MARCH 5 NOTES

1. 14.2: The Fundamental Theorem of Galois Theory

Our goal is to prove the Fundamental Theorem of Galois Theory. Here's where we left off:

Theorem 1.1. *If $\sigma_1, \dots, \sigma_n$ are distinct embeddings of K into L, then they are linearly independent over L.*

Theorem 1.2. *Let K be a field and $G = \{1 =: \sigma_1, \sigma_2, \dots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$. Let F be the fixed field. Then, $[K : F] = n = |G|$.*

Proof. Suppose first the $n > [K : F]$. Last time, we used linear algebra to get a contradiction.

Now, suppose $n < [K : F]$. We do more linear algebra. This implies there are more than n basis vectors for K over F; let $k_1, \dots, k_{n+1}$ be $n + 1$ of them. Then, the system

$$\sigma_1(k_1)x_1 + \sigma_1(k_2)x_2 + \cdots + \sigma_1(k_{n+1})x_{n+1} = 0$$
$$\dots$$
$$\sigma_n(k_1)x_1 + \sigma_n(k_2)x_2 + \cdots + \sigma_n(k_{n+1})x_{n+1} = 0$$

has n equations in $n+1$ unknowns so has a nontrivial solution $\beta_1, \dots, \beta_{n+1}$. The elements β_i cannot all be elements of F: in the first equation, σ_1 is the identity, and if each β_i were in F, this would give a nontrivial relation among the basis vectors $\{k_1, \dots, k_{n+1}\}$.

Now, among all nontrivial solutions $\beta_1, \dots, \beta_{n+1}$, choose the one with the minimal number r of nonzero β_i and renumber and divide by β_r to assume we have a system of equations ($\star$) (for each $1 \le i \le n$):

$$\sigma_i(k_1)\beta_1 + \cdots + \sigma_i(k_{r-1})\beta_{r-1} + \sigma_i(k_r) = 0.$$

As at least one of the $\beta_i \notin F$, we may assume $\beta_1 \notin F$. However, since $\beta_1 \notin F$, it is not fixed by at least one element σ_l, i.e. $\sigma_l(\beta_1) \neq \beta_1$. Applying this automorphism to each of the previous equations, we have

$$\sigma_l\sigma_i(k_1)\sigma_l(\beta_1) + \cdots + \sigma_l\sigma_i(k_{r-1})\sigma_l(\beta_{r-1}) + \sigma_l\sigma_i(k_r) = 0.$$

But, because G is a *group*, the set $\{\sigma_l\sigma_i\}_{i=1}^n$ is *equal* to G, and therefore (letting σ_j be the element $\sigma_l\sigma_i$, we have the system of equations (†) $1 \le j \le n$

$$\sigma_j(k_1)\sigma_l(\beta_1) + \cdots + \sigma_j(k_{r-1})\sigma_j(\beta_{r-1}) + \sigma_j(k_r) = 0.$$

Finally, subtracting the equations † from the equations $\star$, we have a system of equations

$$\sigma_i(k_1)(\beta_1 - \sigma_l(\beta_1)) + \cdots + \sigma_i(k_{r-1})(\beta_r - \sigma_i(\beta_{r-1})) = 0.$$

which is not identically zero because $\beta_1 \neq \sigma_l(\beta_1)$, but has fewer nonzero coefficients than our minimum number r, so we have reached a contradiction.

Therefore, we finally obtain $n = [K : F]$. □

Corollary 1.3. Let K/F be any finite extension. Then, $|\mathrm{Aut}(K/F)| \le [K : F]$ with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof. Let F_1 be the fixed field of $\mathrm{Aut}(K/F)$. Then, $F \subset F_1 \subset K$ and $[K : F] \ge [K : F_1] = \mathrm{Aut}(K/F)$ with equality if and only if $F = F_1$. □

Corollary 1.4. A finite extension K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Corollary 1.5. Let $G \leq \mathrm{Aut}(K)$ be a finite subgroup of the automorphisms of K. Let F be the fixed field. Then, K/F is Galois with Galois group G.

Proof. By assumption, $G \leq |\mathrm{Aut}(K/F)|$, but $[K : F] = |G| \leq |Aut(K/F)| \leq [K : F]$, so $G = \mathrm{Aut}(K/F)$. □

Corollary 1.6. If $G_1 \neq G_2$ are distinct finite subgroups of $\mathrm{Aut}(K)$ for a field K, then their fixed fields are distinct.

