

§50 Algebraic Extensions

Let E/K be a field extension and let $a \in E$ be algebraic over K . Then there is a nonzero polynomial f in $K[x]$ such that $f(a) = 0$. Hence the subset $A = \{f \in K[x] : f(a) = 0\}$ of $K[x]$ does not consist only of 0. We observe that A is an ideal of $K[x]$, because A is the kernel of the substitution homomorphism $T_a: K[x] \rightarrow E$.

Thus A is an ideal of $K[x]$ and $A \neq \{0\}$. Since $K[x]$ is a principal ideal domain, $A = K[x]f_0 = (f_0)$ for some nonzero polynomial f_0 in $K[x]$. For any polynomial $g \in K[x]$, the relation $(g) = A = (f_0)$ holds if and only if g and f_0 are associate in $K[x]$, that is to say, if and only if $g(x) = cf_0(x)$ for some c in K^\times . There is a unique $c_0 \in K^\times$ such that the leading coefficient of $c_0f_0(x)$ is equal to 1. With this c_0 , we put $g_0(x) = c_0f_0(x)$. Then g_0 is the unique monic polynomial in $K[x]$ satisfying $(g_0) = A = \{f \in K[x] : f(a) = 0\}$, and $f(a) = 0$ for a polynomial f in $K[x]$ if and only if $g_0|f$ in $K[x]$. In particular, we have $\deg g_0 \leq \deg f$ for any $f \in K[x]$ having a as a root.

In this way, we associate with $a \in E$ a unique monic polynomial g_0 in $K[x]$. This g_0 is the monic polynomial in $K[x]$ of least degree having a as a root.

g_0 is irreducible over K : if there are polynomials $p(x), q(x)$ in $K[x]$ with $g_0(x) = p(x)q(x)$, $1 \leq \deg p(x) < \deg g_0(x)$ and $1 \leq \deg q(x) < \deg g_0(x)$, then $0 = g_0(a) = p(a)q(a)$ would imply $p(x) \in A$ or $q(x) \in A$, hence $g_0|p$ or $g_0|q$ in $K[x]$, which is impossible in view of the conditions on $\deg p(x)$ and $\deg q(x)$.

0

We proved the following theorem.

50.1 Theorem: *Let E/K be a field extension and $a \in E$. If a is algebraic over K , then there is a unique nonzero monic polynomial $g(x)$ in $K[x]$ such that*

$$\text{for all } f(x) \in K[x], \quad f(x) = 0 \text{ if and only if } g(x)|f(x) \text{ in } K[x].$$

In particular, a is a root of $g(x)$ and $g(x)$ has the smallest degree among the nonzero polynomials in $K[x]$ admitting a as a root. Moreover, $g(x)$ is irreducible over K . \square

50.2 Definition: Let E/K be a field extension and let $a \in E$ be algebraic over K . The unique polynomial $g(x)$ of Theorem 50.1 is called the *minimal polynomial of a over K* .

The minimal polynomial of a over K is also called the *irreducible polynomial of a over K* . Given an element a of E , algebraic over K , and a polynomial $h(x)$ in $K[x]$, in order to find out whether $h(x)$ is the minimal polynomial of a over K , it seems we had to check whether $h(x)|f(x)$ for all the polynomials $f(x) \in K[x]$ having a as a root. Fortunately, there is another characterization of minimal polynomials.

50.3 Theorem: Let E/K be a field extension and $a \in E$. Assume that a is algebraic over K . Let $h(x)$ be a nonzero polynomial in $K[x]$. If

- (i) $h(x)$ is monic,
- (ii) a is a root of $h(x)$,
- (iii) $h(x)$ is irreducible over K ,

then $h(x)$ is the minimal polynomial of a over K .

