Corollary Factorization of an Irreducible over a Splitting Field

Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$. Then $f(x)$ has the form

$$a(x - a_1)^n(x - a_2)^n \cdots (x - a_t)^n,$$

where $a_1, a_2, \ldots, a_t$ are distinct elements of E and $a \in F$.

We conclude this chapter by giving an example of an irreducible polynomial over a field that does have a multiple zero. In particular, notice that the field we use is not perfect.

EXAMPLE 9 Let $F = Z_2(t)$ be the field of quotients of the ring $Z_2[t]$ of polynomials in the indeterminate t with coefficients from Z_2. (We must introduce a letter other than x, since the members of F are going to be our coefficients for the elements in $F[x]$.) Consider $f(x) = x^2 - t \in F[x]$. To see that $f(x)$ is irreducible over F, it suffices to show that it has no zeros in F. Well, suppose that $h(t)/k(t)$ is a zero of $f(x)$. Then $(h(t)/k(t))^2 = t$, and therefore $(h(t))^2 = t(k(t))^2$. Since $h(t), k(t) \in Z_2[t]$, we then have $h(t^2) = tk(t^2)$ (see Exercise 49 in Chapter 13). But deg $h(t^2)$ is even, whereas deg $tk(t^2)$ is odd. So, $f(x)$ is irreducible over F.

Finally, since t is a constant in $F[x]$ and the characteristic of F is 2, we have $f'(x) = 0$, so that $f'(x)$ and $f(x)$ have $f(x)$ as a common factor. So, by Theorem 20.5, $f(x)$ has a multiple zero in some extension of F. (Indeed, it has a single zero of multiplicity 2 in $K = F[x]/\langle x^2 - t \rangle$.) ∎

Exercises

I have yet to see any problem, however complicated, which, when you looked at it in the right way, did not become still more complicated.

Paul Anderson, *New Scientist*

1. Describe the elements of $Q(\sqrt[3]{5})$.
2. Show that $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.
3. Find the splitting field of $x^3 - 1$ over Q. Express your answer in the form $Q(a)$.
4. Find the splitting field of $x^4 + 1$ over Q.
5. Find the splitting field of

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$$

over Q.

6. Let $a, b \in \mathbf{R}$ with $b \neq 0$. Show that $\mathbf{R}(a + bi) = \mathbf{C}$.
7. Let F be a field, and let a and b belong to F with $a \neq 0$. If c belongs to some extension of F, prove that $F(c) = F(ac + b)$. (F "absorbs" its own elements.)
8. Let $F = Z_2$ and let $f(x) = x^3 + x + 1 \in F[x]$. Suppose that a is a zero of $f(x)$ in some extension of F. How many elements does $F(a)$ have? Express each member of $F(a)$ in terms of a. Write out a complete multiplication table for $F(a)$.
9. Let $F(a)$ be the field described in Exercise 8. Express each of a^5, a^{-2}, and a^{100} in the form $c_2a^2 + c_1a + c_0$.
10. Let $F(a)$ be the field described in Exercise 8. Show that a^2 and $a^2 + a$ are zeros of $x^3 + x + 1$.
11. Describe the elements in $Q(\pi)$.
12. Let $F = Q(\pi^3)$. Find a basis for $F(\pi)$ over F.
13. Write $x^7 - x$ as a product of linear factors over Z_3. Do the same for $x^{10} - x$.
14. Find all ring automorphisms of $Q(\sqrt[3]{5})$.
15. Let F be a field of characteristic p and let $f(x) = x^p - a \in F[x]$. Show that $f(x)$ is irreducible over F or $f(x)$ splits in F.
16. Suppose that β is a zero of $f(x) = x^4 + x + 1$ in some extension field E of Z_2. Write $f(x)$ as a product of linear factors in $E[x]$.
17. Find a, b, c in Q such that

$$(1 + \sqrt[3]{4})/(2 - \sqrt[3]{2}) = a + b\sqrt[3]{2} + c\sqrt[3]{4}.$$

Note that such a, b, c exist, since

$$(1 + \sqrt[3]{4})/(2 - \sqrt[3]{2}) \in Q(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in Q\}.$$

