Algebra Notes

Nov. 4: Splitting Fields (continued), Algebraic Extensions and Characteristic of a Field

Geoffrey Scott

Last time we proved that splitting fields exist. Today, we'll prove that every splitting field is unique, then discuss algebraic closures and the characteristic of a field.

Splitting fields are unique up to isomorphism

In the definition of a splitting field, it is not clear how many splitting fields there are for some fixed $f \in F[x]$. In this section, we prove that any two such splitting fields are isomorphic.

Observation: If $\varphi : F \to F'$ is a homomorphism, then

$$\tilde{\varphi} : F[x] \to F'[x]$$
$$a_0 + a_1 x + \cdots + a_n x^n \mapsto \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$$

is a ring homomorphism. If $\varphi : F \to F'$ is an isomorphism, then $\tilde{\varphi}$ is also an isomorphism, and for any $f \in F[x]$, it sends the ideal $\langle f \rangle$ to the ideal $\langle \tilde{\varphi}(f) \rangle$.

Proposition: Let $\varphi : F \to F'$ be an isomorphism, and $f \in F[x]$ be irreducible in $F[x]$. If α is a root of f in some extension of F, and β is a root of $\tilde{\varphi}(f)$ in some extension of F', then there is an isomorphism $\psi : F(\alpha) \to F'(\beta)$ such that $\psi(\alpha) = \beta$, and $\psi\big|_F = \varphi$.

Proof: Because f is irreducible in $F[x]$, $\varphi(f)$ is irreducible in $F'[x]$. Because $\tilde{\varphi}$ sends $\langle f \rangle$ to $\langle \tilde{\varphi}(f) \rangle$, the map $F[x] \mapsto F'[x]/\langle \tilde{\varphi}(f) \rangle$ will have kernel equal to $\langle f \rangle$, so we have an isomorphism

$$\frac{F[x]}{\langle f \rangle} \to \frac{F'[x]}{\langle \varphi(f) \rangle}$$

that sends a coset $[q]$ to $[\tilde{\varphi}(q)]$. The composition of isomorphisms

$$F(\alpha) \to \frac{F[x]}{\langle f \rangle} \to \frac{F'[x]}{\langle \tilde{\varphi}(f) \rangle} \to F'(\beta)$$

gives the desired isomorphism.

Example: We can apply the above proposition to the identity isomorphism $\mathbb{Q} \to \mathbb{Q}$, the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, and the roots $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\beta = \xi\sqrt[3]{2} \in \mathbb{C}$, where $\xi = e^{2\pi i/3}$.

The isomorphism ψ from

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_i \in \mathbb{Q}\}$$

to

$$\mathbb{Q}(\beta) = \mathbb{Q}(\xi\sqrt[3]{2}) = \{b_0 + b_1\xi\sqrt[3]{2} + b_2(\xi\sqrt[3]{2})^2 \mid b_i \in \mathbb{Q}\}$$

is the identity on $\mathbb{Q}$ and sends $\sqrt[3]{2}$ to $\xi\sqrt[3]{2}$, so by the properties of homomorphisms it sends

$$a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mapsto a_0 + a_1\xi\sqrt[3]{2} + a_2(\xi\sqrt[3]{2})^2$$

Notice also that the irreducible factorization of f in $\mathbb{Q}(\sqrt[3]{2})$ is given by

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

while the irreducible factorization of f in $\mathbb{Q}(\xi\sqrt[3]{2})$ is given by

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

and notice that $\tilde{\psi}$ sends $(x^2 - \sqrt[3]{2}x + (\sqrt[3]{2})^2)$ to $(x^2 - \xi\sqrt[3]{2}x + (\xi\sqrt[3]{2})^2)$. If we wanted to, we could apply the proposition again, applied to the isomorphism $\psi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\xi\sqrt[3]{2})$ and the polynomial $(x^2 - \sqrt[3]{2}x + (\sqrt[3]{2})^2)$. The proposition would give us new field extensions of $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\xi\sqrt[3]{2})$, and an isomorphism between these two extensions that agrees with ψ (and therefore equals the identity on $\mathbb{Q}$). This logic is the key idea in the proof that splitting fields are unique.

Theorem: Let $\varphi : F \to F'$ be an isomorphism, and f be *any* polynomial in $F[x]$. If E is a splitting field for f in F, and E' is a splitting field for $\tilde{\varphi}(f)$ in F', then there is an isomorphism $\psi : E \to E'$ such that $\psi\big|_F = \varphi$.

