

§53 Splitting Fields

Given a field K and a polynomial $f(x) \in K[x] \setminus K$, is it possible to find an extension field E of K such that $f(x)$ can be written as a product of polynomials in $E[x]$ of first degree? In this paragraph, we study this problem.

This problem is related to another important question in the theory of field extensions: whether a field isomorphism can be extended to a field isomorphism of the extension field. More precisely, if E_1/K_1 and E_2/K_2 are field extensions and if $\varphi: K_1 \rightarrow K_2$ is a field isomorphism, can we find a field isomorphism $\psi: E_1 \rightarrow E_2$ such that $\psi|_{K_1} = \varphi$? The answer is negative in general, but in the important case of simple algebraic extensions, it turns out to be positive.

Let us recall that, for any field isomorphism $\varphi: K_1 \rightarrow K_2$, we have a ring isomorphism $\hat{\varphi}: K_1[x] \rightarrow K_2[x]$ given by $(\sum_{i=0}^n a_i x^i)\hat{\varphi} = \sum_{i=0}^n (a_i \varphi) x^i$ (Lemma 33.7, Theorem 33.8).

53.1 Lemma: *Let E_1/K_1 and E_2/K_2 be field extensions and let $\varphi: K_1 \rightarrow K_2$ be a field isomorphism. Assume $f_1(x) \in K_1[x]$ is an irreducible polynomial in $K_1[x]$ and let $f_2(x) = (f_1(x))\hat{\varphi} \in K_2[x]$ be its image under $\hat{\varphi}$. Let $u_1 \in E_1$ be a root of $f_1(x)$ and $u_2 \in E_2$ a root of $f_2(x)$. Let $K_1(u_1) \subseteq E_1$ be the subfield of E_1 generated by u_1 and let $K_2(u_2) \subseteq E_2$ be the subfield of E_2 generated by u_2 . Then φ extends to an isomorphism of fields $K_1(u_1) \cong K_2(u_2)$ that maps u_1 to u_2 ; that is, there is a field isomorphism $\psi: K_1(u_1) \rightarrow K_2(u_2)$ such that $u_1\psi = u_2$ and $\psi|_{K_1} = \varphi$. Moreover, there is only one isomorphism ψ with these properties.*

Proof: We make use of Theorem 50.6 and Theorem 30.18. Since u_1 is a root of $f_1(x)$ and $f_1(x)$ is irreducible in $K_1[x]$, we see that $c_0^{-1}f_1(x)$ is the minimal polynomial of u_1 over K_1 , where c_0 is the leading coefficient of $f_1(x)$ (Theorem 50.3; as $f_1(x)$ is irreducible, it is not the zero polynomial or a polynomial of degree zero). Now $(c_0^{-1}f_1)\hat{\varphi} = (f_2)$ and from Theorem 50.6 and its proof (which depends on Theorem 30.17 and Theorem 30.18), we know that

$$\alpha: K_1(u_1) \rightarrow K_1[x]/(f_1)$$

$$\sum_i a_i u_1^i \rightarrow \sum_i a_i (x + (f_1))^i$$

is a field isomorphism. Likewise there is a field isomorphism

$$\beta: K_2(u_2) \rightarrow K_2[x]/(f_2).$$

$$\sum_i a_i u_2^i \rightarrow \sum_i a_i (x + (f_2))^i$$

Besides, we have an isomorphism of rings

$$\hat{\varphi}: K_1[x] \rightarrow K_2[x].$$

Here (f_1) is an ideal of $K_1[x]$, therefore $\text{Im } \hat{\varphi}|_{(f_1)} = (f_2)$ is an ideal of $K_2[x]$ and $K_1[x]/(f_1) \cong K_2[x]/\text{Im } \hat{\varphi}|_{(f_1)} = K_2[x]/(f_2)$ by Theorem 30.19(7). More specifically, we have the isomorphism

$$\begin{aligned} \lambda: K_1[x]/(f_1) &\rightarrow K_2[x]/(f_2). \\ g + (f_1) &\rightarrow g\hat{\varphi} + (f_2) \end{aligned}$$

Hence $\alpha\lambda\beta^{-1}: K_1(u_1) \rightarrow K_2(u_2)$ is a (ring, and therefore also a) field isomorphism. We write $\psi = \alpha\lambda\beta^{-1}$. Then $a\psi = (a\alpha)\lambda\beta^{-1} = a\lambda\beta^{-1} = [a + (f_1)]\lambda\beta^{-1} = [a + (f_2)]\beta^{-1} = a\beta^{-1} = a$ for any $a \in K_1$ (we regard K_1 as a subfield of $K_1[x]/(f_1)$ and K_2 as a subfield of $K_2[x]/(f_2)$ as in Kronecker's theorem (Theorem 51.1)) and $u_1\psi = (u_1\alpha)\lambda\beta^{-1} = (x + (f_1))\lambda\beta^{-1} = (x + (f_2))\beta^{-1} = u_2$. Thus ψ is an extension of φ such that $u_1\psi = u_2$.