18. Express $(3 + 4\sqrt{2})^{-1}$ in the form $a + b\sqrt{2}$, where $a, b \in Q$.
19. Show that $Q(4 - i) = Q(1 + i)$, where $i = \sqrt{-1}$.
20. Find a polynomial $p(x)$ in $Q[x]$ such that $Q(\sqrt{1 + \sqrt{5}})$ is ring-isomorphic to $Q[x]/\langle p(x)\rangle$.
21. Let $f(x) \in F[x]$ and let $a \in F$. Show that $f(x)$ and $f(x + a)$ have the same splitting field over F.
22. Recall that two polynomials $f(x)$ and $g(x)$ from $F[x]$ are said to be relatively prime if there is no polynomial of positive degree in $F[x]$ that divides both $f(x)$ and $g(x)$. Show that if $f(x)$ and $g(x)$ are relatively prime in $F[x]$, they are relatively prime in $K[x]$, where K is any extension of F.
23. Determine all of the subfields of $Q(\sqrt{2})$.

24. Describe the elements of the extension $Q(\sqrt[4]{2})$ over the field $Q(\sqrt{2})$.

25. What is the order of the splitting field of $x^5 + x^4 + 1 = (x^2 + x + 1) \cdot (x^3 + x + 1)$ over Z_2?

26. Let E be an extension of F and let a and b belong to E. Prove that $F(a, b) = F(a)(b) = F(b)(a)$.

27. Write $x^3 + 2x + 1$ as a product of linear polynomials over some extension field of Z_3.

28. Express $x^8 - x$ as a product of irreducibles over Z_2.

29. Prove or disprove that $Q(\sqrt{3})$ and $Q(\sqrt{-3})$ are ring-isomorphic.

30. For any prime p, find a field of characteristic p that is not perfect.

31. If β is a zero of $x^2 + x + 2$ over Z_5, find the other zero.

32. Show that $x^4 + x + 1$ over Z_2 does not have any multiple zeros in any extension field of Z_2.

33. Show that $x^{21} + 2x^8 + 1$ does not have multiple zeros in any extension of Z_3.

34. Show that $x^{19} + x^8 + 1$ has multiple zeros in some extension of Z_3.

35. Let F be a field of characteristic $p \neq 0$. Show that the polynomial $f(x) = x^{p^n} - x$ over F has distinct zeros.

36. Find the splitting field for $f(x) = (x^2 + x + 2)(x^2 + 2x + 2)$ over $Z_3[x]$. Write $f(x)$ as a product of linear factors.

37. Let F be a field and E an extension field of F that contains a_1, $a_2, \ldots, a_n$. Prove that $F(a_1, a_2, \ldots, a_n)$ is the intersection of all subfields of E that contain F and the set $\{a_1, a_2, \ldots, a_n\}$. (This exercise is referred to in this chapter.)

38. Find the splitting field $x^4 - x^2 - 2$ over Z_3.

39. Suppose that $f(x)$ is a fifth-degree polynomial that is irreducible over Z_2. Prove that every nonidentity element is a generator of the cyclic group $(Z_2[x]/\langle f(x)\rangle)^*$.

40. Show that $Q(\sqrt{7}, i)$ is the splitting field for $x^4 - 6x^2 - 7$.

41. Suppose that $p(x)$ is a quadratic polynomial with rational coefficients and is irreducible over Q. Show that $p(x)$ has two zeros in $Q[x]/\langle p(x)\rangle$.

42. If $p(x) \in F[x]$ and $\deg p(x) = n$, show that the splitting field for $p(x)$ over F has degree at most $n!$.

43. Let p be a prime, $F = Z_p(t)$ (the field of quotients of the ring $Z_p[x]$) and $f(x) = x^p - t$. Prove that $f(x)$ is irreducible over F and has a multiple zero in $K = F[x]/\langle x^p - t\rangle$.

