Solution 23

Solvability by Radicals. Recap.

1. Prove that the groups S_2, S_3 and S_4 are solvable.

   Solution: The group S_2 is commutative, hence solvable by definition, because we can consider the chain of normal subgroups $1 \lhd S_2$.

   The group S_3 contains the normal subgroup A_3 of index 2. Hence the quotient group S_3/A_3 has cardinality 2 so that it is cyclic and hence abelian. Since A_3 is abelian, too (it is cyclic of cardinality 3), S_3 is solvable by considering the chain of normal subgroups $1 \lhd A_3 \lhd S_3$.

   The group S_4 contains the normal subgroup A_4 of index 2, so that S_4/A_4 is commutative. In A_4, which has $4!/2 = 12$ elements, there is a subgroup of 4 elements $V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,2)(3\,4)\}$. We claim that V_4 is isomorphic to the Klein four-group. Its elements are indeed of order 2, so they coincide with their inverses. Moreover, the product of two non-trivial elements in V_4 coincides with the remaining non-trivial element, proving that the claim (i.e., $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Since V_4 contains all permutations of cyclic type $1+1+1+1$ and $2+2$, it is a normal subgroup of S_4 and hence of A_4. Moreover, A_4/V_4 has three elements, so it is an abelian group. Finally, V_4 is abelian since it is isomorphic to the Klein four-group; hence S_4 is solvable via $1 \lhd V_4 \lhd A_4 \lhd S_4$.

2. Let k be a field and $n = 2d$ a positive even integer. Let $f = \sum_{j=0}^{n} a_j X^j \in k[X]$ be a monic polynomial of degree n without multiple roots and suppose that f has no root in k. Suppose moreover that f is palindromic, that is, $a_j = a_{n-j}$ for each $j \in \{0, \dots, d\}$. Let E be the splitting field of f.

   (a) Prove that $x \mapsto \frac{1}{x}$ is a well-defined bijection on the set of roots of f.

   (b) Deduce that $\#\operatorname{Gal}(E/k)$ divides $2^d d!$.

   Solution:

   (a) Let $x \in E$ be a root of f, so $0 = f(x) = \sum_{j=0}^{n} a_j x^j$. We know that $x \neq 0$ because f has no root in k, so x admits an inverse $1/x$ in E. We deduce that

$$f(1/x) = \sum_{j=0}^{n} a_j \frac{1}{x^j} = \frac{1}{x^n} \sum_{j=0}^{n} a_j x^{n-j} \overset{a_j = a_{n-j}}{=} \frac{1}{x^n} \sum_{j=0}^{n} a_{n-j} x^{n-j} = \frac{1}{x^n} f(x) = 0,$$

thus $x \mapsto \frac{1}{x}$ is a well-defined map on the set S of roots of f. Since this map is its own inverse, it is a bijection.

(b) By assumption, f has $n = 2d$ distinct roots. Since the map $x \mapsto 1/x$ is an involution with fixed points $\pm 1 \in k$ and those are not roots of f by assumption, the set S is the union of d orbits of 2 elements under the action of $\mathbb{Z}/2\mathbb{Z}$ on it generated by $x \mapsto \frac{1}{x}$. This means that $S = \{x_1^{\pm 1}, \dots, x_d^{\pm 1}\}$ for some distinct $x_1, \dots, x_d$ in $\overline{k}$ with $x_i \neq \frac{1}{x_j}$ for each i and j.

The Galois group $\mathrm{Gal}(E/k)$ embeds into S_{2d} via its action on S, explicitly so by setting $x_{i+d} := x_i^{-1}$ for $i \in \{1, \dots, d\}$ and mapping $\sigma \in \mathrm{Gal}(E/k)$ to $\tau_\sigma \in S_{2d}$ determined by $\sigma(x_i) = x_{\tau_\sigma(i)}$. Moreover, for $\sigma \in \mathrm{Gal}(E/k)$ we know that $\sigma(x_i^{-1}) = (\sigma(x_i))^{-1}$. So for each $i \in \{1, \dots, d\}$ there exists a unique $j \in \{1, \dots, d\}$ with $\sigma(\{x_i, x_i^{-1}\}) = \{x_j, x_j^{-1}\}$.

