

Galois 対応

L/K は有限次 Galois 拡大であると仮定する.

このとき, $\text{Gal}(L/K) = \{L \text{ の } K \text{ 上での体の自己同型全体}\}$ について,

$$|\text{Gal}(L/K)| = [L:K]$$

でかつ以下の一対一対応が得られる: ← Galois 対応と呼ぶ

$$\{L/K \text{ の中間体全体}\} \longleftrightarrow \{\text{Gal}(L/K) \text{ の部分群全体}\}$$

$$M \longmapsto \{\sigma \in \text{Gal}(L/K) \mid \sigma(a) = a \ (a \in M)\}$$

$$L^H = \{\beta \in L \mid \sigma(\beta) = \beta \ (\sigma \in H)\} \longleftarrow H$$

Galois の
基本定理

さらに,

(1) この対応は包含関係を逆転させる. → 問題 11-1 (1)

(2) L/L^H も Galois 拡大になり, $\text{Gal}(L/L^H) = H$. 特に $[L:L^H] = |H|$

(3) L^H/K が Galois 拡大 $\iff H$ は $\text{Gal}(L/K)$ の正規部分群.

(2)より, 位数 r の $\text{Gal}(L/K)$ の部分群 H に対応する L/K の部分体 M は $[L:M] = r$ でかつ $\sigma(\beta) = \beta \ (\beta \in M, \sigma \in H)$ をみたすものになる

問題 11-1 Galois の基本定理をみとめて, Galois の基本定理の状況で

$G = \text{Gal}(L/K)$ の部分群 H_1, H_2 と L/K の中間体 M_1, M_2 が Galois 対応によって対応しているとき, 以下が成立することを示せ:

(1) $H_1 \supset H_2 \iff M_1 \subset M_2$.

(2) Galois 対応によって, $H_1 \cap H_2$ と $M_1 M_2$ が対応し, $\langle H_1, H_2 \rangle$ と $M_1 \cap M_2$ が対応する. 特に M_1 と M_2 が K の Galois 拡大ならば $M_1 M_2$ と $M_1 \cap M_2$ も K の Galois 拡大になる.

記号 $M_1 M_2$ は M_1 と M_2 を含む L の最小の部分体であり,
 $\langle H_1, H_2 \rangle$ は H_1 と H_2 を含む G の最小の部分群である. \square

解答例 (標準的な話題なので教科書を見てもよい.)

(1) $H_1 \supset H_2$ と仮定する. H_i には Galois 対応によって $M_i = L^{H_i} = \{\beta \in L \mid \sigma(\beta) = \beta \ (\forall \sigma \in H_i)\}$ が対応している. $\beta \in M_1 = L^{H_1}$ のとき, $\sigma \in H_2$ について, $H_1 \supset H_2$ より $\sigma \in H_1$ でもあるので $\sigma(\beta) = \beta$ となり, $\beta \in M_2$ であることがわかる. ゆえに, $M_1 \subset M_2$.

つづく

(1) つづき, $M_1 \subset M_2$ と仮定する. M_i には Galois 対応によって,

(1) はやさしい

$$H_i = \text{Gal}(L/M_i) = \{\sigma \in \text{Gal}(L/K) \mid \sigma(\beta) = \beta \ (\forall \beta \in M_i)\}$$

が対応している. $\sigma \in H_2$ のとき, $\beta \in M_1$ について, $M_1 \subset M_2$ なので $\beta \in M_2$ でもあるのて $\sigma(\beta) = \beta$ となり, $\sigma \in H_1$ であることがわかる. ゆえに $H_1 \supset H_2$.
これで (1) を示せた.

(Galois 対応をひとめは)

← やさしい

(2) $H_1 \cap H_2$ と $M_1 M_2$ が Galois 対応することを示そう. (本質的に (1) のみから出る.)

$H_1 \cap H_2$ と L/K の中間体 M が Galois 対応し,

M_1, M_2 と $\text{Gal}(L/K)$ の部分群 H が Galois 対応している と仮定する.

$H_1 \cap H_2 \subset H_i$ ($i=1,2$) と (1) より, $M \supset M_i$ ($i=1,2$).

ゆえに, $M \supset M_1 M_2$. これと (1) より, $H_1 \cap H_2 \subset H$.

$M_i \subset M_1 M_2$ ($i=1,2$) と (1) より, $H_i \supset H$ ($i=1,2$).

