

*Handout 24: Galois theory, part VI: to groups!*

We're finally ready to turn fields into groups. The following result is fundamental in the study of Galois groups:

**Theorem (5.31).** Let  $k \subseteq K \subseteq E$  be fields in which  $K/k$  and  $E/k$  are both normal extensions. (Recall this means that each of  $K$  and  $E$  is a splitting field of some polynomial in  $k[x]$ .) Then  $\text{Gal}(E/K) \trianglelefteq \text{Gal}(E/k)$  and

$$\text{Gal}(E/k)/\text{Gal}(E/K) \cong \text{Gal}(K/k).$$

It's worth taking a moment to process roughly what this theorem is saying: starting with an extension  $E$  of  $k$ , if we quotient out the automorphisms that fix an intermediate extension  $K$ , the resulting object can be studied by looking only at the structure of automorphisms of the intermediate extension.

This should make sense, intuitively: we're passing the information about the action of automorphisms on  $K$  from the group  $\text{Gal}(E/k)$  to the quotient group,  $\text{Gal}(K/k)$ , essentially by ignoring the portion of those maps that fix  $K$  (that portion contains no information about  $K$  anyway).

*Proof.* The corollary Theo pointed out in a recent class guarantees that any  $\sigma \in \text{Gal}(E/k)$  will fix  $K$  setwise. That is,  $\sigma(K) = K$ . Thus it makes sense for us to define  $\rho : \text{Gal}(E/k) \rightarrow \text{Gal}(K/k)$  by restriction,  $\rho(\sigma) = \sigma|_K$ .

What's the kernel of  $\rho$ , and why?

What's the image of  $\rho$ , and why?

What's the FHT for groups now tell us?

In a moment we'll discuss two more lemmas that take this theorem even further, but we first need a

**Definition.** Let  $n$  be a number. An  $n$ th root of unity is a complex number  $\zeta$  such that  $\zeta^n = 1$ . For those of you who've studied complex analysis, you may note that each  $\zeta$  has the form  $e^{2k\pi i/n}$  for some  $k \in \{0, 1, \dots, n-1\}$ .

**Proposition.** The set of  $n$ th roots of unity forms a group under the operation of multiplication, and this group is isomorphic to  $(\mathbb{Z}_n, +)$ . Any  $\zeta$  that generates this group is called a *primitive*  $n$ th root of unity, and such elements  $\zeta$  have the form  $e^{2k\pi i/n}$  where  $(n, k) = 1$ .

**Example.** Find the 4th roots of unity and draw them in the complex plane. Which ones are primitive?

**Lemma (5.33).** Let  $k$  be a field of characteristic  $\neq p$ , and let  $k(u)/k$  be a pure extension of prime type  $p$ . If  $k$  contains the  $p$ th roots of unity and if  $u \notin k$ , then  $\text{Gal}(k(u)/k) \cong \mathbb{Z}_p$ .

Note that this lemma will apply to  $k = \mathbb{C}$  since clearly it contains all roots of unity and its characteristic is 0.

*Proof of Lemma 5.33.* Let  $G = \text{Gal}(k(u)/k)$  and let  $a = u^p \in k$ . Let  $\omega$  be a primitive  $p$ th root of unity; by hypothesis,  $\omega \in k$ .

What are the roots of the polynomial  $f(x) = x^p - a$  in  $k(u)$ ? How many are there?

From the above work,  $k(u)$  must be the splitting field for  $f$  over  $k$ , and thus given  $\sigma \in G$ ,  $\sigma$  must permute the roots of  $f$ . Therefore  $\sigma(u) = \omega^i u$  for some  $i \in \mathbb{Z}_p$ .

Define  $\phi : G \rightarrow \mathbb{Z}_p$  by  $\phi(\sigma) = i$  when  $\sigma(u) = \omega^i u$ .

Here's the key question: why is  $\phi$  an isomorphism?

All righty...ready for the other shoe to drop?

**Theorem (5.34.i).** Let  $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$  be a radical tower of fields such that for all  $i = 1, \dots, t$ ,  $K_i$  is a pure extension of  $K_{i-1}$  of prime type  $p_i$  and  $p_i$  is different from the characteristic of  $k$ . Suppose also that  $k$  contains the  $p_i$ th roots of unity, for each  $p_i$ . Then if  $K_t$  is a splitting field for some polynomial  $f(x) \in k[x]$ , we have the following *descending normal sequence* of groups:

$$\text{Gal}(K_t/k) \supseteq \text{Gal}(K_t/K_1) \supseteq \text{Gal}(K_t/K_2) \supseteq \cdots \supseteq \text{Gal}(K_t/K_{t-1}) \supseteq \text{Gal}(K_t/K_t) = \{1\}.$$

Moreover, each quotient  $\text{Gal}(K_t/K_i)/\text{Gal}(K_t/K_{i+1})$  is a cyclic group of prime order.

*Proof.* The statement of the proof (long as it is!) pretty much says it all. In the space below, fill in the details, assuming that  $K_i = K_{i-1}(u_i)$ ,  $u_i^{p_i} \in K_{i-1}$ .

Our next goal will be to understand the groups that permit us to find such descending sequences inside of them...these groups are the only ones that could be Galois groups of “nice” extensions!