Lecture 1-13: Galois theory

January 13, 2025

As promised last time, I now bring groups into the picture.

Definition, p. 558

Given an extension K of a field F, the *automorphism group of K over F*, denoted $\mathrm{Aut}(K/F)$, is the group of automorphisms of K fixing every element of F.

Here are two easy examples (p. 559). If $F = \mathbb{Q}, K = Q(\sqrt{2})$, then an automorphism of F fixing K must send $\sqrt{2}$ either to itself or its negative. The latter possibility indeed works since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ and $-\sqrt{2}$ is a root of this polynomial. Hence $\mathrm{Aut}(K/F)$ is cyclic of order 2. On the other hand, if $K = F(\alpha) = F(2^{1/3})$, then α is the only root of $x^3 - 2$ in K (the other two roots being complex), so $\mathrm{Aut}(K/F)$ is the trivial group.

The key result is then

Theorem

If K is a finite extension of F, then $\mathrm{Aut}(K/F)$ has order at most $[K : F]$. Equality holds if and only if K is the splitting field of a separable polynomial over F.

Proof.

Let K be generated by $\alpha_1, \ldots, \alpha_m$ over F (for example, let the α_i be a basis of K over F). Let p_1 be the minimal polynomial of α_1 over F, of degree d_1. An automorphism ϕ of K fixing F must send α_1 to a root of p_1; there are at most d_1 roots of p_1 in K, so at most d_1 choices for $\phi(\alpha_1)$. Having chosen $\beta_1 = \phi(\alpha_1)$, let $F_1 = F(\alpha_1), F_1' = F(\beta_1)$, and let p_2 be the minimal polynomial of α_2 over F_1, of degree d_2. Then $\beta_2 = \phi(\alpha_2)$.must be a root of $\phi(p_2) \in F'[x]$; there are at most d_2 choices for this root. $\square$

Proof.

Continuing in this way, defining polynomials $p_3, p_4, \ldots$ of degrees $d_3, \ldots, d_m$, one finds that there are at most $d = d_1 d_2 \ldots d_m$ choices for ϕ and the degree $[K : F]$ equals d, whence the first assertion. If K is the splitting field of a separable polynomial q over F then one can choose the α_i above to be roots of q and all the polynomials $p_i, \phi(p_i)$ divide $\phi(q) = q$; moreover, there are always exactly d_i choices for $\phi(\alpha_i)$, since q has a full complement of distinct roots in K. Hence equality holds in the theorem. Conversely, if equality holds, then for any choice of α_i, K must contain all roots of the minimal polynomial q_i of α_i over F and these roots are distinct, since otherwise the count of automorphisms of K over F would fall behind the maximum value and could never catch up. Since the q_i are irreducible no two of them have any roots in common. Hence K is the splitting field of the separable product q of the distinct q_i. $\square$

The splitting field K of a separable polynomial p over a field F is called a Galois extension of F and $\mathrm{Aut}(K/F)$ is called the Galois group of K over F (p. 562); it is often denoted $\mathrm{Gal}(K/F)$. It is also called the Galois group of p (over F). Thus we see that among finite extensions Galois extensions are precisely those with the maximum symmetry.

Theorem 13, p. 572

If K is finite and Galois over F then it contains the splitting field over F of any of its elements and all of its elements are separable.

Indeed, if $\alpha \in K$ has minimal polynomial q, of degree d, then by counting automorphisms as in the theorem, starting with counting homomorphisms of $F(\alpha)$ into K, we see that if K fails to have d distinct roots of p then it admits fewer than $[K : F]$ automorphisms fixing K. This proof also shows that any automorphism of a subfield L of K fixing F extends to an automorphism of K.

In a similar way, by counting homomorphisms of a field into a suitable extension, we can derive a criterion for a finite extension to be separable.

Proposition

A finite extension K of F is separable if and only if it admits $[K : F]$ distinct homomorphisms fixing F into a suitable extension L, or if and only if it is generated by separable elements over F.

Proof.

As in the proof of the previous theorem, let $\alpha_1, \ldots, \alpha_m$ be a set of generators of K over F and let p_1 be the minimal polynomial of α_1 over F, of degree d_1. If p_1 is not separable, then there are fewer than d_1 distinct homomorphisms of $F(\alpha_1)$ into any extension L of K, hence ultimately fewer than $[K : F]$ homomorphisms of K into L. If on the other hand α_i is separable over F for all i, with minimal polynomial q_i over $F(\alpha_1, \ldots, \alpha_{i-1})$, then q_i divides the minimal polynomial p_i of α_i over F and so is separable if p_i is. Then we get $[K : F]$ distinct homomorphisms of K fixing F into (for example) a splitting field of the product of the p_i. □

Moreover, finite separable extensions always sit inside Galois extensions:

Corollary 23, p. 594

Any finite separable extension K of a field F is contained in a unique smallest Galois extension.

Let p be the product of the distinct minimal polynomials of a set of generators of K. The splitting field of p over F is the desired Galois extension; it contains K since it contains a set of generators of it.

The minimal Galois extension of a separable extension K is called the Galois closure of K and often denoted by $\overline{K}$.

As an example, every finite field F_{p^n} is Galois over its prime subfield F_p, being the splitting field of $x^{p^n} - x$ over F_p. It consists entirely of the roots of this polynomial and nothing else, since if a, b are two roots then so are $a+b$, $a-b$, and ab, by the Frobenius map, so that the set of roots is closed under the field operations. Its Galois group is cyclic of order n, being generated by the Frobenius map sending x to x^p. More generally, if m divides n, then F_{p^n} is also Galois over F_{p^m}, having cyclic Galois group of order $\frac{n}{m}$. It is generated by the mth power of the Frobenius map, which fixes all elements of F_{p^m}. As a consequence of above results, F_{p^n} is also a splitting field for all irreducible polynomials of degree n over F_p and all such polynomials divide $x^{p^n} - x$. There must be at least one such polynomial, since F_{p^n} is generated over F_p by a single element, for example a cyclic generator of its multiplicative group. See section 14.3 of the text.

Now we head toward the Galois correspondence between subgroups of the Galois group G of a Galois extension K of F and fields between F and K. Note first that if H is any subgroup of $\mathrm{Aut}(K/F)$, then the fixed field K^H of elements of K fixed by H is clearly a subfield containing F. If H_1, H_2 are two such groups with $H_1 \subset H_2$, then we have $K^{H_1} \supset K^{H_2}$.

Lemma

Let K/F be a Galois extension with Galois group G. Then the fixed field K^G is F.

The elements of G fix all elements of F by definition. Conversely, if $\alpha \in K, \alpha \notin F$, then α has a minimal polynomial p of degree larger than one; by a previous proposition all roots of p in its splitting field are present in K and G acts transitively on them (by the proof of our first theorem). Thus K^G is exactly F, as claimed.

Proposition; see Theorem 14, p. 574

If K/F is Galois with Galois group G, then every field L between F and K takes the form K^H for some subgroup H of G and K is Galois over L.

We know that K is the splitting field of some polynomial p over F, whence it is also the splitting field of the same polynomial over L and K is Galois over L. Hence L is the fixed field K^H of the Galois group of K over L, which is by definition a subgroup of G.