Proof: We must show only that $h(x)$ divides any polynomial $f(x) \in K[x]$ having a as a root. Let $f(x)$ be a polynomial in $K[x]$ and assume that a is a root of $f(x)$. We divide $f(x)$ by $h(x)$ and get

$$f(x) = q(x)h(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg h(x)$$

with suitable $q(x), r(x) \in K[x]$. Substituting a for x , we obtain

$$0 = f(a) = q(a)h(a) + r(a) = q(a)0 + r(a) = r(a).$$

If $r(x)$ were distinct from the zero polynomial in $K[x]$, then the irreducible polynomial $h(x)$ would have a common root a with the polynomial $r(x)$ whose degree is smaller than the degree of $h(x)$. This is impossible by Theorem 35.18(4). Hence $r(x) = 0$ and $f(x) = q(x)h(x)$. Therefore $h(x)|f(x)$ for any polynomial $f(x) \in K[x]$ having a as a root, as was to be proved. \square

50.4 Examples: (a) Let us find the minimal polynomial of $i \in \mathbb{C}$ over \mathbb{R} . Since i is a root of the polynomial $x^2 + 1 \in \mathbb{R}[x]$, which is monic and irreducible over \mathbb{R} , Theorem 50.3 tells us that $x^2 + 1$ is the minimal polynomial of i over \mathbb{R} . In the same way, we see that $x^2 + 1 \in \mathbb{Q}[x]$ is the minimal polynomial of i over \mathbb{Q} . On the other hand, $x^2 + 1 \in (\mathbb{Q}(i))[x]$ is not irreducible over $\mathbb{Q}(i)$, because $x^2 + 1 = (x - i)(x + i)$ in $(\mathbb{Q}(i))[x]$. Now $x - i$ is a monic irreducible polynomial in $(\mathbb{Q}(i))[x]$ having i as a root, and thus $x - i$ is the minimal polynomial of $i \in \mathbb{C}$ over $\mathbb{Q}(i)$.

(b) Let us find the minimal polynomial of $u = \sqrt{2} + \sqrt{3} \in \mathbb{R}$ over \mathbb{Q} . The calculations

$$\begin{aligned} u &= \sqrt{2} + \sqrt{3} \\ u - \sqrt{2} &= \sqrt{3} \\ u^2 - 2\sqrt{2}u + 2 &= 3 \end{aligned}$$

(u)

$$\begin{aligned} u^2 - 1 &= 2\sqrt{2}u \\ u^4 - 2u^2 + 1 &= 8u^2 \\ u^4 - 10u^2 + 1 &= 0 \end{aligned}$$

show that $\sqrt{2} + \sqrt{3}$ is a root of the monic polynomial $f(x) = x^4 - 10x^2 + 1$ in $\mathbb{Q}[x]$. We will prove that $f(x)$ is irreducible over \mathbb{Q} . Theorem 50.3 will then yield that $f(x)$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} .

In view of Lemma 34.11, it will be sufficient to show that $f(x)$ is irreducible over \mathbb{Z} . Since the numbers $\mp 1/\mp 1 = \mp 1$ are not roots of $f(x)$, we learn from Theorem 35.10 (rational root theorem) that $f(x)$ has no polynomial factor in $\mathbb{Z}[x]$ of degree one. If there were a factorization in $\mathbb{Z}[x]$ of $f(x)$ into two polynomials of degree two, which we may assume to be

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

(e)

without loss of generality, then the integers a, b, c, d would satisfy

$$a + c = 0, \quad d + ac + b = -10, \quad ad + bc = 0, \quad bd = 1$$

and this would force $b = d = \mp 1$ and the first two equations would give

$$\begin{aligned} a + c = 0, \quad ac = -12 & \quad \text{or} & \quad a + c = 0, \quad ac = -8 \\ a^2 = 12 & \quad \text{or} & \quad a^2 = 8, \end{aligned}$$

whereas no integer has a square equal to 8 or 12. Thus $f(x)$ is irreducible in $\mathbb{Z}[x]$ and, as remarked earlier, $f(x)$ is therefore the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} .

