$\sigma_a((e,c)) = (e,c)$ となる．

$\sigma_a((b,e)) = (b^3,e)$, (b,c) または (b^3,c) とすると，$\sigma_a^2((b,e)) = (b,e)$ より (9) に矛盾．

したがって，σ は自明なものとなり矛盾．

(2-3) $S_2 \simeq C_2 \times C_2 \times C_2$ のとき．定理 4.2 より，$\mathrm{Aut}\,(C_2 \times C_2 \times C_2) = \mathrm{GL}(3, \mathbb{F}_2)$ である．群 $\mathrm{GL}(3, \mathbb{F}_2)$ の位数は $7 \cdot 6 \cdot 4 = 168$ であるので，3-シロー部分群の位数は 3 である．よって，$\mathrm{GL}(3, \mathbb{F}_2)$ の位数 3 の元は，

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ または } \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2$$

に共役である．よって，

$$P^{-1}\sigma_a P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{または} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2$$

を満たすような $P \in \mathrm{GL}(3, \mathbb{F}_2)$ がある．すると，$f := P$, $g : C_3 \to C_3$ を $g(a) = a$ または a^{-1} で定まるものとすると，定理 3.5 によって，すべて同型となるので，この場合は群 $\underline{(C_2 \times C_2 \times C_2) \rtimes C_3}$ が一つ定まる．

(2-4) $S_2 \simeq D_8$ のとき． $D_8 = <A, B>$, $A^4 = B^2 = E$, $BAB^{-1} = A^{-1}$ とおく．位数を考えると，$\sigma_a(A) = A$ または A^3 だが，もし $\sigma_a(A) = A^3$ なら $\sigma_a^2(A) = A$ となるので (9) に矛盾．よって，$\sigma_a(A) = A$ である．

また $\sigma_a(B) = B, A^2, AB, A^2B, A^3B$ のいずれかとわかる．

$\sigma_a(B) = A^2$ なら $\sigma_a(B) = \sigma_a(A)^2$ で矛盾．$\sigma_a(B) = AB, A^2B, A^3B$ なら (9) に矛盾．よって，$\sigma_a(B) = B$ である．

したがって，σ が自明なものになり矛盾する．

(2-5) $S_2 \simeq Q_8$ のとき． $Q_8 = <A, B>$, $A^4 = B^4 = E$, $BAB^{-1} = A^{-1}$ とおく．位数を考えると，$\sigma_a(A)$ の候補は，A, A^3, B, AB, A^2B, A^3B のいずれかであり，$\sigma_a(B)$ の候補としては上の 6 個から $\sigma_a(A)$ と $\sigma_a(A)^{-1}$ を除いた 4 個．よって，${}^{\#}\mathrm{Aut}\, Q_8 \leq 24$ とわかる．

逆に上の 24 個の候補は，$\sigma_a(A)^4 = \sigma_a(B)^4 = E$, $\sigma_a(B)\sigma_a(A)\sigma_a(B)^{-1} = \sigma_a(A)^{-1}$ を満たすので，すべて Q_8 から Q_8 への準同型写像になる．よって，${}^{\#}\mathrm{Aut}\, Q_8 = 24$ である．

$\sigma, \tau : C_3 \to \mathrm{Aut}\, Q_8$ を非自明な準同型とする．すると，$o(\sigma_a) = o(\tau_a) = 3$ である．シローの定理より，$<\sigma_a> = f^{-1} <\tau_a> f$ を満たす Q_8 の自己同型写像 f がある．これにより，$\sigma_a = f^{-1}\tau_a f$ または $f^{-1}{\tau_a}^2 f$ が成立することがわかる．

前者の場合は $g = Id_{C_3}$ とし，後者の場合は $g : C_3 \to C_3$ を $g(a) = a^{-1}$ で定まるものとすれば，任意の $c \in C_3$ に対して，

$$f\sigma_c = \tau_{g(c)} f$$

が成立するので，定理 3.5 により $Q_8 \underset{\sigma}{\rtimes} C_3$ と $Q_8 \underset{\tau}{\rtimes} C_3$ は同型である．したがって，この場合は一つの群 $\underline{Q_8 \rtimes C_3}$ が定まる．

