

- c. Show that if E is a splitting field over F of a polynomial $f(x) \in F[x]$, then $G(E/F)$ can be viewed in a natural way as a certain group of permutations.
29. Let K be the splitting field of $x^3 - 2$ over \mathbb{Q} . Use Exercise 28 to show that $G(K/\mathbb{Q})$ is isomorphic with S_3 , the symmetric group on three letters. [Hint: Use Theorem 43.18 and complex conjugation to find enough elements that the Theorem of Lagrange and Exercise 28 imply the result.]
30. Show that for a prime p , the splitting field over \mathbb{Q} of $x^p - 1$ is of degree $p - 1$ over \mathbb{Q} . [Hint: Refer to Corollary 28.18.]
31. Let P be a finite set of polynomials with coefficients in the field F . Prove that a splitting field of P over F exists without using the algebraic closure of F .
32. Let $\sigma : F \rightarrow F'$ be a field isomorphism. Show that $\sigma_x : F[x] \rightarrow F'[x]$, as defined in Definition 44.4, is a ring isomorphism.

SECTION 45 SEPARABLE EXTENSIONS

Counting Zeros of Irreducible Polynomials

There is a technical issue in Galois theory that we have not yet discussed. Is it possible for an irreducible polynomial $f(x)$ over a field F to have fewer than $\deg(f(x))$ zeros in a splitting field over F ? We will see, for essentially all the fields we will consider, that the answer is no. We start with a calculus-based proof of this fact for subfields of the complex numbers.

45.1 Theorem Let $f(x)$ be an irreducible polynomial of degree n with coefficients in the field $F \leq \mathbb{C}$. Then the splitting field for $f(x)$ over F contains n distinct zeros of $f(x)$.

Proof We can assume that the coefficient of x^n is 1. We can also assume that $n \geq 2$ since otherwise the theorem is trivially true. Then

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

Since \mathbb{C} is algebraically closed, we can write $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the zeros of $f(x)$ in \mathbb{C} . Since $f(x)$ is monic and irreducible, $f(x)$ is the minimal polynomial over F for α_k . We show that no two of the α_k are equal. We use proof by contradiction and assume that two of the α_k are equal. Then in $\mathbb{C}[x]$, $f(x) = (x - \alpha_k)^2 q(x)$ for some polynomial $q(x)$. Since we are considering polynomials over \mathbb{C} , we can use the derivative of a polynomial, which we denote in the standard way as $f'(x)$. The product rule gives

$$f'(x) = 2(x - \alpha_k)q(x) + (x - \alpha_k)^2 q'(x) = (x - \alpha_k)(2q(x) + (x - \alpha_k)q'(x)).$$

Therefore α_k is a zero of $f'(x)$. By the usual formula for the derivative of a polynomial

$$f'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

and $f'(x) \in F[x]$. Since $f'(x)$ has degree $n-1 \geq 1$ and α_k is a zero of $f'(x)$, $f'(x)$ is not the minimal polynomial for α_k over F . This gives a contradiction and proves that the α_k are distinct.

We can construct a splitting field of $f(x)$ over F as a subfield of \mathbb{C} . So a splitting field for $f(x)$ over F contains n distinct zeros for $f(x)$. Since splitting fields are unique up to isomorphism, in any splitting field for $f(x)$ over F , $f(x)$ has n distinct zeros. ◆

Although the above proof applies to a special (but very important) case, essentially the same proof can be used for any field of characteristic zero. We can simply define the derivative of any polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ to be

$$D(f)(x) = f'(x) = a_1 + (2 \cdot a_2)x + (3 \cdot a_3)x^2 + \cdots + (n \cdot a_n)x^{n-1},$$

where an integer times an element in a field has the usual meaning. In calculus this formula is derived using the limit definition of derivatives. For our purposes, we simply use this formula as the definition of the derivative, $D(f)(x) = f'(x)$. Exercise 15 in Section 42 uses this definition to prove the product rule and other essential rules that are required for the proof of Theorem 45.1. Exercise 13 in this Section asks for the details of the proof of Theorem 45.2.

45.2 Theorem Let $f(x)$ be an irreducible polynomial of degree n with coefficients in a field F of characteristic zero. Then $f(x)$ contains n distinct zeros in the splitting field for $f(x)$ over F .