The irreducibility of $f(x)$ of degree four over \mathbb{Q} could be proved by showing the irreducibility of another polynomial, of degree *less* than four, over a field *larger* than \mathbb{Q} . As this gives a deeper insight to the problem at hand, we will discuss this method. The equation (u) states that $\sqrt{2} + \sqrt{3}$ is a root of the polynomial $f_2(x) = x^2 - 2\sqrt{2}x - 1 \in (\mathbb{Q}(\sqrt{2}))[x]$. Let $g(x) \in (\mathbb{Q}(\sqrt{2}))[x]$ be the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. Then $g(x)|f_2(x)$ in $(\mathbb{Q}(\sqrt{2}))[x]$ and, if $g(x) \neq f_2(x)$, then $\deg g(x)$ would be one and $g(x)$ would be $x - (\sqrt{2} + \sqrt{3})$, since the latter is the unique monic polynomial of degree one having $\sqrt{2} + \sqrt{3}$ as a root. But $g(x) \in (\mathbb{Q}(\sqrt{2}))[x]$ and this would imply $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so $\sqrt{3} = m + n\sqrt{2}$ with suitable $m, n \in \mathbb{Q}$, where certainly $m \neq 0 \neq n$, so $3 = m^2 + 2\sqrt{2}mn + n^2$, so $\sqrt{2} = (3 - m^2 - 2n^2)/2mn$ would be a rational number, a contradiction. Thus $f_2(x) = g(x)$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$.

Now the irreducibility of $f(x)$ over \mathbb{Q} follows very easily. $f(x)$ has no factor of degree one in $\mathbb{Q}[x]$. If $f(x)$ had a factorization (e) in $\mathbb{Q}[x]$, where a, b, c, d are rational numbers (not necessarily integers), then $\sqrt{2} + \sqrt{3}$ would be a root of one of the factors on the right hand side of (e), say of $x^2 + ax + b$. But then $x^2 + ax + b$, being a polynomial in $(\mathbb{Q}(\sqrt{2}))[x]$ having $\sqrt{2} + \sqrt{3}$ as a root, would be divisible, in $(\mathbb{Q}(\sqrt{2}))[x]$, by the minimal poly-nomial $f_2(x) = x^2 - 2\sqrt{2}x - 1$ of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. Comparing degrees and leading coefficients, we would obtain $x^2 - 2\sqrt{2}x - 1 = x^2 + ax + b$, so $2\sqrt{2} = -a \in \mathbb{Q}$, a contradiction. Hence $f(x)$ is irreducible over \mathbb{Q} .

The next lemma crystalizes the argument employed in the last example.

50.5 Lemma: *Let $K_1 \subseteq K_2 \subseteq E$ be fields and $a \in E$. If a is algebraic over K_1 , then a is algebraic over K_2 . Moreover, if f_1, f_2 are, respectively, the minimal polynomials of a over K_1 and K_2 , then $f_2|f_1$ in $K_2[x]$.*

Proof: If a is algebraic over K_1 and $f_1(x)$ is the minimal polynomial of a over K_1 , then $f_1(a) = 0$. Since $f_1(x) \in K_1[x] \subseteq K_2[x]$, we conclude that a is algebraic over K_2 . Then, from $f_1(a) = 0$ and $f_1(x) \in K_2[x]$, we obtain $f_2(x)|f_1(x)$ in $K_2[x]$ by the very definition of the minimal polynomial $f_2(x)$ of a over K_2 . \square

We proceed to describe simple algebraic extensions. Let us recall that we found $\mathbb{Q}[i] = \mathbb{Q}(i)$. This situation obtains whenever we consider a simple extension generated by an algebraic element.

50.6 Theorem: *Let E/K be a field extension and $a \in E$. Assume that a is algebraic over K and let f be its minimal polynomial over K . We denote by $K[x]f =: (f)$ the principal ideal generated by f in $K[x]$. Then*

$$K(a) = K[a] \cong K[x]/(f).$$

Proof: Consider the substitution homomorphism $T_a: K[x] \rightarrow E$. Here $\text{Ker } T_a = \{h \in K[x]: h(a) = 0\} = (f)$ by Theorem 50.1 and $\text{Im } T_a = K[a]$ by Lemma 49.5(1). Hence $K[x]/(f) = K[x]/\text{Ker } T_a \cong \text{Im } T_a = K[a]$.