ゆえに, $H_1 \cap H_2 \supset H$. これと (1) より, $M \subset M_1 M_2$.

$$\left. \begin{array}{l} H_1 \cap H_2 \subset H_i \ (i=1,2) \text{ と (1) より, } M \supset M_i \ (i=1,2). \\ \text{ゆえに, } \underline{M \supset M_1 M_2}. \text{ これと (1) より, } \underline{H_1 \cap H_2 \subset H}. \\ M_i \subset M_1 M_2 \ (i=1,2) \text{ と (1) より, } H_i \supset H \ (i=1,2). \\ \text{ゆえに, } \underline{H_1 \cap H_2 \supset H}. \text{ これと (1) より, } \underline{M \subset M_1 M_2}. \end{array} \right\} \text{ ゆえに } \begin{cases} H_1 \cap H_2 = H \\ \underline{M = M_1 M_2} \end{cases}$$

つづく

(2) つづき. $\langle H_1, H_2 \rangle$ と $M_1 \cap M_2$ が Galois 対応することを示そう. (上と同様)

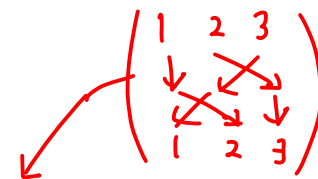
$\langle H_1, H_2 \rangle$ と L/K の中間体 M が Galois 対応し, $M_1 \cap M_2$ と $\text{Gal}(L/K)$ の部分群 H が Galois 対応していると仮定する. (注 $\langle H_1, H_2 \rangle$ は H_1 と H_2 を含む最小の部分群)

$$\left. \begin{array}{l} \langle H_1, H_2 \rangle \supset H_i \quad (i=1,2) \text{ と (1) より, } M \subset M_i \quad (i=1,2). \\ \text{ゆえに, } \underline{M \subset M_1 \cap M_2}. \text{ これと (1) より, } \underline{\langle H_1, H_2 \rangle \supset H}. \\ M_i \supset M_1 \cap M_2 \quad (i=1,2) \text{ と (1) より, } H_i \subset H \quad (i=1,2). \\ \text{ゆえに, } \underline{\langle H_1, H_2 \rangle \subset H}, \text{ これと (1) より, } \underline{M \supset M_1 \cap M_2}. \end{array} \right\} \therefore \begin{cases} \underline{\langle H_1, H_2 \rangle = H} \\ \underline{M = M_1 \cap M_2}. \end{cases}$$

つづく

例 S_3 の部分群 $H_1 = \langle (1,2) \rangle$, $H_2 = \langle (2,3) \rangle$ について,

$$H_1 H_2 = \{ \sigma_1 \sigma_2 \mid \sigma_1 \in H_1, \sigma_2 \in H_2 \} = \{ 1, (1,2), (2,3), (1,2)(2,3) = (1,2,3) \}$$



は S_3 の部分群にならない. H_1 と H_2 を含む S_3 の最小の部分群は S_3 全体になる;
 $\langle H_1, H_2 \rangle = S_3$.

(注) 群 G の部分群 H と正規部分群 N については $\langle H, N \rangle = HN = NH$ になる.

(2) つづき、 M_1 と M_2 が K の Galois 拡大のとき、 $M_1 \cap M_2$ と $M_1 M_2$ も K の Galois 拡大になることを示そう。

L/K の中間体 M と $\text{Gal}(L/K)$ の部分群 H が Galois 対応しているとき、

M/K が Galois 拡大 $\iff H$ は G の正規部分群
となることを使う、

M_i に Galois 対応している $\text{Gal}(L/K)$ の部分群 H_i は正規部分群になっている。

$M_1 \cap M_2$ と $M_1 M_2$ のそれぞれには $\langle H_1, H_2 \rangle$ と $H_1 \cap H_2$ が Galois 対応している。

H_1, H_2 が $G = \text{Gal}(L/K)$ の正規部分群であることから、 $\langle H_1, H_2 \rangle = H_1 H_2$ と $H_1 \cap H_2$ も G の正規部分群になる、ゆえに $M_1 \cap M_2$ と $M_1 M_2$ は K の Galois 拡大になる、 g.e.d.