Proof See Exercise 13. ◆

45.3 Definition Let $f(x) \in F[x]$, and let α be a zero of $f(x)$ in a splitting field E over F . If v is the largest positive integer such that $(x - \alpha)^v$ is a factor of $f(x)$ in $E[x]$, then α is a zero of $f(x)$ with multiplicity v . ■

Definition 45.3 does not specify which splitting field over F is to be used. It can be any splitting field that contains α . In Exercise 19, you are asked to show that the definition is independent of which splitting field is used. An equivalent statement of Theorem 45.2 is that if $f(x)$ is an irreducible polynomial with coefficients in a field F of characteristic 0, then every zero of $f(x)$ in any splitting field over F has multiplicity one.

Characteristic p

We have seen that for irreducible polynomials over a field F of characteristic zero, zeros of multiplicity two or greater cannot occur. We now turn our attention to the case where the characteristic is not zero.

45.4 Theorem Let F be a finite field of characteristic p . Any irreducible polynomial $f(x) \in F[x]$ has $k = \deg(f(x))$ distinct zeros in its splitting field.

Proof Let $E \leq \bar{F}$ be the splitting field of $f(x)$ over F and α a zero of $f(x)$ in E . Then $|E| = p^n$, for some n . We can assume that the leading coefficient of $f(x)$ is 1. Therefore $f(x)$ is the minimal polynomial for α over F . By Theorem 42.3, α is a zero of the polynomial $x^{p^n} - x$, which implies that $f(x)$ divides $x^{p^n} - x$. The p^n zeros of $x^{p^n} - x$ are distinct in the algebraic closure \bar{E} by Lemma 42.8, so the linear factors of

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

must also be distinct in E , and therefore, $f(x)$ has k distinct zeros in its splitting field. ◆

Theorems 45.2 and 45.4 say that any irreducible polynomial $f(x) \in F[x]$, where the field F is either finite or it has characteristic zero, has $\deg(f(x))$ distinct zeros of multiplicity one in its splitting field over F . The next example shows that this is not the case for all infinite fields of characteristic p .

45.5 Example Let p be a prime and $E = \mathbb{Z}_p(y)$, where y is an indeterminate. We let $F = \mathbb{Z}_p(y^p) \leq E$. For convenience, we let $t = y^p$, so $F = \mathbb{Z}_p(t)$. The extension E over F is algebraic since y is a zero of the polynomial $x^p - t$. By Corollary 39.14, $\text{irr}(y, F)$ divides $x^p - t$. We can factor $x^p - t$ in E as

$$x^p - t = x^p - y^p = (x - y)^p,$$

since we are in characteristic p . Furthermore, $y \notin F$, so the degree of $\text{irr}(y, F)$ is at least two. Therefore the number of distinct zeros of $\text{irr}(y, F)$ is one, but its degree is greater than one, showing that the finite assumption in Theorem 45.4 is necessary. \blacktriangle

Counting Automorphisms

Our goal is to associate intermediate fields in a field extension $F \leq K$ with subgroups of the group of automorphisms of K that fix F . In order to apply this correspondence, it is very helpful to know the number of automorphisms under consideration. Knowing that all irreducible polynomials in F have zeros of multiplicity one in a splitting field K gives us the information we need to count the automorphisms in $G(K/F)$.

- 45.6 Definition** An irreducible polynomial $f(x) \in F[x]$ of degree n is **separable** if in the splitting field K of $f(x)$ over F , $f(x)$ has n distinct zeros. An element α in an extension field of F is **separable** if $\text{irr}(\alpha, F)$ is a separable polynomial. A field extension $F \leq E$ is **separable** if every $\alpha \in E$ is separable over F . If every finite extension of a field F is separable, then F is **perfect**. \blacksquare

It is clear that an irreducible polynomial $f(x) \in F[x]$ is separable if and only if every zero of $f(x)$ in its splitting field over F has multiplicity one.

- 45.7 Theorem** Every field of characteristic 0 is perfect and every finite field is perfect.

Proof Let $F \leq E$ be a finite field extension, where either F has characteristic 0 or F is finite. Let $g(x)$ be the minimal polynomial for $\alpha \in E$ over F . By Theorems 45.2 and 45.4, $g(x)$ has $\deg(g(x))$ distinct zeros in the splitting field of $g(x)$ over F . \blacklozenge

- 45.8 Theorem** Let K be a separable extension of the field F and E an intermediate field. Then both the extensions K over E and E over F are separable.

Proof Let $\alpha \in K$. Then $\text{irr}(\alpha, F)$ has $\deg(\alpha, F)$ zeros, each with multiplicity one, in the splitting field of $\text{irr}(\alpha, F)$ over F , as K is separable over F . Since $\text{irr}(\alpha, E)$ divides $\text{irr}(\alpha, F)$, $\text{irr}(\alpha, E)$ has $\deg(\alpha, E)$ zeros, each with multiplicity one. Thus α is separable over E and K is a separable extension of E .