The uniqueness of ψ as an extension of φ with $u_1\psi = u_2$ follows from the fact that powers of u_1 form a K_1 -basis of $K_1(u_1)$ (Theorem 50.7). Indeed, if $\mu: K_1(u_1) \rightarrow K_2(u_2)$ is a field isomorphism such that $u_1\mu = u_2$ and $\mu|_K = \varphi$,

then μ maps any element $t = \sum_i a_i u_1^i$ of $K_1(u_1)$, where $a_i \in K_1$, to $t\mu =$

$$\sum_i (a_i u_1^i)\mu = \sum_i a_i \mu(u_1\mu)^i = \sum_i a_i \varphi u_2^i = \left(\sum_i a_i u_1^i\right)\varphi = t\psi, \text{ and so } \mu = \psi. \quad \square$$

53.2 Theorem: Let E_1/K and E_2/K be field extensions and let $u_1 \in E_1$ and $u_2 \in E_2$ be algebraic over K . Then the minimal polynomial of u_1 over

K coincides with the minimal polynomial of u_2 if and only if there is an isomorphism (necessarily unique) of fields $\psi:K(u_1) \rightarrow K(u_2)$ that maps u_1 to u_2 and whose restriction to K is the identity mapping on K .

Proof: If u_1 and u_2 have the same minimal polynomial over K , then we apply Theorem 53.1 with the identity mapping $\iota: K \rightarrow K$ in place of φ and conclude that the identity isomorphism can be extended to a unique isomorphism $\psi: K(u_1) \rightarrow K(u_2)$ such that $u_1\psi = u_2$.

Conversely, suppose that $\psi:K(u_1) \rightarrow K(u_2)$ is a field isomorphism such that

$u_1\psi = u_2$ and $a\psi = a$ for all $a \in K$. Let $f(x) = \sum_{i=0}^n a_i x^i$ be the minimal poly-

nomial of u_1 over K . Then $0 = f(u_1) = \sum_{i=0}^n a_i u_1^i$. Hence $0 = 0\psi = \left(\sum_{i=0}^n a_i u_1^i\right)\psi$

$= \sum_{i=0}^n (a_i u_1^i)\psi = \sum_{i=0}^n a_i \psi u_1^i \psi = \sum_{i=0}^n a_i (u_1\psi)^i = \sum_{i=0}^n a_i u_2^i = f(u_2)$. Thus u_2 is a

root of $f(x)$ and $f(x) \in K[x]$ is a monic irreducible polynomial, which means that $f(x)$ is the minimal polynomial of u_2 over K . \square

53.3 Remark: Theorem 53.1 should not mislead the reader to believe that any field isomorphism can be extended to larger fields. Consider, for example, the isomorphism $\varphi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ given by $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$ ($a, b \in \mathbb{Q}$). Now $\mathbb{Q}(\sqrt[4]{2})$ is an extension field of $\mathbb{Q}(\sqrt{2})$. If $\varphi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ could be extended to an isomorphism $\psi: \mathbb{Q}(\sqrt[4]{2}) \rightarrow \mathbb{Q}(\sqrt[4]{2})$, we would have $-\sqrt{2} = (\sqrt{2})\varphi = (\sqrt{2})\psi = ((\sqrt[4]{2})^2)\psi = ((\sqrt[4]{2})\psi)^2$, a contradiction, since the square of $(\sqrt[4]{2})\psi \in \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ has to be positive. So φ cannot be extended to an isomorphism of $\mathbb{Q}(\sqrt[4]{2})$.

The most important application of Theorem 53.1 is that any two splitting fields of a polynomial are isomorphic. We now discuss this matter.

53.4 Definition: Let E/K be a field extension and $f(x) \in K[x] \setminus K$. If $f(x)$ can be written as a product of linear polynomials in $E[x]$, i.e., if there are $a_0, a_1, a_2, \dots, a_m$ in E such that $f(x) = a_0(x - a_1)(x - a_2) \dots (x - a_m)$, then $f(x)$ is said to *split in E* . If $f(x)$ splits in E but not in any proper subfield of E containing K , then E is called a *splitting field of $f(x)$ over K* .

