

Handout 20: Galois theory, part III: the structure of the Galois group

Let's see if we can pin down the Galois group a little more precisely. We'll need a couple of preliminary lemmas:

Lemma (Corollary 5.19). Let $k \leq E \leq K$ where E is the splitting field of some polynomial $f \in k[x]$. If $\sigma \in \text{Aut}(K)$ such that σ fixes k , then $\sigma(E) = E$.

Note. We're not saying that every element of E is fixed by σ , only that as a set E is closed under the action of σ .

Proof. Let's use the fact that $E = k(z_1, \dots, z_n)$, where the z_i s are the roots of f .

Why is it true that $\sigma(E) \subseteq E$? Here's some room to check this:

In fact, since σ is injective (why?), $\sigma(E) \cong E$ as finite-dimensional vector spaces, and therefore the spaces must have the same dimension.

Thus any maximal linearly independent set of vectors in $\sigma(E)$ (*i.e.*, any basis for $\sigma(E)$) must also be a maximal linearly independent set of vectors for E . That is,

$$\sigma(E) = \text{span}(b_1, \dots, b_m) = E$$

For some basis $\{b_i\}_{i=1}^m$ of $\sigma(E)$.

Proposition (5.20). Let k be a field. If $E = k(z_1, \dots, z_n)$ for z_i algebraic over k , and if $\sigma \in \text{Aut}(E)$ fixes all z_i s, then σ is the identity automorphism on E .

Proof. Let's induct on n .

For the base case, $n = 1$, every element of $E = k(z_1)$ can be written in the form $\frac{f(z_1)}{g(z_1)}$ for $f, g \in k[x]$, $g \neq 0$. Here's some room to check that such an element is fixed by σ :

Now assume we've proven the proposition for n , and let $E = k(z_1, \dots, z_{n+1}) = (k(z_1, \dots, z_n))(z_{n+1}) = K(z_{n+1})$. Now you can do the same computation you just did above, with K in place of k :

Finally, we can prove our first really nice structural result concerning Galois groups:

Theorem (5.21). Let k be a field and let $f(x) \in k[x]$. Then the Galois group of k , $\text{Gal}(E/k)$, is isomorphic to a subgroup of S_n , where $n = \deg(f)$.

Proof. Let $X = \{z_1, \dots, z_n\}$ be the set of roots of f . Define $\phi : \text{Gal}(E/k) \rightarrow S_X$ by $\phi(\sigma) = \sigma|_X$. Here's some room for you to prove how this gives the desired result:

I'll hold off on more homework for now and let you concentrate on the problems I assigned in the last class.