44. Let $f(x)$ be an irreducible polynomial over a field F. Prove that the number of distinct zeros of $f(x)$ in a splitting field divides $\deg f(x)$.

In 1799, Gauss, at the age of 22, proved that **C** is algebraically closed. This fact was considered so important at the time that it was called the Fundamental Theorem of Algebra. Over a 50-year period, Gauss found three additional proofs of the Fundamental Theorem. Today more than 100 proofs exist. In view of the ascendancy of abstract algebra in the 20th century, a more appropriate phrase for Gauss's result would be the Fundamental Theorem of Classical Algebra.

Exercises

It matters not what goal you seek
Its secret here reposes:
You've got to dig from week to week
To get Results or Roses.

Edgar Guest

1. Prove Theorem 21.2 and Theorem 21.3.
2. Let E be the algebraic closure of F. Show that every polynomial in $F[x]$ splits in E.
3. Prove that $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ is an algebraic extension of Q but not a finite extension of Q. (This exercise is referred to in this chapter.)
4. Let E be an algebraic extension of F. If every polynomial in $F[x]$ splits in E, show that E is algebraically closed.
5. Suppose that F is a field and every irreducible polynomial in $F[x]$ is linear. Show that F is algebraically closed.
6. Suppose that $f(x)$ and $g(x)$ are irreducible over F and that $\deg f(x)$ and $\deg g(x)$ are relatively prime. If a is a zero of $f(x)$ in some extension of F, show that $g(x)$ is irreducible over $F(a)$.
7. Let a and b belong to Q with $b \neq 0$. Show that $Q(\sqrt{a}) = Q(\sqrt{b})$ if and only if there exists some $c \in Q$ such that $a = bc^2$.
8. Find the degree and a basis for $Q(\sqrt{3} + \sqrt{5})$ over $Q(\sqrt{15})$. Find the degree and a basis for $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2})$ over Q.
9. Suppose that E is an extension of F of prime degree. Show that, for every a in E, $F(a) = F$ or $F(a) = E$.
10. If $[F(a):F] = 5$, find $[F(a^3):F]$. Does your argument apply equally well if a^3 is replaced with a^2 or a^4?
11. Without using the Primitive Element Theorem, prove that if $[K:F]$ is prime, then K has a primitive element.
12. Let a be a complex number that is algebraic over Q. Show that $\sqrt{a}$ is algebraic over Q.

13. Let β be a zero of $f(x) = x^5 + 2x + 4$ (see Example 8 in Chapter 17). Show that none of $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}$ belongs to $Q(\beta)$.
14. Prove that $Q(\sqrt{2}, \sqrt[3]{2}) = Q(\sqrt[6]{2})$.
15. Let a and b be rational numbers. Show that $Q(\sqrt{a}, \sqrt{b}) = Q(\sqrt{a} + \sqrt{b})$.
16. Find the minimal polynomial for $\sqrt[3]{2} + \sqrt[3]{4}$ over Q.
17. Let K be an extension of F. Suppose that E_1 and E_2 are contained in K and are extensions of F. If $[E_1:F]$ and $[E_2:F]$ are both prime, show that $E_1 = E_2$ or $E_1 \cap E_2 = F$.
18. Let a be a nonzero algebraic element over F of degree n. Show that a^{-1} is also algebraic over F of degree n.
19. Suppose that a is algebraic over a field F. Show that a and $1 + a^{-1}$ have the same degree over F.
20. If ab is algebraic over F and $b \neq 0$, prove that a is algebraic over $F(b)$.
21. Let E be an algebraic extension of a field F. If R is a ring and $E \supseteq R \supseteq F$, show that R must be a field.
22. Prove that $\pi^2 - 1$ is algebraic over $Q(\pi^3)$.
23. If a is transcendental over F, show that every element of $F(a)$ that is not in F is transcendental over F.
24. Suppose that E is an extension of F and $a, b \in E$. If a is algebraic over F of degree m, and b is algebraic over F of degree n, where m and n are relatively prime, show that $[F(a, b):F] = mn$.
25. Let K be a field extension of F and let $a \in K$. Show that $[F(a):F(a^3)] \leq 3$. Find examples to illustrate that $[F(a):F(a^3)]$ can be 1, 2, or 3.
26. Find an example of a field F and elements a and b from some extension field such that $F(a, b) \neq F(a)$, $F(a, b) \neq F(b)$, and $[F(a, b):F] < [F(a):F][F(b):F]$.
27. Let E be a finite extension of $\mathbf{R}$. Use the fact that $\mathbf{C}$ is algebraically closed to prove that $E = \mathbf{C}$ or $E = \mathbf{R}$.
28. Suppose that $[E:Q] = 2$. Show that there is an integer d such that $E = Q(\sqrt{d})$ where d is not divisible by the square of any prime.
29. Suppose that $p(x) \in F[x]$ and E is a finite extension of F. If $p(x)$ is irreducible over F, and deg $p(x)$ and $[E:F]$ are relatively prime, show that $p(x)$ is irreducible over E.
30. Let E be an extension field of F. Show that $[E:F]$ is finite if and only if $E = F(a_1, a_2, \ldots, a_n)$, where $a_1, a_2, \ldots, a_n$ are algebraic over F.
31. If α and β are real numbers and α and β are transcendental over Q, show that either $\alpha\beta$ or $\alpha + \beta$ is also transcendental over Q.

