Galois theory notes, week 2, day 1 of 4

Soham

July 2016

1. Recall that when we have a field automorphism L/K, we define the group of K-automorphisms of L and denote it $G_{L/K}$. When this extension is Galois (= normal and separable), it is called the Galois group $\mathrm{Gal}(L/K)$.
2. If H is a finite group of automorphisms of L, write L^H for the fixed field of H.
3. If $[L:K]$ is finite, then $G_{L/K} \leq [L:K]$.

Theorem. If L is any field and H a finite group of auts of L, then $[L:F_H] = |H|$.

Proof. We'll show $[L:F_H] \leq |H| =: s$ by showing that any set of $s+1$ elements of L are linearly dependent over F_H.

Once we have this, the other direction follows from the last theorem from last week, and we get that

$$|H| \leq [L:F_H]$$

Suppose $a_1, \ldots, a_{s+1} \in L$. We want to see if they can be linearly independent over F_H.

Consider all the images of the a_i under the elements of H:

$$v_i := (\sigma_1(a_i), \sigma_2(a_2), \ldots, \sigma_s(a_i))^t$$

which is an $s+1$-set in L^s, so it must be linearly dependent over L. Rearranging, we get

$$\sigma_i(a_{s+1}) = b_1\sigma_i(a_1) + \cdots + b_s\sigma_i(a_s) \tag{1}$$

Apply, say, $\sigma := \sigma_k \in H$.

$$(\sigma\sigma_i)(a_{s+1}) = \sigma(b_1)(\sigma\sigma_i)(a_1) + \cdots + \sigma(b_s)(\sigma\sigma_i)(b_s) \tag{2}$$

but these are just the old equations in some other order (multiplication by a group element is an automorphism, so is, in particular, bijective) and we get a smaller dependence relation.

So what we should have done is started with a minimal dependence relation among some of the vectors v_i. By the same argument, we get

$$v_k = \sum b_i v_i \tag{3}$$

$$v_k = \sum \sigma(b_i) v_i \tag{4}$$

By the minimality of the dependence relation, $b_i - \sigma(b_i)$ is zero, so the b_i are linearly dependent over F_H.

Look at the first coordinate of each vector. This tells us that $a_1, a_2, \cdots, a_k$ are linearly dependent over F_H, so extending to the full set of $s+1$ vectors does the same thing. □

1 Splitting fields

A *splitting field* of a nonconstant $f \in k[x]$ is an extension L/k such that

1. f splits in $L[x]$
2. $L = k[a_1, \ldots, a_d]$ where the a_i are the roots of f in L

Theorem. Splitting fields exist.

Proof. Take an irred factor g of f. Then

$$k \subseteq k[x]/(g) =: k_1$$

is a field extension in which g has a root $a_1 := \bar{x}$.

In $k_1[x]$, $f(x) = (x - a_1)f_1(x)$. Now f_1 is a lower-degree polynomial. Repeat. □

Lemma ("Fundamental lemma")**.** If

1. k and K are fields which are isomorphic under $\varphi : k \to K$

2. $f \in k[x]$, $F \in K[x]$

3. $l = spl_k(f), L = spl_K(F)$

then there is an isomorphism $l \to L$ extending φ.

2 Day 2

Theorem (Different definitions of normality)**.** For a field extension L/k of finite degree, TFAE:

1. L is a splitting field of some $f \in k[x]$

2. If $g \in k[x]$ is irred and has a root in L, then g splits in L.

Proof. 1. $[L : k]$ is finite, so we can pick a finite basis $\{a_i\}_i$ of L over k. Let $g_i = min_k(a_i)$ be the minimal polynomial of a_i over k, which split in L.

Now set $g = \Pi g_i$. f splits in $L[x]$ and, among possibly others, its roots include the a_i. So L is a splitting field for f. (What about minimality of the splitting field?)

2. Now we assume that L is a splitting field of $f \in k[x]$. Say $g \in k[x]$ is irred and has a root $a \in L$.

Take a splitting field S (ugh) for g over L. In particular, this is a splitting field for fg over k. We wish to show that $S = L$.

Consider another root b of $g \in S$. We have the diagram, here in two parts because I can't live-TeX properly:

$$k \subseteq k(a) \subseteq L \subseteq L(b) \subseteq S$$

$$k \subseteq k(b) \subseteq L(b) \subseteq S$$

Notice that $k(a) \cong k(b)$. In fact, this is a k-isomorphism. By the "fundamental lemma", the isom extends the obvious map that sends a to b.