(3) $S_2 \not\lhd G$, $S_3 \lhd G$ のとき．このときは，$G = S_3 \underset{\sigma}{\rtimes} S_2$ である．ただし， $\sigma : S_2 \to \mathrm{Aut}\, S_3$ 非自明な準同型写像である．$S_3 \simeq C_3$ であり第 4 節の結果により，$\mathrm{Aut}\, S_3 = (\mathbb{Z}/3\mathbb{Z})^\times = \{\pm 1\}$ である．$S_3 := <a>$ とおく．

S_2 の構造によって，次の五通りに場合分けする．

(3-1) $S_2 \simeq C_8$ のとき．$C_8 := <b>$ とする．位数を考えると非自明なものは，$\sigma_a(b) = -1$ で決まるもののみ．よって，この場合は群 $\underline{C_3 \rtimes C_8}$ が一つ定まる．

(3-2) $S_2 \simeq C_4 \times C_2$ のとき．$C_4 \times C_2 := <b> \times <c>$ とする．準同型定理より，${}^{\#}\operatorname{Ker}\sigma = 4$ とわかる．

(3-2-1) $\operatorname{Ker}\sigma \simeq C_4$ なら基底を取り替えることにより，σ は

$$\begin{array}{rccc} \sigma: & C_4 \times C_2 & \longrightarrow & (\mathbb{Z}/3\mathbb{Z})^{\times} \\ & (b,e) & \longmapsto & 1 \\ & (e,c) & \longmapsto & -1 \end{array}$$

としてよい．このとき G は唯一つに定まる．この群は，$\underline{D_{24}}$ に同型である．

(3-2-2) $\operatorname{Ker}\sigma \simeq C_2 \times C_2$ なら，σ は

$$\begin{array}{rccc} \sigma: & C_4 \times C_2 & \longrightarrow & (\mathbb{Z}/3\mathbb{Z})^{\times} \\ & (b,e) & \longmapsto & -1 \\ & (e,c) & \longmapsto & 1 \end{array}$$

である．このときも G は唯一つに定まる．この群は，$\underline{Q_{24}}$ に同型である．

また，(3-2-1) の中心には位数 4 の元があるが，(3-2-2) の中心にはないので二つは同型ではない．

(3-3) $S_2 \simeq C_2 \times C_2 \times C_2$ のとき．$C_2 \times C_2 \times C_2 := <b> \times <c> \times <d>$ とおく．準同型定理より，${}^{\#}\operatorname{Ker}\sigma = 4$ とわかる．よって $\operatorname{Ker}\sigma \simeq C_2 \times C_2$ である．基底を取り替えることにより，σ は

$$\begin{array}{rccc} \sigma: & C_2 \times C_2 \times C_2 & \longrightarrow & (\mathbb{Z}/3\mathbb{Z})^{\times} \\ & (b,e,e) & \longmapsto & 1 \\ & (e,c,e) & \longmapsto & 1 \\ & (e,e,d) & \longmapsto & -1 \end{array}$$

としてよい．このときも唯一つに群 $\underline{C_3 \rtimes (C_2 \times C_2 \times C_2)}$ が定まる．

(3-4) $S_2 \simeq D_8$ のとき．$D_8 := <A, B>$, $A^4 = B^2 = E$, $BAB^{-1} = A^{-1}$ とする．準同型定理より，${}^{\#}\operatorname{Ker}\sigma = 4$ とわかる．

(3-4-1) $\operatorname{Ker}\sigma \simeq C_4$ なら σ は

$$\begin{array}{rccc} \sigma: & D_8 & \longrightarrow & (\mathbb{Z}/3\mathbb{Z})^{\times} \\ & A & \longmapsto & 1 \\ & B & \longmapsto & -1 \end{array}$$