It remains to show $K(a) = K[a]$. Since $K[a] \subseteq K(a)$, we must prove only $K(a) \subseteq K[a]$. To this end, we need only prove that $1/g(a) \in K[a]$ for any $g(x) \in K[x]$ with $g(a) \neq 0$ (Lemma 49.5). Indeed, if $g(x) \in K[x]$ and $g(a) \neq 0$, then $f \nmid g$ and, since f is irreducible in $K[x]$, the polynomials $f(x)$ and $g(x)$ are relatively prime in $K[x]$ (Theorem 35.18(3)). Thus there are polynomials $r(x), s(x)$ in $K[x]$ such that

$$f(x)r(x) + g(x)s(x) = 1.$$

Substituting a for x and using $f(a) = 0$, we obtain $g(a)s(a) = 1$. Hence $1/g(a) = s(a) \in K[a]$. This proves $K[a] = K(a)$. (Another proof. Since $K[x]$ is a principal ideal domain and f is irreducible in $K[x]$, the factor ring $K[x]/(f)$ is a field by Theorem 32.25; thus $K[a]$, being a ring isomorphic to the field $K[x]/(f)$, is a subfield of E , and $K[a]$ contains K and a . So $K(a) \subseteq K[a]$ and $K(a) = K[a]$.)

□

50.7 Theorem: *Let E/K be a field extension and $a \in E$. Suppose that a is algebraic over K and let f be its minimal polynomial over K . Then*

$$[K(a):K] = \deg f$$

(the degree of the field $K(a)$ over K is the degree of the minimal polynomial f in $K[x]$). *In fact, if $\deg f = n$, then $\{1, a, a^2, \dots, a^{n-1}\}$ is a K -basis of $K(a)$ and every element in $K(a)$ can be written in the form*

$$k_0 + k_1 a + k_2 a^2 + \dots + k_{n-1} a^{n-1} \quad (k_0, k_1, k_2, \dots, k_{n-1} \in K)$$

in a unique way.

Proof: We prove that $\{1, a, a^2, \dots, a^{n-1}\}$ is a K -basis of $K(a)$. Let us show that it spans $K(a)$ over K . We know $K(a) = K[a]$ from Theorem 50.6 and $K[a] = \{g(a) \in E : g \in K[x]\}$ from Lemma 49.5(1). Thus any element u of $K(a)$ can be written as $g(a)$, where $g(x)$ is a suitable polynomial in $K[x]$. Dividing this polynomial $g(x)$ by $f(x)$, which has degree n , we get

$$g(x) = q(x)f(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) \leq n - 1$$

with some polynomials $q(x), r(x)$ in $K[x]$. Substituting a for x , we obtain

$$u = g(a) = q(a)f(a) + r(a) = q(a)0 + r(a) = r(a).$$

If, say, $r(x) = k_0 + k_1x + k_2x^2 + \dots + k_{n-1}x^{n-1}$, where $k_0, k_1, k_2, \dots, k_{n-1} \in K$,

then
$$u = k_0 + k_1a + k_2a^2 + \dots + k_{n-1}a^{n-1}$$

and thus $\{1, a, a^2, \dots, a^{n-1}\}$ spans $K(a)$ over K .

Now let us show that $\{1, a, a^2, \dots, a^{n-1}\}$ is linearly independent over K . If $k_0, k_1, k_2, \dots, k_{n-1}$ are elements of K such that

$$k_0 + k_1a + k_2a^2 + \dots + k_{n-1}a^{n-1} = 0,$$

then a is a root of the polynomial $h(x) = k_0 + k_1x + k_2x^2 + \dots + k_{n-1}x^{n-1}$ in $K[x]$, so $f(x) | h(x)$ by Theorem 50.1. Here $h(x) \neq 0$ would yield the contradiction $n = \deg f \leq \deg h \leq n - 1$. Therefore $h(x) = 0$, which means that $k_0 = k_1 = k_2 = \dots = k_{n-1} = 0$. Hence $\{1, a, a^2, \dots, a^{n-1}\}$ is linearly independent over K .

