資料12-1

7-2からコピー

$\boxed{\text{Galois対応}}$ L/K は有限次 Galois 拡大であると仮定する。

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

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

でかつ以下の一対一対応が得られる： ← Galois対応と呼ぶ

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

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

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

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，$\mathrm{Gal}(L/L^H) = H$。 特に $[L:L^H] = |H|$

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

Galoisの基本定理

(2)より，位数 r の $\mathrm{Gal}(L/K)$ 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

$\boxed{\text{問題11-1}}$ Galoisの基本定理をみとめて，Galoisの基本定理の状況で $G=\mathrm{Gal}(L/K)$ 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．

$\boxed{\text{記号}}$ $M_1 M_2$ 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． □

$\boxed{\text{解答例}}$ （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

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

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 $\beta \in M_2$ でもあるので $\sigma(\beta)=\beta$ 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。

(2) $H_1 \cap H_2$ と M_1M_2 が Galois 対応することを示そう。 $\underbrace{\text{(本質的に(1)のみから出る。)}}_{\text{Galois 対応をみとめれば}}$ ← やさしい

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

M_1M_2 と $\mathrm{Gal}(L/K)$ 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、$\underline{M \supset M_1M_2}$。 これと(1)より、$\underline{H_1 \cap H_2 \subset H}$。

$M_i \subset M_1M_2 \ (i=1,2)$ と(1)より、$H_i \supset H \ (i=1,2)$。

ゆえに、$\underline{H_1 \cap H_2 \supset H}$。 これと(1)より、$\underline{M \subset M_1M_2}$。

ゆえに $\begin{cases} \underline{H_1 \cap H_2 = H} \\ \underline{M = M_1M_2} \end{cases}$.

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 $\mathrm{Gal}(L/K)$ 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)

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

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

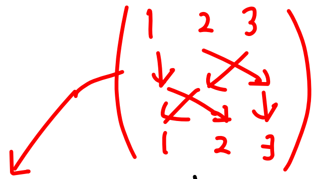
$M_i \supset M_1 \cap M_2$ $(i=1,2)$ と (1) より、$H_i \subset H$ $(i=1,2)$.

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

$$\therefore \begin{cases} \langle H_1, H_2\rangle = H \\ M = M_1 \cap M_2 \end{cases}$$

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、



$$H_1H_2 = \{\sigma_1\sigma_2 \mid \sigma_1 \in H_1, \sigma_2 \in H_2\} = \{1, (1,2), (2,3), (1,2)(2,3) = (1,2,3)\}$$

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 $\mathrm{Gal}(L/K)$ 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 $\mathrm{Galois}(L/K)$ 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 $G = \mathrm{Gal}(L/K)$ 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. q.e.d.

◎ H_1, H_2 が群 G の正規部分群 $\Rightarrow$ $\langle H_1, H_2 \rangle = H_1 H_2$ 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, $\langle H_1, H_2 \rangle = H_1 H_2$. $H_1 H_2$ と $H_1 \cap H_2$ 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!

q.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；

LとK'を含む体Ωが与えられているとする．

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

証明 L/Kが有限次分離的なことより，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，$\sigma: L' \to \overline{L'}$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．

$\sigma \in \mathrm{Gal}(LK'/K')$とする．$\sigma$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$\sigma$の$L$への制限を$\sigma|_L$と書くと，$\sigma|_L \in \mathrm{Gal}(L/K)$．

σをσ|Lに対応させる写像は群の準同型になる

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

$\sigma|_L = 1$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．

$H=\{\sigma|_L \mid \sigma \in \mathrm{Gal}(LK'/K')\}$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$\sigma$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$H=\mathrm{Gal}(L/L\cap K')$．これで$(*)$が示された．

q.e.d.