① H_1, H_2 が群 G の正規部分群 $\implies \langle H_1, H_2 \rangle = H_1 H_2$ も $H_1 \cap H_2$ も G の正規部分群

証明 $\langle H_1, H_2 \rangle \supset H_1 H_2$ は自明、 H_2 が G の正規部分群であることより、 $H_1 H_2$ が G の部分群になることがわかる。ゆえに、 $\langle H_1, H_2 \rangle = H_1 H_2$ 、 $H_1 H_2 \supset H_1 \cap H_2$ が G の正規部分群になることは容易。

略したところを自分で埋めよ!

g.e.d.

問題11-2の準備

L/K を有限次 Galois 拡大とし, K'/K を任意の拡大とする. このとき, 合成体 LK' について, LK'/K' も有限次 Galois 拡大になり, 次の群の同型が得られる:

$$(*) \quad \text{Gal}(LK'/K') \cong \text{Gal}(L/L \cap K'), \quad \sigma \mapsto \sigma|_L = (\sigma \text{ の } L \text{ への制限})$$

証明 L/K が有限次分離的なることより, LK'/K' もそうである.

$L' = LK'$ とおき, L' の代数閉包を $\overline{L'}$ と書き, $\sigma: L' \rightarrow \overline{L'}$ は K' 同型とする.

$K' \supset K$ より, σ は K 同型でもあり, L/K は正規拡大なので $\sigma(L) = L$ となり,

$\sigma(L') = \sigma(LK') = \sigma(L)K' = LK' = L'$ となる. ゆえに, $L' = LK'$ は K' の正規拡大である.

これで LK'/K' が有限次 Galois 拡大になることがわかった,

$\sigma \in \text{Gal}(LK'/K')$ とする. σ は K 同型でもあるので, L/K が正規拡大であることより, $\sigma(L) = L$ となる. ゆえに σ の L への制限を $\sigma|_L$ と書くと, $\sigma|_L \in \text{Gal}(L/K)$.

σ は K' 同型なので $L \cap K'$ 同型でもある. ゆえに, $\sigma|_L \in \text{Gal}(L/L \cap K')$.

$\sigma|_L = 1$ とすると, σ が K' 上でも L 上でも恒等写像になるので $\sigma = 1$ となる. ゆえに, $\sigma \mapsto \sigma|_L$ は単射である.

$H = \{\sigma|_L \mid \sigma \in \text{Gal}(LK'/K')\}$ に Galois 対応する L/K の中間体を M とする. すべての $\sigma|_L$ で不変な L の元はすべての σ で不変な (つまり K' の元であるような) L の元なので $M = L \cap K'$. ゆえに $H = \text{Gal}(L/L \cap K')$. これで (*) が示された.

L と K'
を含む
体 Ω が
与えられて
いるとする,

σ と $\sigma|_L$
に
対応
させる
写像は
群の
準同型
になる

q.e.d.

問題 11-2 L_1, L_2 が体 K の有限次 Galois 拡大であるとき, $L_1 L_2$ と $L_1 \cap L_2$ も
 そうであり, 完全列

$L_1, L_2 \subset \bar{K}$
 と考えることにする.

$$1 \rightarrow \text{Gal}(L_1 L_2 / L_1 \cap L_2) \rightarrow \text{Gal}(L_1 L_2 / K) \rightarrow \text{Gal}(L_1 \cap L_2 / K) \rightarrow 1$$

と同型

← (注) 1 は
 $\{1\}$ の略記

$$\text{Gal}(L_1 L_2 / L_1 \cap L_2) \cong \text{Gal}(L_1 / L_1 \cap L_2) \times \text{Gal}(L_2 / L_1 \cap L_2)$$

が得られる. 特に

$$L_1 \cap L_2 = K \Leftrightarrow [L_1 L_2 : K] = [L_1 : K][L_2 : K]$$

$$\Leftrightarrow \text{Gal}(L_1 L_2 / K) \cong \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K).$$

以上を示せ.

□

解答例 L_1, L_2 が体 K の有限次正規拡大 (もしくは分離拡大) ならば $L_1 L_2, L_1 \cap L_2$ も
 そうである. ゆえに, L_1, L_2 が体 K の有限次 Galois 拡大ならば $L_1 L_2, L_1 \cap L_2$ もそう
 である.

