Homework 7 Solutions

Enrique Treviño

Most exercises are from the Judson textbook.

1. Compute each of the following Galois groups. Which of these field extensions are normal field extensions? If the extension is not normal, find a normal extension of $\mathbb{Q}$ in which the extension field is contained.

   (a) $G(\mathbb{Q}(\sqrt{30})/\mathbb{Q})$

   (b) $G(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q})$

   (c) $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$

   Solution 1.

   (a) It is a normal extension, since it's the splitting field of $x^2 - 30$. Because the degree is 2, the Galois group is isomorphic to $\mathbb{Z}_2$.

   (b) The Galois group is It is not a normal extension, because the polynomial $x^4 - 5$ has a couple of roots in $\mathbb{Q}(\sqrt[4]{5})$, but not all of them. Namely, it doesn't include, $\sqrt[4]{5}i$. A normal extension that contains this field extension is $\mathbb{Q}(\sqrt[4]{5}, i)$.

   (c) The Galois group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ because you can send $\sqrt{2}$ to $\sqrt{2}$ or $-\sqrt{2}$. Similarly for the $\sqrt{3}, \sqrt{5}$. You can think of $(a, b, c) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ as representing $\sqrt{2} \to (-1)^a\sqrt{2}$, $\sqrt{3} \to (-1)^b\sqrt{3}$, $\sqrt{5} \to (-1)^c\sqrt{5}$. It is a normal extension.

2. Determine the Galois groups of each of the following polynomials in $\mathbb{Q}[x]$; hence, determine the solvability by radicals of each of the polynomials.

   (a) $x^5 - 12x^2 + 2$

   (b) $x^5 - 4x^4 + 2x + 2$

   Solution 2.

   (a) It is irreducible by Eisenstein with $p = 2$. Therefore, the Galois group G satisfies $5||G|$ and that the roots are all irrational. We also know $G \leq S_5$. Now, the roots of the derivative are 0 and $\sqrt[3]{24/5}$, therefore there are at most 3 real roots. Using the intermediate value theorem we can confirm there are roots in the following intervals: (-1,0), (0,1), (2,3). None of those contain 0 or $\sqrt[3]{24/5}$, therefore the polynomial is separable. We also know it has exactly 3 roots, therefore it has 2 complex roots. Therefore conjugation is a valid automorphism of order 2. Since we have an element of order 5 (Cauchy's theorem) and an element of order 2, by a Lemma proved in class, $G \cong S_5$. Not solvable by radicals.

   (b) Irreducible by Eisenstein with $p = 2$, so $5||G|$ and all roots are irrational. Let $f(x) = x^5 - 4x^4 + 2x + 2$. $f'(x) = 5x^4 - 16x^3 + 2, f''(x) = 20x^3 - 48x^2$. The second derivative has roots at 0 (multiplicity 2) and at 12/5. One can hence verify $f''(x) \leq 0$ for $x < 12/5$ and $f''(x) > 0$ for $x > 12/5$. Therefore, $f'(x)$ is decreasing on $x < 12/5$ and increasing afterwards. That means $f'(x)$ has at most two real roots. This means $f(x)$ has at most 3 real roots. Note that $f(-1) < 0, f(0) > 0, f(1) > 0, f(2) < 0, f(3.5) < 0, f(4) > 0$. Therefore, there are real roots of f on the intervals $(-1, 0), (1, 2), (3.5, 4)$. Therefore, it has exactly 3 real roots. We also know they don't math the roots of $f'(x)$ because the roots of $f'(x)$ are in $(0, 1) \cup (2, 3.5)$. By the same reasoning as above, the Galois group is therefore S_5. Not solvable by radicals.

3. Determine the Galois groups of each of the following polynomials in $\mathbb{Q}[x]$; hence, determine the solvability by radicals of each of the polynomials.

   (a) $x^3 - 5$

   (b) $x^4 - x^2 - 6$

   Solution 3.

   (a) The roots are $\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2$, where $\omega = e^{2\pi i/3}$. Since $\sqrt[3]{5}$ is not rational, then the cubic is irreducible, therefore $|G|$ is a multiple of 3. It can be S_3 or $\mathbb{Z}_3$. But it has two complex roots, so it has a transposition, therefore $G \cong S_3$. It is solvable by radicals.