$\boxed{\text{問題11-2}}$ L_1, L_2 が体 K の有限次 Galois 拡大であるとき，L_1L_2 と $L_1\cap L_2$ も そうであり，完全列

$$1 \to \mathrm{Gal}(L_1L_2/L_1\cap L_2) \to \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1\cap L_2/K) \to 1$$

と同型

$$\mathrm{Gal}(L_1L_2/L_1\cap L_2) \cong \mathrm{Gal}(L_1/L_1\cap L_2) \times \mathrm{Gal}(L_2/L_1\cap L_2)$$

が得られる．特に

$$L_1\cap L_2 = K \iff [L_1L_2:K] = [L_1:K][L_2:K]$$
$$\iff \mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K)\times \mathrm{Gal}(L_2/K).$$

以上を示せ．　□

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

注 1 は $\{1\}$ の略記

$\boxed{\text{解答例}}$ 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_1L_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_1L_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

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

という同型がGalois対応によって得られるのであった。これは完全列

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{Gal}(L/M) & \to & \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(M/K) & \to & 1 \\ & & & & \sigma & \mapsto & \sigma|_M & & \end{array}$$

exact sequence

が得られることを意味している。

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

$$1 \to \mathrm{Gal}(L_1L_2/L_1\cap L_2) \to \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1\cap L_2/K) \to 1$$

が得られる。

つづく

$\mathrm{Gal}(L_1L_2/L_1\cap L_2) \cong \mathrm{Gal}(L_1/L_1\cap L_2)\times \mathrm{Gal}(L_2/L_1\cap L_2)$ 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 $L_1L_2,\ L_1\cap L_2,\ L_i$ の場合に適用すると、

Galois対応によって、L_i が $G=\mathrm{Gal}(L_1L_2/L_1\cap L_2)$ の部分群 H_i に対応するとすると、

$$\left.\begin{aligned} L_i &\longleftrightarrow H_i = \mathrm{Gal}(L_1L_2/L_i) \\ L_1\cap L_2 &\longleftrightarrow \langle H_1, H_2\rangle = \mathrm{Gal}(L_1L_2/L_1\cap L_2) = G \\ L_1L_2 &\longleftrightarrow H_1\cap H_2 = \mathrm{Gal}(L_1L_2/L_1L_2) = 1 \end{aligned}\right\}$$ 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、

$L_1\cap L_2$ は有限次Galois拡大 L_i/K の中間体

$$\mathrm{Gal}(L_1L_2/L_1\cap L_2) = G \cong H_1\times H_2 = \mathrm{Gal}(L_1L_2/L_1)\times\mathrm{Gal}(L_1L_2/L_2).$$

群論の一般論より

上の"準備"を $L=L_1L_2$, $K=L_i$, $K'=L_j$ $((i,j)=(1,2)$ or $(2,1))$ に適用すると、

$$\mathrm{Gal}(L_1L_2/L_j) = \mathrm{Gal}(L_iL_j/L_j) \cong \mathrm{Gal}(L_i/L_i\cap L_j) = \mathrm{Gal}(L_i/L_1\cap L_2).$$

直積群の特徴付けの一般論

ゆえに、

$$\begin{aligned} \mathrm{Gal}(L_1L_2/L_1\cap L_2) &\cong \mathrm{Gal}(L_1L_2/L_1)\times\mathrm{Gal}(L_1L_2/L_2) \\ &\cong \mathrm{Gal}(L_1/L_1\cap L_2)\times\mathrm{Gal}(L_2/L_1\cap L_2). \end{aligned}$$

つづく

$$[L_1L_2:K]=[L_1:K][L_2:K] \underset{①}{\Leftrightarrow} L_1\cap L_2=K \underset{②}{\Leftrightarrow} \mathrm{Gal}(L_1L_2/K)\cong \mathrm{Gal}(L_1/K)\times \mathrm{Gal}(L_2/K)$$

を示そう.

$\mathrm{Gal}(L_1L_2/L_1\cap L_2) \overset{(*)}{\cong} \mathrm{Gal}(L_1/L_1\cap L_2)\times \mathrm{Gal}(L_2/L_1\cap L_2)$ より

$$[L_1L_2:L_1\cap L_2]=[L_1:L_1\cap L_2][L_2:L_1\cap L_2].$$

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

$$[L_1L_2:K][L_1\cap L_2:K] \overset{(**)}{=} [L_1:K][L_2:K].$$

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

ゆえに, $L_1\cap L_2=K \Leftrightarrow [L_1\cap L_2:K]=1 \Leftrightarrow [L_1L_2:K]=[L_1:K][L_2:K]$.