つづく (長い)

一般に L/K が有限次 Galois 拡大でその中間体 M が K の Galois 拡大ならば

$$\text{Gal}(L/K)/\text{Gal}(L/M) \xrightarrow{\sim} \text{Gal}(M/K), \quad \sigma \in \text{Gal}(L/M) \mapsto \sigma|_M = (\sigma \text{ の } M \text{ への制限})$$

という同型が Galois 対応によって得られるのである、これは完全列

$$1 \rightarrow \text{Gal}(L/M) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(M/K) \rightarrow 1$$

$\sigma \quad \mapsto \quad \sigma|_M$

↑ exact sequence

が得られることを意味している。

この一般的结果を $L=L_1L_2$, $M=L_1 \cap L_2$ に適用すれば完全列

$$1 \rightarrow \text{Gal}(L_1L_2/L_1 \cap L_2) \rightarrow \text{Gal}(L_1L_2/K) \rightarrow \text{Gal}(L_1 \cap L_2/K) \rightarrow 1$$

が得られる。

つづく

$\text{Gal}(L_1 L_2 / L_1 \cap L_2) \cong \text{Gal}(L_1 / L_1 \cap L_2) \times \text{Gal}(L_2 / L_1 \cap L_2)$ を示そう、これは問題11-1の記号

問題11-1結果を L, K, M_i がそれぞれ $L_1 L_2, L_1 \cap L_2, L_i$ の場合に適用すると
Galois対応によつて, L_i が $G = \text{Gal}(L_1 L_2 / L_1 \cap L_2)$ の部分群 H_i に対応するとすると,

$$L_i \longleftrightarrow H_i = \text{Gal}(L_1 L_2 / L_i)$$

$$L_1 \cap L_2 \longleftrightarrow \langle H_1, H_2 \rangle = \text{Gal}(L_1 L_2 / L_1 \cap L_2) = G$$

$$L_1 L_2 \longleftrightarrow H_1 \cap H_2 = \text{Gal}(L_1 L_2 / L_1 L_2) = 1$$

} と Galois 対応する.

直積の
特徴
付け

さらに, $L_i / L_1 \cap L_2$ が Galois 拡大になっていることより, H_i は G の正規部分群
になっている. ゆえに, 直積は有限次 Galois 拡大 L_i / K の中間体

$$\text{Gal}(L_1 L_2 / L_1 \cap L_2) = G \cong H_1 \times H_2 = \text{Gal}(L_1 L_2 / L_1) \times \text{Gal}(L_1 L_2 / L_2).$$

群論の
一般論より

上の "準備" を $L = L_1 L_2, K = L_i, K' = L_j$ ($(i, j) = (1, 2) \text{ or } (2, 1)$) に適用すると,

$$\text{Gal}(L_1 L_2 / L_j) = \text{Gal}(L_i L_j / L_j) \cong \text{Gal}(L_i / L_i \cap L_j) = \text{Gal}(L_i / L_1 \cap L_2).$$

直積群の
特徴付け
の一般論

ゆえに,

$$\text{Gal}(L_1 L_2 / L_1 \cap L_2) \cong \text{Gal}(L_1 L_2 / L_1) \times \text{Gal}(L_1 L_2 / L_2)$$

$$\cong \text{Gal}(L_1 / L_1 \cap L_2) \times \text{Gal}(L_2 / L_1 \cap L_2).$$

っく

$$[L_1 L_2 : K] = [L_1 : K][L_2 : K] \stackrel{\textcircled{1}}{\Leftrightarrow} L_1 \cap L_2 = K \stackrel{\textcircled{2}}{\Leftrightarrow} \text{Gal}(L_1 L_2 / K) \cong \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K)$$

を示そう,

$$\text{Gal}(L_1 L_2 / L_1 \cap L_2) \stackrel{(*)}{\cong} \text{Gal}(L_1 / L_1 \cap L_2) \times \text{Gal}(L_2 / L_1 \cap L_2) \text{ より}$$

$$[L_1 L_2 : L_1 \cap L_2] = [L_1 : L_1 \cap L_2][L_2 : L_1 \cap L_2],$$

両辺に $[L_1 \cap L_2 : K]$ の 2 乗を かけると, 次の 式が得られる:

$$[L_1 L_2 : K][L_1 \cap L_2 : K] \stackrel{(**)}{=} [L_1 : K][L_2 : K].$$

$$\begin{aligned} & [L_1 : L_1 \cap L_2][L_1 \cap L_2 : K] \\ &= [L_1 : K] \text{ など} \end{aligned}$$

$$\text{ゆえに, } L_1 \cap L_2 = K \Leftrightarrow [L_1 \cap L_2 : K] = 1 \Leftrightarrow [L_1 L_2 : K] = [L_1 : K][L_2 : K].$$

