HOMEWORK 5 SOLUTIONS

1. Problem 1

Solution. Suppose by way of contradiction that α could be written as such a sum $\sqrt{a_1} + \cdots + \sqrt{a_n}, \quad a_i \in \mathbf{Q}$, then letting $\mathbb{F}$ be the splitting field of the minimal polynomial of α. We have the following inclusion

$$\mathbb{Q} \subset \mathbb{F} \subset \mathbb{Q}[\sqrt{a_1}, \cdots, \sqrt{a_n}]$$

as $\mathbb{Q}[\sqrt{a_1}, \cdots, \sqrt{a_n}]$ is the splitting field of the polynomial $\prod_{i=1}^{n}(x - \sqrt{a_i})$ and $\sqrt{a_1} + \cdots + \sqrt{a_n} \in \mathbb{Q}[\sqrt{a_1}, \cdots, \sqrt{a_n}]$, so by a theorem proved in class, its minimal polynomial must also split in the same splitting extension.

Next we see note that since $a_i \in \mathbb{Q}$, each $\sqrt{a_i}$ satisfies a degree 2 polynomial and hence have at most 1 other Galois conjugate. Thus, it follows that the Galois group of $\mathbb{Q}[\sqrt{a_1}, \cdots, \sqrt{a_n}]$ can only possibly have automorphisms of the form

$$\begin{aligned} \sqrt{a_1} &\to \pm\sqrt{a_1} \\ &\vdots \\ \sqrt{a_n} &\to \pm\sqrt{a_n} \end{aligned}$$

Hence, it is a product of C_2 cyclic groups, which is abelian.

We claim that $G = Aut(\mathbb{F}/\mathbb{Q}) = D_4$.

We see that $\sqrt{1+\sqrt{3}}$ is a root of the polynomial $p(x) = x^4 - 2x^2 - 2$ which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with prime 2, hence this is its minimal polynomial.

Now, we see that the four roots of $p(x)$ are

$$\begin{aligned} &\sqrt{1+\sqrt{3}}, -\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}}, -\sqrt{1-\sqrt{3}} \\ = &\sqrt{1+\sqrt{3}}, -\sqrt{1+\sqrt{3}}, i\sqrt{\sqrt{3}-1}, -i\sqrt{\sqrt{3}-1} \end{aligned}$$

Hence, we have that the splitting field of $p(x)$ is,

$$\mathbb{Q}[\sqrt{1+\sqrt{3}}, -\sqrt{1+\sqrt{3}}, i\sqrt{\sqrt{3}-1}, -i\sqrt{\sqrt{3}-1}] = \mathbb{Q}[\sqrt{1+\sqrt{3}}, i\sqrt{\sqrt{3}-1}]$$

We claim this is a degree 8 extension, as we have the following chain of subextensions,

$$\mathbb{Q} \subset \underbrace{\mathbb{Q}[\sqrt{1+\sqrt{3}}]}_{\text{Degree 4}} \subset \underbrace{\mathbb{Q}[\sqrt{1+\sqrt{3}}, i\sqrt{\sqrt{3}-1}]}_{\text{Degree 2}}$$

Where the first extension is degree 4, since the minimal polynomial of $\sqrt{1+\sqrt{3}}$ is $p(x)$ of degree four. The second extension is degree 2 since $(i\sqrt{\sqrt{3}-1})^2 = 1-\sqrt{3} \in \mathbb{Q}[\sqrt{1+\sqrt{3}}]$ (we see this as $2-(\sqrt{1+\sqrt{3}})^{2} = 1-\sqrt{3}$)

Hence the splitting field of $p(x)$ is degree 8, which implies $|G| = 8$. Now the only degree 8 subgroup of S_4 is the dihedral group D_4, hence $|G| = D_4$.

We recall that, $\mathbb{F} \subset \mathbb{Q}[\sqrt{a_1}\cdots\sqrt{a_n}]$ which has an Abelian Galois Group as shown above, call this G_2, so $G = D_4$ is a quotient of G_2 by a theorem proved in class, but it is non abelian, which is a contradiction.

$\blacksquare$

2. Problem 2

Theorem 2.1. *If $\alpha \in \mathbb{C}$ is a nested square root and G is the Galois group of its minimal polynomial over $\mathbb{Q}$ then the order of G is a power of 2.*

Proof. By definition, if α is a nested square root then there exists a sequence of fields $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$ such that each extension has $\deg(F_{i+1}/F_i) = 2$ and $\alpha \in F_n$.

Note that F_1 is a degree 2 extension of $\mathbb{Q}$ so it is the splitting field of some quadratic equation over $\mathbb{Q}$ and thus it is a Galois extension.