53.5 Examples: (a) Consider $x^2 + 1 \in \mathbb{R}[x]$. Now $x^2 + 1 = (x - i)(x + i)$ in $\mathbb{C}[x]$, so $x^2 + 1$ splits in \mathbb{C} . It does not split in any proper subfield of \mathbb{C} containing \mathbb{R} because \mathbb{R} is the only proper subfield of \mathbb{C} containing \mathbb{R} and $x^2 + 1$ does not split in $\mathbb{R}[x]$. So \mathbb{C} is a splitting field of $x^2 + 1$ over \mathbb{R} .

\mathbb{C} is not a splitting field of $x^2 + 1$ over \mathbb{Q} , because $x^2 + 1$ splits in the field $\mathbb{Q}(i) \subset \mathbb{C}$. Now $x^2 + 1$ does not split in \mathbb{Q} which is the only proper subfield of $\mathbb{Q}(i)$ containing \mathbb{Q} . Hence $\mathbb{Q}(i)$ is a splitting field of $x^2 + 1$ over \mathbb{Q} .

(b) $\mathbb{Q}(\sqrt{2})$ is a splitting field of $x^2 - 2 \in \mathbb{Q}[x]$ over \mathbb{Q} .

(c) $x^3 - 2 \in \mathbb{Q}[x]$ does not split in $\mathbb{Q}(\sqrt[3]{2})$ because $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$ in $\mathbb{Q}(\sqrt[3]{2})[x]$ and the second factor is irreducible in $\mathbb{Q}(\sqrt[3]{2})[x]$. On the other hand, $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$ in $\mathbb{Q}(\sqrt[3]{2}, \omega)[x]$, so $x^3 - 2$ splits in $\mathbb{Q}(\sqrt[3]{2}, \omega)[x]$. In fact $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field of $x^3 - 2$ over \mathbb{Q} . Notice that $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is the field generated by the roots of $x^3 - 2$ over \mathbb{Q} .

(d) Let E/K be a field extension and $f(x) \in K[x]$ a polynomial of positive degree n . Assume that E contains n roots a_1, a_2, \dots, a_n of $f(x)$ (counted with multiplicity). Then $H = K(a_1, a_2, \dots, a_n)$ is a splitting field of $f(x)$ over K . Indeed, with the leading coefficient $a_0 \in K$, we have the factorization $f(x) = a_0(x - a_1)(x - a_2) \dots (x - a_n)$ in $H[x]$ since each factor $x - a_k$ belongs to $H[x]$. Hence $f(x)$ splits in $H[x]$. On the other hand, if L is any intermediate field of E/K in which $f(x)$ splits, then $x - a_k$ is in $L[x]$ and so a_k is in L for all k , thus $\{a_1, a_2, \dots, a_n\} \subseteq L$ and $H = K(a_1, a_2, \dots, a_n) \subseteq L$. Hence $f(x)$ does not split in any proper subfield of H containing K . Therefore, H is a splitting field of $f(x)$ over K . This argument shows in fact that $K(a_1, a_2, \dots, a_n)$ is the unique intermediate field of E/K which is a splitting field of $f(x)$ over K . In particular, E is a splitting field of $f(x)$ if and only if $E = K(a_1, a_2, \dots, a_n)$.

(e) Let E/K be a field extension, L an intermediate field of this extension and $f(x) \in K[x] \setminus K$. Assume that E is a splitting field of $f(x)$ over K . Then E is a splitting field of $f(x)$ over L , too, since $f(x)$ splits in E but not in any proper subfield of E containing K so that all the more so $f(x)$ does not split in any proper subfield of E containing L .

(f) Let p be prime. Any greatest common divisor of $x^{p^n} - x$ with its derivative $p^n x^{p^n-1} - 1 = -1$ is a unit in $\mathbb{F}_p[x]$. Hence $x^{p^n} - x \in \mathbb{F}_p[x]$ has no multiple roots (Theorem 35.18(2)). Thus an extension field of \mathbb{F}_p in which $x^{p^n} - x$ splits must have at least the p^n distinct roots of $f(x)$. We know that $x^{p^n} - x$ splits in the field \mathbb{F}_{p^n} with p^n elements (Lemma 52.4(3)). Thus \mathbb{F}_{p^n} is a splitting field of $x^{p^n} - x$ over \mathbb{F}_p .

