東大数理 2025 専門 B 第 4 問　解答メモ

@Metachick_2021

2026 年 5 月 9 日

1　解答の準備

1.1　群の半直積

【定義 1.1】内部半直積

G を群、N, H を G の部分群とする。$N \triangleleft G$ であって、$G = NH$ かつ $N \cap H = \{e\}$ を満たすとき、G は N と H の (内部) 半直積であるといい、$G = N \rtimes H$ と表す。

ここで、H も G の正規部分群であれば内部直積の定義そのものとなる。したがって、半直積は直積を自然に拡張したより広い概念だといえる。

内部半直積の定義は、あらかじめ「全体となる大きな群 G」が存在していることが前提であった。しかし、群 N と H だけから G を構成したい (G の構造を復元したい) 場合には、この定義とは異なる別のアプローチが必要である。そこで、全体の群 G を前提とせず、N と H という独立した 2 つの群のみから新たな群を構成する方法として外部半直積を導入し、結果として G と同型な群を構成する。

【定義 1.2】外部半直積

N, H を群とし、$\phi : H \to \mathrm{Aut}(N)$ を群準同型写像とする。直積集合 $N \times H$ 上に、以下の演算を定めた群を N と H の（外部）半直積とよび、$N \rtimes_\phi H$ で表す。

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \phi(h_1)(n_2), h_1 h_2)$$

実際、これが群をなすことは簡単に確認できる。結合法則については $\phi(h)$ が群準同型であることから直積集合の演算として成立する。単位元が (e, e) であることは、

- $(n, h) \cdot (e, e) = (n\phi(h)(e), he) = (ne, h) = (n, h), \quad (e, e) \cdot (n, h) = (n\mathrm{id}_N(e), he) = (n, h)$

から従う。また、(n, h) の逆元は $(\phi(h^{-1})(n^{-1}), h^{-1})$ である。実際、以下のように計算できる。

- $(n, h) \cdot (\phi(h^{-1})(n^{-1}), h^{-1}) = (n\phi(h)(\phi(h^{-1})(n^{-1})), hh^{-1}) = (nn^{-1}, e) = (e, e)$
- $(\phi(h^{-1})(n^{-1}), h^{-1}) \cdot (n, h) = (\phi(h^{-1})(n^{-1})\phi(h^{-1})(n), h^{-1}h) = (e, e)$

【補題 1.3】

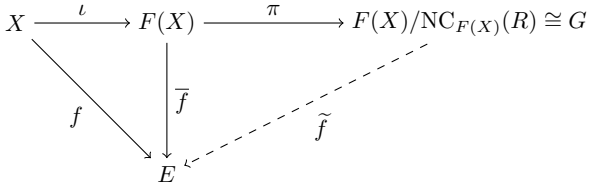
$\phi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ を $1 \mapsto (n \mapsto -n)$ で定める。このとき、次の同型が成り立つ。

$$\mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z} \cong \langle x, y \mid x^4 = y^4 = e, yxy^{-1} = x^3 \rangle$$

$\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ などから、ϕ の候補は $1 \mapsto (n \mapsto n)$ か、$1 \mapsto (n \mapsto -n)$ のみであることがわかる。恒等写像による半直積は直積になるので、結局、$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$ によって作れる非自明な半直積は一つである。

証明　$E = \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}, G = \langle x, y \mid x^4 = y^4 = e, yxy^{-1} = x^3 \rangle, X = \{x, y\}$ とおく。E において $u = (1,0), v = (0,1)$ とおく。いま、計算により $u^4 = (4,0) = (0,0), v^4 = (0,4) = (0,0), vuv^{-1} = u^3$ がわかるから、対応 $f : X \to E$ を $x \mapsto u, y \mapsto v$ で定めれば、自由群の普遍写像性質から f を $F(X)$ に拡張して得られる準同型写像 $\overline{f} : F(X) \to E$ は well-defined であり、$\iota : X \to F(X)$ を自然な包含写像として、$\overline{f} \circ \iota = f$ が成り立つ。ただし、$F(X)$ は X 上の自由群である。

