September 14:

Math 432 Class Lecture Notes

- Galois theory
- Examples

0.1 Galois theory

We know that the following are equivalent:

- E is a galois extension of F.
- E is the splitting field over F of a separable polynomial.
- $\#\mathrm{Aut}_F(E) = [E : F]$.

If E/F is a galois extension then the group $G(E/F) := \mathrm{Aut}_F(E)$ is called the **galois** group of the extension, and the basic idea is that the knowledge of this group conveys a lot of information about the fields involved.

One of the most basic way in which this is manifested is in the (famous) correspondence between subfields and subgroups, sometimes called the fundamental galois correspondence.

Let E/F be a (finite) galois extension, and let $G := G(E/F) = \mathrm{Aut}_F(E)$ be its galois groups. If H is a subgroup of G then let

$$E^H := \{x \in E \mid h(x) = x, \quad \forall\, h \in H\}\,.$$

One checks in a very straightforward fashion that the fixed fields E^H of H is in fact a subfield, and that the map from subgroups to subfields is inclusion reversing:

$$H \subset H' \Longrightarrow E^H \supset E^{H'}.$$

Now suppose that K is an intermediate field, i.e., that $F \subset K \subset E$. Define

$$\operatorname{stab}(K) := \{g \in G : g(x) \in K \text{ for all } x \in K\}.$$

One checks in a very straightforward fashion that the stabilizer of K is a subgroup of G, and that the map from subfields to subgroups is inclusion reversing:

$$K \subset K' \Longrightarrow \operatorname{stab}(K) \supset \operatorname{stab}(K').$$

One also checks in a straightforward fashion that

$$\begin{aligned} K &\subset E^{\operatorname{stab}(K)} \\ H &\subset \operatorname{stab}(E^H). \end{aligned}$$

The Fundamental Theorem of Galois Theorem says that these inclusions are equalities, and that the fixed field and stabilizer operations are mutually inverse bijections.

Theorem 1. There is a one-to-one correspondence between subgroups of G and intermediate fields between F and E. Specifically,

$$\begin{aligned} K &= E^{\operatorname{stab}(K)} \\ H &= \operatorname{stab}(E^H) \end{aligned}$$

so that "taking the fixed field" and "taking the stabilizer" are inverse bijections. Normal subgroups of G correspond to subfields of E that are themselves galois extensions of F.

0.2 Examples

Example 2. Let F be a field of characteristic not equal to 2, and let E/F be an extension of degree 2, i.e., a quadratic extension. Then $E = F(\alpha)$ where the minimal polynomial of α has degree 2. This polynomial splits in E, and has distinct roots, so E is a galois extension.

In fact, it is easy to see that any quadratic extension in characteristic not equal to 2 has the form $F(\sqrt{d})$.

Example 3. Some cubic extensions are galois, and others aren't. In a later homework exercise we'll learn how to find equations satisfied by $\cos(2\pi/n)$, and in particular will find that

$$(x - \cos(2\pi/7))(x - \cos(4\pi/7))(x - \cos(6\pi/7)) = x^3 + x^2 - 2x - 1.$$

By simple trigonometric identities, the second two roots are polynomials in the first one, so that $\mathbf{Q}(2\pi/7)$ is actually a splitting field for the cubic polynomial on the right. Thus, there is a cubic galois extension.

Example 4. Let $f(x) = x^3 - 2$, and let E be the splitting field of f over $\mathbf{Q}$. Since two of the roots are complex, the root field $\mathbf{Q}(\sqrt[3]{2})$ isn't a splitting field. The polynomial f factors as a linear times a quadratic over this field, and consequently E has degree 6 over $\mathbf{Q}$. The galois group $G = G(E/\mathbf{Q})$ is of order 6, and it permutes the three roots of f, so in fact G is isomorphic to the symmetric group of degree 3, S_3. The isomorphism is obvious: a permutation of three things corresponds to the automorphism of E that effects that permutation on the roots.

According to the Fundamental Theorem, the subgroups of G correspond to the intermediate fields. The trivial subgroup corresponds to E, and the entire group corresponds to $\mathbf{Q}$.

There are three (conjugate) subgroups of order 2, so there are three cubic fields inside E, namely each of the fields generated by a root of f; since these fields are all root fields they are isomorphic, but they are distinct subfields.

There is a unique subgroup of order 3, namely the alternating group A_3 of order 3. Its subfields turns out to be $\mathbf{Q}(\sqrt{-3})$.