Proof. Suppose F_1 and F_2 are the fixed fields of G_1 and G_2. If $F_1 = F_2$, then G_1 fixes F_2, so $G_1 \subset G_2$. Similarly, $G_1 \subset G_1$ so we conclude $G_1 = G_2$. □

This can actually characterize Galois extensions!

Definition 1.7. If K/F is Galois and $\alpha \in K$, the elements $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(K/F)$ are called the **Galois conjugates** of α.

Theorem 1.8. *An extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case, then every irreducible polynomial with coefficients in F which has a root in K has all of its roots in K. In particular, K/F is separable.*

Proof. We already know that a splitting field of a separable polynomial is Galois.

We'll first show that if K/F is Galois, then every irreducible polynomial $p(x) \in F[x]$ with a root in K splits completely in K. Let $G = \mathrm{Gal}(K/F) = \{1, \sigma_2, \dots, \sigma_n\}$ and let α be a root of $p(x)$. Let $\{\alpha, \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$ be the Galois conjugates of α. Let $\alpha, \alpha_2, \dots, \alpha_r$ be the distinct Galois conjugates. For any $\tau \in G$, because $\tau G = G$, applying τ to the set $\alpha, \alpha_2, \dots, \alpha_r$ just permutes these elements, so the polynomial

$$f(x) = (x - \alpha)(x - \alpha_2) \dots (x - \alpha_r)$$

has coefficients fixed by G because the elements of G just permute the factors. Therefore, $f(x)$ is in the fixed field of G, which is F by the previous corollary, so $f(x) \in F[x]$. Since $p(x)$ was the minimal polynomial of α, we know $f(x) \mid p(x)$, but we also know that $p(x)$ has each α_i as a root, so $p(x) \mid f(x)$, and therefore $p(x) = f(x)$. This shows that $p(x)$ is separable and splits completely in K.

Finally, suppose K/F is Galois and let $\beta_1, \dots, \beta_n$ be a basis for K/F, and let $p_i(x)$ be the minimal polynomial of β_i. Each $p_i(x)$ is therefore separable with all of its roots in K. Let $g(x)$ be the polynomial obtained by removing any "repeated factors" from the product $p_1(x) \dots p_n(x)$, which has the same splitting field as $p_1(x) \dots p_n(x)$, but is separable. Because the splitting field of $p_1(x) \dots p_n(x)$ is K, this shows that K is the splitting field of $g(x)$ which is separable. □

The proof of this theorem tells us something very useful! Namely:
in a Galois extension K/F, for any $\alpha \in F$, the roots of the minimal polynomial of α are just the distinct Galois conjugates of α.

We can use this to find minimal polynomials! For example:

Example 1.9. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

We know that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ which is a Galois extension of $\mathbb{Q}$ with Galois group $\{1, \sigma, \tau, \sigma\tau\}$ where $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\tau(\sqrt{3}) = -\tau 3$. To find the minimal polynomial, we just find the conjugates and multiply: the conjugates are

$$\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}$$

so the minimal polynomial is

$$(x - (\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3})) = x^4 - 10x^2 + 1.$$

Finally, let's prove the Fundamental Theorem.

Theorem 1.10. *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.*

Proof. Given any subgroup $H \leq G$, there is a unique fixed field $E = K^H$ by a previous Corollary. This says the correspondence right to left is injective. Now, if K is the splitting field of the separable polynomial $f(x) \in F[x]$, then $f(x) \in E[x]$ for any subfield $F \subset E \subset K$ so K is also the splitting field of $f(x)$ over E and hence K/E is Galois. Therefore, E is the fixed field of $\mathrm{Aut}(K/E) \leq G$, so every subfield E is the fixed field of some subgroup of G and hence the correspondence is surjective. Therefore, we have proved the bijection. We have also already shown that the automorphisms fixing E are exactly $\mathrm{Aut}(K/E)$ so these correspondences are inverses.

Now, let's prove the sub-statements. We have already proved (1) and (3). For (2), if $E = K^H$ is the fixed field of $H \leq G$, then $[K : E] = |H|$ an $[K : F] = |G|$, which gives $[E : F] = |G : H|$.

