# FEBRUARY 29 NOTES

## 1. 14.1: Introduction to Galois Theory

Some reminders from last time:

**Proposition 1.1.** *Let $E$ be the splitting field over $F$ of the polynomial $f(x) \in F[x]$. Then,*

$$|\mathrm{Aut}(E/F)| \leq [E : F]$$

*with equality if $f(x)$ is separable.*

**Definition 1.2.** Let $K/F$ be a finite extension. Then, $K$ is a **Galois extension of** $F$ or **Galois over** $F$ if $|\mathrm{Aut}(K/F)| = [K : F]$.

If $K/F$ is Galois, the group $\mathrm{Aut}(K/F)$ is called the **Galois group** of $K/F$ and denoted by $\mathrm{Gal}(K/F)$.

**Corollary 1.3.** If $K$ is the splitting field over $F$ of a separable polynomial $f(x)$, then $K/F$ is Galois.

In this case, we say the **Galois group of** $f(x)$ is $\mathrm{Gal}(K/F)$.

**Example 1.4.** Every quadratic extension $K$ of $F$ (for characteristic different than 2) is given by $K = F(\sqrt{D})$ and is Galois. If $\sqrt{D} \notin F$, then $[K : F] = 2$ and $\mathrm{Aut}(K/F)$ has two elements: 1 and the automorphism sending $\sqrt{D} \to -\sqrt{D}$. If $\sqrt{D} \in F$, then $[K : F] = 1$ and therefore $\mathrm{Aut}(K/F)$ is trivial but again this extension is Galois.

**Example 1.5.** $\mathbb{Q}(\sqrt[4]{2})$ is not Galois over $\mathbb{Q}$: there are four roots, $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$ but the only allowed automorphism is sending $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$.

**Example 1.6.** The extension of finite fields $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois because it is the splitting field of the separable polynomial $x^{p^n} - x$. In this case, the Galois group is cyclic of order $n$, with $\sigma_p(\alpha) := \alpha^p$ (the Frobenius) as the generator. This is an automorphism and any power of it is an automorphism, and $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$, so $\sigma_p^n$ is the identity. Also, no lower power of $\sigma_p$ can be the identity, because that would imply that $\alpha^{p^i} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$, but the polynomial $x^{p^i} - x$ has only $p^i$ and therefore cannot have all $\alpha \in \mathbb{F}_{p^n}$ as a root.

So far, we have taken a field extension $K/F$ and associated a group $\mathrm{Aut}(K/F)$ (or, $\mathrm{Gal}(K/F)$ if it is Galois) to it. This process is 'reversible':

**Proposition 1.7.** *Let $K$ be a field and $H \subset \mathrm{Aut}(K)$ a subgroup. Then, the collection $F$ of elements of $K$ fixed by all elements of $H$ is a subfield of $K$. It is called the* ***fixed field of*** *$H$.*

*Proof.* Let $h \in H$ and $a, b \in F$. Then, $h(a) = a$ and $h(b) = b$, so $h(a \pm b) = h(a) \pm h(b) = a \pm b$, and $h(ab) = h(a)h(b) = ab$, and $h(a^{-1}) = (h(a))^{-1} = a^{-1}$. Therefore, $F$ is closed under the field operations and hence a subfield of $K$. □

**Proposition 1.8.** *The association of groups to fields and fields to groups above is inclusion reversing:*

*(1) if $F_1 \subset F_2 \subset K$, then $\mathrm{Aut}(K/F_2) \subset \mathrm{Aut}(K/F_1)$.*
*(2) If $H_1 \subset H_2 \subset \mathrm{Aut}(K)$, then the fixed fields $F_1$ and $F_2$ satisfy $F_2 \subset F_1$.*

In the previous examples, if $H = \mathrm{Aut}(K)$, for $K = \mathbb{Q}(\sqrt{2})$, we have the fixed field of $H$ is $\mathbb{Q}$. If $K = \mathbb{Q}(\sqrt[3]{2})$, we have the fixed field is $\mathbb{Q}(\sqrt[3]{2})$.

**Example 1.9.** The extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ has Galois group the Klein-4 group given by the four elements

$$\sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}$$
$$\sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}$$
$$\sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}$$
$$\sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}.$$

We label these as $1, \sigma, \tau$, and $\sigma\tau$.

Furthermore: for each subgroup of $\mathrm{Gal}(K/F)$, we can write down the fixed field: the fixed field of $\{1\}$ is $K$, the fixed field of $\{1, \sigma\}$ is $\mathbb{Q}(\sqrt{3}$; the fixed field of $\{1, \tau\}$ is $\mathbb{Q}(\sqrt{2}$; the fixed field of $\{1, \sigma\tau\}$ is $\mathbb{Q}(\sqrt{6})$, and the fixed field of the whole group is $\mathbb{Q}$. This suggests a correspondence between *all* subfields of $K$ and the fixed fields of $\mathrm{Gal}(K/F)$.....

This is the *Fundamental Theorem of Galois Theory*, which is the content of the next section.

