LECTURE MARCH 23: THE MAIN THEOREM OF GALOIS THEORY

1. Review of Galois extensions and fixed fields

Recall the definition of Galois:

Definition 1.1. *Let E/F be an algebraic extension of fields. E/F is* Galois *if both conditions hold:*

- *E/F is a splitting field.*
- *E/F is separable.*

Under these circumstances, we use the special notation $\mathrm{Gal}(E/F)$ to mean $\mathrm{Aut}(E/F)$. It is the Galois group of the extension E/F.

If E/F is a finite extension of fields, then

$$E/F \text{ is Galois } \iff [E:F] = \mathrm{Aut}(E/F).$$

We had also said that if E/F is any extension of fields, and if $H \subset \mathrm{Aut}(E/F)$ is a subgroup, then

$$E^H = \left\{ \alpha \in E \;\middle|\; \sigma(\alpha) = \alpha \forall \sigma \in H \right\}$$

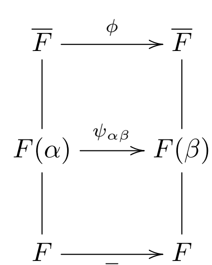
is a field lying between F and E, called the *fixed field* of H.

So we might ask about $E^{\mathrm{Aut}(E/F)}$, the fixed field of all symmetries of E/F. Generally this is unstable, but when E/F is Galois, it must be the ground field F:

Theorem 1.2. *Let E/F be a Galois extension. Then $E^{\mathrm{Gal}(E/F)} = F$.*

Proof. The containment $F \subset E^{\mathrm{Gal}(E/F)}$ is "obvious". In the other direction, suppose $\alpha \in E^{\mathrm{Gal}(E/F)}$. Assume for the purposes of contradiction that $\alpha \notin F$. This means that the degree of α over F must be > 1. Let $f(x) \in F[x]$ be the minimal polynomial of α over F, so that $\deg f > 1$. Since E/F is separable, $f(x)$ must not have repeated roots. There must be another root $\beta \in \overline{F}$, $\beta \neq \alpha$. Since E/F is a splitting field, $\beta \in E$.

There exists an isomorphism $\psi_{\alpha\beta}\colon F(\alpha) \to F(\beta)$, which is the identity on F and which satisfies $\psi_{\alpha\beta}(\alpha) = \beta$. By the isomorphism extension theorem, we have a diagram



where ϕ is an automorphism of $\overline{F}$ fixing F. Since E/F is a splitting field, $\phi(E) = E$. Let σ be the restriction of ϕ to E, so that $\sigma \in \mathrm{Gal}(E/F)$. We have $\sigma(\alpha) = \beta$ by construction. But this contradicts the fact that $\alpha \in E^{\mathrm{Gal}(E/F)}$. Thus $\alpha \in F$. $\square$

2. Intermediate extensions to a Galois extension E/F

Theorem 2.1. *Let E/F be a Galois extension, and let K be intermediate: $F \subset K \subset E$. Then E/K is also Galois, and* $\mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/F)$ *is a subgroup.*

Proof. Let $\alpha \in E$. We must show that (a) α is separable over K, and (b) all K-conjugates of α lie in E.

Let $f(x) \in F[x]$ be the minimal polynomial of α over F. Let also $f_K(x) \in K[x]$ be the minimal polynomial of α over K. Since $f(\alpha) = 0$, and $f_K(x)$ must divide every polynomial in $K[x]$ with α as a root, we must have $f_K(x)|f(x)$.

Since E/F is separable, $f(x)$ is separable, and therefore so is $f_K(x)$. Thus E/K is separable.

Since $f_K(x)|f(x)$, the set of K-conjugates of α is a subset of the set of F-conjugates of α, and since all of the latter lie in E, so do all of the former. Thus E/K is a splitting field.