This proves $\{1, a, a^2, \dots, a^{n-1}\}$ is a K -basis of $K(a)$. It follows that

$$|K(a):K| = \dim_K K(a) = |\{1, a, a^2, \dots, a^{n-1}\}| = n = \deg f(x)$$

and, by Theorem 42.8, every element of $K(a)$ can be written uniquely in the form

$$k_0 + k_1a + k_2a^2 + \dots + k_{n-1}a^{n-1}. \quad \square$$

50.8 Definition: Let E/K be a field extension and $a \in E$. Suppose a is algebraic over K . Then the degree of its minimal polynomial over K , which is also the degree of $K(a)$ over K , is called the *degree of a over K* .

50.9 Examples: (a) The minimal polynomial of $i \in \mathbb{C}$ over \mathbb{Q} is the polynomial $x^2 + 1$ in $\mathbb{Q}[x]$ (Example 50.4(a)), and $x^2 + 1$ has degree 2. Thus $i \in \mathbb{C}$ is (algebraic and) has degree 2 over \mathbb{Q} . Likewise, the minimal polynomial of $i \in \mathbb{C}$ over \mathbb{R} is $x^2 + 1 \in \mathbb{R}[x]$ and i has degree 2 over \mathbb{R} .

(b) The minimal polynomial of $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ over \mathbb{Q} was found to be $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ (Example 50.4(b)). Thus $\sqrt{2} + \sqrt{3}$ has degree 4 over \mathbb{Q} . This follows also from Theorem 50.7. In fact, the numbers $1, \sqrt{2}$ form a \mathbb{Q} -basis of the field $\mathbb{Q}(\sqrt{2})$, hence $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2$. Observe that

$$\begin{array}{r|l}
 & \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
 & \\
 & \\
 x^4 - 10x^2 + 1 & \\
 \text{degree 4} & \mathbb{Q}(\sqrt{2}) \\
 & \\
 & \\
 & \mathbb{Q}
 \end{array}
 \begin{array}{l}
 \\
 \\
 \\
 x^2 - 2\sqrt{2}x + 1 \\
 \text{degree 2} \\
 \\
 x^2 - 2 \\
 \text{degree 2} \\
 \\
 \\
 \end{array}$$

$\sqrt{2} = -\frac{9}{2}(\sqrt{2} + \sqrt{3}) + \frac{1}{2}(\sqrt{2} + \sqrt{3})^3$, so $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and therefore $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Thus $\mathbb{Q}(\sqrt{2})$ is an intermediate field of the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$. From Theorem 48.13, we infer that

$$\begin{aligned}
 4 = |\mathbb{Q}(\sqrt{2} + \sqrt{3}):\mathbb{Q}| &= |\mathbb{Q}(\sqrt{2} + \sqrt{3}):\mathbb{Q}(\sqrt{2})| |\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = |\mathbb{Q}(\sqrt{2} + \sqrt{3}):\mathbb{Q}(\sqrt{2})| 2 \\
 &|\mathbb{Q}(\sqrt{2} + \sqrt{3}):\mathbb{Q}(\sqrt{2})| = 2
 \end{aligned}$$

and $\sqrt{2} + \sqrt{3}$ has degree 2 over $\mathbb{Q}(\sqrt{2})$.

