$\boxed{4.1.13}$ 演習4.1.3の結果を用いると

$\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$ なので D_4 について調べる

$|D_4| = 8$ より

D_4 の非自明な部分群 $\Longleftrightarrow$ 位数2, 4の部分群

(i) 位数2の部分群について。位数2の部分群は

生成元の位数が2の巡回群と同値なので

$\langle r \rangle, \langle t^2 \rangle, \langle rt \rangle\ \langle rt^2 \rangle, \langle rt^3 \rangle$ となる

(ii) 位数4の部分群について

位数4の部分群は可換群で $(2^2 = 4)$ 有限アーベル群の

基本定理より $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ か $\mathbb{Z}/4\mathbb{Z}$ に同型

$\mathbb{Z}/4\mathbb{Z}$ に同型な群の場合、それは位数4の元を生成元とする巡回群なので

$\langle t \rangle$ となる。

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ に同型な場合、位数1,2の元しか含まれないので

$\{1, r, t^2, rt, rt^2, rt^3\}$ で構成される。仮に r を含むとすると

$r(rt) = t$, $r(rt^3) = t^3$ となるので その部分群は $\{1, r, rt^2, t^2\}$

となるしかないが、これは実際に部分群になる

※ $rt^2 = t^2r$ を利用すると rt^2 の形になることを利用して示すとよい

r を含まないときについて考える。rt, rt^2, rt^3 のうちでどれか2つが含まれるとすると

$(rt)(rt^2) = t^3$, $(rt^3)(rt^2) = t$ より

rt, rt^3 を含むしかない

このときその部分群は $rt^3rt = t^2$ より $\{1, t^2, rt, rt^3\}$ となる必要があるが

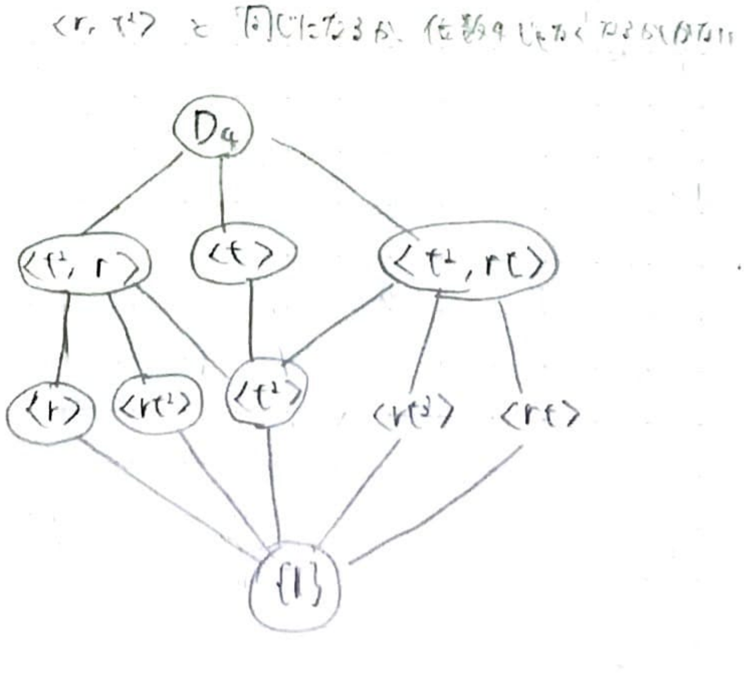
これは実際部分群となる。

rt, rt^2, rt^3 のうちどれか1つしか含まないとすると、その部分群でも r, t^2 を含むしかないので

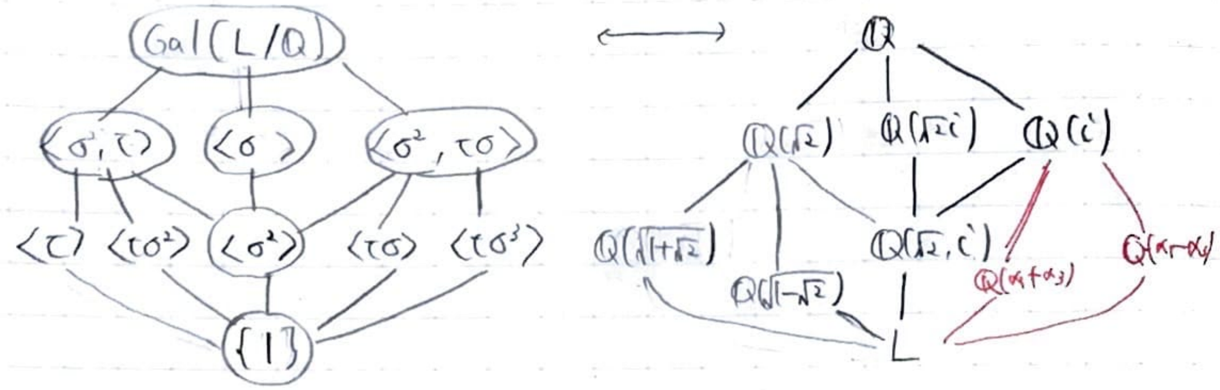
ここまででできた $\langle r, t^2 \rangle$ と同じになるか、位数4じゃなくなるしかない

(i), (ii) より

丸でつけたのは
正規部分群



同型判.



ただし $\alpha_1=\sqrt{1+\sqrt{2}}$, $\alpha_2=-\alpha_1$, $\alpha_3=\sqrt{1-\sqrt{2}}$, $\alpha_4=-\alpha_3$ とすると

$\sigma, \tau \in Gal(L/\mathbb{Q})$ は

$\sigma(\alpha_1)=\alpha_4$ $\sigma(\alpha_2)=\alpha_3$, τは複素共役