The containment $\mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/F)$ is by definition. □

Theorem 2.2 (The primitive element theorem)**.** *Let E/F be a separable finite extension. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.*

Example 2.3. $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Example 2.4. *The counterexample is this: Let $F = \mathbf{Z}_p(t, u)$. Let $E = \mathbf{Z}_p(t^{1/p}, u^{1/p})$. Note that E/F has degree p^2. Then E/F cannot be generated by one element! For instance $F(t^{1/p} + u^{1/p})$ is not equal to E, because $t^{1/p} + u^{1/p}$ only has degree p: it is the root of $x^p - t - u$.*

Assume forever that E/F is a finite Galois extension. We can now describe functions in both directions between the sets:

(1) Fields K intermediate to E/F.
(2) Subgroups of $\mathrm{Gal}(E/F)$.

To a field K we can associate the subgroup

$$\mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/F).$$

And then in the other direction, to a subgroup $H \subset \mathrm{Gal}(E/F)$, we can associate the fixed field E^H.

Theorem 2.5. *These two operations cancel each other out. That is:*

(1) *Given K intermediate to E/F, we have $E^{\mathrm{Gal}(E/K)} = K$.*
(2) *Given a subgroup $H \subset \mathrm{Gal}(E/F)$, we have*

$$\mathrm{Gal}(E/E^H) = H.$$

Taken together, these two statements show that there is a *bijection* between intermediate fields and subgroups of E/F. (It isn't even obvious that there are only finitely many intermediate fields!)

Proof. We already proved the first assertion (with F instead of K, but it doesn't matter). So suppose $H \subset \mathrm{Gal}(E/F)$ is a subgroup. The containment $H \subset \mathrm{Gal}(E/E^H)$ is "obvious": elements of H fix elements of E^H by definition.

Since E/E^H is finite and separable, the primitive element theorem says that $E = E^H(\alpha)$, for some $\alpha \in E$. Consider the polynomial

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

Since $e \in H$, α is a root of $f(x)$. What's a little harder to see is that the coefficients of $f(x)$ are in E^H.

As an example, suppose that $H = \{1, \sigma\}$ has order 2. Then our polynomial is

$$f(x) = (x - \alpha)(x - \sigma(\alpha)) = x^2 - (\alpha + \sigma(\alpha))x + \alpha\sigma(\alpha).$$

The claim was that the coefficients $\alpha + \sigma(\alpha)$ and $\alpha\sigma(\alpha)$ must be fixed by H, which is the same as saying that they are fixed by σ. Now observe:

$$\begin{aligned} \sigma(\alpha + \sigma(\alpha)) &= \sigma(\alpha) + \sigma^2(\alpha) = \alpha + \sigma(\alpha) \\ \sigma(\alpha\sigma(\alpha)) &= \sigma(\alpha)\sigma^2(\alpha) = \alpha\sigma(\alpha) \end{aligned}$$

By the way, these elements $\alpha + \sigma(\alpha)$ and $\alpha\sigma(\alpha)$ are called the trace and norm, respectively.

I will leave it to you to see why $f(x) \in E^H[x]$ in general. This polynomial has α as a root. The degree of $f(x)$ is just $\#H$, so that $\#\operatorname{Gal}(E/E^H) = [E^H(\alpha) : E^H] \leqslant \#H$. Together with the fact that $H \subset \operatorname{Gal}(E/E^H)$, this shows that $H = \operatorname{Gal}(E/E^H)$. $\square$

Example 2.6. *Let $E/\mathbf{Q}$ be the splitting field of the polynomial $x^8 - 1$. Find all subfields of E.*

First let's observe that the roots of $x^8 - 1$ in $\mathbf{C}$ are exactly $1, z, z^2, \ldots, z^7$, where $z = e^{2\pi i/8}$ is a primitive 8th root of 1. Thus the splitting field of $x^8 - 1$ is exactly $\mathbf{Q}(z)$. Note the factorization

$$x^8 - 1 = (x^4 - 1)(x^4 + 1).$$

Since $z^4 = e^{\pi i} = -1$, so that z is a root of the second factor, $x^4 + 1$.

