Solution 20

Solvability by Radicals. Recapitulation.

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 $V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,2)(3\,4)\}$. Its elements are indeed of order 2, so that they coincide with their inverses, and the product of two non-trivial elements in V_4 coincides with the remaining non-trivial element, proving that it is indeed a subgroup isomorphic to the Klein four-group (i.e., $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). 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 that it is an abelian group. Finally, V_4 is abelian since it is isomorphic to the Klein four-group and this lets us conclude that S_4 is solvable. We have indeed obtained the sequence of subgroups $1 \lhd V_4 \lhd A_4 \lhd S_4$.

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 $E = \mathrm{Sf}(f)$.

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

   (b) Deduce that $\mathrm{Card}(\mathrm{Gal}(E/k))$ divides $2^d d!$

   Solution:

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

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

   so that $x \mapsto \frac{1}{x}$ is a well-defined map $R(f) \longrightarrow R(f)$. 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 (i.e., it coincides with its inverse) whose fixed points are $\pm 1 \in k$ and those cannot be roots of f by assumption, the set $R(f)$ 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 $R(f) = \{x_1, x_1^{-1}, x_2, x_2^{-1}, \dots, x_d, x_d^{-1}\}$ for some $x_1, \dots, x_d$ in $\overline{k}$ distinct and such that $x_i \neq \frac{1}{x_j}$ for each i and j.

The Galois group $\mathrm{Gal}(E/k)$ embeds into S_{2d} via its action on $R(f)$. We write the embedding $\mathrm{Gal}(E/k) \hookrightarrow S_{2d}$ explicitly by defining $x_{i+d} := x_i^{-1}$ for $i \in \{1, \dots, d\}$ and send $\sigma \in \mathrm{Gal}\, E/k$ to $\sigma_0 \in S_{2d}$ such that $\sigma_0(i) = j$ for $i, j \in \{1, \dots, 2d\}$ if and only if $\sigma(x_i) = x_j$. Moreover, for $\sigma \in \mathrm{Gal}(E/k)$ we know that $\sigma(x_i^{-1}) = (\sigma(x_i))^{-1}$, so that for each $i \in \{1, \dots, d\}$ there exists a unique $j \in \{1, \dots, d\}$ such that $\sigma(\{x_i, x_i^{-1}\}) = \{x_j, x_j^{-1}\}$.

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

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

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 that $\mathrm{Card}(\mathrm{Gal}(E/k))$ divides $\mathrm{Card}(W_d)$. For each $\sigma \in W_d$, the $\tau \in S_d$ (permuting the subsets $\{i, i+d\}$) appearing in the definition of W_d is uniquely determined. For each $\tau \in S_d$, there are 2^d permutations σ determining that 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 can conclude that

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

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

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

(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 $\mathbb{Q}$. We compute its roots in $\mathbb{C}$ by using Exercise 1(a). If $x \in \mathbb{C}$ is a root of f, then so is x^{-1}. For $x \neq \pm 1$, we know that $x^{-1} \neq x$. But $f(\pm 1) \neq 0$ because it is an odd integer. Hence the roots of f in $\mathbb{C}$ are given by $a_1, a_1^{-1}, a_2, a_2^{-1}$ for some eventually equal $a_1, a_2 \in \mathbb{C}$. 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 roots of the equation (in α) $\alpha^2 - 2\alpha - 1 = 0$, that is,

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

This implies that the only decomposition of f into monic polynomials. The roots of f are the roots of the two equations $x^2 + (1 \pm \sqrt{2})x + 1 = 0$, that is,

$$R(f) = \{-1 - \sqrt{2} \pm \sqrt{-1 + 2\sqrt{2}}, -1 + \sqrt{2} \pm i\sqrt{1 + 2\sqrt{2}}\}.$$

There are four distinct roots (two real and two non-real ones) and we can apply Exercise 2(b) which tells us that $|\operatorname{Gal}(E/\mathbb{Q})|$ divides $2^2 \cdot 2! = 8$, where $E = \operatorname{Sf}(f)$. Moreover, we see that

$$E = \mathbb{Q}(R(f)) \supset \mathbb{Q}(i, \sqrt{-1 + 2\sqrt{2}})$$

and since $i \notin \mathbb{Q}(\sqrt{-1 + 2\sqrt{2}})$ we know that

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(i, \sqrt{-1 + 2\sqrt{2}})] \cdot 2 \cdot [\mathbb{Q}(\sqrt{-1 + 2\sqrt{2}}) : \mathbb{Q}].$$

We claim that $\sqrt{-1 + 2\sqrt{2}}$ has degree 4 over $\mathbb{Q}$, so that by the above formula $8 | [E : \mathbb{Q}]$ and since $[E : \mathbb{Q}] | 8$ as well, we deduce that $[E : \mathbb{Q}] = 8$.

