7. Galois Work-Out.

1. Let E be the splitting field of $f(X) = X^4 - 4X^2 + 1$ over $K = \mathbf{Q}$.
(i) Describe the Galois group of E/K.
(ii) Find the intermediate fields $E \supset F \supset K$.

2. Repeat Exercise 1 with $f(X) = X^4 - 4X^2 - 1$.

3. For any $c \in \mathbf{Z}$, let G_c be the Galois group of $f_c(X) = X^4 - 4X^2 - c$.
(i) Find an integer c such that G_c is isomorphic to the dihedral group of order 8.
(ii) Show that G_c is never isomorphic to the quaternion group.

4. For $K = \mathbf{Q}$, consider the polynomial $f(X) = X^3 + X + 1 \in K[X]$.
(i) Show that $f(X)$ is irreducible in $K[X]$.
(ii) Find the splitting field E of $f(X)$ over K, and describe $\mathrm{Aut}_K(E)$.

5. If $K = \mathbf{F}_2(t)$ is the rational function field, consider the polynomial $f(X) = X^4 + tX^2 + 1$.
(i) Show that $f(X)$ is irreducible in $K[X]$.
(ii) Find the splitting field E of $f(X)$ over K, and describe $\mathrm{Aut}_K(E)$.

6. If $K = \mathbf{F}_2(t, u)$ is the rational function field, consider the extension $E = K(\sqrt{t}, \sqrt{u})$.
(i) Show that there is no $\theta \in E$ such that $K(\theta) = E$.
(ii) Show that there are infinitely many intermediate fields $E \supset F \supset K$.

Les petits riens.

- Find the sum of all cubes in $\mathbf{F}_{73}$. Explain.
- Describe the subfield lattice of $\mathbf{F}_q$ for $q = 2^{75}$.
- Find a quadratic polynomial having the same splitting field as $X^{24} - 1$ over $\mathbf{F}_5$.
- Describe the set of polynomials $f(X) \in F_q[X]$ with $f(a) = 0$ for all $a \in \mathbf{F}_q$.
- Show: if F/K is algebraic, every $f(X) \in F[X]$ divides some $g(X) \in K[X]$.
- Find the Galois group of $\alpha = 2^{1/4}$ over $\mathbf{Q}$. Ditto for $\beta = \cos 40°$.
- Prove: if $f(X), g(X) \in \mathbf{Q}[X]$ are relatively prime, they have no common root in $\mathbf{C}$.
- Prove: if $\alpha, \beta \in \mathbf{C}$ are algebraic over $\mathbf{Q}$, so are $\alpha + \beta$ and $\alpha\beta$.
- Let E be a finite extension of $K = \mathbf{F}_q$. Prove that the trace $E^+ \to K^+$ is surjective.
- Let E be a finite extension of $K = \mathbf{F}_q$. Prove that the norm $E^\times \to K^\times$ is surjective.
- If L/K is a separable field extension, it has no K-linear derivations $\neq 0$.
- A separable polynomial is irreducible iff its roots are permuted transitively by the Galois group.