   (b) We can solve $y^2 - y - 6 = 0$, which yields

   $$y = \frac{1 \pm \sqrt{25}}{2} = 3, -2.$$

   Therefore, the roots are $\sqrt{3}, -\sqrt{3}, \sqrt{2}i, -\sqrt{2}i$. Note that $\phi(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$ since $3 = \phi(3) = \phi(\sqrt{3})^2$. Similarly for $\sqrt{2}i$. Therefore the Galois group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Determine the Galois groups of each of the following polynomials in $\mathbb{Q}[x]$; hence, determine the solvability by radicals of each of the polynomials.

   (a) $x^5 + 1$

   (b) $(x^2 - 2)(x^2 + 2)$

   (c) $x^8 - 1$

   Solution 4.

   (a)

   (b)

   (c)

5. Prove that the Galois group of an irreducible quadratic polynomial is isomorphic to $\mathbb{Z}_2$.

   Solution 5. Since the polynomial is irreducible, the roots live outside of F. Since it's quadratic, there are exactly two roots and they are conjugate of each other. Therefore, the field extension is of degree 2, so the Galois group has 2 elements, so it's isomorphic to $\mathbb{Z}_2$.

6. Prove that the Galois group of an irreducible cubic polynomial is isomorphic to S_3 or $\mathbb{Z}_3$.

   Solution 6. Let G be the Galois group. Since the polynomial is cubic and irreducible, the field extension has degree n with $1 < n \leq 6$. Since the degree must divide 6, then the degree is 2, 3 or 6. If it has degree 3, then G is isomorphic to $\mathbb{Z}_3$. If it has degree 6, then G could be S_3 or $\mathbb{Z}_6$ (the only two groups of order 6). To be $\mathbb{Z}_6$, G would need to have an element of order 6, but it cannot have elements of order greater than 3. Therefore, it must be S_3. Finally, we need to show $n \neq 2$. For $n = 2$, we would need the degree of the field extension to be 2. This means, one of the roots is a root of a quadratic, but then the cubic would not be irreducible. Contradiction!

   Alternatively, one can say that $G \leq S_3$. The subgroups of S_3 are $\mathbb{Z}_3, \mathbb{Z}_2$, and $\{1\}$. Since the polynomial is irreducible, it cannot be $\{1\}$. Since the polynomial is cubic, it cannot be divisible by a quadratic, so $G \neq \mathbb{Z}_2$.

7. Let G be the Galois group of a polynomial of degree n. Prove that $|G|$ divides $n!$.

   Solution 7. This is because G can be associated with a subgroup of S_n. Therefore $|G||n!$.

8. Construct a polynomial $f(x)$ in $\mathbb{Q}[x]$ of degree 7 that is not solvable by radicals.

Solution 8.

9. Let $\sigma \in \text{Aut}(\mathbb{R})$. If a is a positive real number, show that $\sigma(a) > 0$.

   Solution 9. Let $a > 0$. Since $a > 0$, then $\sqrt{a} \in \mathbb{R}$. But then

   $$\sigma(a) = \sigma(\sqrt{a} \cdot \sqrt{a}) = \big(\sigma(\sqrt{a})\big)^2 .$$

   Therefore $\sigma(a) \geq 0$. Suppose $\sigma(a) = 0$, then $\sigma(2a) = 0$, but that means σ is not 1-1. Therefore $\sigma(a) \neq 0$. We can conclude $\sigma(a) > 0$.

10. Determine all of the subfields of $\mathbb{Q}(\sqrt[4]{3}, i)$.

    Solution 10. Following the example in the book, we see the subfields must be

    $$\mathbb{Q}(\sqrt[4]{3}, i), \mathbb{Q}(\sqrt[4]{3}), \mathbb{Q}(\sqrt[4]{3}i), \mathbb{Q}(\sqrt{3}, i), \mathbb{Q}((1+i)\sqrt[4]{3}), \mathbb{Q}((1-i)\sqrt[4]{3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{3}i), \mathbb{Q}.$$