FEBRUARY 27 NOTES

1. 14.1: Introduction to Galois Theory

Definition 1.1. Let K be a field. An **automorphism** of K is an isomorphism $\sigma : K \to K$. The collection of all automorphisms of K is denoted by $\mathrm{Aut}(K)$. If $\alpha \in K$ is an element, Dummit and Foote write $\sigma\alpha$ to denote $\sigma(\alpha)$.

The identity map $id : K \to K$ is always an automorphsim called the **trivial** automorphism and often denoted $1 \in \mathrm{Aut}(K)$.

If $\sigma \in \mathrm{Aut}(K)$ is an automorphism, it is said to **fix** an element $\alpha \in K$ if $\sigma(\alpha) = \alpha$. If F is a subset of K, we say σ **fixes** F if $\sigma(\alpha) = \alpha$ for all $\alpha \in F$.

Definition 1.2. If K/F is a field extension, $\mathrm{Aut}(K/F)$ is the set of automorphisms of K fixing F.

Recall that the prime subfield of K is the field generated by 1_1K and is either $\mathbb{Q}$ or $\mathbb{F}_p$ depending on the characteristic of K. Any automorphism σ satisfies $\sigma(1) = 1$ so $\sigma(n) = n$ for all $n \in \langle 1 \rangle$. This implies that σ fixes the prime subfield F of K, so any automorphism of K is also an element of $\mathrm{Aut}(K/F)$, i.e. $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$ where F is the prime subfield of K.

Taking K to be either $\mathbb{Q}$ or $\mathbb{F}_p$, this implies that $\mathrm{Aut}(K) = \{1\}$.

In general, we have the following:

Proposition 1.3. $\mathrm{Aut}(K)$ *is a group under composition and* $\mathrm{Aut}(K/F)$ *is a subgroup.*

Proof. Exercise. □

Proposition 1.4. *Let K/F be a field extension and $\alpha \in K$ algebraic over F. Then, for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is a root of $m_{\alpha,F}$. In other words,* $\mathrm{Aut}(K/F)$ *permutes the roots of irreducible polynomials and any polynomial with coefficients in F having α as a root also has $\sigma(\alpha)$ as a root.*

Proof. Suppose $m_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Then,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

and applying σ, because σ fixes F, we have $\sigma(a_i) = a_i$, so this says

$$(\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$$

so $\sigma(\alpha)$ is also a root of $m_{\alpha,F}(x)$. □

Example 1.5. Let $K = \mathbb{Q}(\sqrt{2})$. Then, for any $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, we know $\tau(\sqrt{2}) = \pm\sqrt{2}$ by the previous proposition. Since τ must fix $\mathbb{Q}$, this determines τ completely: $\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}$.

Therefore, there are only two possible automorphisms: the identity map, or the map σ sending $\sqrt{2}$ to $-\sqrt{2}$. Therefore, $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{1, \sigma\} \cong \mathbb{Z}_2$.

Example 1.6. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then, for any $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, we know $\tau(\sqrt[3]{2})$ must be another root of the minimal polynomial $x^3 - 2$. *However*, the other roots are complex numbers, and hence not in K. Therefore, we must have $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ and therefore $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$.

Example 1.7. What is $\mathrm{Aut}(K/F)$ for $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbb{Q}$? We know $[K : F] = 4$ because K is the splitting field of $(x^2 - 2)(x^2 - 3)$. We also can write down four automorphisms of K fixing

F (we know these have to permute roots of each individual irreducible polynomial, so we have $\sqrt{2}$ going to $\pm\sqrt{2}$, and $\sqrt{3}$ goint to $\pm\sqrt{3}$):

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

Claim: these are all of the automorphisms. We will verify this with a theorem momentarily.

If we label these as $1, \sigma, \tau$, and $\sigma\tau$, it is straightforward to compute that $\mathrm{Aut}(K/F)$ is the Klein-4 group. Try it as an exercise!

Galois theory stems from connecting the study of field extensions to the study of their automorphism groups. We will want to generalize the behavior in the first example, not the second.

Proposition 1.8. *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.

Proof. We prove a more general statement: suppose $\phi : F \to F'$ is an isomorphism. We know by previous results that this can be extends to an isomorphism $\sigma : E \to E'$, where E' is the splitting field of $f' = \phi(f) \in F'[x]$. We will show that the number of possible σ's is at most $[E : F]$ with equality if and only if $f(x)$ is separable by induction on $[E : F]$. If $[E : F] = 1$, then there is only one choice $F = E \cong E' = F'$ and hence $\phi = \sigma$. Now, suppose $[E : F] > 1$ and that $p(x)$ is an irreducible factor of $f(x)$ of degree > 1. Let $p' = \phi(p)$. Let α be a root of $p(x)$. Then, if σ is any extension of ϕ to E, then σ restricted to $F(\alpha)$ is an isomorphism τ from $F(\alpha)$ to a subfield of E'. This is determined by $\tau(\alpha)$, which must be a root of β of $p'(x)$, so we have an isomoprhism $F(\alpha) \cong F'(\beta)$. Conversely, if β is any root, the isomorphisms τ, σ exists. Therefore, the number of extensions of ϕ to $\tau : F(\alpha) \to F'(\beta)$ is the number of distinct roots β of $p'(x)$ which is equal to the number of distinct roots α of $p(x)$, and hence the number of possible τ's is at most $[F(\alpha) : F]$ with equality if the roots are distinct.

Now, since E is the splitting field of $f(x)$ over $F(\alpha)$ and $[E : F(\alpha)] < [E : F]$. the inductive hypothesis implies that the number of extensions of τ to σ is at most $[E : F(\alpha)]$ with equality if $f(x)$ has distinct roots.

Therefore, the number of possible σ's is at most $[E : F(\alpha)][F(\alpha) : F] = [E : F]$ with equality if $f(x)$ is separable. □

Definition 1.9. 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 1.10. 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 1.11. $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ which has the same size as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ and hence is a Galois extension, and the Galois group is $\mathbb{Z}_2$.

Because $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$, this extension is not Galois.

Because $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is the Klein-4 group and the extension has degree 4, this extension is Galois over $F = \mathbb{Q}$.

Example 1.12. 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.