In terms of the embedding into S_{2d}, this translates to saying that the image of $\mathrm{Gal}(E/k)$ in S_{2d} lies in the subset

$$W_d := \{\tau \in S_{2d} : \exists \tau' \in S_d : \forall i \in \{1, \dots, d\}, \tau(\{i, i+d\}) = \{\tau'(i), \tau'(i) + d\}\},$$

that is, the subsets of permutations of $\{1, \dots, 2d\}$ respecting the partition $\{1, d+1\}, \{2, d+2\}, \dots, \{d, 2d\}$. Since this property is stable under composition and inversion, the subset W_d is actually a subgroup of S_{2d}. Hence the image of $\mathrm{Gal}(E/k)$ under its embedding into S_{2d} is a subgroup of W_d, so $\#\,\mathrm{Gal}(E/k)$ divides $\# W_d$. For each $\tau \in W_d$, the associated $\tau' \in S_d$ in the definition of W_d is uniquely determined. On the other hand, for each $\tau' \in S_d$, there are 2^d permutations τ associated τ', because for each $i \in \{1, \dots, d\}$ we have two ways to map $\{i, i+d\}$ onto $\{\tau'(i), \tau'(i) + d\}$. Hence we conclude that

$$\#\,\mathrm{Gal}(E/k) \mid \# W_d = d! \cdot 2^d,$$

as desired.

3. For each of the following polynomials, determine the Galois group of its splitting field:

(a) $X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$ *Hint.* Exercise 2

(b) $X^4 + X + 1 \in \mathbb{F}_2[X]$

(c) $X^5 + \frac{5}{4}X^4 - \frac{5}{21} \in \mathbb{Q}[X]$

Hint. Show that the polynomial has precisely three real roots and deduce that the Galois group contains a transposition and a 5-cycle.

(d) $X^{81} - t \in \mathbb{F}_3(t)[X]$

Solution:

(a) The polynomial $f = X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$ has no root in $\mathbb{Q}$: If it did, it would have a root in $\mathbb{Z}$. Since the product of the roots is 1 (the constant coefficient), this root would have to be a unit in $\mathbb{Z}$, i.e. ± 1. But $f(\pm 1) \neq 0$. We compute its roots in $\mathbb{C}$ by using Exercise 2(a). If $x \in \mathbb{C}$ is a root of f, then so is x^{-1} because f is palindromic. Since $x \neq \pm 1$, we know that $x^{-1} \neq x$. Hence the roots of f in $\mathbb{C}$ are given by $a_1, a_1^{-1}, a_2, a_2^{-1}$ for some $a_1, a_2 \in \mathbb{C}$. Since $(X - a_j)(X - a_j^{-1}) = X^2 - (a_j + a_j^{-1})X + 1$ for $j = 1, 2$, we can define $\alpha_j := -(a_j + a_j^{-1})$ which lets us write down the decomposition

$$X^4 + 2X^3 + X^2 + 2X + 1 = f = (X^2 + \alpha_1 X + 1)(X^2 + \alpha_2 X + 1).$$

Comparing the coefficients in this equality we obtain the system of equations

$$\begin{cases} \alpha_1 + \alpha_2 = 2 \\ \alpha_1 \alpha_2 + 2 = 1 \end{cases}$$

Hence α_1 and α_2 are the two solutions of the equation $\alpha^2 - 2\alpha - 1 = 0$, so

$$\alpha_{1,2} = 1 \pm \sqrt{1+1} = 1 \pm \sqrt{2}.$$

Therefore, f is irreducible over $\mathbb{Q}$ because its quadratic factors do not lie in $\mathbb{Q}[X]$ and it has no rational roots. The roots of f are precisely the solutions of the two equations $x^2 + (1 \pm \sqrt{2})x + 1 = 0$; hence

$$a_1 = -\frac{1}{2}\left(1 + \sqrt{2} - \sqrt{2\sqrt{2} - 1}\right) \quad \text{and} \quad a_2 = -\frac{1}{2}\left(1 - \sqrt{2} - i\sqrt{2\sqrt{2} + 1}\right).$$

There are four distinct roots (two real and two complex ones) and we can apply Exercise 2(b) which tells us that $|\mathrm{Gal}(E/\mathbb{Q})|$ divides $2^2 \cdot 2! = 8$, where E is the splitting field of f. Since E contains a_1, the splitting field of f contains the field extension $\mathbb{Q}(a_1)$ of $\mathbb{Q}$. This containment is strict because the roots of f are not all real, while $\mathbb{Q}(a_1) \subset \mathbb{R}$. This means that $4 < |\mathrm{Gal}(E/\mathbb{Q})|$. The only remaining possibility is that $|\mathrm{Gal}(E/\mathbb{Q})| = 8$.

