

Handout 23: Galois theory, part V: two theorems and a bunch o' definitions

We're nearing the heart of Galois theory now, at which point we'll see the relationship between field extensions and descending chains of subgroups that will help us prove the insolvability of general quintic polynomials by radicals.

We'll need just a couple more preliminary results and a passel of definitions. Let's start with

Lemma (5.28). Let B/k be a splitting field for some $f(x) \in k[x]$. If $p(x) \in k[x]$ is irreducible over k but factors as a product

$$p(x) = \prod_{i=1}^t q_i(x)$$

of irreducibles over B , then all of the polynomials q_i all have the same degree.

Example. From this result we can obtain another proof of the fact that \mathbb{R} cannot be the splitting field of any $f(x) \in \mathbb{Q}[x]$. If this were the case, why is the polynomial $x^3 - 2$ at odds with the above lemma?

Proof of Lemma 5.28. For the most part this is a string of already-proven results. Work with $f(x) \in k[x] \subseteq B[x]$ and $E = B(z_1, \dots, z_n)$, where we arrange for each z_i to be a root of the corresponding $q_i(x)$. Now define the right isomorphisms and extend away!

The following result once again relates back to our example from the previous page:

Theorem (5.29). Let E/k be a field extension. Then E is the splitting field of some polynomial in $k[x]$ if and only if every polynomial in $k[x]$ that has a root in E splits in E .

Proof. One direction is easy, using the previous lemma. Which direction, and how do you prove it?

For the converse, say we know that every polynomial $f \in k[x]$ with a root in E splits over E . If $E = k$ we're done. Otherwise, we can create a chain of finite extensions

$$k \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_{t-1} \subseteq B_t = E$$

such that each is obtained from the last by adjoining a single root. Describe this process more carefully below:

The sort of extensions we've just described will be useful to us, so we'll give them a name:

Definition. Given an extension E/k , we call E a *normal* extension of k if every irreducible $p \in k[x]$ with a root in E splits in E .

Examples.

(1) Is \mathbb{R} a normal extension of \mathbb{Q} ?

(2) Is $\mathbb{Z}_5(\sqrt{2})$ a normal extension of \mathbb{Z}_5 ? (*Hint:* consider the polynomial $f(x) = x^4 + 1$.)

Here are the last definitions we'll need in order to approach the heart of Galois theory:

Definitions. Let k be a field. A *pure extension of type m* is an extension $k(u)/k$ such that $u^m \in k$ for some $m \geq 1$. An extension K/k is called a *radical extension* if there is some *radical tower* of fields

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t = K,$$

where each K_{i+1}/K_i is a pure extension of type m_i , $i = 1, \dots, t-1$.

If $f \in k[x]$ has splitting field E , we say that f is *solvable by radicals* if there is a radical extension K of k such that $E \subseteq K$.

Roughly, this is saying that we can find enough "simple radicals" to express all of the roots of f in terms of those simple radicals.

Example. Every quadratic polynomial in $\mathbb{Q}[x]$ is solvable by radicals. Indeed, let $ax^2 + bx + c \in \mathbb{Q}[x]$ be given. We may as well assume $a, b, c \in \mathbb{Z}$. Why?

Now apply a certain well-known formula to show that the roots of f lie in some pure extension of \mathbb{Q} of type 2:

On our next handout we'll work towards developing the correspondence between field extensions and sequences of subgroups.

Homework. The following problems are due on *Friday, April 24th*. Neither of them are committee problems.

- (1) Let k be a field. For each of the following sorts of extensions, state whether k is an extension of itself of the given type:
 - (a) extension
 - (b) finite extension
 - (c) algebraic extension
 - (d) normal extension
 - (e) pure extension
 - (f) radical extension
- (2) Let $k = \mathbb{Q}$ be fixed, and let \mathcal{E} be the collection of all extensions of k . Draw a Venn diagram illustrating the containment of the sets of each of the sorts of extensions of k indicated in (1), where \mathcal{E} is, of course, the universe of all elements in consideration.

If you claim that one of these sets, A , contains another B , prove it! If you claim that A *properly* contains B , prove it by giving an example of an extension of \mathbb{Q} in A but not B .