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 $a_1, \dots, a_{s+1} \in L$. 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:

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

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. $\square$

1 Splitting fields

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. $\square$

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.

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

Theorem. If L/K is a finite Galois extension, then

1. There is a bijective correspondence between subgroups of $G_{L/K}$ and intermediate fields $L/M/K$.
2. $G_{L/M}$ is normal in $G_{L/K}$ iff M is normal in K.