We now let $\beta \in E$. Therefore, $\beta \in K$, which implies that $\text{irr}(\beta, F)$ has $\deg(\beta, F)$ zeros in the splitting field of $\text{irr}(\beta, F)$ over F . Thus E is a separable extension of F . \blacklozenge

The following theorem is very useful for our purposes. It counts the number of isomorphisms mapping an intermediate field E , of a separable splitting field $F \leq K$, onto a subfield of K . In particular, using $E = K$, the theorem tells us the number of automorphisms in $G(K/F)$.

- 45.9 Theorem** Let K be a splitting field over F and $F \leq E \leq K$. If K is a separable extension over F , then the number of isomorphisms that map E onto a subfield of K that fix all the elements of F is $[E : F]$.

Proof Let $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. We use induction on n to show that for each $1 \leq k \leq n$ the number of isomorphisms that fix elements of F and map $F(\alpha_1, \alpha_2, \dots, \alpha_k)$ onto a subfield of K is $[F(\alpha_1, \alpha_2, \dots, \alpha_k) : F]$. To save writing, we let $E_k = F(\alpha_1, \alpha_2, \dots, \alpha_k)$. For $n = 1$, $E_1 = F(\alpha_1)$ and $[E_1 : F] = \deg(\alpha_1, F)$. Furthermore, Corollary 43.19 says there is exactly one isomorphism that fixes elements of F and maps E_1 onto a subfield of K for each zero of $\text{irr}(\alpha_1, F)$ in K . Since K is a splitting field and α_1 is a zero of $\text{irr}(\alpha_1, F)$, Corollary 44.12 says that $\text{irr}(\alpha_1, F)$ splits into linear factors. But the extension E over F

is separable, so $\text{irr}(\alpha_1, F)$ has exactly $\deg(\alpha_1, F)$ zeros in K . Thus the number of isomorphisms mapping E_1 onto a subfield of K is

$$\deg(\alpha, F) = [E_1 : F].$$

We proceed with the induction step. We assume there are $[E_k : F]$ isomorphisms that fix F and map E_k onto a subfield of K . Let σ be one of these isomorphisms. We let $g(x) = \text{irr}(\alpha_{k+1}, E_k)$. Since $\sigma_x(g(x))$ is a factor of $\sigma_x(\text{irr}(\alpha_{k+1}, F)) = \text{irr}(\alpha_{k+1}, F)$, it follows that $\sigma_x(g(x))$ factors into $\deg(g(x))$ linear factors in $K[x]$. By Theorem 45.8, K is separable over E_k . Thus $\sigma_x(g(x))$ has exactly $\deg(g(x))$ distinct zeros in K . The map σ can be extended to exactly

$$\deg(\text{irr}(\alpha_{k+1}, E_k)) = [E_{k+1} : E_k]$$

isomorphisms from $E_{k+1} = E_k(\alpha_{k+1})$ onto a subfield of K by Lemma 44.5. By the induction hypothesis there are exactly $[E_k : F]$ isomorphisms σ that fix elements of F and map E_k onto a subfield of K , giving us a total of

$$[E_{k+1} : E_k] \cdot [E_k : F] = [E_{k+1} : F]$$

isomorphisms that fix elements of F and map E_{k+1} onto a subfield of K . This completes the induction step, and we conclude that there are exactly $[E_n : F] = [E : F]$ isomorphisms mapping E onto a subfield of K that fix elements of F . \blacklozenge

In the case where E is a separable splitting field over F , Theorems 44.11 and 45.9 imply that $G(E/F) = [E : F]$. However, if E is not a splitting field of F , then some of the isomorphisms fixing F and mapping E onto a subfield of K will map onto a subfield of K other than E .

45.10 Corollary Let E be a separable splitting field over F . Then $|G(E/F)| = [E : F]$.

Proof The Corollary follows immediately from Theorem 45.9. \blacklozenge

45.11 Corollary Let E be a splitting field over F where F is either a field of characteristic 0 or a finite field. Then $|G(E/F)| = [E : F]$.

Proof Since F is perfect by Theorem 45.7, the result follows from Corollary 45.10. \blacklozenge

45.12 Example In Example 43.4, we explicitly determined four automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that fix elements of \mathbb{Q} . Corollary 45.11 shows that there are exactly

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

automorphisms without explicitly writing out the formulas.