これで ① の同値性を示せた,

$$(*) \text{ より, } L_1 \cap L_2 = K \text{ ならば } \text{Gal}(L_1 L_2 / K) \cong \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K).$$

$$(**) \text{ より, } |\text{Gal}(L_1 L_2 / K)| = |\text{Gal}(L_1 \cap L_2 / K)| = |\text{Gal}(L_1 / K)| |\text{Gal}(L_2 / K)| \text{ なので}$$

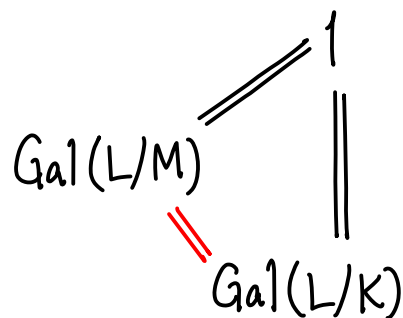
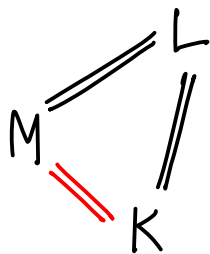
$$\begin{aligned} \text{Gal}(L_1 L_2 / K) \cong \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K) &\Leftrightarrow [L_1 L_2 : K] = |\text{Gal}(L_1 L_2 / K)| = 1 \\ &\Leftrightarrow L_1 \cap L_2 = K. \end{aligned}$$

これで ② の同値性も示せた.



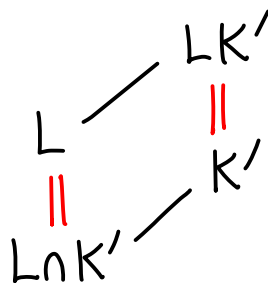
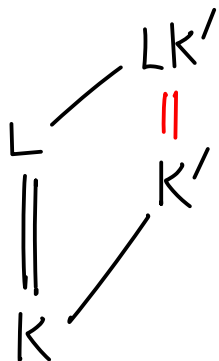
まとめ 2重線は Galois 拡大 や 正規部分群 (全部有限次拡大とする).

①



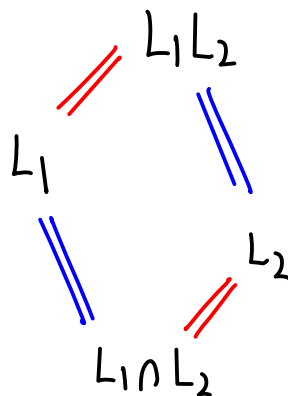
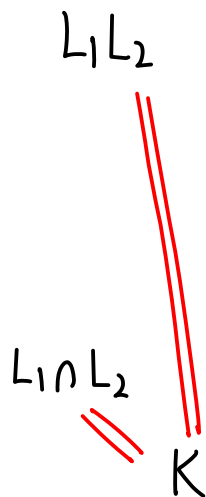
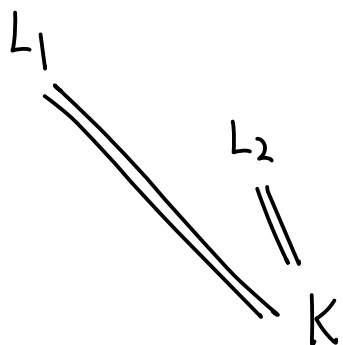
$$\text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Gal}(M/K)$$

②



$$\text{Gal}(LK'/K') \cong \text{Gal}(L/L \cap K')$$

③



$$\text{Gal}(L_1L_2/L_1 \cap L_2)$$

$\uparrow \int$

$$\text{Gal}(L_1L_2/L_1) \times \text{Gal}(L_1L_2/L_2)$$

$\downarrow \int$

$$\text{Gal}(L_1/L_1 \cap L_2) \times \text{Gal}(L_2/L_1 \cap L_2)$$

問題 11-3 問題 11-2 の結果をもちいて, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ が $K = \mathbb{Q}$ の 4 次 Galois 拡大になり, $\text{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となることを示せ.

さらに, その場合の Galois 対応を図示せよ.