I claim $x^4 + 1$ this is irreducible over $\mathbf{Q}$, and thus the minimal polynomial of z. This follows from Eisenstein's criterion at the prime 2, applied to

$$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2.$$

Thus $[\mathbf{Q}(z) : \mathbf{Q}] = 4$. The full set of roots of x^4+1 are $\{z, z^3, z^5, z^7\}$. Since we're in characteristic 0, $\mathbf{Q}(z)/\mathbf{Q}$ is necessarily separable. Therefore it is Galois.

What is $\operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q})$? It is certainly a group of order 4. Each $\sigma \in \operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q})$ must carry z onto either z, z^3, z^5, z^7. So

$$\operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q}) = \{e, \sigma_3, \sigma_5, \sigma_7\},$$

wnhere $\sigma_j(z) = z^j$. Note that

$$\sigma_j\sigma_{j'}(z) = \sigma_j(z^{j'}) = \sigma_j(z)^{j'} = z^{jj'}$$

The rule is that $\sigma_j\sigma_{j'} = \sigma_{jj'}$, where the product is considered modulo 8, and σ_1 is the identity. Thus $\operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q})$ is isomorphic to the group of units in the ring $\mathbf{Z}_8$. We have $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, so that $\operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q})$ is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.

The subgroups of $\operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q})$ are:

(1) $\operatorname{Gal}(\mathbf{Q}(z)/\mathbf{Q})$
(2) $H_3 = \{e, \sigma_3\}$
(3) $H_5 = \{e, \sigma_5\}$
(4) $H_7 = \{e, \sigma_7\}$
(5) $\{e\}$

For each of these subgroups H, we can try to figure out $\mathbf{Q}(z)^H$. First let's compute the fixed field of H_7. Looking for an element of $\mathbf{Q}(z)$ which doesn't change when you apply σ_7. First note that $\sigma_7(z^7) = z^{49} = z$. If $\alpha = z + z^7$, then $\sigma_7(\alpha) = z^7 + z = \alpha$. Therefore $\alpha \in \mathbf{Q}(z)^{H_7}$. What is α? (Note that $z^8 = 1$, so $z^7 = z^{-1}$.)

$$\alpha = z + z^7 = e^{2\pi i/8} + e^{-2\pi i/8} = 2\cos(2\pi/8) = \sqrt{2}.$$

We could have also argued:

$$(z + z^7)^2 = z^2 + 2zz^7 + z^{14} = z^2 + 2 + z^{-2} = i + 2 + (-i) = 2.$$

The result is that $\mathbf{Q}(z)^{H_7} = \mathbf{Q}(\sqrt{2})$.

The same argument shows that $\mathbf{Q}(z)^{H_3} = \mathbf{Q}(\beta)$, where $\beta = z + z^3$. We note here that

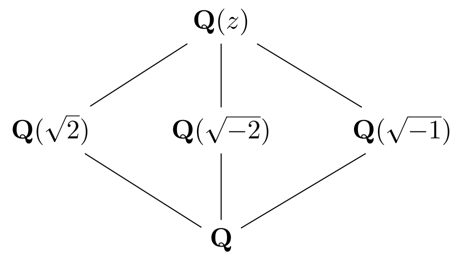
$$z = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

and

$$z^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

Thus $\beta = i\sqrt{2} = \sqrt{-2}$. Thus $\mathbf{Q}(z)^{H_3} = \mathbf{Q}(\sqrt{-2})$. The remaining field has to be $\mathbf{Q}(\sqrt{-1})$, because $i = z^2$. We can see that

$$\sigma_5(i) = i^5 = i.$$



Since $\sqrt{-2}, \sqrt{2} \in \mathbf{Q}(z)$, we must have $\sqrt{-4} = 2\sqrt{-1} \in \mathbf{Q}(z)$ as well.

3. Inseparable extensions are a nightmare

Let $F = \mathbf{Z}_p(t, u)$, and let $E = F(t^{1/p}, u^{1/p})$. Then E/F has degree p^2. We had already observed that E/F is not a primitive extension: there is no $\alpha \in E$ for which $E = F(\alpha)$. It is also the case that $\mathrm{Aut}(E/F) = \{e\}$, the trivial group. It gets worse than this:

Theorem 3.1. *There are infinitely many distinct intermediate fields between F and E.*

Indeed, $K = F(t^{1/p} + u^{a/p})$, as a ranges through integers not divisible by p, gives an infinite family of distinct intermediate extensions.