In order to prove the claim we just used, notice that $\sqrt{2} \in \mathbb{Q}(\sqrt{-1 + 2\sqrt{2}})$, so that

$$[\mathbb{Q}(\sqrt{-1 + 2\sqrt{2}}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-1 + 2\sqrt{2}}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

because $-1 + 2\sqrt{2}$ is not a square in $\mathbb{Q}(\sqrt{2})$ (which can be proved by noticing that its norm over $\mathbb{Q}$ is $N(-1 + 2\sqrt{2}) = (-1 + 2\sqrt{2})(-1 - 2\sqrt{2}) = 1 - 8 = 7$ which is not a square, see Assignment 12, Exercise 7; alternatively, one can prove directly that the equality $(a+\sqrt{2}b)^2 = -1+2\sqrt{2}$ cannot hold for $a,b\in\mathbb{Q}$).

By the proof given to Exercise 2, this means that $\mathrm{Gal}(E/\mathbb{Q})$, seen as a subgroup of S_4, is precisely the subgroup W_2 of permutations respecting the partition $\{1,2,3,4\} = \{1,3\}\cup\{2,4\}$. This is given by

$$W_2 = \{\mathrm{id}, (1\,3)(2\,4), (1\,2)(3\,4), (1\,4)(2\,3), (1\,2\,3\,4), (1\,4\,3\,2), (1\,3), (2\,4)\},$$

which by numbering the vertices of a square counterclockwise from 1 to 4 can be seen to be isomorphic to D_4, the dihedral group on 4 elements (see Assignment 8, Exercise 7).

(b) 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 $4\cdot 21 f = 4\cdot 21X^5 + 5\cdot 21X^4 - 5\cdot 4 \in \mathbb{Z}[X]$ 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 three real roots: one in $(-\infty,-1)$, one in $(-1,0)$ and $(0,+\infty)$. We are therefore in position of applying Theorem II.20 and conclude that $\mathrm{Gal}(\mathrm{Sf}(f)/\mathbb{Q}) \cong S_5$.

(c) 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 that $\mathbb{F}_2(x) = \mathrm{Sf}(f)$. The same equality can be obtained by noticing that $\mathbb{F}_2(x)$ is a finite field of 2^4 elements so that it is the splitting field of $X^{16}-X\in\mathbb{F}_2[X]$ as seen in class in the characterization of finite fields, so that being normal it must contains all roots of f by Assignment 19, Exercise 4. Hence

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

by Corollary II.19 (Week 16).

(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 that $\mathrm{Sf}(f) = \mathbb{F}_3(t)(u)$ (in particular, the polynomial and hence its splitting field are not separable). Since a $\mathbb{F}_3(t)$-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, we conclude that $|\,\mathrm{Gal}(\mathrm{Sf}(f)/\mathbb{F}_3(t))| = \{\mathrm{id}\}$.

4. Let k be a field.

   (a) Prove that k is an extension of a field k_0, called *prime field*, given by $k_0 = \mathbb{F}_p$ if $\mathrm{char}(k) = p > 0$ and $k_0 = \mathbb{Q}$ if $\mathrm{char}(k) = 0$.

   (b) Prove that any field homomorphism restricts to the identity on the prime fields.

Solution:

   (a) The characteristic of the field k can be defined as the non-negative generator of the kernel of the unique ring homomorphism $\varphi : \mathbb{Z} \longrightarrow k$.

   If $\mathrm{char}(k) > 0$, then it is a prime number p and by the first homomorphism theorem φ induces an injection $\varphi : \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \longrightarrow k$ and k_0 coincides with the additive subgroup of k generated by 1_k.

   If $\mathrm{char}(k) = 0$, then φ is an injective map and since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, the inclusion φ extends to an inclusion of $\mathbb{Q}$ insider k.

