

## *Handout 21: A Thoroughgoingly Ample Example*

The last couple of weeks have seen us struggle mightily with some overwhelming and often burdensome notation and terminology. All at once have come at us field extensions, splitting fields, elements algebraic and transcendental, Galois groups, and a host of other horrendous concepts and ideas.

Feeling lost, tossed, and gold-embossed?

I hope that this handout will help.

I'd just like to run through an example *thoroughly*, from start to finish, pointing out every sight along the way, showing how it all fits together, how all the bits and pieces intermesh and intertwine. If you're feeling iffy on the ideas we've studied for the past week or so, take a little while when you get this handout and run through it to make sure you understand it all.

Ready? Let's dive in...

**Example.** From now until further notice, let's assume that  $k = \mathbb{Q}$ ,  $K = \mathbb{R}$ , and  $f(x) = x^4 - 12x^2 + 35 \in k[x]$ .

We note that  $f$  is not irreducible, as indeed it can be written as  $f(x) = (x^2 - 5)(x^2 - 7)$ . However, each of these quadratic terms is irreducible over  $\mathbb{Q}$  (by Eisenstein's Criterion, for example), and so we need to look further to find a splitting field.

Although  $f$  certainly splits over  $K = \mathbb{R}$ , but  $\mathbb{R}$  is by no means efficient enough to be the splitting field  $E$  of  $f$ : by definition  $E$  will be the extension  $k(\alpha, \beta, \gamma, \delta)$ , where the four elements adjoined to  $k$  are all of the roots of  $f$ . (This is merely the smallest subfield of  $K$  containing both  $k$  and each of these four roots.)

Well, what is this extension? We easily see that  $x^2 - 5$  has roots  $\pm\sqrt{5}$  and  $x^2 - 7$  has roots  $\pm\sqrt{7}$ , so we really just have to adjoin these roots to get the desired  $E$ :

$$E = k(\pm\sqrt{5}, \pm\sqrt{7}) = k(\sqrt{5}, \sqrt{7}),$$

the latter being sufficient since clearly if  $\sqrt{5}$  is present then so is  $-\sqrt{5}$  and similarly for  $\pm\sqrt{7}$ . Of course, we could have adjoined these guys one at a time if we'd liked:

$$k(\sqrt{5}, \sqrt{7}) = (k(\sqrt{5}))(\sqrt{7}).$$

For those of you who'd really like to see how  $k(\sqrt{5})$  comes about formally, recall that

$$k(\sqrt{5}) \cong k[x]/(x^2 - 5) = \{g(x) + (x^2 - 5) \mid g(x) \in k[x]\},$$

where we identify  $\sqrt{5}$  with  $x + (x^2 - 5)$ . Then the Division Algorithm told us that

$$k(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in k\}.$$

Once we've got  $k(\sqrt{5})$  we obtain  $k(\sqrt{5}, \sqrt{7})$  from it by adjoining  $\sqrt{7}$  to  $k(\sqrt{5})$  in exactly the same fashion; thus

$$\begin{aligned} k(\sqrt{5}, \sqrt{7}) &= (k(\sqrt{5}))(\sqrt{7}) \\ &= \{A + B\sqrt{7} \mid A, B \in k(\sqrt{5})\} \\ &= \{a + b\sqrt{5} + (a' + b'\sqrt{5})\sqrt{7} \mid a, a', b, b' \in k\} \\ &= \{a + b\sqrt{5} + a'\sqrt{7} + b'\sqrt{35} \mid a, a', b, b'\}. \end{aligned}$$

This construction makes painfully obvious the fact the  $[k(\sqrt{5}, \sqrt{7}) : k] = 4$ , since the dimension of  $k(\sqrt{5}, \sqrt{7})$  as a vector space over  $k$  is 4:  $\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$  is a handy basis!

Okay, now we know a splitting field for  $f$ :  $E = k(\sqrt{5}, \sqrt{7})$  will do. Recall that this finite extension is also algebraic: any  $z \in E$  we pick will be the root of some polynomial with coefficients in  $\mathbb{Q}$ , even though proving that fact directly might be troublesome. Our next step is to see if we can figure out the Galois group  $\text{Gal}(E/k)$  corresponding to  $E$  over  $k$  (or, equivalently,  $f$  over  $k$ ).

Take  $\sigma \in \text{Gal}(E/k)$ ; that is,  $\sigma \in \text{Aut}(E)$  satisfies  $\sigma(a) = a$  for all  $a \in k$ . By one of our most recent propositions (5.18, if memory serves),  $\sigma$  must permute the roots of  $f$ . On the face of it, there are  $4! = 24$  possible permutations of the root set  $\{\pm\sqrt{5}, \pm\sqrt{7}\}$ . However, as we'll see in a moment,  $\sigma$  can't be just any old permutation.

