Problem Set 11

Here are some problems that we will do this week. Something like one of these may appear on the final test.

We are going to use this simplified version of Galois's main theorem about field extensions.

Theorem. *Let K be an algebraic, normal, and separable extension of the field F. There is a one-to-one inclusion-reversing correspondence between subfields of K containing F and subgroups of $\mathrm{Aut}(K/F)$. Each subfield E is associated to the group $\mathrm{Aut}(K/E)$. Each subgroup $H \leq \mathrm{Aut}(K/F)$ is associated to its fixed field, $\mathcal{F}(H)$.*

Some comments:

- Algebraic: Every element of K is the root of some polynomial in $F[x]$.
- Normal: K is the splitting field of some polynomial in $F[x]$.
- Separable: Don't worry about it. Every field extension in characteristic 0 is separable, and $\mathbb{F}_{p^n}/\mathbb{F}_p$ is always separable.
- Fixed field: The fixed field of a subgroup H of $\mathrm{Aut}(K/F)$ is

$$\mathcal{F}(H) = \{\alpha \in K : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

- Inclusion-reversing: If

$$F \subseteq E_1 \subseteq E_2 \subseteq K$$

  is a tower of fields. The associate groups satisfy

$$\mathrm{Aut}(K/F) \supseteq \mathcal{F}(E_1) \supseteq \mathcal{F}(E_2) \supseteq \{\mathrm{id}\}$$

- One more thing: An automorphism σ of $F(\alpha)$ over F is completely determined by the image of α. This is because every element of $F(\alpha)$ is a sum of powers of α, and $\sigma(\alpha^k) = \big(\sigma(\alpha)\big)^k$.

To understand the material above let's do some examples, starting with finite fields, which are the simplest way to show the intricacies of Galois's theorem.

Exercises 11.1. Consider $\mathbb{F}_{2^6}$ (or really any $\mathbb{F}_{p^6}$).

(a) The Frobenius map is $\varphi : \alpha \longmapsto \alpha^2$. Explain why the order of φ is 6.

(b) Explain why the automorphism group $\mathrm{Aut}(\mathbb{F}_{2^6}/\mathbb{F}_2)$ is isomorphic to $\mathbb{Z}_6$.

(c) Find all subgroups of the automorphism group and find the associated fixed field.

(d) Draw the lattice of subfields of $\mathbb{F}_{2^6}$ and the corresponding lattice of subgroups of $\mathrm{Aut}(\mathbb{F}_{2^6}/\mathbb{F}_2)$.

(e) Generalize to $\mathbb{F}_{p^n}/\mathbb{F}_p$ (or perhaps just to $\mathbb{F}_{p^{12}}/\mathbb{F}_p$).

Exercises 11.2. Splitting fields of a product of quadratics.

(a) Find the splitting field K of $(x^2-5)(x^2-7)$.

(b) Convince yourself, and a friend, that the automorphism group is $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Find the Galois correspondence between subfields of K and subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Illustrate with lattice diagrams.

(d) Argue that $K = \mathbb{Q}(\sqrt{5}+\sqrt{7})$. This involves showing that $\sqrt{5}+\sqrt{7}$ does not satisfy any quadratic polynomial.

Exercises 11.3. Splitting field of a simple cubic polynomial.

We found the splitting field of x^3-2 over $\mathbb{Q}$ in class.

(a) This field has four proper subfields besides $\mathbb{Q}$ itself. Find them and find their dimensions over $\mathbb{Q}$.

(b) Factor x^3-2 over each of these subfields.

Exercises 11.4. The splitting field of x^n-1 over $\mathbb{Q}$ is called a **cyclotomic field**.

For $n \geq 5$, the field is usually written $\mathbb{Q}(\zeta_n)$, where ζ_n is the nth root of unity in the first quadrant of the complex plane.

(a) Show that the cyclotomic fields for $n = 3, 4, 6$ are all simply quadratic extensions of $\mathbb{Q}$.

(b) Show that x^n-1 splits in $\mathbb{Q}(\zeta_n)$.

(c) An automorphism of $\mathbb{Q}(\zeta_n)$ is completely determined by the image of ζ_n. Show that this implies $\mathrm{Aut}(\mathbb{Q}(\zeta_n) \cong U_n$, the multiplicative group of $\mathbb{Z}/n$.

(d) Find the Galois lattice correspondence and diagram for $n = 5$.
(One proper subfield.)

(e) Find the Galois lattice correspondence and diagram for $n = 7$.
(Two proper subfields.)

(f) Find the Galois lattice correspondence and diagram for $n = 8$.
(Three proper subfields.)

- Verify that the factorization of x^8-1 is $x^8-1 = (x-1)(x+1)(x^2+1)(x^4+1)$ and argue that the splitting field is isomorphic to $\mathbb{Q}[x]/\langle x^4+1\rangle$.
- Explain why $\zeta_8 = \frac{\sqrt{2}}{2}(1+i)$.
- Show that $\mathrm{Aut}(\mathbb{Q}(\zeta_8)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
- There are 3 different proper subfields of $\mathbb{Q}(\zeta_4)$. Find them.
- Find the factorizations of x^4+1 as a product of quadratics over each of these subfields.
- Explain the relationship between the factorizations of x^4+1 that you found in (b) and the fields you found in (c).