また、$R = \{x^4, y^4, yxy^{-1}x^{-3}\}$ とおくと、u, v は E においてこれらの関係式を満たすため、表示を持つ群の普遍写像性質から、準同型写像 $\widetilde{f} : G \to E$ が以下の図式を可換にするように一意に定まる。



いま、外部半直積の定義から集合として $E = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ であるため、$|E| = |\mathbb{Z}/4\mathbb{Z}| \cdot |\mathbb{Z}/4\mathbb{Z}| = 16$ である。さらに、E の任意の元は $(i,j) = (i,0)(0,j) = u^i v^j$ と表せるため、$E = \{u^i v^j \mid 0 \le i \le 3, 0 \le j \le 3\}$ である。$\overline{f}$ の定義から $\overline{f}(x^i y^j) = u^i v^j$ であり、可換性から $\widetilde{f}$ は全射である。したがって $|G| \ge |E| = 16$ が成り立つ。一方、G においては関係式 $yxy^{-1} = x^3$（すなわち $yx = x^3 y$）を繰り返し適用することで、x を左側に、y を右側に集めることができる。さらに $x^4 = e, y^4 = e$ であるため、G の任意の元は $x^i y^j$（$0 \le i \le 3, 0 \le j \le 3$）の形に表せる。ゆえに G の元の個数は高々 16 個であり、$|G| \le 16$ である。以上より、$|G| = |E| = 16$ であり、全射準同型 $\widetilde{f}$ は有限群間の全単射となるため、同型写像である。よって $\mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z} \cong G$ が示された。 □

【命題 1.4】内部半直積と外部半直積の同型 1

群 G がその部分群 N, H によって $G = N \rtimes H$ と表せるとき、準同型を $\phi(h)(n) = hnh^{-1}$ で定めれば、写像 $\Psi : N \rtimes_\phi H \to G, \quad (n, h) \mapsto nh$ は自然な同型写像となる。

この命題により、全体となる「大きな群 G」が存在する場合には、$N \rtimes_H$ と $N \rtimes_\phi H$ は同一視することができる。記号も外部直積であっても $N \rtimes H$ を採用することもある。

証明　写像 $\Psi : N \rtimes_\phi H \to G$ が群準同型であることを示す。外部半直積の演算の定義および $\phi(h)(n) = hnh^{-1}$ により、任意の $(n_1, h_1), (n_2, h_2) \in N \rtimes_\phi H$ に対して次が成り立つ。

$$\begin{aligned}\Psi((n_1, h_1) \cdot (n_2, h_2)) &= \Psi(n_1\phi(h_1)(n_2),\ h_1h_2) \\ &= n_1(h_1n_2h_1^{-1})(h_1h_2) = n_1h_1n_2h_2\end{aligned}$$

一方、$\Psi(n_1, h_1)\Psi(n_2, h_2) = (n_1h_1)(n_2h_2) = n_1h_1n_2h_2$ であるから、$\Psi((n_1, h_1)\cdot(n_2, h_2)) = \Psi(n_1, h_1)\Psi(n_2, h_2)$ となり、Ψ は群準同型である。次に、Ψ が全単射であることを示す。全射性は、条件 $G = NH$ から直ちに従う。単射性について、$\Psi(n, h) = e$ と仮定すると、$nh = e$ より $n = h^{-1}$ である。$N \cap H = \{e\}$ により $n = h = e$ となるから単射である。以上により、Ψ は群同型写像である。この写像は、部分群 N, H の元を単に G における積として対応させるものであり、生成元の選び方に依存しないため、特に自然な同型であるといえる。□

【命題 1.5】内部半直積と外部半直積の同型 2（余談）

N, H を群とし、$\phi : H \to \mathrm{Aut}(N)$ を群準同型写像とする。$\widetilde{N} = \{(n, e_H) \mid n \in N\}, \widetilde{H} = \{(e_N, h) \mid h \in H\}$ はそれぞれ N, H と同型な $N \rtimes_\phi H$ の部分群であり、さらに $N \rtimes_\phi H = \widetilde{N} \rtimes \widetilde{H}$ が成り立つ。