Thus, nothing like the main theorem of Galois theory holds for inseparable extensions.

4. But finite fields are a dream

Let F be a finite field, with q elements. Thus q is a power of a prime. If $\overline{F}$ is an algebraic closure of F, then F is the set of roots of $x^q - x$ in $\overline{F}$.

For each integer $n \geqslant 1$, there is exactly one extension of F of degree n. Namely, let E be the set of roots of $x^{q^n} - x$ in $\overline{F}$. Then E/F is an extension of degree n. We have $\#E = q^n$. We have that $\mathrm{Gal}(E/F)$ is cyclic of order n, generated by the Frobenius element σ. For all $\alpha \in E$, $\sigma(\alpha) = \alpha^q$. Note that σ really does have order n, since $\sigma^n(\alpha) = \alpha^{q^n} = \alpha$.

Fields intermediate to E/F are in correspondence with subgroups of $\mathrm{Gal}(E/F) \cong \mathbf{Z}_n$. There is one subgroup for each divisor d of n, namely the subgroup generated by $\sigma^{n/d}$. For each d, we have the subgroup generated by σ^d, of order n/d but index d. The fixed field of σ^d is the set of all $\alpha \in E$ satisfying $\alpha^{q^d} = \alpha$, which is to say, the roots of $x^{q^d} - x$. These form a subfield K, of degree d over F.

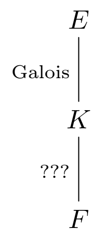
5. The relation between normal extensions and normal subgroups

In this section we're going to add some details to the Main Theorem of Galois Theory. Let E/F be a finite Galois extension. Then there is a bijection between the following two sets:

- Intermediate fields K between E and F.
- Subgroups of $\mathrm{Gal}(E/F)$.

The bijection carries K onto the subgroup $\mathrm{Gal}(E/K)$, and in the reverse direction, it carries a subgroup $H \subset \mathrm{Gal}(E/F)$ onto its fixed field E^H.

Also recall that for an intermediate field K, the extension E/K is Galois, but there's no guarantee about K/F:



So when is K/F Galois? If so, what is its group?

Theorem 5.1. *Assume that E/F is a finite Galois extension. Let $H \subset \mathrm{Gal}(E/F)$, with fixed field $K = E^H$. Then K/F is Galois if and only if H is a normal subgroup of $\mathrm{Gal}(E/F)$. If this is the case, then we have an isomorphism*

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/H.$$

We remark that splitting fields are also sometimes called normal extensions. So this theorem says that normal subgroups correspond to normal fields.

Example 5.2. *Consider the splitting field E of $x^3 - 2$ over $\mathbf{Q}$.*

Let $\theta = \sqrt[3]{2}$. Then the roots of $x^3 - 2$ are $\theta, \omega\theta, \omega^2\theta$, where

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}.$$

Thus $E = \mathbf{Q}(\theta, \omega\theta, \omega^2\theta) = \mathbf{Q}(\theta, \omega)$. We found earlier that $\mathrm{Gal}(E/\mathbf{Q}) \cong S_3$,

$$\mathrm{Gal}(E/\mathbf{Q}) = \left\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\right\}.$$

Here, τ takes ω to ω^2 but fixes θ, while σ fixes ω but takes θ to $\omega\theta$.

The only nontrivial proper normal subgroup is $A_3 = \left\{e, \sigma, \sigma^2\right\}$. The fixed field of A_3 is $\mathbf{Q}(\omega)$, which is Galois over $\mathbf{Q}$. The Galois group of $\mathbf{Q}(\omega)/\mathbf{Q}$ is $S_3/A_3 \cong \mathbf{Z}_2$.

Meanwhile, $H = \{e, \tau\}$ is a non-normal subgroup. The fixed field of H is $\mathbf{Q}(\theta)$, and this is not Galois over $\mathbf{Q}$ (it is not a splitting field).