□

解答例 $K = \mathbb{Q}$, $L_1 = \mathbb{Q}(\sqrt{2})$, $L_2 = \mathbb{Q}(\sqrt{3})$ とすると, L_i は K の 2 次 Galois 拡大であり, $\text{Gal}(L_i/K) \cong \mathbb{Z}/2\mathbb{Z}$ となる.

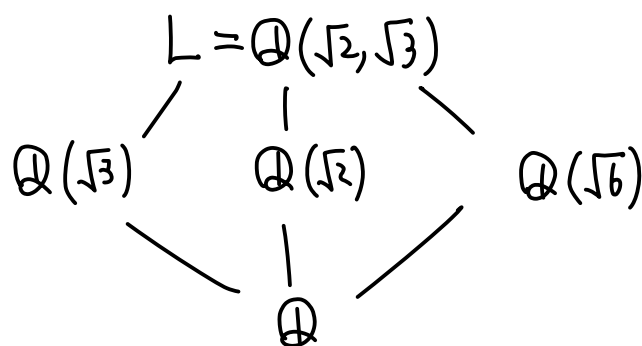
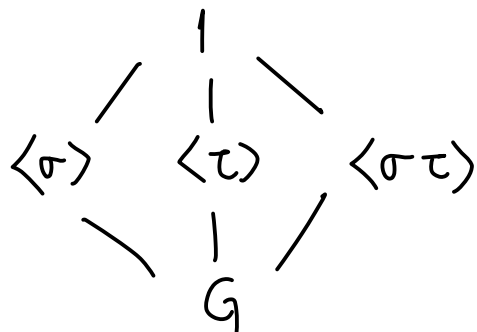
$$L_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, L_2 = \{c + d\sqrt{3} \mid c, d \in \mathbb{Q}\}$$

$L_1 L_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = L$, $L_1 \cap L_2 = \mathbb{Q} = K$ となるので問題 11-2 の結果より,

$$\begin{cases} [L:K] = [L_1 L_2:K] = [L_1:K][L_2:K] = 2 \times 2 = 4, \\ \text{Gal}(L/K) = \text{Gal}(L_1 L_2/K) \cong \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \end{cases}$$

Galois 対応は以下のように図示される: $G = \text{Gal}(L/K)$ とおく.

$\sigma, \tau \in G$, $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$ とすると,



\mathbb{Q} 上での
L の基底として
 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$
をとる.
↓
L
||
 $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$

□

問題11-4 $L = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-3})$ が $K = \mathbb{Q}$ の有限次 Galois 拡大になることを示し, L/K に関する Galois 対応を図示せよ.

Galois 対応を理解したい人にとってのもっとも基本的な例

解答例 1 の原始 3 乗根の 1 つを $\omega = \frac{-1 + \sqrt{-3}}{2}$ と書き, $\alpha = \sqrt[3]{5}$ とおくと,

$$\begin{aligned} L = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-3}) &= \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \\ &= (K = \mathbb{Q} \text{ 上での } x^3 - 5 \text{ の最小分解体}) \end{aligned}$$

なので L/K は有限次 Galois 拡大になる. L/K の中間体 M を

$$M = \mathbb{Q}(\omega) = \mathbb{Q}(\omega, \omega^2) = (\mathbb{Q} \text{ 上での } x^2 + x + 1 \text{ の最小分解体})$$

と定めると, $M = \mathbb{Q}(\omega)$ は $K = \mathbb{Q}$ 上の 2 次の Galois 拡大になる. L/K の中間体 K' を $K' = \mathbb{Q}(\alpha)$ と定めると, K' は $K = \mathbb{Q}$ の 3 次拡大になる (Galois 拡大ではない).

このとき, 問題 11-2 の準備を L, K, K' がそれぞれ $M = \mathbb{Q}(\omega), K = \mathbb{Q}, K' = \mathbb{Q}(\alpha)$ の場合に適用すると, $MK' = \mathbb{Q}(\omega, \alpha) = L$ は $K' = \mathbb{Q}(\alpha)$ の有限次 Galois 拡大であり, $M \cap K' = \mathbb{Q}$ より,

$$\text{Gal}(\mathbb{Q}(\omega, \alpha)/\mathbb{Q}(\alpha)) \cong \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

ゆえに, $\text{Gal}(\mathbb{Q}(\omega, \alpha)/\mathbb{Q}(\alpha)) = \langle b \rangle$, $b(\omega) = \omega^2$, $b(\alpha) = \alpha$, $b^2 = 1$.