(c) Since $x^2 + 1 \in \mathbb{R}[x]$ is the minimal polynomial of $i \in \mathbb{C}$ over \mathbb{R} , Theorem 50.6 states that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}(i)$. In the ring $\mathbb{R}[x]/(x^2 + 1)$, we have the equality $x^2 + \mathbb{R}[x](x^2 + 1) = -1 + \mathbb{R}[x](x^2 + 1)$, and calculations are carried out just as in the ring $\mathbb{R}[x]$, but we replace $[x + \mathbb{R}[x](x^2 + 1)]^2 = x^2 + \mathbb{R}[x](x^2 + 1)$ by $-1 + \mathbb{R}[x](x^2 + 1)$. In the same way, calculations are carried out in $\mathbb{R}(i) = \mathbb{C}$ just as though i were an indeterminate over \mathbb{R} , and we write -1 for i^2 wherever we see i^2 . This is what the isomorphism $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}(i) = \mathbb{C}$ means.

(d) Likewise, if E/K is a field extension and $a \in E$, and if a is algebraic over K with the minimal polynomial $x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0$ over K so that

$$a^n = -c_{n-1}a^{n-1} - c_{n-2}a^{n-2} - \cdots - c_1a - c_0,$$

then $K(a)$ consists of the elements

$$k_0 + k_1a + \cdots + k_{n-2}a^{n-2} + k_{n-1}a^{n-1} \quad (k_0, k_1, \dots, k_{n-2}, k_{n-1} \in K)$$

and computations are carried out in $K(a)$ just as though a were an indeterminate over K and then replacing a^n by $-c_{n-1}a^{n-1} - c_{n-2}a^{n-2} - \cdots - c_1a - c_0$ wherever it occurs.

For instance, writing a for $\sqrt{2} + \sqrt{3} \in \mathbb{R}$, we have $a^4 = 10a^2 - 1$ in $\mathbb{Q}(a)$. If $t = 2 + a - a^2 + 3a^3 \in \mathbb{Q}(a)$ and $u = a + a^2 + 2a^3 \in \mathbb{Q}(a)$, then

$$t + u = 2 + 2a + 5a^3 \in \mathbb{Q}(a)$$

and

$$\begin{aligned} tu &= (2 + a - a^2 + 3a^3)(a + a^2 + 2a^3) \\ &= 2a + 2a^2 + 4a^3 + a^2 + a^3 + 2a^4 - a^4 - a^4 - 2a^5 + 3a^4 + 3a^5 + 6a^6 \\ &= 2a + 3a^2 + 4a^3 + 4a^4 + a^5 + 6a^6 \\ &= 2a + 3a^2 + 4a^3 + 4(10a^2 - 1) + a(10a^2 - 1) + 6a^2(10a^2 - 1) \\ &= 2a + 3a^2 + 4a^3 + 40a^2 - 4 + 10a^3 - a + 60(10a^2 - 1) - 6a^2 \\ &= -64 + a + 637a^2 + 14a^3 \in \mathbb{Q}(a). \end{aligned}$$

Let us find the inverse of $a^2 + a + 1$. According to Theorem 50.6, we must find polynomials $r(x), s(x)$ in $\mathbb{Q}[x]$ such that

$$(x^4 - 10x^2 + 1)r(x) + (x^2 + x + 1)s(x) = 1$$

and this we do by the Euclidean algorithm:

$$\begin{aligned} x^4 - 10x^2 + 1 &= (x^2 - x - 10)(x^2 + x + 1) + (11x + 11) \\ x^2 + x + 1 &= \left(\frac{1}{11}x\right)(11x + 11) + 1, \end{aligned}$$

so that

$$\begin{aligned} 1 &= (x^2 + x + 1) - \left(\frac{1}{11}x\right)(11x + 11) \\ &= (x^2 + x + 1) - \left(\frac{1}{11}x\right)[(x^4 - 10x^2 + 1) - (x^2 - x - 10)(x^2 + x + 1)] \\ &= (x^2 + x + 1)\left(1 + \left(\frac{1}{11}x\right)(x^2 - x - 10)\right) - \left(\frac{1}{11}x\right)(x^4 - 10x^2 + 1), \\ 1 &= (x^2 + x + 1)\left(\frac{1}{11}x^3 - \frac{1}{11}x^2 - \frac{10}{11}x + 1\right) - \left(\frac{1}{11}x\right)(x^4 - 10x^2 + 1) \end{aligned}$$

