問題 1

拡大体 $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ について、以下の問いに答えよ

1. $\mathbb{Q}(\sqrt{3})/\mathbb{Q} = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ であることを確認せよ.また拡大次数 $[\mathbb{Q}(\sqrt{3}); \mathbb{Q}]$ を求めよ.
2. $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ のガロア群 $Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ を求めたい.
   (a) f を $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ の自己同型写像とする. $f(1)$ および $f(\sqrt{3})$ が決まれば、写像 f 自体が定まることを示せ.
   (b) f が $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ の自己同型写像となるための、$f(1)$ および $f(\sqrt{3})$ に関する条件を求め $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ の自己同型写像を列挙せよ。
   (c) $\mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})}$ を求めよ。
   (d) $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ はガロア拡大かどうか判定せよ。

解答

1. $f(x) = x^2 - 3 \ \in \mathbb{Q}[x]$. $f(x)$ はアイゼンシュタインの判定法より $\mathbb{Q}[x]$ 上の既約多項式であり、$\sqrt{3} \ \notin \mathbb{Q}$ より、$\sqrt{3}$の $\mathbb{Q}[x]$ 上の最小多項式の次数は 2 以上. よって、$f(x)$ は $\mathbb{Q}[x]$ 上の最小多項式. したがって、$\mathbb{Q}(\sqrt{3})$ は $\mathbb{Q}$ 上のベクトル空間としての次元は 2 であり、基底として $\{1, \sqrt{3}\}$ が取れるので、$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$
   $[\mathbb{Q}(\sqrt{3}); \mathbb{Q}] = 2$
2. (a) $\forall a + b\sqrt{3}$に対して、f が $\mathbb{Q}-$ 自己同型写像であることに注意して、$f(a + b\sqrt{3}) = f(a) + f(\sqrt{3}) = a \cdot f(1) + b \cdot f(\sqrt{3})$. よって、$f(1), f(\sqrt{3})$ によって f が定まる。
   (b) f が $\mathbb{Q}-$ 自己同型写像であることから, $f(1) = 1$.
   $f(\sqrt{3}) \cdot f(\sqrt{3}) = f(\sqrt{3}^2) = f(3) = 3$. よって、$f(\sqrt{3}) = \pm\sqrt{3}$.
   以上から、『$f(1) = 1$』かつ『$f(\sqrt{3}) = \pm\sqrt{3}$』
   よって、$Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, \sigma\}$. (ただし, $\sigma(\sqrt{3}) = -\sqrt{3}$となる写像)
   (c) $\mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})} = \{\alpha \in \mathbb{Q}(\sqrt{3}) \ \mid \forall\sigma \in Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q}),\ \sigma(\alpha) = \alpha\} = \mathbb{Q}$ を示す。
   - $\subset$
     $\forall\alpha = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})}$に対して, $\sigma(a + b\sqrt{3}) = a - b\sqrt{3}$より、
     $a + b\sqrt{3} = a - b\sqrt{3}$. ($\because \mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})}$の定義)
     $\Leftrightarrow 2b\sqrt{3} = 0$
     $\Leftrightarrow b = 0$
     よって, $\alpha = a \in \mathbb{Q}$
   - $\supset$ は明らか

   以上から、$\mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})} = \mathbb{Q}$
   (d) $\mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})} = \mathbb{Q}$ より、ガロア拡大
   $\mid \mathbb{Q}(\sqrt{3})/\mathbb{Q}^{Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q})} \mid = [\mathbb{Q}(\sqrt{3}); \mathbb{Q}] = 2$ からガロア拡大と言ってもよい

問題 2

ガロア理論の基本定理を $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ について、確認したい

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ の拡大次数を求めよ。
2. $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ を求めよ。
3. 中間体 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ に対応する。$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ の部分群を求めよ。
4. $f \in Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ を $f(1) = 1,\ f(\sqrt{2}) = -\sqrt{2},\ f(\sqrt{3}) = \sqrt{3}$で定める自己同型写像とする。$\{id, f\}$ は $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ の部分群となるが、これに対応する中間体を求めよ。