The degree $[S : k(a)]$ equals $[S : k(b)]$. Now, by the tower law,

$$[L(b) : k(a)] = [L(b) : k(b)]$$
$$[L(b) : L][L : k(a)] = [L(b) : k(b)]$$

$L(b)$ is a splitting field of f over $k(b)$, and L is a splitting field of f over $k(a)$. Using the fundamental lemma again,

$$[L : k(a)] = [L(b) : k(b)]$$

which implies that $[L(b) : L] = 1$, so that $b \in L$.

□

Definition. An extension of fields is *Galois* if it is normal and separable.

Theorem (Fundamental theorem of Galois theory)**.** If L/K is a finite Galois extension, then

1. There is a bijective correspondence

$$\{\text{subgroups of } G_{L/K}\} \longleftrightarrow \{\text{intermediate fields } L/M/K\}$$

2. $G_{L/M}$ is normal in $G_{L/K}$ iff M is normal in K.

Suppose $L/M/K$ is a tower of normal extensions, so $G_{L/M}$ is normal in $G_{L/K}$. What is the quotient $G_{L/K}/G_{L/M}$?

We can restrict $\sigma \in G_{L/K}$ to M to get a K-aut of M. We need that $m \in M \implies \sigma(m) \in M$, but this holds because the minimal polynomial of $\sigma(m)$ is the same as that of m (fundamental lemma again). We get that

$$G_{L/K}/G_{L/M} \cong G_{M/K}$$

Proof.

1. Start with H and take F_H and $G = G_{L/F_H}$. We wish to show that $G = H$. First, $H \subseteq G$ "by logic". The other direction is simply that $|G| \leq [L : F_H] = |H|$, and we're done.

2. Compare $[L : M]$ and $[L : F_{G_{L/M}}] = |G_{L/M}|$. We need to show that these two are equal. First, normality of L/K implies L/M. The same goes for separability.

   So we need to show that L normal and separable implies that there are exactly $[L : M]$ of L. We will use induction.

   (a) The basis step M/M is trivial.

   (b) Take any $a \in L$, with $a \notin K$. If $m_a(x)$ is the minimal polynomial of a over K, with $\deg m_a = d$, then m_a has d distinct (because separable) roots in L (because normal).

   Say the roots are $a = a_1, a_2, \ldots, a_d$. We have

   $$K \subseteq K(a) \subseteq L$$

   where the first extension is degree d and the second one is $[L : K]/d$.

   By the induction hypothesis, we have $[L : K]/d$ K-automorphisms of L that fix a. We now want to show that there are, for each i, exactly $[L : K]/d$ K-automorphisms that send a to a_i.

   We use the standard isomorphism

   $$\varphi_i : K(a) \cong K[x]/\langle m_a(x)\rangle \cong K(a_i)$$

   Now L is a splitting field (normality) of some $f \in K[x]$, so it is the splitting field of that same f over both $K(a)$ and $K(a_i)$. Using the fundamental lemma, there is a K-automorphism of L extending φ_i sending a to a_i.

   The trick now is to compose this K-automorphism, call it σ, with the $s = [L : K]/d$ K-automorphisms of L that fix a, to get

   $$\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_s$$

   which are exactly K-automorphisms of L that send a to a_i. In all, we have $sd = [L : K]$ K-automorphisms of L.

□

3 Toward unsolvability of the quintic

Given a polynomial $f \in \mathbb{Q}[x]$, one can determine whether or not the roots of f can be computed using radicals, starting from the coefficients, by looking at $\mathrm{Gal}(L/\mathbb{Q})$. In particular, we have the following:

Theorem. f is solvable by radicals $\iff$ $\mathrm{Gal}(L/\mathbb{Q})$ is "solvable".

3.1 Solvable groups

For a group G, the *commutator* of $a, b \in G$ is the element $[a, b] := aba^{-1}b^{-1}$. The *commutator subgroup* $G' = [G, G]$ is the subgroup generated by all the commutators.

It is easily checked that G/G' is abelian. Furthermore, the commutator subgroup satisfies a kind of universal property:

Theorem. G/N is abelian $\iff$ $N \supseteq [G, G]$.

Now we define solvable groups:

Theorem. (-definition) TFAE:

1. The chain of subgroups

   $$G \supseteq G' \supseteq G'' \supseteq \cdots$$

   hits 1 after a finite number of steps.