On the other hand, in Example 43.14, even though

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

there is only one automorphism of $\mathbb{Q}(\sqrt[3]{2})$. This is due to the fact that that $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field over \mathbb{Q} and Theorem 45.9 does not apply. \blacktriangle

The Primitive Element Theorem

The primitive element theorem is a classic of field theory. It says that any finite separable extension of a field is a simple extension. We will find it useful in Section 46 where we prove the Galois correspondence.

45.13 Theorem **Primitive Element Theorem** Let E be a finite separable extension of a field F . Then there is an $\alpha \in E$ such that $E = F(\alpha)$. Any such element α is called a **primitive element**.

Proof We first consider the case where F is a finite field. In this case E^* , the units in E , is a cyclic group under multiplication by Theorem 28.7. Clearly $E = F(\alpha)$ where α is a generator of the cyclic group E^* .

We next assume that F is infinite and show that if $E = F(\beta, \gamma)$, then E has a primitive element. If $\gamma \in F$, then β is a primitive element. We therefore assume that γ is not in F . We seek a primitive element of the form $\alpha = \beta + a\gamma$ where $a \in F$. Let $f(x) = \text{irr}(\beta, F)$ and $g(x) = \text{irr}(\gamma, F)$. In the splitting field of $\{f(x), g(x)\}$ over E , let $\beta = \beta_1, \beta_2, \dots, \beta_n$ be the zeros of $f(x)$ and $\gamma = \gamma_1, \gamma_2, \dots, \gamma_m$ the zeros of $g(x)$. Since γ is not in F , $m \geq 2$. The only conditions we need on the element a are that $a \in F$ and that for each $1 \leq i \leq n$ and $2 \leq j \leq m$,

$$a \neq \frac{\beta_i - \beta}{\gamma - \gamma_j}.$$

There is certainly such an element $a \in F$ due to the fact that F is infinite and we only eliminate a finite number of possible values for a . Since $\beta_1 = \beta$ and $m \geq 2$, $a \neq 0$. We let

$$\alpha = \beta + a\gamma.$$

If $\alpha = \beta_i + a\gamma_j$ for some i and $j \neq 1$, then

$$\begin{aligned}\beta_i + a\gamma_j &= \beta + a\gamma \quad \text{and} \\ a &= \frac{\beta_i - \beta}{\gamma - \gamma_j},\end{aligned}$$

which is a contradiction. Thus for any i and $j \neq 1$, $\alpha \neq \beta_i + a\gamma_j$ or equivalently,

$$\alpha - a\gamma_j \neq \beta_i.$$

We now let

$$h(x) = f(\alpha - ax) \in F(\alpha)[x].$$

Since $h(x)$ is in $F(\alpha)[x]$ and $f(x) = \text{irr}(\beta, F) \in F[x] \leq F(\alpha)[x]$, the greatest common divisor of $h(x)$ and $f(x)$ is a polynomial in $F(\alpha)[x]$. For $j \neq 1$,

$$\begin{aligned}h(\gamma) &= f(\alpha - a\gamma) = f(\beta) = 0 \quad \text{and} \\ h(\gamma_j) &= f(\alpha - a\gamma_j) \neq 0,\end{aligned}$$

since the only zeros of $f(x)$ are the β_i and $\alpha - a\gamma_j \neq \beta_i$ for any i . Therefore the only common factor of $h(x)$ and $f(x)$ is $x - \beta$, so the greatest common divisor of $h(x)$ and $f(x)$ is $x - \beta$. Thus $x - \beta \in F(\alpha)[x]$ and $\beta \in F(\alpha)$. Since $\alpha, \beta \in F(\alpha)$,

$$\gamma = \frac{\alpha - \beta}{a} \in F(\alpha).$$

We conclude that $F(\beta, \gamma) \leq F(\alpha)$. Clearly $F(\alpha) \leq F(\beta, \gamma)$, so

$$F(\alpha) = F(\beta, \gamma).$$

By a straightforward induction argument, any finite separable extension of F has a primitive element. \blacklozenge

To illustrate the construction of a primitive element for a given extension we provide the following example.

45.14 Example In Example 44.13, we saw that $\sqrt{2} + \sqrt{3}$ is a primitive element for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let us follow the proof of Theorem 45.13 to find other primitive elements $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $f(x) = \text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ and $g(x) = \text{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$. So

$$\beta = \beta_1 = \sqrt{2}, \quad \beta_2 = -\sqrt{2}, \quad \gamma = \gamma_1 = \sqrt{3}, \quad \text{and} \quad \gamma_2 = -\sqrt{3}.$$