つづく

$$|Gal(\mathbb{Q}(w, \alpha)/\mathbb{Q})| = [\mathbb{Q}(w, \alpha) : \mathbb{Q}] = [\mathbb{Q}(w, \alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6.$$

$$6 = [\mathbb{Q}(w, \alpha) : \mathbb{Q}] = [\mathbb{Q}(w, \alpha) : \mathbb{Q}(w)][\mathbb{Q}(w) : \mathbb{Q}] = [\mathbb{Q}(w, \alpha) : \mathbb{Q}(w)] \times 2 \quad \text{よって}$$

$$[\mathbb{Q}(w, \alpha) : \mathbb{Q}(w)] = 3. \quad \text{ゆえに, } Gal(\mathbb{Q}(w, \alpha)/\mathbb{Q}(w)) = \langle a \rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

そこで, $a \in Gal(\mathbb{Q}(w, \alpha)/\mathbb{Q}(w))$, $a(w) = w$, $a(\alpha) = w\alpha$, $a^3 = 1$ と仮定しよう。すると a と b とは

$a, b \in Gal(\mathbb{Q}(w, \alpha)/\mathbb{Q})$ は $ba = a^2b$ みたす:

$$ba(\alpha) = b(w\alpha) = w^2\alpha$$

$$ba(w) = b(w) = w^2$$

$$a^2b(\alpha) = a^2(\alpha) = \alpha$$

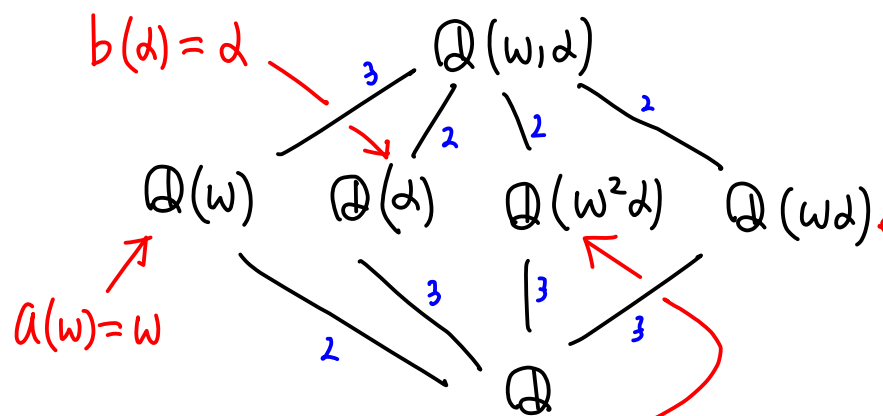
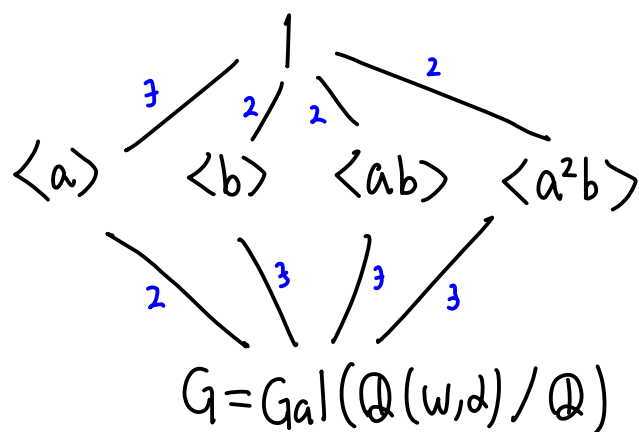
$$a^2b(w) = a^2(w^2) = w$$

以上のまとめ

$$Gal(\mathbb{Q}(w, \alpha)/\mathbb{Q}) = \langle a, b \rangle$$

$$\begin{cases} a^3 = b^2 = 1 \\ ba = a^2b \end{cases} \quad \begin{matrix} \text{位数} \\ \text{は } 6 \end{matrix}$$

以上より, $Gal(\mathbb{Q}(w, \alpha)/\mathbb{Q}) = \{1, a, a^2, b, ab, a^2b\} \cong D_3 \cong S_3$.



$$ab(w^2\alpha) = a(w\alpha) = w^2\alpha, \quad a^2b(w\alpha) = a^2(w^2\alpha) = w^4\alpha = w\alpha$$

□