ALGEBRA: HOMEWORK 5

Problem 1. Does there exist a normal extension $L \supset \mathbb{Q}(\sqrt{3}) \supset \mathbb{Q}$ with cyclic Galois group $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$?

Proof. The answer is No. We will prove by contradiction. Assume there exists such L and we will have $[L : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Assume $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) =: G$ is a generator. Since $\sqrt{3} \notin \mathbb{Q} = L^G$, $\sigma(\sqrt{3}) \neq \sqrt{3}$. Since $3 = \sigma(3) = \sigma(\sqrt{3}^2) = \sigma(\pm\sqrt{3})^2$, we have $\sigma(\sqrt{3}) = -\sqrt{3}, \sigma(-\sqrt{3}) = \sqrt{3}$. So $\sqrt{3} \in L^{\{\sigma^2, id\}}$ and $\mathbb{Q}(\sqrt{3}) = L^{\{\sigma^2, id\}}$.

By elementary computations we know that there exists $c \in L \backslash \mathbb{Q}(\sqrt{3})$ such that $c^2 = a + b\sqrt{3}$, where $a, b \in \mathbb{Q}$. Then c is a root of

$$(x^2 - a)^2 - 3b^2 = 0.$$

Then $c, \sigma(c), \sigma^2(c), \sigma^3(c)$ are 4 different roots of above equation. So $a, b \neq 0$. Assume the 4 roots are $\pm c, \pm d$, where d satisfies that $d^2 = a - b\sqrt{3}$. $\sigma(c^2) = \sigma(a + b\sqrt{3}) = a - b\sqrt{3} \neq c^2$, so $\sigma(c) \neq \pm c$. By the same reason we have $\sigma(d) \neq \pm d$. W.L.O.G we may assume $\sigma(c) = d$ and then $\sigma^2(c) = -c$. Consider the relation between roots and coefficients we have $(cd)^2 = c^2d^2 = a^2 - 3b^2$. Since $\sigma(cd) = -cd$, $cd \in L^{\{\sigma^2, id\}} = \mathbb{Q}(\sqrt{3}) = \mathbb{Q} + \mathbb{Q}\sqrt{3}$, and further $cd \in \mathbb{Q}\sqrt{3}$. Assume $e = cd/\sqrt{3} \in \mathbb{Q}$ and we have $3e^2 = a^2 - 3b^2$. So $3x^2 = y^2 - 3z^2$ has nontrivial solutions in $\mathbb{Z}$. Assume x, y, z is a nontrivial solution and $\gcd(x, y, z) = 1$. Then $3|y$, and $x^2 + z^2 = 3(y/3)^2 = 0 \pmod 3$. By coprimeness $3 \nmid x$ or $3 \nmid z$, so $x^2 + z^2 \neq 0 \pmod 3$, contradictory. $\square$

Problem 2. Determine all subfields of $\mathbb{Q}(\zeta_9)$.

Proof. First we note that ζ_9 has minimal polynomial $x^6 + x^3 + 1$, and other roots of this polynomial is $\zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8$.

Then $\zeta \mapsto \zeta^2$ induces a $\mathbb{Q}$-automorphism σ on $\mathbb{Q}(\zeta_9)$, and we can prove σ is of order 6. Since $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$, $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ is normal and

$$Gal(\mathbb{Q}(\zeta_9)/\mathbb{Q}) =< \sigma >\cong C_6.$$

C_6 has subgroups isomorphic to $\{e\}, C_2, C_3, C_6$. It is easy to check that $\mathbb{Q}(\zeta_9^3)$ and $Q(\zeta_9 + \bar{\zeta}_9)$ are two subfields of $\mathbb{Q}(\zeta_9)$, and $[\mathbb{Q}(\zeta_9^3) : \mathbb{Q}] = 2, [\mathbb{Q}(\zeta_9 + \bar{\zeta}_9) : \mathbb{Q}] = 3$. So by Galois theory, $\mathbb{Q}(\zeta_9)$ has 4 subgroups $\mathbb{Q}, \mathbb{Q}(\zeta_9^3), \mathbb{Q}(\zeta_9 + \bar{\zeta}_9), \mathbb{Q}(\zeta_9)$, with corresponding Galois groups $C_6, C_3, C_2, \{e\}$ respectively. $\square$

Problem 3. Determine a polynomial $f \in \mathbb{Z}[x]$ whose roots generate a cyclic extension of $\mathbb{Q}$ of order 5.