32. Let $f(x)$ be a nonconstant element of $F[x]$. If a belongs to some extension of F and $f(a)$ is algebraic over F, prove that a is algebraic over F.

33. Let $f(x) = ax^2 + bx + c \in Q[x]$. Find a primitive element for the splitting field for $f(x)$ over Q.

34. Let $f(x)$ and $g(x)$ be irreducible polynomials over a field F and let a and b belong to some extension E of F. If a is a zero of $f(x)$ and b is a zero of $g(x)$, show that $f(x)$ is irreducible over $F(b)$ if and only if $g(x)$ is irreducible over $F(a)$.

35. Let $f(x) \in F[x]$. If $\deg f(x) = 2$ and a is a zero of $f(x)$ in some extension of F, prove that $F(a)$ is the splitting field for $f(x)$ over F.

36. Let a be a complex zero of $x^2 + x + 1$ over Q. Prove that $Q(\sqrt{a}) = Q(a)$.

37. If F is a field and the multiplicative group of nonzero elements of F is cyclic, prove that F is finite.

38. Let a be a complex number that is algebraic over Q and let r be a rational number. Show that a^r is algebraic over Q.

39. Prove that, if K is an extension field of F, then $[K:F] = n$ if and only if K is isomorphic to F^n as vector spaces. (See Exercise 27 in Chapter 19 for the appropriate definition. This exercise is referred to in this chapter.)

40. Let a be a positive real number and let n be an integer greater than 1. Prove or disprove that $[Q(a^{1/n}):Q] = n$.

41. Let a and b belong to some extension field of F and let b be algebraic over F. Prove that $[F(a, b):F(a)] \leq [F(a, b):F]$.

42. Let F, K, and L be fields with $F \subseteq K \subseteq L$. If L is a finite extension of F and $[L:F] = [L:K]$, prove that $F = K$.

43. Let F be a field and K a splitting field for some nonconstant polynomial over F. Show that K is a finite extension of F.

44. Prove that $\mathbf{C}$ is not the splitting field of any polynomial in $Q[x]$.

45. Prove that $\sqrt{2}$ is not an element of $Q(\pi)$.

46. Let $\alpha = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$ and $\beta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Prove that β is not in $Q(\alpha)$.

47. Let m be a positive integer. If a is transcendental over a field F, prove that a^m is transcendental over F.

48. Suppose K is an extension of F of degree n. Prove that K can be written in the form $F(x_1, x_2, \ldots, x_n)$ for some $x_1, x_2, \ldots, x_n$ in K.

49. Prove that there are no positive integers m and n such that $\sqrt{2}^m = \pi^n$.