Proof: Let p be an irreducible factor of f of degree ≥ 2. Let $\alpha_1 \in E$ be a root of p and $\beta_1 \in E'$ be root of $\tilde{\varphi}(p)$. By the previous proposition, there is an isomorphism $F(\alpha_1) \to F'(\beta_1)$ that restricts to φ on F. If we repeat this process (until f no longer has any irreducible factors of degree ≥ 2, then we have a isomorphism $F(\alpha_1, \ldots, \alpha_k) \to F'(\beta_1, \ldots, \beta_k)$ that restricts to φ on F. Because f splits in $F(\alpha_1, \ldots, \alpha_k)$, and $\varphi(f)$ splits in $F'(\beta_1, \ldots, \beta_k)$, it follows that $E = F(\alpha_1, \ldots, \alpha_k)$ and $E' = F'(\beta_1, \ldots, \beta_k)$, which completes the proof.

Corollary: Let F be a field, and $f \in F[x]$. Any two splitting fields for f over F are isomorphic. Moreover, this isomorphism restricts to the identity isomorphism on F.

Proof: Apply the previous theorem to the case when $F' = F$ and φ is the identity map.

Corollary: Let F be a field, and $f \in F[x]$. Any splitting field for f over F is algebraic.

Proof: The construction of a splitting field consists of adjoining a finite number of algebraic elements to a field. Each of these extensions has finite degree, so the degree of the total extension will also have finite degree, and therefore be algebraic.

Algebraic Closure

The *splitting field* of a polynomial is, intuitively, the field extension obtained from adjoining all the roots of a certain polynomial to a field. As we will see, the *algebraic closure* of a field is the field extension obtained by adjoining all roots of all polynomials to a field.

Proposition: Let $F \subseteq E$ and $E \subseteq K$ be algebraic field extensions. Then $F \subseteq K$ is an algebraic field extension.

Proof: It suffices to prove that $[F(\alpha) : F] < \infty$ for every $\alpha \in K$. Since α is algebraic over E, it is the root of some polynomial $e_0 + e_1x + \cdots + e_nx^n$, where $e_i \in E$. Then

$$[F(\alpha, e_0, e_1, \ldots, e_n) : F] = [F(\alpha, e_0, e_1, \ldots, e_n) : F(e_0, e_1, \ldots, e_n)][F(e_0, e_1, \ldots, e_n) : F]$$

and both terms on the right are finite (the first because α is algebraic over $F(e_0, \ldots, e_n)$, the second because each e_i is algebraic over F), so the term on the left is finite. Since $F(\alpha)$ is a subfield of $F(\alpha, e_0, \ldots, e_n)$, it must have finite degree over F also.

Corollary: Let E be a field extension of F. If $a, b \in E$ are algebraic over F, then so are $a + b, a - b, ab$, and a/b (assuming $b \neq 0$). Hence the set of elements of E that are algebraic over F is a field.

Proof: Because $F(a,b) = F(a)(b)$ has finite degree over F (by the previous proposition), then the subfields $F(a+b), F(a-b), F(ab), F(a/b)$ of $F(a,b)$ must also have finite degree over F, hence be algebraic extensions. Therefore, the elements $a+b$, $a-b$, ab, and a/b must all be algebraic over F.

Definition: Let E be a field extension of F. The **algebraic closure of F in E** is the subfield of E consisting of all elements of E that are algebraic over F. It is an algebraic extension of F.

Characteristic of a Field

Many of the fields that we study, like $\mathbb{Q}(\sqrt{2})$ or $\mathbb{R}$ or $\mathbb{C}$, have infinitely many elements, while other fields we study, like $\mathbb{Z}_5$ or $\mathbb{Z}_2/\langle x^2+x+1\rangle$, have finitely many elements. There are some fields, such as the field of fractions of $\mathbb{Z}_5[x]$, that have infinitely many elements, but still share many similarities with finite fields, like the property that if you keep adding an element to itself, you'll eventually get zero. The definition of the *characteristic* of a field helps distinguish, conceptually, between "infinite fields that really behave like infinite fields" and "fields that may or may not be finite, but in some ways behave like finite fields."

Definition: The **characteristic** of a field is the smallest positive number n such that $1+1+\cdots+1=0$, where there are n copies of 1 written. If no such number exists (for example, in $\mathbb{Q}$) then the characteristic is zero.

Claim: The characteristic of a field is either zero or a prime number.

Proof: If the characteristic were composite, say $n = ab$, then the product of $(1+1+\cdots+1)$ (written a times) with $(1+1+\cdots+1)$ (written b times) would be zero. Since fields have no zero divisors, and n is defined to be the *smallest* positive integer such that n copies of 1 added together equals zero, this gives the contradiction.