Now suppose that for some i we have an extension $F_i \subset F_i'$ that is a Galois extension of $\mathbb{Q}$ of degree 2^k for some $k \in \mathbb{N}$. We can see that F_{i+1} is a quadratic extension of F_i so it is equal to $F_i[\sqrt{\delta}]$ for some $\delta \in F_i$. If we let G_i be the Galois group $Aut(F_i'/\mathbb{Q})$ then we can set F_{i+1}' to be the field $F_i'[\sqrt{g\delta} : g \in G_i]$ which includes $F_i[\sqrt{\delta}] = F_{i+1}$

As F_i' is Galois over $\mathbb{Q}$ it is the splitting field of some polynomial $p(x)$ so we can consider the following polynomial. As it is fixed by all the permutations $g \in G_i$ it is a polynomial over the base field $\mathbb{Q}$.

$$q(x) = p(x) \cdot \prod_{g \in G_i} (x^2 - g\delta)$$

The roots of this polynomial are given by the roots of p, which are all in $F_i' \subset F_{i+1}'$, or the square roots $\sqrt{g\delta}$, which are in F_{i+1}' by construction, so q splits in $F_{i+1}'[x]$. However, the roots of p generate F_i' over $\mathbb{Q}$ and the roots $\sqrt{g\delta}$ generate F_{i+1}' over F_i', so F_{i+1}' is generated over $\mathbb{Q}$ by the roots of q so it is the splitting field.

Adjoining each root $\sqrt{g\delta}$ will either not increase the degree over F_i' or increase it by a multiple of 2, so as F_i' is of degree 2^k over $\mathbb{Q}$ we find that F_{i+1}' is degree $2^{k+\ell}$ over $\mathbb{Q}$ for some $0 \leq \ell \leq |G_i|$. We thus have an extension $F_{i+1} \subset F_{i+1}'$ that is a Galois extension over $\mathbb{Q}$ of degree $2^{k+\ell}$.

By induction we thus have a Galois extension $\mathbb{Q} \subset F_n'$ of degree 2^k for some $k \in \mathbb{N}$. However, $\alpha \in F_n \subset F_n'$ so the splitting field of its minimal polynomial must be some intermediate extension $\mathbb{Q} \subset K \subset F_n'$, so the degree of this extension must divide 2^k, and thus must also be a power of 2. As this extension $\mathbb{Q} \subset K$ is Galois, the size of its Galois group is equal to this degree, so the order of the Galois group is a power of 2.

Therefore, if $\alpha \in \mathbb{C}$ is a nested square root and G is the Galois group of its minimal polynomial over $\mathbb{Q}$ then the order of G is a power of 2. $\square$

3. Problem 3

By the Theorem in the question, G (with $|G| = 2^n$) has a subgroup of index p, or a subgroup of order 2^{n-1}. Similarly, we can find a subgroup of this subgroup with order 2^{n-2}. Thus it follows that there is a chain of subgroups $G = K_0 \supset K_1 \supset \cdots \supset K_n = \{e\}$, and by Galois correspondence there exists a chain of subfields $F_n \supset F_{n-1} \supset \cdots \supset F_0 = \mathbb{Q}$, where $\alpha \in F_n$ and $\deg(F_i/F_{i-1}) = 2$ as desired.

If $p = 2^n + 1$, then ζ_p has degree 2^n over $\mathbb{Q}$. We know that the other roots of the minimal polynomial of ζ_p are just powers of ζ_p (roots of unity), so the Galois extension we want is simply $\mathbb{Q}[\zeta_p]$ which has degree 2^n. Thus ζ_p is a nested square root.

4. Problem 4

Consider the roots of $x^6 + 3$, they are of the form $i(3)^{\frac{1}{6}}\zeta_6^j$ where $j \in \{0, \ldots, 5\}$, since $(i(3)^{\frac{1}{6}}\zeta_6^i)^6 + 3 = -3 + 3 = 0$. Furthermore, as a degree 6 polynomial $x^6 + 3$ has 6 roots so we have accounted for all of them. Then the splitting field of $x^6 + 3$ is $\mathbb{Q}[i(3)^{\frac{1}{6}}, \ldots, i(3)^{\frac{1}{6}}\zeta_6^5]$ but:

$$\begin{aligned}
i(3)^{\frac{1}{6}}\zeta_6^j &= (-3)^{\frac{1}{6}} * (\zeta_6)^i \\
\implies (-3)^{\frac{1}{6}}\zeta_6^i &\in \mathbb{Q}[i(3)^{\frac{1}{6}}, \zeta_6] \\
\implies \mathbb{Q}[i(3)^{\frac{1}{6}}, \ldots, i(3)^{\frac{1}{6}}\zeta_6^5] &\subset \mathbb{Q}[i(3)^{\frac{1}{6}}, \zeta_6] \\
\implies i(3)^{\frac{1}{6}} &\in \mathbb{Q}[i(3)^{\frac{1}{6}}, \ldots, i(3)^{\frac{1}{6}}\zeta_6^5] \\
\zeta_6 &= i(3)^{\frac{1}{6}}\zeta_6 * (i(3)^{\frac{1}{6}})^{-1} \\
\implies \zeta_6 &\in \mathbb{Q}[(-3)^{\frac{1}{6}}, \ldots, (-3)^{\frac{1}{6}}\zeta_6^5] \\
\implies \mathbb{Q}[(-3)^{\frac{1}{6}}, \ldots, (-3)^{\frac{1}{6}}\zeta_6^5] &= \mathbb{Q}[(-3)^{\frac{1}{6}}, \zeta_6] =: K
\end{aligned}$$