   (b) If $\theta : k \longrightarrow \ell$ is a field homomorphism, then the composition of ring homomorphisms $\mathbb{Z} \xrightarrow{\varphi_k} k \xrightarrow{\theta} \ell$ must coincide with the unique homomorphism $\varphi_\ell : \mathbb{Z} \longrightarrow \ell$. Moreover θ is necessarily injective (because the image of $x \in k^\times = k \smallsetminus \{0\}$ has inverse $\theta(x^{-1})$, hence it cannot be zero). Hence

$$\ker(\varphi_\ell) = \{m \in \mathbb{Z} : \varphi_k(m) \in \ker(\theta)\} = \{m \in \mathbb{Z} : \varphi_k(m) = 0\} = \ker(\varphi_k)$$

   so that k and ℓ have the same characteristic.

   If the two fields have characteristic $p > 0$, then they contain the prime field $\mathbb{F}_p$ as images of φ_k and φ_ℓ and those prime fields are mapped "identically" because $\varphi_\ell = \theta\varphi_k$.

   If the two fields have characteristic 0, then θ maps each integer $m \cdot 1_k$ to $m \cdot 1_\ell$. The inclusion $\varphi_k : \mathbb{Z} \longrightarrow k$ extends to an inclusion $\overline{\varphi_k} : \mathbb{Q} \longrightarrow k$ by sending $m/n \mapsto \varphi_k(m)\varphi_k(n)^{-1}$ for $m, n \in \mathbb{Z}$ with $n \neq 0$. Similarly for φ_ℓ extending to $\overline{\varphi_\ell} : \mathbb{Q} \longrightarrow \ell$. In order to conclude, it is enough to prove that $\overline{\varphi_\ell} = \theta \circ \overline{\varphi_k}$, so that θ is the "identity" on the prime fields $\mathbb{Q}$ seen as images of $\overline{\varphi_k}$ and $\overline{\varphi_\ell}$. This is done by using the fact that $\varphi_\ell = \theta\varphi_k$: for all $m, n \in \mathbb{Z}$ with $n \neq 0$,

$$\begin{aligned}(\theta \circ \overline{\varphi_k})(m/n) &= \theta(\overline{\varphi_\ell}(m/n)) = \theta(\varphi_\ell(m)\varphi_\ell(n)^{-1}) \\ &= (\theta\varphi_\ell)(m) \cdot (\theta\varphi_\ell)(n)^{-1} = \varphi_\ell(m)\varphi_\ell(n)^{-1} = \overline{\varphi_\ell}(m/n).\end{aligned}$$

5. We say that a field k is *perfect* if every algebraic field extension of k is separable.

   (a) Prove that a field k is perfect if and only if every polynomial $f \in k[X]$ is separable.

   (b) Show that fields of characteristic zero are perfect.

(c) Suppose that $\mathrm{char}(k) = p > 0$. Prove that k is perfect if and only if the Frobenius homomorphism $\varphi : k \longrightarrow k$ sending $x \mapsto x^p$ is surjective.

(d) Deduce that finite fields are perfect.

Solution:

(a) Let k be a perfect field and $f_0 \in k[X]$ an irreducible polynomial. Let $x \in \overline{k}$ be a root of f_0. Then $k(x)$ is a field extension of k and by assumption it is separable. Hence x is a separable element, meaning that $\mathrm{irr}(x; k) = f_0$ is a separable polynomial. Now let $f \in k[X]$ be an arbitrary polynomial. Every irreducible factor of f is separable by arbitrarity of f_0 in the initial argument, which implies that f is separable by definition.

Conversely, assume that every polynomial in $k[X]$ is separable and let ℓ/k be an algebraic field extension. For every $\alpha \in \ell$, the minimal polynomial $\mathrm{irr}(\alpha, k)$ exists because ℓ/k is algebraic; it is a separable polynomial by assumption, meaning that α is separable. Hence ℓ/k is a separable field extension.

(b) By Corollary II.10 (Week 16), we know that every irreducible polynomial in $k[X]$ has no multiple root. This means that every irreducible polynomial in $k[X]$ is separable. Then, for every $f \in k[X]$, each irreducible factor of f is separable, so that f is separable as well.

(c) Suppose that k is a perfect field and let us prove that each $y \in k$ has a p-th root in k. Since k is perfect, the polynomial $f = X^p - y \in k[X]$ must be separable. For $x \in \overline{k}$ a root of f, we have a factorization

$$f = (X - x)^p.$$

Hence x is the only root of f in $\overline{k}$ and a factor of f in $k[X]$ has no multiple roots in $\overline{k}$ if and only if it is a linear factor. As each irreducible factor of f in $k[X]$ must have no multiple root, the only possibility is that f splits completely in $k[X]$. In particular, $x \in k$.