証明　$G = N \rtimes_\phi H$ とおく。$\widetilde{N}, \widetilde{H}$ がそれぞれ N, H と同型な部分群であることは、$n \mapsto (n, e_H)$ および $h \mapsto (e_N, h)$ が単射な準同型であることから直ちに従う。$\widetilde{N}$ が正規部分群であることは、任意の $(n, e_H) \in \widetilde{N}$ および $(m, h) \in G$ に対し、

$$\begin{aligned}(m, h)(n, e_H)(m, h)^{-1} &= (m\phi(h)(n), h)(\phi(h^{-1})(m^{-1}), h^{-1}) \\ &= (m\phi(h)(n) \cdot \phi(h)(\phi(h^{-1})(m^{-1})),\ hh^{-1}) \\ &= (m\phi(h)(n)m^{-1}, e_H) \in \widetilde{N}\end{aligned}$$

が成り立つことから従う。前者は G の任意の元 $(n, h) \in G$ が $(n, e_H)(e_N, h)$ と書けるので $G = \widetilde{N}\widetilde{H}$ であり、また、明らかに $\widetilde{N} \cap \widetilde{H} = \{(e_N, e_H)\}$ である。したがって、$G = \widetilde{N} \rtimes \widetilde{H}$ が成り立つ。□

1.2　推進定理の一般化

【補題 1.6】

L/K を体拡大、M_1, M_2 を中間体とする。$M_1 \cdot M_2/M_1 \cap M_2$ と $M_1/M_1 \cap M_2$ がともに有限次 Galois 拡大であるとする。このとき、次が成り立つ：

$$\mathrm{Gal}(M_1 \cdot M_2/M_1 \cap M_2) \cong \mathrm{Gal}(M_1 \cdot M_2/M_1) \rtimes \mathrm{Gal}(M_1 \cdot M_2/M_2)$$

証明　$G = \mathrm{Gal}(M_1M_2/M_1 \cap M_2)$, $N = \mathrm{Gal}(M_1M_2/M_1)$, $H = \mathrm{Gal}(M_1M_2/M_2)$ とおく。Galois 理論の基本定理より、以下が成り立つ。

- $N \trianglelefteq G$：$M_1/M_1 \cap M_2$ が Galois 拡大であるため
- $N \cap H = \{e\}$：$N \cap H = \mathrm{Gal}(M_1 \cdot M_2/M_1 \cdot M_2)$ であるため
- $NH = G$：$NH = \langle N, H \rangle = \mathrm{Gal}(M_1 \cdot M_2/M_1 \cap M_2) = G$ であるため

以上の 3 条件より、$G = N \rtimes H$ である。 □

2　問題の解答

問題 2.1 (★★★★★)　(2025 年度 東京大学大学院数理科学研究科)

複素数体 $\mathbb{C}$ の部分体 $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, \sqrt{3+\sqrt{3}}\right)$ を考える。

(1) K は Galois 拡大であることを示し、その拡大次数を求めよ。
(2) $K/\mathbb{Q}$ の中間体で、$\mathbb{Q}$ 上 4 次であるものを全て求め、$\mathbb{Q}(\alpha)$ の形で表せ。
(3) $K/\mathbb{Q}$ の中間体 M_1, M_2 で以下の条件を満たすものを 1 つ与えよ：M_1, M_2 は $\mathbb{Q}$ の Galois 拡大であり、$\mathrm{Gal}(M_1/\mathbb{Q}), \mathrm{Gal}(M_2/\mathbb{Q})$ は位数が等しいが同型でない非可換群である。

解答

(1)　$\mathrm{ch}(\mathbb{Q}) = 0$ より、$\mathbb{Q}$ の代数拡大はすべて分離拡大である。$\alpha = \sqrt{2+\sqrt{2}}, \alpha' = \sqrt{2-\sqrt{2}}, \beta = \sqrt{3+\sqrt{3}}, \beta' = \sqrt{3-\sqrt{3}}$ とおく。また、K は多項式 $f(x) := (x^4 - 4x^2 + 2)(x^4 - 6x^2 + 6)$ の最小分解体になっている。実際、$f(x) = 0$ の根は $\pm\alpha, \pm\alpha', \pm\beta, \pm\beta'$ の 8 つであるが、$\sqrt{2}, \sqrt{3}, \sqrt{6}, \alpha, \beta \in K$ と、$\alpha' = \sqrt{2}^{-1}, \beta' = \sqrt{6}\beta^{-1}$ であるからこれらはすべて含まれている。したがって、$K/\mathbb{Q}$ は Galois 拡大である。