and, substituting a for x , we get

$$1 = (a^2 + a + 1)\left(\frac{1}{11}a^3 - \frac{1}{11}a^2 - \frac{10}{11}a + 1\right),$$

$$1/(a^2 + a + 1) = \frac{1}{11}a^3 - \frac{1}{11}a^2 - \frac{10}{11}a + 1.$$

Notice that a is treated here merely as a symbol that satisfies the relation $a^4 - 10a^2 + 1 = 0$. The *numerical* value of $a = \sqrt{2} + \sqrt{3} = 3.14626337\dots$ as a real number is totally ignored. This is algebra, the calculus of symbols. This allows enormous flexibility: we can regard a as an element in *any* extension field E of \mathbb{Q} in which the polynomial $x^4 - 10x^2 + 1$ has a root. This idea will be pursued in the next paragraph.

50.10 Theorem: *Let E/K be a finite dimensional extension. Then E is algebraic over K and also finitely generated over K .*

Proof: Let $[E:K] = n \in \mathbb{N}$. To prove that E is algebraic over K , we must show that every element of a is a root of a nonzero polynomial in $K[x]$. If u is an arbitrary element of E , then the $n + 1$ elements $1, u, u^2, \dots, u^{n-1}, u^n$ of E cannot be linearly independent over K , by Steinitz' replacement theorem. Thus there are $k_0, k_1, k_2, \dots, k_{n-1}, k_n$ in K , not all of them zero, with

$$k_0 + k_1u + k_2u^2 + \dots + k_{n-1}u^{n-1} + k_nu^n = 0.$$

Then $g(x) = k_0 + k_1x + k_2x^2 + \dots + k_{n-1}x^{n-1} + k_nx^n$ is a nonzero polynomial in $K[x]$, in fact of degree $\leq n$, and u is a root of $g(x)$. Thus u is algebraic over K . Since u was arbitrary, E is algebraic over K .

Secondly, if $\{b_1, b_2, \dots, b_n\} \subseteq E$ is a K -basis of E , then

$$\begin{aligned} E = s_K(b_1, b_2, \dots, b_n) &= \{k_1b_1 + k_2b_2 + \dots + k_nb_n\} \\ &\subseteq \{f(b_1, b_2, \dots, b_n) \in E : f \in K[x_1, x_2, \dots, x_n]\} \\ &= K(b_1, b_2, \dots, b_n) \\ &\subseteq E, \end{aligned}$$

thus $E = K(b_1, b_2, \dots, b_n)$ is finitely generated over K . □

As a separate lemma, we record the fact that the polynomial $g(x)$ in the preceding proof has degree $\leq n$.

50.11 Lemma: *Let E/K be a field extension of degree $|E:K| = n \in \mathbb{N}$. Then every element of E is algebraic over K and has degree over K at most equal to n . \square*

Next we show that an extension generated by algebraic elements is algebraic.

50.12 Theorem: *Let E/K be a field extension and let $a_1, a_2, \dots, a_{n-1}, a_n$ be finitely many elements in E . Suppose that $a_1, a_2, \dots, a_{n-1}, a_n$ are algebraic over K . Then $K(a_1, a_2, \dots, a_{n-1}, a_n)$ is an algebraic extension of K . In fact, $K(a_1, a_2, \dots, a_{n-1}, a_n)$ is a finite dimensional extension of K and*

$$|K(a_1, a_2, \dots, a_{n-1}, a_n):K| \leq |K(a_1):K| |K(a_2):K| \dots |K(a_n):K|$$