(g) Let E/K be a field extension and $f(x) \in K[x] \setminus K$. Let $a_1 \in E$ be a root of $f(x)$ and let $L = K(a_1)$ be the subfield of E generated by a_1 over K , so that $f(x) = (x - a_1)g(x)$ for some $g(x) \in L[x]$. We claim that, if ($g(x)$ has positive degree and) E is a splitting field of $g(x)$ over L , then E is also a splitting field of $f(x)$ over K . Indeed, if E is a splitting field of $g(x)$ over L , then $g(x) = c(x - a_2)\dots(x - a_n)$ where $c \in K$ and $a_2, \dots, a_n \in E$. We know that $E = L(a_2, \dots, a_n)$ from Example 53.5(d). Then $f(x) = c(x - a_1)(x - a_2)\dots(x - a_n)$ in $E[x]$ and $f(x)$ splits in $E[x]$. On the other hand, if E' is any intermediate field of E/K and $f(x)$ splits in E' , then $c(x - a_1)(x - a_2)\dots(x - a_n)$ in $E'[x]$, so $a_1 \in E'$, so $L = K(a_1) \subseteq E'$ and $a_2, \dots, a_n \in E'$, so $L(a_2, \dots, a_n) \subseteq E'$ and $E \subseteq E'$. Thus $f(x)$ cannot split in any proper subfield of E containing K and E is a splitting field of $f(x)$ over K .

(h) We saw in Example 53.5(c) that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field of $x^3 - 2$ over \mathbb{Q} . Likewise, $\mathbb{Q}(\sqrt[3]{2})[y]/(y^2 + y + 1)$ and $\mathbb{Q}(\omega)[y]/(y^3 - 2)$ are splitting fields of $x^3 - 2$ over \mathbb{Q} (here y is an indeterminate over \mathbb{Q}). In these fields, $x^3 - 2$ splits as

$$[x - (\sqrt[3]{2} + (y^2 + y + 1))] [(x - (\sqrt[3]{2}y + (y^2 + y + 1))) [x - (\sqrt[3]{2}y^2 + (y^2 + y + 1))] \quad \text{and} \quad [x - (y + (y^3 - 2))] [x - (\omega y + (y^3 - 2))] [x - (\omega^2 y + (y^3 - 2))],$$

respectively.

A natural question is whether any polynomial has a splitting field. We show now this is indeed the case. The following theorem is due to Kronecker.

53.6 Theorem: *Let $f(x)$ be an arbitrary polynomial of positive degree over an arbitrary field K . Then there is an extension field E of K such that $|E:K| \leq (\deg f(x))!$ and E is a splitting field of $f(x)$ over K .*

Proof: We make induction on $n = \deg f(x)$. If $n = 1$, then $f(x) = c(x - a)$ for some $c, a \in K$ and so K is a splitting field of $f(x)$ over K and we have $|E:K| = 1 \leq 1!$. So the claim is established when $n = 1$.

Suppose now $\deg f(x) = n \geq 2$ and the theorem is true for any polynomial over any field if its degree is $n - 1$. We construct an extension field L of K in which $f(x)$ has a root a and $|L:K| \leq n$ (Theorem 51.5; possibly $L = K$). Then, by theorem 35.6, $f(x) = (x - a)g(x)$ for some $g(x)$ in $L[x]$. Now $\deg g(x) = n - 1$ and, by induction, there is an extension field E of L such that E is a splitting field of $g(x)$ over L and $|E:L| \leq (n - 1)!$. From Example 53.5(g), we conclude that E is a splitting field of $f(x)$ over K . Moreover, $|E:K| = |E:L||L:K| \leq (n - 1)!|L:K| \leq (n - 1)!n = n!$.

□

We see that Theorem 53.6 is nothing but repeated application of Kronecker's theorem (Theorem 51.5). We use Theorem 51.5 successively until we find a field which contains *all* the roots of $f(x)$. In the proof of Theorem 53.6, the successive adjunction of roots is replaced by an inductive argument.

We now turn to the question of uniqueness. Example 53.5(h) reveals that there can be many distinct splitting fields of a polynomial. However, as has already been remarked, all splitting fields of a polynomial are isomorphic. We prove a slightly more general theorem.