解答

1.
   - $f(x) = x^2 - 2$ は $\sqrt{2} \notin \mathbb{Q}$ より、$\mathbb{Q}$ 上の最小多項式. よって、$[\mathbb{Q}(\sqrt{2}); \mathbb{Q}] = 2$
   - $g(x) = x^2 - 3$ は $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ より、$\mathbb{Q}(\sqrt{2})$ 上の最小多項式。よって、$[\mathbb{Q}(\sqrt{2},\ \sqrt{3}); \mathbb{Q}(\sqrt{2})] = 2$

   以上から、$[\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}(\sqrt{2})]\ [\mathbb{Q}(\sqrt{2}); \mathbb{Q}] = 4.$
2. $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ について
   - まず、$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ がガロア拡大であることを示す
     $\sqrt{2} \notin \mathbb{Q}$ より、$\sqrt{2}$の $\mathbb{Q}$ 上の最小多項式は $x^2 - 2$ であり、$\mathbb{Q}$ 上の共役は $\pm\sqrt{2}.$
     $\sqrt{3} \notin \mathbb{Q}$ より、$\sqrt{3}$の $\mathbb{Q}$ 上の最小多項式は $x^2 - 3$ であり、$\mathbb{Q}$ 上の共役は $\pm\sqrt{3}$
     $\pm\sqrt{3}, \pm\sqrt{2} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ より、$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は正規拡大なので、ガロア拡大
     また、$x^2 - 3$ は $\mathbb{Q}(\sqrt{2})$ 上の最小多項式でもあるので、拡大次数は $[\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}(\sqrt{2})]\ [\mathbb{Q}(\sqrt{2}); \mathbb{Q}] = 4$ となる。
   - $\forall\sigma \in Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ に対して、$\sigma(\sqrt{2})$ は$\sqrt{2}$の K 上の共役となるので、$\sigma(\sqrt{2}) = \pm\sqrt{2}$. 同様に、$\sigma(\sqrt{3}\,)$ は$\sqrt{3}$の K 上の共役となるので、$\sigma(\sqrt{3}) = \pm\sqrt{3}$
     よって、$id, \sigma\ (\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sigma 3), \tau\ (\tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}), \phi\ (\phi(\sqrt{2}) = -\sqrt{2}, \phi(\sqrt{3}) = -\sqrt{3}),\ Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ の元であり、拡大次数が 4 であることからこれが $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ の全ての元である。

   以上から、$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \phi\}$
3. ガロア理論の基本定理より、中間体 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ に対応するガロア群は $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}))$ である。$[\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}(\sqrt{2}] = 2$ より $\mid Gal(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}) \mid = 2.$
   よって、$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})); \mathbb{Q}(\sqrt{2})$ は位数 2 の部分群である。
   $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}))/\mathbb{Q}(\sqrt{2}))$ は $\mathbb{Q}(\sqrt{2})$ の元を不変にするので、$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}))/\mathbb{Q}(\sqrt{2})) = \{id, \tau\}$
4. $H = \{id, f\}$ とおく.ガロア理論の基本定理から、$\mathbb{Q}(\sqrt{2}, \sqrt{3})^H$が H に対応する中間体である。$\mathbb{Q}(\sqrt{2}, \sqrt{3})^H = \{\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \forall\sigma \in H,\ \sigma(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{3})$

   $*\{id, f\}$ は $\mathbb{Q}(\sqrt{3})$ の元を固定するので、対応する中間体は $\mathbb{Q}(\sqrt{3})$

中間体との対応のまとめ

1. 中間体が与えられたときにガロア群を求める方法の概要
   中間体を固定するような K-自己同型群を求める

2. ガロア群が与えられたときに中間体を求める方法の概要
与えられたガロア群で固定されている中間体を求める

問 3

$K = \mathbb{Q}(\sqrt{2}),\ L = \mathbb{Q}(\sqrt[4]{3})$ とする。全問と同様, K は $\mathbb{Q}$ のガロア拡大である。

1. L は K のガロア拡大であることを示せ。
2. L は $\mathbb{Q}$ のガロア拡大出ないことを示せ。