Algebra Notes

Nov. 2: Splitting Fields

Geoffrey Scott

So far, we've learned about two important ways of constructing field extensions: by adjoining elements to a field, and by quotienting a polynomial ring by an irreducible polynomial. Today, we learn another way to construct field extensions. Given a polynomial $f \in F[x]$, the *splitting field* of f over F is intuitively the field you get when you adjoint *all* the roots of f to F.

Splitting fields: definitions and examples

Definition: Let $f \in F[x]$. An extension field E of F is called a **splitting field for f over F** if the following two conditions are satisfied:

1. f factors into linear polynomials ("splits" or "splits completely") in $E[x]$.
2. f does *not* split completely in $K[x]$ for any $F \subsetneq K \subsetneq E$.

Example: $\mathbb{Q}(\sqrt{2})$ is a splitting field for $x^2 - 2$ over $\mathbb{Q}$. Let's check that the two conditions are satisfied

1. The polynomial $x^2 - 2$ splits as $(x + \sqrt{2})(x - \sqrt{2})$ in $\mathbb{Q}(\sqrt{2})[x]$.
2. Because $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, there are no fields K for which $F \subsetneq K \subsetneq E$, so the second condition is vacuously true.

Non-Example: $\mathbb{Q}(\sqrt[3]{2})$ is *not* a splitting field for $x^3 - 2$ over $\mathbb{Q}$. This is because the polynomial $x^3 - 2$ does *not* split in $\mathbb{Q}(\sqrt[3]{2})[x]$. Certainly it has a root $\sqrt[2]{2}$, and therefore it has a linear factor, $(x - \sqrt[3]{2})$, but if we divide by this linear factor, we find that

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$$

and that the second factor in the above decomposition is irreducible in $\mathbb{Q}(\sqrt[3]{2})$ (the roots of it are complex, and everything in $\mathbb{Q}(\sqrt[3]{2})$ is real).

The second example raises the question: What *is* a splitting field for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$? Well, we could take $\mathbb{Q}(\sqrt[3]{2})$ and adjoin a root of $(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2)$ (or, equivalently, take $\mathbb{Q}(\sqrt[3]{2})[x]/\langle(x^2+\sqrt[3]{2}x + (\sqrt[3]{2})^2)\rangle$). This idea of "keep adding roots of irreducible factors" is the core idea in the proof that every polynomial has a splitting field. But before we get to this proof, this discussion also leads us to the next idea: if you're studying some polynomial and you know of an extension field in which you can find *all* the roots of the polynomial, then you can obtain a splitting field by adjoining these roots to your original field.

Proposition: Let $f \in F[x]$, and E be an extension field of F. If E contains roots $\alpha_1, \ldots, \alpha_n$ of f and f splits in $F(\alpha_1, \ldots, \alpha_n)[x]$, then $F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over F.

Proof: Because f splits in $F(\alpha_1, \ldots, \alpha_n)$, it suffices to show that it doesn't split in a proper subfield containing F. If E is such a field, then it must not contain one of the roots α_i. But this would mean that f would not split in this proper field (if it did, then α_i would be a root of one of the linear factors in $E[x]$, which is impossible because $\alpha_i \notin E$).

This guarantees that if you can find "all the roots" of a polynomial in some extension field, then you can construct a splitting field easily. This is great for polyonmials in $\mathbb{Q}[x]$, because it's often easy to find roots in $\mathbb{C}$. But what about more obscure fields like $\mathbb{Z}_7$, where we don't have a firm understanding of its extension fields? In this case, it's not immediately obvious that polynomials with coefficients in these obscure fields necessarily have splitting fields – but they do!

Proposition: For any field F and any $f \in F[x]$, there is an extension E of F which is a splitting field for f over F.

Proof: Let $f = p_1 p_2 \dots p_k$ be the irreducible decomposition of f. If each p_i is linear, then f already splits completely in $F[x]$ and F is itself a splitting field for f over F. Otherwise, let p_i be a non-linear irreducible factor of f, and let $F_1 = F[x]/\langle p_i \rangle$. Then F_1 is a field extension of F in which p_i has a root α_1, so f has more linear terms in $F_1[x]$ than in $F[x]$. If $f \in F_1[x]$ still does not completely split, then we repeat the process. Eventually, f will split in $F_k[x]$, where $F_k = F(\alpha_1, \alpha_2, \dots, \alpha_k)$ for roots α_i.

Example: There are two ways to form a splitting field for $x^3 - 2$ over $\mathbb{Q}$. The first is to apply the previous proposition, which stated that if we can find roots for $x^3 - 2$ over $\mathbb{Q}$, then we can adjoin these roots. We know from high school that the roots of $x^3 - 2$ in $\mathbb{C}$ are $\{\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3}\}$, so $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3})$ is a splitting field.

The second way is to follow the proof of the proposition above. Recall that every time you form a quotient $F_k[x]/\langle p_i \rangle$ in the proof above, this field extension is the same as adjoining a root of p_i (if you can find one) to F_k therefore, the first step is to adjoin $\alpha_1 = \sqrt[3]{2}$ to get the extension $\mathbb{Q}(\sqrt[3]{2})$. In $\mathbb{Q}(\sqrt[3]{2})[x]$, the polynomial $x^3 - 2$ factors as

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$$

so we can adjoin a root of the non-linear term, $\alpha_2 = \sqrt[3]{2}(\frac{-1}{2} + \frac{\sqrt{3}}{2}i)$. Then the polynomial splits in

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}(\frac{-1}{2} + \frac{\sqrt{3}}{2}i))$$

We can slightly simplify the above description of the splitting field by noticing that it's equal to

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$$

Example: The splitting field for $(x^2 - 3)(x^2 - 5)$ is the field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. We saw that this has degree 4 over $\mathbb{Q}$ earlier in the course.

Example: The polynomial $x^4 + 4 \in \mathbb{Q}[x]$ has irreducible factorization

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

The roots of the first factor in $\mathbb{C}$ are $-1 + i$ and $-1 - i$, and the roots of the second factor are $1 + i$ and $1 - i$. Adjoining all these roots to $\mathbb{Q}$ is the same as $\mathbb{Q}(i)$. A splitting field for $x^4 + 4$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$.