Let's suppose that  $\sigma$  fixes  $\sqrt{5}$ . We claim that  $\sigma$  must also fix  $-\sqrt{5}$ . Indeed, let's start with the equation  $(-\sqrt{5})^2 - 5 = 0$  and apply  $\sigma$  to it:

$$\sigma((-\sqrt{5})^2 - 5) = \sigma(0) = 0 \Rightarrow (\sigma(-\sqrt{5}))^2 - \sigma(5) = 0,$$

because  $\sigma$  is a homomorphism. Since  $\sigma$  fixes  $k = \mathbb{Q}$ ,  $\sigma(5) = 5$ , and we get  $(\sigma(-\sqrt{5}))^2 = 5$ , so  $\sigma(-\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$ . Since  $\sigma$  is injective,  $\sigma(-\sqrt{5}) \neq \sqrt{5}$ , so  $\sigma(-\sqrt{5}) = -\sqrt{5}$ , as claimed.

However,  $\sigma$  might exchange  $\sqrt{7}$  and  $-\sqrt{7}$ , even if it fixes each of  $\pm\sqrt{5}$ . Likewise  $\sigma$  could fix both  $\pm\sqrt{7}$  while exchanging  $\sqrt{5}$  and  $-\sqrt{5}$ . So far this gives us 4 possible automorphisms.

Are there any other possibilities? Let's suppose that  $\sigma(\sqrt{5}) = \pm\sqrt{7}$ . Arguing much as above, let's start with the equation  $(\sqrt{5})^2 - 5 = 0$  and apply  $\sigma$ :

$$\sigma((\sqrt{5})^2 - 5) = \sigma(0) = 0 \Rightarrow (\sigma(\sqrt{5}))^2 - 5 = 0 \Rightarrow 2 = 0,$$

a contradiction. Thus  $\sigma$  can only take the two square roots of 5 to one another and similarly for the two square roots of 7. Therefore we have only the 4 permutations found above.

Our Galois group  $\text{Gal}(E/k)$  therefore consists of 4 elements, which we may write as the pairs

$$\{(\epsilon, \epsilon), (\epsilon, \leftrightarrow), (\leftrightarrow, \epsilon), (\leftrightarrow, \leftrightarrow)\},$$

where  $\epsilon$  indicates that we don't switch signs in the corresponding coordinate (first  $\sqrt{5}$ , second  $\sqrt{7}$ ), and  $\leftrightarrow$  indicates that we do.

Below is a multiplication table for this group (recall that the operation, as always for automorphisms, is composition). It's not too hard to see that the group is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , with identity element  $(\epsilon, \epsilon)$ :

$\circ$	$(\epsilon, \epsilon)$	$(\epsilon, \leftrightarrow)$	$(\leftrightarrow, \epsilon)$	$(\leftrightarrow, \leftrightarrow)$
$(\epsilon, \epsilon)$	$(\epsilon, \epsilon)$	$(\epsilon, \leftrightarrow)$	$(\leftrightarrow, \epsilon)$	$(\leftrightarrow, \leftrightarrow)$
$(\epsilon, \leftrightarrow)$	$(\epsilon, \leftrightarrow)$	$(\epsilon, \epsilon)$	$(\leftrightarrow, \leftrightarrow)$	$(\leftrightarrow, \epsilon)$
$(\leftrightarrow, \epsilon)$	$(\leftrightarrow, \epsilon)$	$(\leftrightarrow, \leftrightarrow)$	$(\epsilon, \epsilon)$	$(\epsilon, \leftrightarrow)$
$(\leftrightarrow, \leftrightarrow)$	$(\leftrightarrow, \leftrightarrow)$	$(\leftrightarrow, \epsilon)$	$(\epsilon, \leftrightarrow)$	$(\epsilon, \epsilon)$

Though we've not yet discussed the matter of "duality" between the subgroups of  $\text{Gal}(E/k)$  and the intermediate fields between  $k$  and  $E$ , it's not too hard to see that the extension  $k(\sqrt{5})$  corresponds to the subgroup  $\{(\epsilon, \epsilon), (\epsilon, \leftrightarrow)\} \cong \mathbb{Z}_2$  (this is the Galois group  $\text{Gal}(E/k(\sqrt{5}))$ ), and the extension  $k(\sqrt{7})$  corresponds to the subgroup  $\{(\epsilon, \epsilon), (\leftrightarrow, \epsilon)\} \cong \mathbb{Z}_2$  (this is the Galois group  $\text{Gal}(E/k(\sqrt{7}))$ ).

**Summary.** We've shown that the splitting field of  $f(x) = x^4 - 12x^2 + 35$  over  $\mathbb{Q}$  is  $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ , that this is a finite (and therefore algebraic) extension of degree 4 over  $\mathbb{Q}$ , and that its Galois group  $\text{Gal}(E/k) = \text{Gal}(\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q})$  is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

Questions? Comments? Anything to add? Please, discuss!