Proof. ζ_{11} has a minimal polynomial

$$f(x) = (x^{11} - 1)/(x - 1) = x^{10} + ... + 1.$$

So $[\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] = 10$ and $\zeta_{11} \mapsto \zeta_{11}^2$ induces a $\mathbb{Q}$-automorphism σ on $\mathbb{Q}(\zeta_{11})$. It is easy to check that the order of σ is 10 and thus $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ is normal with Galois group C_{10}. Since $\sigma^5(\zeta_{11}) = \zeta_{11}^{32} = \zeta_{11}^{-1} = \bar{\zeta}_{11}$, $\zeta_{11} + \bar{\zeta}_{11}$ is invariant under σ^5. Then

$$\mathbb{Q} \subsetneq \mathbb{Q}(\zeta_{11} + \bar{\zeta}_{11}) \subset \mathbb{Q}(\zeta_{11})^{\{\sigma^5, id\}},$$

So by Galois theory

$$\{\sigma^5, id\} \subset Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\zeta_{11} + \bar{\zeta}_{11})) \subsetneq Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\zeta_{11})) = C_{10}$$

So $\{\sigma^5, id\} = Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\zeta_{11} + \bar{\zeta}_{11}))$, and

$$Gal(\mathbb{Q}(\zeta_{11} + \bar{\zeta}_{11})/\mathbb{Q}) = C_{10}/\{\sigma^5, id\} = C_5.$$

Now we just need to compute the minimal polynomial of $\zeta_{11} + \bar{\zeta}_{11}$, which is

$$\begin{aligned}&(x - (\zeta_{11} + \bar{\zeta}_{11}))(x - (\zeta_{11}^2 + \bar{\zeta}_{11}^2))...(x - (\zeta_{11}^5 + \bar{\zeta}_{11}^5))\\ =&x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.\end{aligned}$$

□

Problem 4. Show that $K := \mathbb{Q}(\sqrt{2 + \sqrt{-5}})$ is normal over $\mathbb{Q}$ and determine its Galois group.

Proof. The minimal polynomial of $\sqrt{2 + \sqrt{-5}}$ is $(x^2 - 2)^2 + 5$, which have 4 different roots $\pm\sqrt{2 + \sqrt{-5}}$. Since $\sqrt{2 + \sqrt{-5}} \cdot \sqrt{2 - \sqrt{-5}} = 3$, we have $\pm\sqrt{2 - \sqrt{-5}} \in \mathbb{Q}(\sqrt{2 + \sqrt{-5}})$. By mapping $\sqrt{2 + \sqrt{-5}}$ to each root we will get 4 different $\mathbb{Q}$-automorphisms. Since $[\mathbb{Q}(\sqrt{2 + \sqrt{-5}}) : \mathbb{Q}] = 4$, $\mathbb{Q}(\sqrt{2 + \sqrt{-5}})/\mathbb{Q}$ is normal.

Assume $\sigma \in Gal(\mathbb{Q}(\sqrt{2 + \sqrt{-5}})/\mathbb{Q})$. If $\sigma(\sqrt{2 + \sqrt{-5}}) = -\sqrt{2 + \sqrt{-5}}$, $\sigma^2(\sqrt{2 + \sqrt{-5}}) = \sigma(-\sqrt{2 + \sqrt{-5}}) = -\sigma(\sqrt{2 + \sqrt{-5}}) = \sqrt{2 + \sqrt{-5}}$. So $\sigma^2 = id$; If $\sigma(\sqrt{2 + \sqrt{-5}}) = \pm\sqrt{2 - \sqrt{-5}}$, $\sigma^2(\sqrt{2 + \sqrt{-5}}) = \sigma(\pm\sqrt{2 - \sqrt{-5}}) = \sigma(\pm 3/\sqrt{2 + \sqrt{-5}}) = \pm 3/\sigma(\sqrt{2 + \sqrt{-5}}) = \sqrt{2 + \sqrt{-5}}$. So $\sigma^2 = id$.

So every element in $Gal(\mathbb{Q}(\sqrt{2 + \sqrt{-5}})/\mathbb{Q})$ is of order 2, and then $Gal(\mathbb{Q}(\sqrt{2 + \sqrt{-5}})/\mathbb{Q}) = C_2 \times C_2$. □

Problem 5. Show that it may happen that $[LK : K] < [L : L \cap K]$.

Proof. Let $K = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\zeta_3\sqrt[3]{2})$, then $L \cap K = \mathbb{Q}$. The minimal polynomial of $\zeta_3\sqrt[3]{2}$ in $\mathbb{Q}$ is $x^3 - 2$, and in $\mathbb{Q}(\sqrt[3]{2})$ is $(x^3-2)/(x-\sqrt[3]{2}) = x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$. So we have

$$[LK : K] = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2 < [L : L \cap K] = 3.$$

$\square$