For (4), suppose $E = K^H$ is the fixed field of the subgroup H. Then, every $\sigma \in G = \mathrm{Gal}(K/F)$ restricted to E gives an embedding $\sigma|_E : E \to \sigma(E) \subset K$. Conversely, if $\tau : E \to \tau(E) \subset \overline{F}$ is any embedding of E into a fixed algebraic closure of F containing K that fixes F, then $\tau(E) \subset K$ because, if $\alpha \in E$ has minimal polynomial $m_\alpha(x)$, $\tau(\alpha)$ is another root of $m_\alpha(x)$, and K contains all of these roots. In other words, as K is the splitting field of $f(x)$ over E, it is also the splitting field of $\tau f(x)$ over $\tau(E)$. Therefore, any isomorphism $\tau : E \to \tau(E)$ extends to an isomorphism $\sigma : K \to K$ which must fix F because τ does, and hence $\sigma \in \mathrm{Aut}(K/F)$. This shows that every such τ is the restriction to E of some $\sigma \in \mathrm{Aut}(K)$.

Now, suppose we have two automorphisms σ, σ' of K. They restrict to the same embedding of E if and only if $\sigma^{-1}\sigma'|_E = id$, which implies that $\sigma^{-1}\sigma' \in H$, or $\sigma' \in \sigma H$. This says that the embeddings of E/F are in bijection with the cosets σH of H in G, so $|Emb(E/F)| = [G : H] = [E : F]$. We therefore need to show that E/F is Galois if and only if $\mathrm{Aut}(E/F) = Emb(E/F)$, i.e. each embedding of E is actually an automorphism of E: $\sigma(E) = E$.

So, suppose $\sigma \in G$. First, we claim that the subgroup of G fixing the field $\sigma(E)$ is the group $\sigma H \sigma^{-1}$, i.e. $\sigma(E) = K^{\sigma H \sigma^{-1}}$. If $\sigma(\alpha) \in \sigma(E)$, then $(\sigma h \sigma^{-1}(\sigma(\alpha)) = \sigma(\alpha)$ for any $h \in H$ because h fixes $\alpha \in E$. Also, the group fixing $\sigma(E)$ must have order equal to $[K : \sigma(E)] = [K : E] = |H|$, but $|\sigma H \sigma^{-1}| = |H|$, so in fact the group fixing $\sigma(E)$ must equal $\sigma H \sigma^{-1}$.

Therefore, by the bijective correspondence, $\sigma(E) = E$ for all $\sigma \in G$ if and only if $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, i.e. H is normal.

We leave it as an exercise to verify that the Galois group is precisely G/H in this and to prove 5. □

2. 14.3: Finite Fields

This section is mostly a recap of things we've seen about finite fields. So far, we know:

1. A finite field has characteristic p for some prime p, and any such field is $\cong \mathbb{F}_{p^n}$ which is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.
2. $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$ with cyclic Galois group $\langle \sigma_p \rangle \cong \mathbb{Z}_n$ where σ_p is the Frobenius.

(3) By the Fundamental Theorem, the subfields of $\mathbb{F}_{p^n}$ correspond to subgroups of $\mathbb{Z}_n$, of which there is exactly one for each divisor d of n: $\langle \sigma_p^d \rangle$. By the classification of finite fields, this must be $\mathbb{F}_{p^d}$.

Proposition 2.1. *The polynomial $x^{p^n} - x$ is the product of all distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d as d ranges through the divisors of n.*

Proof. If $p(x)$ is any irreducible polynomial of degree d with some root α, then $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$, so d must be a divisor of n and the extension must be $\mathbb{F}_{p^d}$. This implies also that the extension is Galois, so that all roots of $p(x)$ are contained in $\mathbb{F}_p(\alpha)$. Because $\mathbb{F}_{p^n}$ is just the set of roots of $x^{p^n} - x$, if we group the factors of this polynomial according to the degree of their minimal polynomials, we find that the polynomial $x^{p^n} - x$ is the claimed product. □

Finally,

Proposition 2.2. *The algebraic closure of $\mathbb{F}_p$ is $\cup_{n \geq 1} \mathbb{F}_{p^n}$.*

Proof. This union consists of all finite extensions of $\mathbb{F}_p$, so must be an algebraic closure. It is a field because there is a partial ordering: given any n_1, n_2, there is a larger field that contains both $\mathbb{F}_{p^{n_1}}$ and $\mathbb{F}_{p^{n_2}}$, namely $\mathbb{F}_{p^{n_1 n_2}}$. So, for instance, given any α, β in this union, $\alpha \in \mathbb{F}_{p^{n_1}}$ for some n_1 and $\beta \in \mathbb{F}_{p^{n_2}}$ for some n_2, so $\alpha, \beta \in \mathbb{F}_{p^{n_1 n_2}}$, which is a field, so $\alpha \pm \beta$, $\alpha\beta$, α/β all exist in $bF_{p^{n_1 n_2}}$ and hence exist in the union. □