By the proof in Exercise 2, this means that $\mathrm{Gal}(E/\mathbb{Q})$, seen as a subgroup of S_4, is precisely the subgroup W_2. Note that W_2 contains the permutations $\sigma = (1234)$ and $\tau = (13)$ because of the relations $\sigma(\{i, i+2\}) = \{\sigma(i), \sigma(i)+2\}$ and $\tau(\{i, i+2\}) = \{\mathrm{id}(i), \mathrm{id}(i) + 2\}$ for $i = 1, 2$. Thus $\mathrm{Gal}(E/\mathbb{Q}) = W_2$ contains the subgroup $< \sigma, \tau >$, which is isomorphic to the dihedral group D_4 of order 8. Hence, by cardinality we have $\mathrm{Gal}(E/\mathbb{Q}) \cong D_4$.

(b) The polynomial $X^4 + X + 1 \in \mathbb{F}_2[X]$ is irreducible in $\mathbb{F}_2[X]$, as we found out in Assignment 15, Exercise 3. Let $x \in \overline{\mathbb{F}_2}$ be a root of f. Then the other roots of f are powers of x, as shown in Exercise 2, Assignment 13, so $E := \mathbb{F}_2(x)$ is the splitting field of f. The same equality can be obtained by noting that $\mathbb{F}_2(x)$ is a finite field of 2^4 elements and thus the splitting field of

$X^{16} - X \in \mathbb{F}_2[X]$. Since it is moreover galois, it must contains all roots of f by Assignment 19, Exercise 3. Hence

$$\mathrm{Gal}(E/\mathbb{F}_2) = \mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) = \mathbb{Z}/4\mathbb{Z}$$

by Assignment 17, Exercise 3.

(c) The polynomial $f = X^5 + \frac{5}{4}X^4 - \frac{5}{21} \in \mathbb{Q}[X]$ is irreducible if and only if the associated primitive polynomial $4 \cdot 21 f = 4 \cdot 21 X^5 + 5 \cdot 21 X^4 - 5 \cdot 4 \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$, which is the case by Eisenstein's Lemma (for $p = 5$).

The derivative of the associated real function $x \mapsto f(x)$ is $f'(x) = 5x^4 + 5x^3$, which is positive for $x < -1$ and $x > 0$, negative for $-1 < x < 0$ and zero on -1 and 0. Hence -1 is a local maximum while 0 is a local minimum. We compute the values of f on those stationary points:

$$\begin{aligned} f(-1) &= -1 + \frac{5}{4} - \frac{5}{21} = \frac{1}{4} - \frac{5}{21} > \frac{1}{4} - \frac{5}{20} = 0 \\ f(0) &= -\frac{5}{21} < 0. \end{aligned}$$

This shows us that f has precisely three real roots: one in $(-\infty, -1)$, one in $(-1, 0)$ and $(0, +\infty)$. We claim that the Galois group $G := \mathrm{Gal}(E/\mathbb{Q})$ contains a transposition and an element of order 5. Since 5 is a prime number, this implies that $G \cong S_5$. We know that f has three real roots α_3, α_4 and α_5; thus the remaining two α_1 and α_2 are complex conjugates. Consider G as a subgroup of S_5. The complex conjugation $\sigma\colon \mathbb{C} \to \mathbb{C}, x \mapsto \bar{x}$ leaves α_3, α_4 and α_5 fixed and interchanges α_1 and α_2. Since $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$ this implies that $\sigma(E) = E$ and that $\sigma|_E \in G < S_5$ is the transposition $(1, 2)$. Since f is irreducible, we know that $\deg f = 5$ divides $|G|$. It follows that G contains a 5-cycle, and we conclude that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$.

(d) Let $u \in \overline{\mathbb{F}_3(t)}$ be a root of $f = X^{81} - t$. Then $u^{81} = t$ and

$$(X - u)^{81} = ((X - u)^3)^{27} = (X^3 - u^3)^{27} = \cdots = X^{81} - u^{81} = X^{81} - t.$$

Hence u is the only root of f in $\overline{\mathbb{F}_3(t)}$ so $E = \mathbb{F}_3(t)(u)$ is the splitting field of f. In particular, f and hence E are not separable, so the extension is not Galois. (Since an $\mathbb{F}_3(t)$-automorphism of $\mathbb{F}_3(t)(u)$ is uniquely determined by the image of u, which in turn needs to be a root of f, the automorphism group $\mathrm{Aut}(E/\mathbb{F}_3(t))$ is in fact trivial.)