Conversely, assume that the Frobenius map $\varphi : k \longrightarrow k$ is surjective and let us prove that every irreducible polynomial f in $k[X]$ is separable, which is enough to prove that k is perfect as noticed in part (a). Suppose that $f \in k[X]$ is irreducible and has multiple roots. Then $\gcd(f, f') \neq 1$ by Lemma II.9 (Week 16). Since f is irreducible, $\gcd(f, f')$ must be divisible by f. But $\gcd(f, f')$ divides f' of degree smaller than f, so that the only possibility is that $\gcd(f, f') = 0$, which can hold only if $f' = 0$. This is the case if and only if $f \in k[X^p]$, because the coefficients of degree not divisible by p do not vanish when we take the formal derivative of f. As φ is surjective, every coefficient of f is a p-th power of an element in k, so that we can write

$$f = \sum_{k=0}^{n} (b_k)^p x^{pk} = \left(\sum_{k=0}^{n} b_k x^k \right)^p,$$

a proper factorization of f in $k[X]$, which is a contradiction to the assumption that f is irreducible. Hence f has no multiple roots.

(d) Let $k = \mathbb{F}_{p^n}$ be a finite field of characteristic p. The Frobenius homomorphism φ is a $\mathbb{F}_p$-field automorphism of $\mathbb{F}_{p^n}$. It is injective because $\ker(\varphi) = 0$ since fields are integral domains. By Assignment 15, Exercise 1, φ is a $\mathbb{F}_p$-linear map between vector spaces of same finite dimension, which implies that it is a bijection and in particular a surjective map. By part (c), $k[X]$ is perfect.

6. Let k be a finite field and consider a finite field extension $k(\alpha, \beta)/k$. Suppose that $k(\alpha) \cap k(\beta) = k$. Prove that $k(\alpha, \beta) = k(\alpha + \beta)$.

Solution: Let $q = \mathrm{card}(k)$ be a power of a prime p. We write $k = \mathbb{F}_q$ and we know that $\mathrm{char}(k) = p$. Fix an algebraic closure $\overline{k}$. Then, as seen in Algebra I, for each power q^t of q there exists a unique subfield of $\overline{k}$ containing q^t elements, it consists of those elements $\alpha \in \overline{k}$ such that $\alpha^{q^t} = \alpha$. The proof of Assignment 13, Exercise 1(b) generalizes to q and tells us that $\mathbb{F}_{q^s} \subset \mathbb{F}_{q^t}$ if and only if $s|t$.

Let $n, m \in \mathbb{N}$ be such that $k(\alpha) = \mathbb{F}_{q^n}$ and $k(\beta) = \mathbb{F}_{q^m}$. Here n is the minimal positive integer h such that $\alpha^{q^h} = \alpha$, because otherwise $k(\alpha)$ would be contained in a strictly smaller subfield of $\mathbb{F}_{q^n}$. Since $k = k(\alpha) \cap k(\beta)$ is the smallest subfield of $\overline{k}$ contained in both $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^m}$, we deduce that $\gcd(m, n) = 1$. Then p divides either m or n, without loss of generality, assume that $p \nmid n$. Moreover, $k(\alpha, \beta)$ is the smallest subfield of $\overline{k}$ containing both $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^m}$, so that $k(\alpha, \beta) = \mathbb{F}_{q^{mn}}$.

We write $k(\alpha + \beta) = \mathbb{F}_{q^t}$. This means that

$$\alpha^{q^t} + \beta^{q^t} = (\alpha + \beta)^{q^t} = \alpha + \beta,$$

implying that

$$\alpha^{q^t} - \alpha = -(\beta^{q^t} - \beta) \in k(\alpha) \cap k(\beta) = k.$$

Write $\alpha^{q^t} = \alpha + \lambda$ for $\lambda \in \mathbb{F}_q$ and repeatedly raising to the q^t-th power, we deduce inductively that

$$\alpha^{q^{tp}} = \alpha + p\lambda = \alpha.$$

This means that $n|tp$ and since $p \nmid n$ we obtain that $n|t$, so that $k(\alpha + \beta) = \mathbb{F}_{q^t}$ contains $k(\alpha)$, so that $\alpha \in k(\alpha + \beta)$. This implies that $\beta = (\alpha + \beta) - \alpha \in k(\alpha + \beta)$, as well. Hence $k(\alpha, \beta) \subset k(\alpha + \beta)$. The other inclusion is obvious and we can conclude that $k(\alpha, \beta) = k(\alpha + \beta)$.