2. There is a chain of normal subgroups (*composition series*?) of G:

   $$G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = 1$$

   where N_i/N_{i+1} is abelian for all i.

3. There is a chain as above, where each N_{i+1} is normal in N_i (but not necessarily in G).

Theorem. There are polynomials $f \in \mathbb{Q}[x]$ such that the Galois group of f ($= \mathrm{Gal}(L/\mathbb{Q})$ with $L =$ the splitting field of f over $\mathbb{Q}$) is S_5.

Here is an explicit example:

$$f(x) = 2x^5 - 10x + 5$$

How do we know?

1. $f(x)$ is 5-Eisenstein and is hence irreducible over $\mathbb{Q}$. Also, look mod 5 to notice that both (purported) polynomial factors of f must have a constant term of 0 mod 5, which would make the constant term of f divisible by 25, which it is not. (I have a feeling that this is basically Eisenstein.)

2. So the splititng field has degree divisible by 5, by the tower law. This tells us that the order of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is divisible by 5.

   Theorem (Cauchy)**.** If G is a finite group with p dividing $|G|$, then G has an order-p element.

   This tells us that $\mathrm{Gal}(L/\mathbb{Q})$ has an order-5 element. This must necessarily be a 5-cycle.

   Now a bit of graphing gives us that f has three real roots, and a pair of complex conjugates. So $z \mapsto \bar{z}$ is a transposition in the Galois group. We can now show that these two elements (the transposition and the 5-cycle) generate S_5.

4 Cubics

Theorem (Roots of a cubic)**.** The reduced cubic

$$f(x) = x^3 = ax = b$$

has roots

$$u_1 + u_2, \zeta u_1 + \zeta^2 u_2, \zeta^2 u_1 + \zeta u_2$$

where

$$u_{12} = \sqrt[3]{\frac{b}{2} \pm \sqrt{D}}$$

$$D = \frac{b^2}{4} - \frac{a^3}{27}$$

Note that to express the roots of f as radicals, you may have to go beyond a splitting field of f. (Why?)

Definition. $f \in \mathbb{Q}[x]$ is solvable by radicals if its splitting field (or, equivalently, one of its roots) is contained in some ["repeated"] *radical extension* of $\mathbb{Q}$.

Definition. A radical extension is a field F obtained from $\mathbb{Q}$ by adjoining an n-th root at each step of a finite tower.

Theorem. If (and only if) $f \in \mathbb{Q}[x]$ is solvable by radicals, the Galois group of the splitting field L, $\mathrm{Gal}(L/\mathbb{Q})$, is a solvable group.

In particular, if $\mathrm{Gal}(L/\mathbb{Q})$ is $S_n, n \geq 5$, then f is not solvable by radicals.

Sketch of proof. We have the radical extension

$$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}[a_1, a_2, \ldots, a_r]$$

which we will extend to a Galois (and still radical) extension of $\mathbb{Q}$. The idea is to take the minimal polynomials of the a_i and use the splitting field of the product F of these. Call this (normal closure?) $L*$.

We have the tower

$$\mathbb{Q} \subseteq L \subseteq L^*$$

where $\mathrm{Gal}(L^*/L)$ is normal, and $\mathrm{Gal}(L^*/\mathbb{Q})/\mathrm{Gal}(L^*/L) \cong \mathrm{Gal}(L/\mathbb{Q})$. Since quotients of solvable groups are solvable, if we can show that $\mathrm{Gal}(L^*/\mathbb{Q})$ is solvable, we are done.

To start, we adjoin all n-th roots of unity that we might need at the beginning. For instance, we use the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$$

instead of the other one to factor $x^4 - 2$.

Proposition. If K contains all n-th roots of unity and $L = K(a)$ where $a^n \in K$, then $\mathrm{Gal}(L/K)$ is abelian.

Proof. $\sigma \in \mathrm{Gal}(L/K)$ is determined by $\sigma(a)$, which must be another root of $x^n - c$.

So $\sigma : a \mapsto \zeta^k a$ for some k. Note that $\zeta \in K$ by assumption. Any two such σ will commute, since they are just multiplication maps. □

Proposition. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian.

Theorem. Obvious.

With this, the tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \cdots \subseteq \mathbb{Q}(a_1, \ldots, a_r)$$

is normal at each step, where the first extension is for the roots of unity (which is okay by the second prop.) and the others are just adjunctions of other roots, which our first proposition takes care of. □