$\sigma(\alpha_3)=\alpha_1$ $\sigma(\alpha_4)=\alpha_2$ となるものである.

まず $\sigma^2(\sqrt{2})=\sigma^2(\alpha_1^2-1)=\alpha_2^2-1=\sqrt{2}$ $\tau(\sqrt{2})=\sqrt{2}$ より

$\mathbb{Q}(\sqrt{2})\subset M_{\langle\sigma^2,\tau\rangle}$

そして $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, より $[L:\mathbb{Q}(\sqrt{2})]=4$

$[L:M_{\langle\sigma^2,\tau\rangle}]=|\langle\sigma^2,\tau\rangle|=4$

よって $M_{\langle\tau,\sigma^2\rangle}=\mathbb{Q}(\sqrt{2})$

また $\tau(i)=-i$. $\sigma(i)=\sigma(\alpha_1\alpha_3)=\alpha_4\alpha_1=-i$ より

$\sigma^2(i)=i$, $\tau\sigma(i)=i$ であるので 同様にして

$M_{\langle\sigma^2,\tau\sigma\rangle}=\mathbb{Q}(i)$

同様に $\sigma^2(\sqrt{2})=\sqrt{2}$, $\sigma^2(i)=i$ より $M_{\langle\sigma^2\rangle}=\mathbb{Q}(\sqrt{2},i)$

$\sigma(\sqrt{2}i)=\sqrt{2}i$ より $M_{\langle\sigma\rangle}=\mathbb{Q}(\sqrt{2}i)$

$\tau(\sqrt{1+\sqrt{2}})=\sqrt{1+\sqrt{2}}$ より $M_{\langle\tau\rangle}=\mathbb{Q}(\sqrt{1+\sqrt{2}})$

$\tau\sigma^2(\sqrt{1-\sqrt{2}})=\tau(\alpha_4)=-\sqrt{1-\sqrt{2}}$ より $M_{\langle\tau\sigma^2\rangle}=\mathbb{Q}(\sqrt{1-\sqrt{2}})$

$\tau\sigma(\alpha_1+\alpha_3)=\tau(\alpha_4+\alpha_1)=\alpha_1+\alpha_3$

で $(\alpha_1+\alpha_3)^2=2+2\sqrt{-1}$ ←これが最小多項式を使っても既約性が証明難しいので.

教科書の手法でいく. 他と $M_{\langle\tau\sigma\rangle}=\mathbb{Q}(\alpha_1+\alpha_3)$

$M_{\langle\tau\sigma^3\rangle}=\mathbb{Q}(\alpha_1-\alpha_3)$ と求める.

自明でない ガロア拡大は $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}i)$

$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2},i)$