## 2. 14.2: The Fundamental Theorem of Galois Theory

**Theorem 2.1.** *Let $K/F$ be a Galois extension with $G = \mathrm{Gal}(K/F)$. There is a bijection*

$$\{ \text{ subfields } E \text{ such that } F \subset E \subset K \ \} \text{ and } \{ \text{ subgroups } H \text{ such that } G \geq H \geq 1 \ \}$$

*given by the correspondences: $E \mapsto$ the elements of $G$ fixing $E$ and $H \mapsto$ the fixed field of $H$.*

*These are inverse to each other and:*

1. *If $E_1, E_2$ correspond to $H_1, H_2$, then $E_1 \subset E_2$ if and only if $H_2 \leq H_1$;*
2. *$[K : E] = |H|$ and $[E : F] = |G : H|$;*
3. *$K/E$ is Galois with Galois group $\mathrm{Gal}(K/E) = H$;*
4. *$E$ is Galois over $F$ if and only if $H$ is a normal subgroup of $G$. In this case, $\mathrm{Gal}(E/F) = G/H$. Even if $H$ is not normal, the isomorphisms of $E$ which fix $F$ are in one-to-one correspondence with the cosets $\{\sigma H\}$ of $H$ in $G$;*
5. *The lattices of subfields and subgroups are compatible with respect to this bijection.*

Our goal over the next two lectures will be to prove this theorem. We need to develop some other terminology first.

**Definition 2.2.** If $\sigma : K \to L$ is an injective homomorphism of fields, it is called an **embedding** of $K$ into $L$. Note that the injectivity implies that $\sigma$ is also a group homomorphism $K^\times \to L^\times$.

These are examples of **characters**, which are group homomorphisms from $\chi : G \to L^\times$ for some group $G$ and some field $L$.

**Definition 2.3.** If $\sigma_1, \ldots, \sigma_n$ are embeddings of a field $K$ into $L$ (or characters), we say they are **linearly independent** over $L$ if whenever $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$ (where this is equality as *functions*) for $a_1, \ldots, a_n \in L$, we have $a_1, \ldots, a_n = 0$.

**Theorem 2.4.** *If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings of $K$ into $L$ (or, more generally, characters), then they are linearly independent over $L$.*

*Proof.* Suppose there is a nontrivial relation $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$. Choose a relation with the minimum number $m$ of nonzero coefficients, relabeling $a_i$ so we have $a_1\sigma_1 + \cdots + a_m\sigma_m = 0$.

Since $\sigma_1 \neq \sigma_m$, we may choose some element $k \in K^\times$, $k \neq 0$, such that $\sigma_1(k) \neq \sigma_m(k)$. Then, for any $x \in K$, we know

$$a_1\sigma_1(x) + \cdots + a_m\sigma_m(x) = 0$$

and

$$a_1\sigma_1(kx) + \cdots + a_m\sigma_m(kx) = 0$$

which implies

$$a_1\sigma_1(k)\sigma_1(x) + \cdots + a_m\sigma_m(k)\sigma_m(x) = 0.$$

Multiplying the first equation by $\sigma_m(k)$ and subtracting it from the second, we get

$$a_1(\sigma_1(k) - \sigma_m(k))\sigma_1(x) + \cdots + a_{m-1}(\sigma_{m-1}(k) - \sigma_m(k))\sigma_{m-1}(x) = 0$$

which is a relation with fewer nonzero coefficients, contradicting the minimality of $m$. $\square$

Let's start proving some things that will lead us to the Fundamental Theorem.

**Theorem 2.5.** *Let $K$ be a field and $G = \{1 =: \sigma_1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$. Let $F$ be the fixed field. Then, $[K : F] = n = |G|$.*

*Proof.* Suppose first the $n > [K : F]$. Let $k_1, \ldots, k_m$ be a basis for $K$ over $F$ and consider the homogenous linear system

$$\begin{gathered}\sigma_1(k_1)x_1 + \sigma_2(k_1)x_2 + \cdots + \sigma_n(k_1)x_n = 0\\ \sigma_1(k_2)x_1 + \sigma_2(k_2)x_2 + \cdots + \sigma_n(k_2)x_n = 0\\ \cdots\\ \sigma_1(k_m)x_1 + \sigma_2(k_m)x_2 + \cdots + \sigma_n(k_m)x_n = 0.\end{gathered}$$

This has $m$ equations and $n$ unknowns with $m < n$ so must have a nontrivial solution $\beta_1, \ldots, \beta_n$ in $K$. If $a_1, \ldots, a_m$ are any $m$ elements of $F$ (remembering that $\sigma_i(a_j) = a_j$ for all $i, j$), we may multiply the $j$th equation above by $a_j$, and then write each $a_j\sigma_i(k_j) = \sigma_i(a_jk_j)$ to get

$$\begin{gathered}\sigma_1(a_1k_1)\beta_1 + \sigma_2(a_1k_1)\beta_2 + \cdots + \sigma_n(a_1k_1)\beta_n = 0\\ \cdots\\ \sigma_1(a_mk_m)\beta_1 + \sigma_2(a_mk_m)\beta_2 + \cdots + \sigma_n(a_mk_m)\beta_n = 0.\end{gathered}$$

Adding these and using that $\sigma_i$ is a homomorphism implies that, for *any* choice $a_1, \ldots, a_m$, we have

$$\sigma_1(a_1k_1 + \cdots + a_mk_m)\beta_1 + \sigma_2(a_1k_1 + \cdots + a_mk_m)\beta_2 + \cdots + \sigma_n(a_1k_1 + \cdots + a_mk_m)\beta_n = 0.$$

Since every element $\alpha \in K$ can be written in this form, we have

$$\beta_1\sigma_1 + \cdots + \beta_n\sigma_n = 0$$

which contradicts the previous theorem that distinct embeddings are linearly independent.

Next time, we will show $n < [K : F]$. We do more linear algebra to prove it! $\square$