$\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ であるから、2 次拡大をちょうど一つ持つ。特に、$\mathbb{Q}(\sqrt{2})$ が 2 次拡大である。いま、$\mathbb{Q}(\beta)/\mathbb{Q}$ は $\sqrt{2}$ を含まない。$\sqrt{2} \in \mathbb{Q}(\beta)$ と仮定する。$\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\beta)$ であるから、$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}(\beta)/\mathbb{Q}$ の中間体である。一方、$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 4$ であるから、$\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ である。$[\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$ であるから、単純拡大体の性質より、$1, \sqrt{2}$ は $\mathbb{Q}(\beta)$ の $\mathbb{Q}(\sqrt{3})$ 上の基底となる。よって、$\beta = a + b\sqrt{2}$ $(a, b \in \mathbb{Q}(\sqrt{3}))$ となる。両辺を二乗して、$\beta^2 = 3 + \sqrt{3} = a^2 + 2b^2 + 2ab\sqrt{2}$ を得る。すなわち、$a^2 + 2b^2 = 3 + \sqrt{3}, ab = 0$ を得る。これにより、$a^2 = 3 + \sqrt{3}$ または $2b^2 = 3 + \sqrt{3}$ が成り立つ。$\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ のノルムを N とすると、$N(a)^2 = N(a^2) = 6$ または $4N(b)^2 = N(2b^2) = 6$ を得るが、$N(a), N(b) \in \mathbb{Q}$ であるためこれは矛盾する。

これにより、$\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}, \mathbb{Q}(\alpha) \cdot \mathbb{Q}(\beta) = K$ であるから、推進定理より、$\mathrm{Gal}(K/\mathbb{Q}(\beta)) = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ を得る。したがって、$[K : \mathbb{Q}] = [K : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 4 \times 4 = 16$ を得る。

(2)　いま、補題 1.6 を用いることによって、

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}(\alpha)) \rtimes \mathrm{Gal}(K/\mathbb{Q}(\beta))$$

計算により、$\mathrm{Gal}(K/\mathbb{Q}(\alpha)) = \mathbb{Z}/4\mathbb{Z}$ と $\mathrm{Gal}(K/\mathbb{Q}(\beta)) \cong \mathbb{Z}/4\mathbb{Z}$ がわかる。また、(1) の議論から $\mathbb{Q}(\beta)/\mathbb{Q}$ は Galois 拡大でないから、$\mathrm{Gal}(K/\mathbb{Q}(\beta))$ は正規部分群でなく、これにより $\mathrm{Gal}(K/\mathbb{Q})$ は非可換である。これより、$\phi : \mathrm{Gal}(K/\mathbb{Q}(\beta)) \to \mathrm{Aut}(\mathrm{Gal}(K/\mathbb{Q}(\alpha)))$ を用いて、$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$ としたとすると、ϕ は自明でない。すなわち、ϕ は $1 \mapsto (n \mapsto -n)$ により定まる準同型となるほかない。したがって、補題 1.3 により、$\mathrm{Gal}(K/\mathbb{Q}) \cong \langle x, y \mid x^4 = y^4 = e, yxy^{-1} = x^3 \rangle$ を得る。

$G = \langle x, y \mid x^4 = y^4 = e, yxy^{-1} = x^3 \rangle$ とおく。$G = \{x^i y^j \mid 0 \leq i, j \leq 3\}$ であり、それぞれの元の位数を計算すると次のようになる。

- 位数 1：e
- 位数 2：x^2, y^2, x^2y^2
- 位数 4：$x, x^3, y, y^3, xy, xy^2, xy^3, x^2y, x^2y^3, x^3y, x^3y^2, x^3y^3$