But $(i(3)^{\frac{1}{6}})^3 = -i\sqrt{3}$ and $-i\sqrt{3} * \frac{-1}{2} + \frac{1}{2} = \zeta_6$. Then $\mathbb{Q}[\zeta_6] \subset \mathbb{Q}[i(3)^{\frac{1}{6}}]$ and thus $K = \mathbb{Q}[\zeta_6, i(3)^{\frac{1}{6}}] = \mathbb{Q}[i(3)^{\frac{1}{6}}]$. **a** By the irreducibly of $x^6 + 3$ by esienstiens critereon this is a degree 6 extention. Hence by the Galois correspondence the Galois group has 6 elements. We label our roots as $i(3)^{\frac{1}{6}}\zeta_6^j$ as α_{j+1}, then $i(3)^{\frac{1}{6}}$ is labelled α_1. By the transitiveity of G there must be some $\phi_k \in G$ such that $\phi_k(1) = \alpha_k$ for all $k \in \{1, \ldots, 6\}$ and by the size of G exactly one. So every automorphism in G is uniquely described as ϕ_k. Consider that $\zeta_6 = \alpha_1^3 \frac{-1}{2} + \frac{1}{2}$ we will use this to compute how some ϕ_k acts on α_1 and ζ_6, from their its action

$\phi_k(\alpha_1) = \alpha_k$

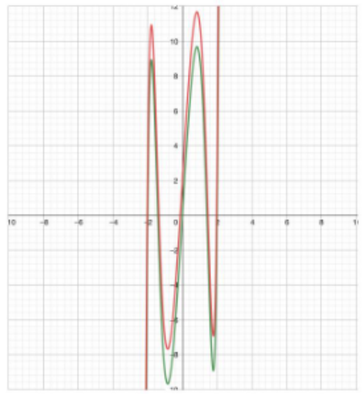

Figure 1: The reducible septic $x^7 - 4x^5 - 4x^3 + 16x$ in green and the irreducible septic $x^7 - 4x^5 - 4x^3 + 16x + 2$ in red, both of which have exactly 5 real roots.

5 Question 5

Theorem 5.1. *There exists a polynomial of degree 7 with Galois group S_7.*

Proof. Suppose we have an irreducible polynomial of degree 7 with 5 real roots $\alpha_1, \ldots, \alpha_5$ and two complex roots β_6, β_7. Let K be the splitting extension of this polynomial over $\mathbb{Q}$ and let G be the Galois group of this extension.

Considering the real roots as the first 5, we have that the permutations that fix these roots are the identity and (67), so if (67) is not in G then the only element that fixes the first 5 roots is the identity. By the Galois correspondence, this would imply that $\mathbb{Q}[\alpha_1, \ldots, \alpha_5] = K$, but this cannot hold as $\mathbb{Q}[\alpha_1, \ldots, \alpha_5]$ is a subset of the real numbers whereas $\beta_6, \beta_7 \notin \mathbb{R}$. We thus have that the transposition (67) is in G.

As the polynomial is irreducible the Galois group must act transitively on the roots, so the orbit of any point $1 \leq k \leq 7$ is the entire set. By the orbit-stabiliser theorem, the size of G is equal to the size of the orbit, which is 7, times the size of the stabiliser, so 7 divides the order of the group. As 7 is prime this implies that there is an element of G of order 7, which must be a 7-cycle. As we have both a transposition and a 7-cycle we thus have that the Galois group must be all of S_7. Therefore, it remains to show that we can find an irreducible polynomial of degree 7 with 5 real roots and 2 complex roots.

Consider the polynomial $x^7 - 4x^5 - 4x^3 + 16x$ which also factors as the following over $\mathbb{C}$.

$$x^7 - 4x^5 - 4x^3 + 16x = x(x-2)(x+2)(x-\sqrt{2})(x+\sqrt{2})(x-i\sqrt{2})(x+i\sqrt{2})$$

This polynomial thus has 5 real roots and 2 imaginary roots, but is clearly reducible over $\mathbb{Q}$. To solve this instead consider the polynomial given by shifting up by 2, so the polynomial

$x^7 - 4x^5 - 2x^3 + 8x + 2$. By applying Eisenstein's criterion for the prime 2 we can see that this is irreducible. We can also check graphically that this still has 5 real roots as in Figure 1, so its Galois group is S_7.

Therefore, we find that there exists a polynomial of degree 7 with Galois group S_7. $\square$