53.7 Theorem: *Let E_1/K_1 and E_2/K_2 be field extensions and let $\varphi: K_1 \rightarrow K_2$ be a field isomorphism. Let $f_1(x) \in K_1[x] \setminus K_1$ and let $f_2(x) = (f_1(x))^{\hat{\varphi}} \in K_2[x] \setminus K_2$ be its image under $\hat{\varphi}$. If E_1 is a splitting field*

of $f_1(x)$ over K_1 and E_2 is a splitting field of $f_2(x)$ over K_2 , then φ extends to a field isomorphism $\Phi: E_1 \rightarrow E_2$ and so $E_1 \cong E_2$.

Proof: E_1 is generated over K_1 by the roots of $f_1(x)$. Since each root of $f_1(x)$ is algebraic over K_1 and there are finitely many roots, Theorem 50.12 yields that $|E_1:K_1|$ is finite. We make induction on $|E_1:K_1|$.

If $|E_1:K_1| = 1$, then $E_1 = K_1$ and $f_1(x)$ splits in K_1 . Then $f_2(x)$ splits in K_2 and $K_2 = E_2$. Thus $E_1 = K_1 \xrightarrow{\varphi} K_2 = E_2$ is the desired isomorphism.

Suppose now $|E_1:K_1| \geq 2$ and suppose that any field isomorphism can be extended to an isomorphism of splitting fields of corresponding polynomials whenever the degree of a splitting field is less than or equal to $n - 1$. Since $|E_1:K_1| \geq 2$ and E is generated over K_1 by the roots of $f_1(x)$, there must be a root of $f_1(x)$ in E_1 which does not belong to K_1 . Let u_1 be a root of $f_1(x)$ in $E_1 \setminus K_1$. Assume $g_1(x) \in K_1[x]$ is the minimal polynomial of u_1 over K_1 and let u_2 be a root of $(g_1(x))^{\widehat{\varphi}} = g_2(x) \in K_2[x]$ in E_2 . From Lemma 53.1, we know that φ can be extended to an isomorphism $\psi: K_1(u_1) \rightarrow K_2(u_2)$. Now $u_1 \in E_1 \setminus K_1$, so $|K_1(u_1):K_1| > 1$ and $|E_1:K_1(u_1)| < n$ (Theorem 48.13). As E_1 is a splitting field of $f_1(x)$ over $K_1(u_1)$ and E_2 is a splitting field of $f_2(x)$ over $K_2(u_2)$ (Example 53.5(e)), we conclude, by induction, that ψ can be extended to an isomorphism $\Phi: E_1 \rightarrow E_2$. This Φ is the desired extension of φ . \square

53.8 Theorem: *Let K be a field and let $f(x)$ be any polynomial of positive degree in $K[x]$. Then any two splitting fields of $f(x)$ over K are isomorphic. In fact, the splitting fields of $f(x)$ are isomorphic by an isomorphism fixing each element of K .*

Proof: Let E_1 and E_2 be splitting fields of $f(x)$ over K and apply Theorem 53.7 with $K_1 = K = K_2$ and $\varphi = \iota =$ identity mapping on K . \square

In the remainder of this paragraph, we discuss algebraically closed fields.

53.9 Definition: A field K is said to be *algebraically closed* if K has no proper algebraic extension field, i.e., if any algebraic extension E of K coincides with K .

53.10 Theorem: Let K be a field. The following statements are equivalent.

- (i) K is algebraically closed.
- (ii) Any irreducible polynomial in $K[x]$ has degree one.
- (iii) Every polynomial of positive degree in $K[x]$ has a root in K .
- (iv) Every polynomial of positive degree in $K[x]$ splits in K .

Proof: (i) \Rightarrow (ii) Assume that K is algebraically closed. If there were an irreducible polynomial $f(x)$ in $K[x]$ with $\deg f(x) > 1$, then $E = K[x]/(f)$ would be an algebraic extension of K with $K \subset E$, contrary to the assumption that K has no proper algebraic extension. Thus every irreducible polynomial in $K[x]$ has degree one.

(ii) \Rightarrow (i) Suppose that any irreducible polynomial in $K[x]$ has degree one. We want to show that K has no proper algebraic extension. If E were a proper algebraic extension of K , then there would be an $a \in E \setminus K$. Now a is algebraic over K and $K \subset K(a)$ since $a \notin K$ (Lemma 49.6(1)). This leads to the contradiction

$$\begin{aligned} 1 < |K(a):K| &= \text{degree of the minimal polynomial of } a \text{ over } K \\ &= \text{degree of an irreducible polynomial in } K[x] = 1. \end{aligned}$$

Thus K is algebraically closed.

