494 Lecture: Splitting fields and the primitive element theorem

Ben Gould

March 30, 2018

1 Splitting Fields

We saw previously that for any field F and (let's say irreducible) polynomial $f \in F[x]$, that there is some extension K/F such that f *splits* over K, i.e. all of the roots of f lie in K. We consider such extensions in depth now.

Definition 1.1. *For F a field and $f \in F[x]$, we say that an extension K/F is a splitting field for f provided that*

- *f splits completely over K, i.e. $f(x) = (x - a_1) \cdots (x - a_r)$ for $a_i \in K$, and*
- *K is generated by the roots of f: $K = F(a_1, ..., a_r)$.*

The second statement implies that for each $\beta \in K$ there is a polynomial $p \in F[x]$ such that $p(a_1, ..., a_r) = \beta$; in general such a polynomial is not unique (since the a_i are algebraic over F).

When F contains $\mathbb{Q}$, it is clear that the splitting field for f is unique (up to isomorphism of fields). In higher characteristic, one needs to construct the splitting field abstractly. A similar uniqueness result can be obtained.

Proposition 1.2. *Three things about splitting fields.*

1. *If $K/L/F$ is a tower of fields such that K is the splitting field for some $f \in F[x]$, K is also the splitting field of f when considered in $K[x]$.*
2. *Every polynomial over any field (!) admits a splitting field.*
3. *A splitting field is a finite extension of the base field, and every finite extension is contained in a splitting field.*

Proof. 1. Obvious!

2. We saw this sometime in the past.

3. Nontrivial. By definition, a splitting field is generated by finitely many elements algebraic over F, so it is algebraic. Conversely, suppose $K = F(b_1, ..., b_k)$. Then we may extend K to the splitting field for $\prod_{i=1}^{k} M_{b_i/F}$, where $M_{b_i/F}$ is the minimal polynomial (in this class, sometimes unfortunately referred to as "the irreducible polynomial") of b_i, for each i. □

We prove now a key result about splitting fields.

Theorem 1.3 (Splitting Theorem, Artin 16.3.2)**.** *Let K/F be a splitting field for some $f \in F[x]$. Then if $g \in K[x]$ is irreducible such that it has one root lying in K, then it splits completely over K.*

A partial converse is also true: in that case, K contains a splitting field for g. Hey, listen up: remember this theorem.

Proof. We are given a root β_1 of g in K; since g is irreducible, we have $g = M_{\beta_1/K}$. Say that the splitting field K is generated by the roots $\alpha_1, ..., \alpha_n$ of f. Choose a polynomial $p_1 \in F[T_1, ..., T_n]$ such that $p_1(\alpha) = \beta_1$.

The symmetric group S_n acts naturally on $F[T_1, ..., T_n]$ by permuting indices. Let $\{p_1, ..., p_k\}$ be the orbit of p_1 under this action, and set $\beta_j := p_j(\alpha)$. Each β_i belongs to K. We prove the theorem by showing that the polynomial

$$h(x) := (x - \beta_1) \cdots (x - \beta_k)$$

has coefficients in F. Assuming this for the moment, we see that as β_1 is a root of h, the irreducible polynomial of β_1, g, divides h. As h splits over F, so will g.

Now, say that $h = x^k - b_1x^{k-1} + b_2x^{k-2} - \cdots \pm b_k$. The coefficients b_i are obtained by evaluating the elementary symmetric functions in k-many variables at β. We introduce abstract symbols $w_1, ..., w_k$, and label the elementary symmetric functions of these variables by $s_1(w), ..., s_k(w)$ (perhaps here we will need an aside on symmetric functions, and the symmetric function theorem). Thus $b_j = s_j(\beta)$.

We examine this evaluation as follows. First, we substitute in $w = p(T)$, i.e. $w_j = p_j(T)$. As s_j is symmetric in w, $s_j \circ p_j$ is symmetric in T. Now we substitute in $T = \alpha$. A corollary of the symmetric function theorem (which I've been told to quote at will) tells us now that each $s_j(p(\alpha))$ lies in F. (This is a bit of a black box for me, too. See Artin, 16.1.12.) Of course we don't forget that $s_j(p(\alpha)) = b_j$, which finishes the proof. □

Definition 1.4. *A finite field extension K of F is called normal provided that it is the splitting field of some polynomial $f \in F[x]$.*

2 Primitive Element Theorem

In this section we depart from Artin. We aim to prove the following.

Theorem 2.1 (Primitive Element Theorem for $\mathbb{Q}$)**.** *Any finite extension of $\mathbb{Q}$ is generated by a single element. In other words, if $K/\mathbb{Q}$ is finite, then $K = \mathbb{Q}(a)$ for some $a \in K$.*

This is called the primitive element theorem because any finite extension generated by a single element is called *primitive*, with the generator called *primitive for the extension.*

We proceed by the way of three lemmas. First, for any extensions K and M of a fixed base field F, write $\mathrm{Mor}_F(K, L)$ for the set of field homomorphisms $K \to L$ such that F is fixed point-wise.

Lemma 2.2. *For a primitive extension $K(a)/K$ and an arbitrary extension M/K, we have a bijection*

$$Mor_K(K(a), M) \longrightarrow \{x \in M : M_{a/K}(x) = 0\}$$

given by $\varphi \mapsto \varphi(a)$.

Proof. First we check that the map is well-defined, i.e. that it maps into the target space. For $\varphi \in \mathrm{Mor}_K(K(a), L)$ and $x \in M$ such that $M_{a/K}(x) = 0$, we see that $M_{a/K}(\varphi(x)) = \varphi(M_{a/K}(x)) = \varphi(0) = 0$, as required.