これで①の同値性を示せた.

(*)より, $L_1\cap L_2=K$ ならば $\mathrm{Gal}(L_1L_2/K)\cong \mathrm{Gal}(L_1/K)\times \mathrm{Gal}(L_2/K)$.

(**)より, $|\mathrm{Gal}(L_1L_2/K)|\,|\mathrm{Gal}(L_1\cap L_2/K)| = |\mathrm{Gal}(L_1/K)|\,|\mathrm{Gal}(L_2/K)|$ なので

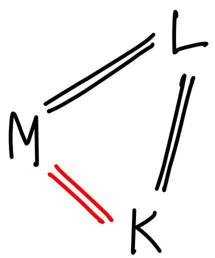
$$\mathrm{Gal}(L_1L_2/K)\cong \mathrm{Gal}(L_1/K)\times \mathrm{Gal}(L_2/K) \Leftrightarrow [L_1\cap L_2:K]=|\mathrm{Gal}(L_1\cap L_2/K)|=1$$
$$\Leftrightarrow L_1\cap L_2=K.$$

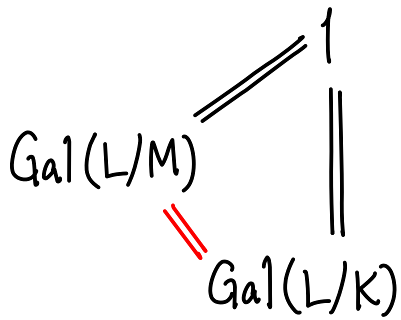
これで②の同値性も示せた.

$\square$

$\boxed{\text{まとめ}}$ 2重線はGalois拡大や正規部分群(全部有限次拡大とする).

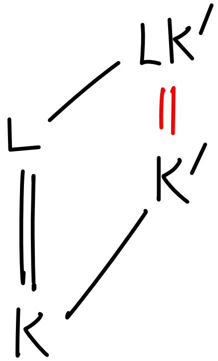
①

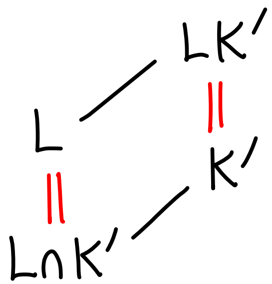




$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$$

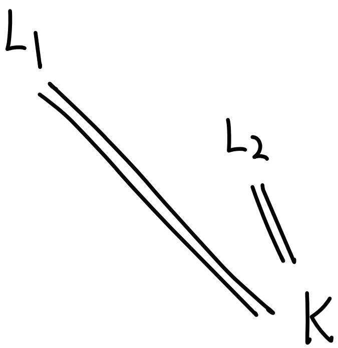
②

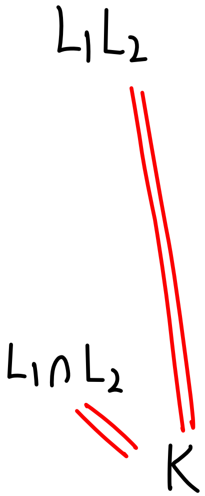


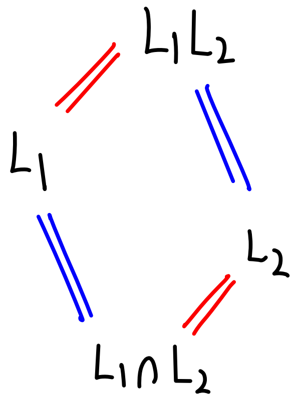


$$\mathrm{Gal}(LK'/K') \xrightarrow{\sim} \mathrm{Gal}(L/L\cap K')$$

③







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

$$\uparrow \wr$$

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

$$\downarrow \wr$$

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

$\boxed{\text{問題 11-3}}$ 問題11-2の結果をみとめて，$L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ が $K=\mathbb{Q}$ の4次Galois拡大になり，$\mathrm{Gal}(L/K)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ となることを示せ．さらに，その場合のGalois対応を図示せよ． □

