

*Handout 22: Galois theory, part IV: the structure of splitting fields*

When we're extending the field  $k \leq K$ , our focus is on  $k$ , and not on  $K$ , and rightly so, as we're about to see. If we're given a polynomial  $f \in k[x]$ , in some sense it doesn't matter where we find the roots which we adjoin to  $k$  to find a splitting field; the resulting splitting field will be the same no matter where we look:

**Proposition (5.22).** Let  $k$  be a field, and let  $f \in k[x]$ . Let  $E$  be a splitting field for  $f$  over  $k$ , and let  $\phi : k \rightarrow k'$  be an isomorphism of fields. We may extend this isomorphism to  $\phi^* : k[x] \rightarrow k'[x]$  in the natural fashion:

$$\phi^*(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n.$$

Let  $E'$  now be a splitting field for  $f^* = \phi^*(f)$  over  $k'$ . Then there exists an isomorphism  $\Phi : E \rightarrow E'$  such that  $\Phi|_k = \phi$ .

Your text goes further, showing how to enumerate the number of possible extensions  $\Phi$  of  $\phi$ .

*Proof.* Induct on  $[E : k]$ .

What happens is  $[E : k] = 1$ ? (What's this mean?)

Suppose  $[E : k] > 1$  and the result has been proven for any smaller degree of extension, and suppose that  $z$  is a root of  $f$  that's not in  $k$ . Let  $p$  be an irreducible polynomial in  $k[x]$  of which  $z$  is a root.

The rest of the proof consists of first extending  $\phi$  to  $\tilde{\phi} : k(z) \rightarrow k'(z')$  for the appropriate choice of  $z'$ , and then to  $\Phi$  from  $\tilde{\phi}$ . Here's some room to finish it up:

**Corollary (Theorem 5.23).** Any two splitting fields of a given polynomial over a field are isomorphic.

*Proof.* In this case we can apply the previous result, with  $k = k'$ . Here's a little space for a proof or a picture:

Immediately we have another nice result:

**Corollary (5.24).** The Galois group of a polynomial over a given field  $k$  is independent of the choice of splitting field.

**Corollary (5.25).** Any two finite fields with  $p^n$  elements are isomorphic to one another.

*Proof.* Let  $|k| = p^n$ . Recall that the set of nonzero elements of a given field is a group under multiplication, and that in a finite group the order of an element divides the order of the group. What's this say about  $a^{p^n-1}$  for any  $a \in k \setminus \{0_k\}$ ?

What does *this* then say about the roots of the polynomial  $f(x) = x(x^{p^n-1} - 1) \in \mathbb{Z}_p[x]$ ? (Note that even  $0_k$  is a root of this polynomial!)

Thus we've managed to show that  $k$  is the splitting field of a very specific polynomial over  $\mathbb{Z}_p$ ; since  $k$  was arbitrary, we're done.