となる．このときは群 $\underline{C_3 \rtimes_{\sigma} C_8}$ が定まる．

(3-4-2) $\mathrm{Ker}\,\sigma \simeq C_2 \times C_2$ なら，σ は D_8 の生成元を取り替えることにより，

$$\begin{array}{rccc} \tau : & D_8 & \longrightarrow & (\mathbb{Z}/3\mathbb{Z})^\times \\ & A & \longmapsto & -1 \\ & B & \longmapsto & -1 \end{array}$$

としてよい．(記号を変える．) このときは群 $\underline{C_3 \rtimes_\tau C_8}$ が定まる．

また，(3-4-1) の中心には位数 4 の元があるが，(3-4-2) の中心にはないので二つは同型ではない．

(3-5) $S_2 \simeq Q_8$ のとき．$Q_8 := <A, B>$, $A^4 = B^4 = E$, $BAB^{-1} = A^{-1}$ とする．準同型定理より，$^\#\,\mathrm{Ker}\,\sigma = 4$ とわかる．Q_8 には位数 4 の部分群は C_4 の形のもののみ．

生成元を取り替えることにより，σ は

$$\begin{array}{rccc} \sigma : & Q_8 & \longrightarrow & (\mathbb{Z}/3\mathbb{Z})^\times \\ & A & \longmapsto & 1 \\ & B & \longmapsto & -1 \end{array}$$

である．このとき G は $\underline{C_3 \rtimes Q_8}$ に同型である．

(4) S_2, $S_3 \ntriangleleft G$ のとき．G の 3-シロー部分群の数 n_3 は，シローの定理より

$$n_3|24, \quad \text{かつ} \quad n_3 \equiv 1 (mod 3)$$

より $n_3 = 4$ である．それを，$A_1, \ldots, A_4$ とおく．このとき，

$$\begin{array}{rccc} \phi : & G & \longrightarrow & \mathfrak{S}_4 \\ & g & \longmapsto & \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ gA_1g^{-1} & gA_2g^{-1} & gA_3g^{-1} & gA_4g^{-1} \end{pmatrix} \end{array}$$

によって写像 ϕ を定義する．この ϕ は準同型写像になっており，A_1 らはシロー部分群なのでシローの定理より互いに共役である．よって，$\mathrm{Im}\,\phi$ は可移的である．したがって，$^\#\,\mathrm{Im}\,\phi$ は 4 の倍数である．準同型定理より，$^\#\,\mathrm{Ker}\,\phi = 1, 2, 3, 6$ のいずれかとなる．

(4-1) $^\#\,\mathrm{Ker}\,\phi = 3, 6$ のとき．$o(a) = 3$ となる $\mathrm{Ker}\,\phi$ の元 a がある．$\forall x \in <a>, \forall g \in G$ について $o(gxg^{-1}) = 1, 3$ のいずれか．また，$gxg^{-1} \in \mathrm{Ker}\,\phi$ より $gxg^{-1} \in <a>$ である (位数 6 の部分群は，必ず位数 3 の部分群を一つだけ含むことに注意)．したがって，$<a> \triangleleft G$ で矛盾．

(4-2) $^\#\,\mathrm{Ker}\,\phi = 2$ のとき．$^\#\,\mathrm{Im}\,\phi = 12$ より $\mathrm{Im}\,\phi = \mathfrak{A}_4$ である．$\mathfrak{A}_4$ の 2 -シロー部分群は $C_2 \times C_2$ と同型な正規部分群になっている．それを H とおく．

準同型定理より，$\mathfrak{A}_4 \simeq G/\operatorname{Ker}\phi$ なので $H \triangleleft G/\operatorname{Ker}\phi$.

$\psi : G \to G/\operatorname{Ker}\phi$: 自然な写像として，$\psi^{-1}(H)$ を考える．ψ は準同型なので，$\psi^{-1}(H) \triangleleft G$ で，${}^{\#}\psi^{-1}(H) = 8$ より矛盾．

(4-3) ${}^{\#}\operatorname{Ker}\phi = 1$ のとき．ϕ は同型写像となるので，$G \simeq \underline{\mathfrak{S}_4}$ となる．

証明終