1 Extra exercises Galois theory

Exercise 1.1. Let $L = \mathbb{Q}(X)$.

1. Let $\sigma \in \mathrm{Aut}(L)$ be the unique automorphism such that $\sigma(X) = X + 1$. Show that the group G generated by σ is infinite and that $L^G = \mathbb{Q}$. Prove that $L^H = \mathbb{Q}$ for every non-trivial subgroup of G.

2. Let $\sigma_i \in \mathrm{Aut}(L)$ for $i = 1, 2, 3$ be such that

$$\sigma_1(X) = -X, \quad \sigma_2(X) = \frac{1}{X}, \quad \sigma_3(X) = 1 - X.$$

   Determine the invariant subfields $L^{<\sigma_i>}$ for $i = 1, 2, 3$.

3. Let σ_i be as above. Show that $\rho = \sigma_2\sigma_3$ has order 3 in $\mathrm{Aut}(L)$ and determine L^ρ.

4. Show that the group G generated by σ_2, σ_3 has order 6 and is siomorphic to S_3. Determine $f \in \mathbb{Q}(X)$ such that $L^G = \mathbb{Q}(f)$.

Exercise 1.2. Let K be a field of characteristic $p > 0$ and $L = K(X)$. Let $\sigma \in \mathrm{Gal}(L/K)$ be defined by $\sigma(X) = X + 1$. Show that σ has finite order and determine an element $f \in L$ such that $L^G = K(f)$.

Exercise 1.3. Let Kbe a field whose characteristic is $\neq 2$.

1. Show that to every quadratic extension L/K there exists an element $m \in K^*$ such that $L = K(\sqrt{m})$.

2. Show that $K(\sqrt{m}) = K(\sqrt{m'})$ if and only if m/m' is a square in K^*.

Show that there exists a quadratic extension of $\mathbb{F}_2$ which is *not* of the form $\mathbb{F}_2(\sqrt{m})$ with $m \in \mathbb{F}_2$.

Exercise 1.4. Suppose that $K \subset K(\alpha)$ is a Galois extension with group G. Prove that the minmal polynomial f of α over K is given by $f(X) = \prod_{\sigma \in G}(X - \sigma(\alpha))$.

Exercise 1.5. For each of the following polynomials in $\mathbb{Q}[X]$ determine the splitting field $L/\mathbb{Q}$, its Galoisgroup, and all intermediate fields.

$$X^4 + 20, \quad X^4 - 4X^2 + 5, \quad X^4 - 5X^2 - 5.$$

Exercise 1.6. For each of the following polynomials in $\mathbb{Q}[X]$ determine the splitting field $L/\mathbb{Q}$, its Galoisgroup, and all intermediate fields.

$$X^4 - 4X^2 + 2, \quad X^4 - 2X^2 + 4, \quad X^4 - 2X^2 + 2.$$

Exercise 1.7. Show that $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ with $\zeta = e^{2\pi i/11}$ has exactly two non-trivial intermediate fields. Write each intermediate field as a simple extension of $\mathbb{Q}$.

Exercise 1.8. Let $f = X^4 + 1 \in \mathbb{Q}[X]$.

1. Prove that f is irreducible over $\mathbb{Q}$.
2. Let α be a zero of f in $\mathbb{C}$ (no need to determine it). Show that the full set of zeros is given by $\{\alpha, -\alpha, i\alpha, -i\alpha\}$.
3. Show that $\alpha^2 = \pm i$. Show that $L = \mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$.
4. What is the degree of L over $\mathbb{Q}$? And the order of $G := \mathrm{Gal}(L/\mathbb{Q})$? List all groups of this order.
5. Why does $\sigma(\alpha) = -\alpha$ define an element of G? Same question for $\tau(\alpha) = \alpha^3$.
6. Show that $\sigma^2 = \tau^2 = \mathrm{id}$ and $\sigma\tau = \tau\sigma$. Determine G.
7. Determine all subgroups of G and the corresponding intermediate fields in $L/\mathbb{Q}$.
8. Write each of the intermediate fields as simple extension of $\mathbb{Q}$.
9. Show that $L = \mathbb{Q}(i, \sqrt{2})$ and express α as $\mathbb{Q}$-linear combination of $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

Exercise 1.9. Let $f = X^3 - 5 \in \mathbb{Q}[X]$.

1. Prove that f is irreducible in $\mathbb{Q}[X]$.
2. Determine the zeros of f in $\mathbb{C}$.
3. Let L be the splitting field of f over $\mathbb{Q}$. Show that $[L : \mathbb{Q}] = 6$.
4. Show that the $G := \mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to S_3. (Hint: G is a subgroup of S_3, why?)
5. Let $\omega = e^{2\pi i/3}$. Show that there exist $\sigma, \tau \in G$ such that $\sigma(\omega) = \omega^2$, $\sigma(\sqrt[3]{5}) = \sqrt[3]{5}$ and $\tau(\omega)\omega$, $\tau(\sqrt[3]{5}) = \omega\sqrt[3]{5}$.
6. Prove that $\sigma^2 = \tau^3 = \mathrm{id}$ and $\sigma\tau\sigma = \tau$. This gives another proof that $G = S_3$.
7. Determine all non-trivial subgroups of S_3 (there are 4 of them) and the corresponding intermediate fields.
8. Why is L normal over all these intermediate fields? Which of the intermediate fields is normal over $\mathbb{Q}$?

9. Which subgroups of S_3 are normal subgroups?

Exercise 1.10. Let $f = X^4 - 5X^2 + 6$.

1. Verify that $f = f_1 f_2$ with $f_1 = X^2 - 2, f_2 = X^2 - 3$.
2. Determine the splitting field L of f over $\mathbb{Q}$. What is the degree $[L : \mathbb{Q}]$?
3. Determine the elements of $G := \mathrm{Gal}(L/\mathbb{Q})$ and their relations. Prove that $G = V_4$, Klein's fourgroup.
4. Determine all subgroups of G and their corresponding intermediate fields.
5. Determine a primitive element γ for L (i.e. $L = \mathbb{Q}(\gamma)$).
6. Determine the minimal polynomial of γ over $\mathbb{Q}$. (in particular, L is also splitting field of this polynomial).

Exercise 1.11. Let $f = X^3 - 2tX + t$ over $K := \mathbb{C}(t)$.

1. Prove that f is irreducible over K.
2. Let α be a zero of f in a splitting field. Prove that $K(\alpha)$ is *not* the splitting field of f over K.
3. Let δ be a zero of $X^2 + 3\alpha^2 - 8t \in K(\alpha)[X]$. Prove that $L = K(\alpha, \delta)$.
4. Prove that $\mathrm{Gal}(L/K) = S_3$.
5. How many non-trivial intermediate fields are there between K and L? Prove that there is a unique intermediate field E/K of degree 2. Is E/K a Galois extension?
6. Determine a polynomial $g \in K[X]$ such that E/K is splitting field of g.