(ii) \Rightarrow (iii) Suppose that any irreducible polynomial in $K[x]$ has degree one. Let $f(x)$ be any polynomial of positive degree in $K[x]$. We show that $f(x)$ has a root in K . Indeed, any irreducible divisor of $f(x)$ has the form $c(x - a)$ with $c, a \in K$ and thus has a root a in K , so $f(x)$ too, has a root in a in K .

(iii) \Rightarrow (iv) Assume that any polynomial of positive degree in $K[x]$ has a root in K and let $f_1(x) \in K[x] \setminus K$. Then $f_1(x)$ has a root a_1 in K and $f_1(x) = (x - a_1)f_2(x)$ for some $f_2(x) \in K[x]$. If $f_2(x)$ has positive degree, then $f_2(x)$ has a root a_2 in K and $f_2(x) = (x - a_2)f_3(x)$ for some $f_3(x) \in K[x]$; so $f_1(x) = (x - a_1)(x - a_2)f_3(x)$. If $f_3(x)$ has positive degree, then $f_3(x)$ has a root a_3 in K and $f_3(x) = (x - a_3)f_4(x)$ for some $f_4(x) \in K[x]$; so $f_1(x)$

$= (x - a_1)(x - a_2)(x - a_3)f_4(x)$. Proceeding in this way, we will meet an $f_n(x)$ of degree zero and $f_1(x) = (x - a_1)(x - a_2)(x - a_3)\dots(x - a_n)f_n$ splits in K .

(iv) \Rightarrow (ii) Suppose every polynomial of positive degree in $K[x]$ splits in K and let $f(x)$ be an irreducible polynomial in $K[x]$. Then, by assumption, $f(x)$ is a product of $\deg f(x)$ polynomials of degree one. Since $f(x)$ is irreducible, the number $\deg f(x)$ of factors must be one: $\deg f(x) = 1$. So any irreducible polynomial in $K[x]$ has degree one. \square

An example of an algebraically closed field is \mathbb{C} . This is a consequence of the result known as the fundamental theorem of algebra, which says that any polynomial with complex coefficients has a root in \mathbb{C} . The name 'fundamental theorem of algebra' is grotesk, for this is neither a fundamental theorem nor a theorem of algebra! Any proof of this result is bound to use some results from analysis.

53.11 Lemma: *Let E/K be a field extension and assume that E is algebraically closed. Let A be the algebraic closure of K in E (Definition 50.15). Then A is an algebraically closed field.*

Proof: It suffices to prove that any polynomial in $A[x] \setminus A$ has a root in A . Let $f(x)$ be a polynomial of positive degree in $A[x]$. Then $f(x)$ is a polynomial of positive degree in $E[x]$ and therefore has a root b in E (Theorem 53.10). Then $A(b)$ is an algebraic extension of A and A is an algebraic extension of K , so $A(b)$ is an algebraic extension of K (Theorem 50.16). Consequently $b \in A(b)$ is algebraic over K and hence $b \in A$ by the definition of A .

\square

53.12 Definition: Let E/K be a field extension. If E is an algebraic extension of K and E is algebraically closed, then E is called an *algebraic closure of K* .

Does every field K have an algebraic closure? The answer is 'yes' and its proof requires Zorn's Lemma. There is no algebraic difficulty in the proof, but there are certain set-theoretical subtleties and we will not give the proof in this book. It is also true that an algebraic closure of a field K is unique in the sense that any two algebraic closures of a field K are isomorphic by an isomorphism that fixes each element of K .

Exercises

1. Construct a splitting field over \mathbb{Q} of
 - (a) $x^2 - 3$;
 - (b) $x^2 - 5$;
 - (c) $x^2 - p$, where $p \in \mathbb{N}$ is a prime number;
 - (d) $x^5 - 1$;
 - (e) $x^p - 1$, where $p \in \mathbb{N}$ is a prime number;
 - (f) $x^4 - 5x^2 + 6$;
 - (g) $x^6 - 10x^4 + 31x^2 - 30$;
 - (h) $x^5 + 3x^4 + x^3 - 8x^2 - 6x + 4$;
 - (i) $x^4 - x^2 + 1$.
2. Let K be a field and let $f(x) \in K[x]$ be of degree $n > 0$. If E is a splitting field of $f(x)$ over K , show that $|E:K|$ divides $n!$.
3. What is the difference between an algebraic closure of a field K and the algebraic closure of K in an extension field?
4. Prove that a finite field cannot be algebraically closed.