Now consider the following simple diagram.

$$\begin{tikzcd}
K(a) \arrow[rr, dotted, "\varphi"] & & L \\
& K \arrow[ul, "g"] \arrow[ur, "f"'] &
\end{tikzcd}$$

where f and g are the (injective) field extension structure morphisms. *By definition*, this diagram commutes. To see that this map is injective, choose $F, G \in \mathrm{Mor}_K(K(a), L)$ such that $F(a) = G(a)$. For each $y \in K(a)$, write $y = k_na^n + k_{n-1}a^{n-1} + \cdots + k_0$ (why can we do this?). Then

$$F(y) = F(k_na^n + k_{n-1}a^{n-1} + \cdots + k_0)$$

$$\begin{aligned}
&= F(k_n)F(a)^n + F(k_{n-1})F(a)^{n-1} + \cdots + F(k_0)\\
&= g(k_n)G(a)^n + g(k_{n-1})G(a) + \cdots g(k_0)\\
&= G(k_n)G(a)^n + G(k_{n-1})G(a) + \cdots G(k_0)\\
&= G(y)
\end{aligned}$$

so that $F = G$.

To see that the map is also surjective, choose a root $x \in L$ of $M_{a/K}$. Consider the evaluation homomorphism $\mathrm{ev}_x : K[T] \to M$ taking $T \mapsto x$. We have $M_{a/K} \in \ker \mathrm{ev}_x$, so that we have a factorization

$$\begin{tikzcd}
K[T] \arrow[rr, "\mathrm{ev}_x"] \arrow[dr, "\pi"'] & & M \\
K(a) \arrow[r, "\sim b"] & K[T]/(M_{a/K}) \arrow[ur, "a"'] &
\end{tikzcd}$$

where a is the map induced by the first isomorphism theorem, and b is an isomorphism of fields, obtained by quotienting out by the minimal polynomial of a. Setting $F = a \circ b$, we obtain the necessary element of $\mathrm{Mor}_K(K(a), L)$, by commutativity of the diagram. □

Lemma 2.3. *For k an infinite field and V a k-vector space, there do not exist finitely many proper subspaces $V_i \subsetneq V$ such that $\bigcup_i V_i = V$.*

The proof of the second lemma is a very good exercise.

Lemma 2.4. *Let L/K and M/K be extensions with L/K finite. We have $|Mor_K(L, M)| \leq [L : K]$.*

Proof. Let $a_1, ..., a_k$ generate L over K. We induct on k: for the base case where L is generated by $a_1 = a$ over K, we have by 2.2

$$\begin{aligned}
|\mathrm{Mor}_K(L, M)| &= |\{x \in M : M_{a/K}(x) = 0\}|\\
&\leq \deg(M_{a/K})\\
&= [L : K].
\end{aligned}$$

We leave the details of the inductive case as an exercise; here is a sketch. Consider the tower

$$K(a_1, ..., a_k)/K(a_1, ..., a_{k-1})/K.$$

By induction the lower extension satisfies the desired inequality, and by the base case the upper one does as well. We need to bridge these two together, which you will do by using the fact that finite field extension degree is multiplicative. □

We dip briefly into materials not covered yet in 494, to lubricate the proof of the primitive element theorem somewhat. We take for granted two facts: first, that every field admits an algebraic closure (this is a Zorn's lemma argument that I hope you will see in the future). The second is that algebraic closures are normal. This second fact is nontrivial, and I'm happy to provide notes on it in the future. (Its proof uses a fact about normal extensions that I have not stated here, but which is totally elementary.)

We are one step away from proving the primitive element theorem. The last brick in the wall is the following.

Definition 2.5. *An element $a \in L$ of an extension L/K is called separable over K provided that all of the roots of $M_{a/K}$ in the (any) splitting field for K are order 1.*

Proposition 2.6. *Let L/K be a finite extension. The following are equivalent.*

1. *Every $a \in L$ is separable over K.*

2. $L = K(a_1, ..., a_s)$ *with each* a_i *separable over* K.

3. For every normal extension M *of* L *such that* M/K *is normal, we have* $|Mor_K(L, M)| = [L : K]$.

Proof. The proofs are mostly trivial. 1 implies 2 certainly is. 2 implies 3 uses the exact same argument as 2.2, with inequalities swapped out for equalities. We can do this since $|\{x \in M : M_{a/K}(x) = 0\}| = \deg(M_{a/K})$, as that set is nonempty (why?), M/K is normal, and a is separable over K. For 3 implies 1, prove the contrapositive, and induct. □

In this case we say that L/K is a *separable extension.* Note in particular that any extension of $\mathbb{Q}$ is separable. We've reached the end.

Proof of 2.1. Let $n = [K : \mathbb{Q}]$, and let $\varphi_1, ..., \varphi_n$ be the elements of $\mathrm{Mor}_{\mathbb{Q}}(K, \overline{L})$ (2.6). For each $i \neq j$, $\varphi_i - \varphi_j$ is a nonzero morphism of $\mathbb{Q}$-extensions; let $W_{i,j} \subset K$ be its kernel. By 2.3, we may choose $a \in K$ such that $a \notin \bigcup_{i,j} W_{i,j}$. Thus $\varphi_i(a) \neq \varphi_j(a)$ for $i \neq j$. Thus $\varphi_i|_{K(a)}$ are n distinct $\mathbb{Q}$-extension homomorphisms $K(a) \to \overline{L}$. As $\mathrm{Mor}_K(\mathbb{Q}(a), \overline{L})$ is a $\mathbb{Q}$-vector subspace of $\mathrm{Mor}_{\mathbb{Q}}(K, \overline{L})$ with the same dimension, we conclude that $K = \mathbb{Q}(a)$, as required. □