G の位数 4（指数も 4）の部分群は位数 2 の元をちょうど 3 つ含むか、位数 4 の元により生成されるかである。これより、G の位数 4 の部分群の個数は 7 である。したがって、$K/\mathbb{Q}$ の次数 4 の中間体の個数も 7 個である。

ここで、以下の 7 個の中間体はすべて相異なり、拡大次数が 4 であるから、これが求める中間体である。

$$\mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\beta'), \mathbb{Q}(\sqrt{2}+\sqrt{3}), \mathbb{Q}(\beta+\beta'), \mathbb{Q}(\beta-\beta'), \mathbb{Q}(\sqrt{6}\alpha)$$

(3)　位数 2 の部分群は $\langle x^2\rangle, \langle y^2\rangle, \langle x^2y^2\rangle$ の 3 つで全てである。それぞれ、関係式の変化を見ることで、剰余群は $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}, D_4, Q_8$ と同型であるとわかる[*1]。これより、$\langle y^2\rangle, \langle x^2y^2\rangle$ に対応する群を H_1, H_2 として、求める中間体は K^{H_1}, K^{H_2} である。いま、x, y は適当な同一視のもとでそれぞれ $\mathrm{Gal}(K/\mathbb{Q}(\alpha))$ の生成元、$\mathrm{Gal}(K/\mathbb{Q}(\beta))$ の生成元として選べる。x は α を固定し、$\beta\mapsto\beta'$ で定まる。y は β を固定し、$\alpha\mapsto\alpha'$ で定まる。

y^2 は β を固定する。一方 α については、$y^2(\alpha)=y(\alpha')=-\alpha$ となる。これにより、$y^2(\alpha^2)=(-\alpha)^2=\alpha^2$ であるため、y^2 は $\alpha^2=2+\sqrt{2}$、すなわち $\sqrt{2}$ を固定する。したがって、y^2 の固定体は $\sqrt{2}$ と β を含む。$[\mathbb{Q}(\sqrt{2},\beta):\mathbb{Q}]=8$ であり、$|G/\langle y^2\rangle|=8$ と一致するため、

$$M_1=\mathbb{Q}(\sqrt{2},\beta)=\mathbb{Q}\left(\sqrt{2},\sqrt{3+\sqrt{3}}\right)$$

となる。

x^2y^2 の作用を考えると、x^2 は α を固定し $\beta\mapsto-\beta$ と写す。y^2 は β を固定し $\alpha\mapsto-\alpha$ と写す。ゆえに、$x^2y^2(\alpha)=-\alpha$ かつ $x^2y^2(\beta)=-\beta$ である。このとき、積 $\alpha\beta$ を考えると $x^2y^2(\alpha\beta)=(-\alpha)(-\beta)=\alpha\beta$ となり、x^2y^2 は $\alpha\beta$ を固定する。$\alpha\beta=\sqrt{2+\sqrt{2}}\sqrt{3+\sqrt{3}}$ の $\mathbb{Q}$ 上の共役元は $\pm\alpha\beta, \pm\alpha'\beta', \pm\alpha\beta', \pm\alpha'\beta$ の 8 個存在するため、$\mathbb{Q}(\alpha\beta)$ の拡大次数 8 以上である。$[K^{\langle x^2y^2\rangle}:\mathbb{Q}]=8$ であるため、

$$M_2=\mathbb{Q}(\alpha\beta)=\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\sqrt{3+\sqrt{3}}\right)$$

となる。

以上より、条件を満たす中間体の組として、次が挙げられる。

$$(M_1,M_2)=\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3+\sqrt{3}}\right),\ \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\sqrt{3+\sqrt{3}}\right)\right)$$

$\Diamond$

[*1] 実は、位数 8 の非可換群は二面体群 D_4 と四元数群 Q_8 のみであるから、解答はこのようになるほかない。

参考文献

1. 佐藤隆夫, **基本群と被覆空間**, 裳華房, 2023.
2. まなか,**「半直積を知ろう（無料記事)」**, note, 2023 年 7 月 22 日, 閲覧日 2026 年 5 月 9 日. https://note.com/manaka_kamogawa/n/n0b98728824e2