

Handout 19: Galois theory, part II: field extensions and their algebra

We've already seen that we can adjoin a single element z to field k and obtain an extension, $k(z)$, of k . Why not adjoin more than one element?

Definition. If $k \leq K$ are fields and $\{z_1, \dots, z_n\} \subseteq K$, then the field $k(z_1, \dots, z_n) \leq K$ is obtained from k by *adjoining* all of the z_i s to k ; that is, $k(z_1, \dots, z_n)$ is the intersection of all subfields of K containing k and all z_i s.

Fact. One can prove inductively that

$$k(z_1, \dots, z_n) = (k(z_1, \dots, z_{n-1}))(z_n) = \cdots \left((k(z_1))(z_2) \cdots \right) (z_n).$$

Your textbook dredges up the following fact from Chapter 4 without offering a proof; one claim is straight from our current work and the other requires that we remember a little more linear algebra.

Proposition (4.32). If K/k is a finite extension, then every $z \in K$ is algebraic over k , and if $K = k(z_1, \dots, z_n)$ where each z_i is algebraic over k , then K is a finite extension of k .

Proof. Let's start with the second claim, proving it by induction.

Here's some room to nail down a base case:

Now assume we've got it for $k(z_1, \dots, z_n)$ and consider $k(z_1, \dots, z_n, z_{n+1})$. What gives?

Now let's go the other way and assume that $[K : k] = n < \infty$. Let $z \in K$. Then consider $\{1, z, \dots, z^n\} \subseteq K$. How big is this set?

Recall that in a vector space of dimension n , any set of $n + 1$ or more vectors is linearly *dependent*; thus, there exist a_0, a_1, \dots, a_n in k such that...

Pretty cool, huh? Essentially “algebraic” extensions are the same thing as finite extensions.

We need one more definition before we continue much further; it piggybacks on something else we’ve talked about recently:

Definition. If $k \leq K$ and $f(x) \in k[x]$, then $E \leq K$ (where E/k) is a *splitting field* of f over k if f splits over E but not over any proper subfield of E .

Proposition (5.16). If $f \in k[x]$ for some field k , then there exists a splitting field E for f over k .

Proof. Let K be an extension in which f splits over k (Kronecker!), say $f(x) = a \prod (x - z_i)$. Then let $E = k(z_1, \dots, z_n)$. Here’s some room to show that E is the guy we’re looking for:

Examples.

(1) What’s the splitting field of $x^2 + 1$ over \mathbb{Q} ?

(2) How big is the splitting field of $x^2 + 1$ over $\mathbb{Z}_3[x]$?

We’re now in a position to investigate the group theoretic properties of field extensions. Our primary tool will be certain automorphisms of splitting fields.

Proposition (5.18). Let $k \leq K$ and let $f(x) \in k[x]$. If $E = k(z_1, \dots, z_n)$ and $\sigma : E \rightarrow E$ is an automorphism of E that fixes k , then σ permutes the roots of f .

Proof. The crux of the proof is the observation that if $z \in E$ is a root of f , then so is $\sigma(z)$. (Then since the roots form a finite set, σ must be a permutation, since it’s injective.) Here’s some room to verify this fact:

Recall that on a recent homework assignment you showed that the set of automorphisms of a ring is a group (under composition). In particular, if E is a field, then the set $\text{Aut}(E)$ of all automorphisms of E is a group.

This sets us up for the next important definition, about which we'll have more to say on Friday:

Definition. Let $k \leq E$ be fields. The *Galois group* of E over k , denoted $\text{Gal}(E/k)$, is the set of $\phi \in \text{Aut}(E)$ that fix k . If $f(x) \in k[x]$ and E is a splitting field of f over k , $\text{Gal}(E/k)$ is called the Galois group of f over k .

Of course, *a priori*, there's no reason that $\text{Gal}(E/k)$ should be a group, just because $\text{Aut}(E)$ is. In fact, I'll ask you to verify that fact in your homework. We'll set to work on a more careful analysis of this group's structure in our next class.

Homework. Here's something to keep you off of the streets this weekend (they're *all* committee problems):

- (1) **(CP)** Prove that if $k \leq E$ are fields then $\text{Gal}(E/k) \leq \text{Aut}(E)$. (*Hint:* just check the subgroup axioms and use facts we've recently established about elements of $\text{Gal}(E/k)$.)
- (2) **(CP)** Describe as carefully as you can the Galois group $\text{Gal}(\mathbb{C}/\mathbb{R})$.
- (3) **(CP)** Describe as carefully as you can the Galois group of $x^2 + 1$ over \mathbb{Q} .
- (4) **(CP)** Describe as carefully as you can the Galois group $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.

Here is a schedule for this homework:

- **Monday, April 13th.** Committee problems due to committees.
- **Wednesday, April 15th.** Committees present reports to class.
- **Friday, April 17th.** All homework due at 5:00 p.m.