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

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

$L_1L_2=\mathbb{Q}(\sqrt{2},\sqrt{3})=L$，$L_1\cap L_2=\mathbb{Q}=K$ となるので問題11-2の結果より，

$$\begin{cases}[L:K]=[L_1L_2:K]=[L_1:K][L_2:K]=2\times 2=4,\\ \mathrm{Gal}(L/K)=\mathrm{Gal}(L_1L_2/K)\cong\mathrm{Gal}(L_1/K)\times\mathrm{Gal}(L_2/K)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.\end{cases}$$

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

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\tau\rangle \arrow[d, dash] & \langle\sigma\tau\rangle \arrow[dl, dash] \\
 & G &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & L=\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\mathbb{Q}$上での Lの基底として $1,\sqrt{2},\sqrt{3},\sqrt{6}$ をとれる．

$L=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Q}\}$

□

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 $\omega=\dfrac{-1+\sqrt{-3}}{2}$ と書き，$\alpha=\sqrt[3]{5}$ とおくと，

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

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，

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

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

つづく

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

$6 = [\mathbb{Q}(\omega,\alpha):\mathbb{Q}] = [\mathbb{Q}(\omega,\alpha):\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}] = [\mathbb{Q}(\omega,\alpha):\mathbb{Q}(\omega)]\times 2$ より

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

ここで、 $a \in \mathrm{Gal}(\mathbb{Q}(\omega,\alpha)/\mathbb{Q}(\omega))$, $a(\omega)=\omega$, $a(\alpha)=\omega\alpha$, $a^3=1$ となるように a をとれる.

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

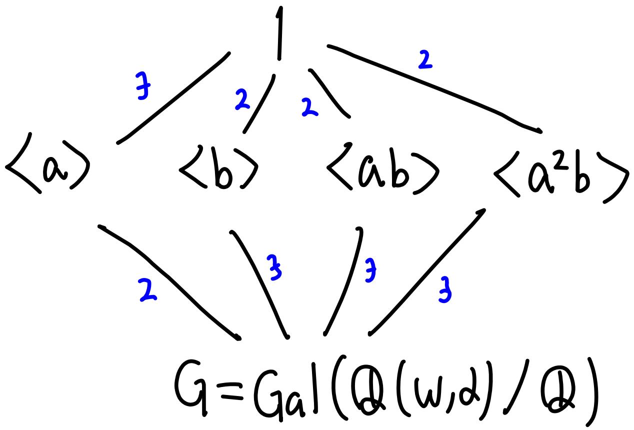
$$ba(\alpha) = b(\omega\alpha) = \omega^2\alpha \qquad ba(\omega) = b(\omega) = \omega^2$$
$$a^2b(\alpha) = a^2(\alpha) \,/\!/ \qquad a^2b(\omega) = a^2(\omega^2) \,/\!/$$

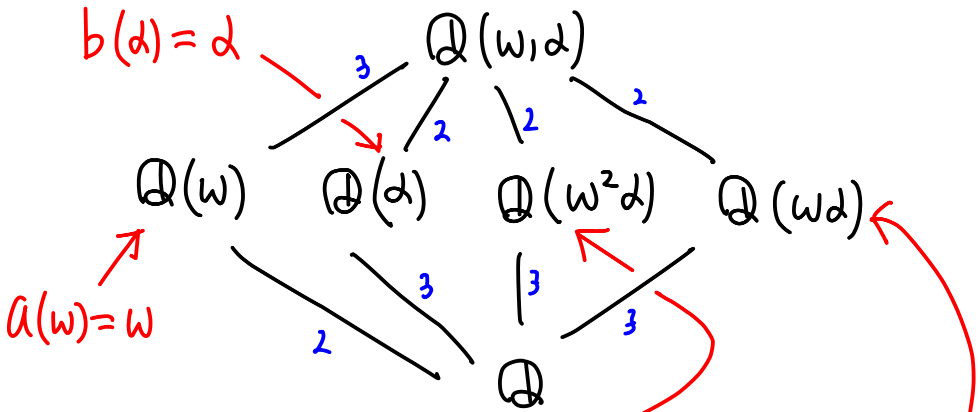
以上のまとめ

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

$\begin{cases} a^3 = b^2 = 1 \\ ba = a^2 b \end{cases}$ 位数は6

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





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

□