Proof: Let $r_1 = |K(a_1):K|$. For each $i = 2, \dots, n-1, n$, the element a_i is algebraic over K , hence also algebraic over $K(a_1, \dots, a_{i-1})$ by Lemma 50.5. This lemma yields, in addition, that the minimal polynomial of a_i over the field $K(a_1, \dots, a_{i-1})$ is a divisor of the minimal polynomial of a_i over K ; so, comparing the degrees of these minimal polynomials and using Theorem 50.7, we get $r_i := |(K(a_1, \dots, a_{i-1}))(a_i):K(a_1, \dots, a_{i-1})| \leq |K(a_i):K|$, this for all $i = 2, \dots, n-1, n$. From

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \dots \subseteq K(a_1, a_2, \dots, a_{n-1}) \subseteq K(a_1, a_2, \dots, a_{n-1}, a_n)$$

and
$$K(a_1, \dots, a_{i-1}, a_i) = (K(a_1, \dots, a_{i-1}))(a_i) \quad \text{for } i = 2, \dots, n-1, n$$

(Lemma 49.6(2)), we obtain

$$|K(a_1, a_2, \dots, a_{n-1}, a_n):K| = r_n r_{n-1} \dots r_2 r_1 \quad \text{(Theorem 48.13)}$$

$$\leq |K(a_n):K| |K(a_{n-1}):K| \dots |K(a_2):K| |K(a_1):K|.$$

Thus $K(a_1, a_2, \dots, a_{n-1}, a_n)$ is a finite dimensional extension of K and, by Theorem 50.10, an algebraic extension of K . \square

50.13 Lemma: *Let E/K be a field extension and $a, b \in E$. If a and b are algebraic over K , then $a + b$, $a - b$, ab and a/b (in case $b \neq 0$) are algebraic over K .*

Proof: If a and b are algebraic over K , then $K(a, b)$ is an algebraic extension of K by Theorem 50.12: every element of $K(a, b)$ is algebraic over K . Since $a + b$, $a - b$, ab and a/b are in $K(a, b)$, they are algebraic over K . \square

50.14 Theorem: *Let E/K be a field extension and let A be the set of all elements of E which are algebraic over K . Then A is a subfield of E (and an intermediate field of the extension E/K).*

Proof: If $a, b \in A$, then a and b are algebraic over K , then $a + b$, $-b$, ab and $1/b$ (the last in case $b \neq 0$) are algebraic over K by Lemma 50.13 and so A is a subfield of E by Lemma 48.2. Since any element of K is algebraic over K (Example 49.8(a)), we have $K \subseteq A$. Thus A is an intermediate field of E/K .

\square

50.15 Definition: Let E/K be a field extension and let A be the subfield of E in Theorem 50.14 consisting exactly of the elements of E which are algebraic over K . Then A is called the *algebraic closure of K in E* .

A is of course an algebraic extension of K . In fact, if $a \in E$, then a is algebraic over K if and only if $a \in A$; and if F is an intermediate field of E/K , then F is algebraic over K if and only if $F \subseteq A$.

The last theorem in this paragraph states that an algebraic extension of an algebraic extension is an algebraic extension, sometimes referred to as the transitivity of algebraic extensions.

50.16 Theorem: *Let F, E, K be fields. If F is an algebraic extension of E and E is an algebraic extension of K , then F is an algebraic extension of K .*

Proof: We must show that every element of F is algebraic over K . Let $u \in F$. Since F is algebraic over E , its element u is algebraic over E , and there is a polynomial $f(x) \in E[x]$ with $f(u) = 0$, say

$$f(x) = e_0 + e_1x + \cdots + e_nx^n.$$

We put $L = K(e_0, e_1, \dots, e_n)$. Then clearly $f(x) \in L[x]$. Since E is algebraic over K , each of e_0, e_1, \dots, e_n is algebraic over K and Theorem 50.12 tells us that L/K is finite dimensional. Also, since $f(u) = 0$ and $f(x) \in L[x]$, we see that u is algebraic over L and Theorem 50.7 tells us that $L(u)/L$ is finite dimensional. So $|L(u):K| = |L(u):L| |K(e_0, e_1, \dots, e_n):K|$ is a finite number: $L(u)$ is a finite dimensional extension of K . By Theorem 50.10, $L(u)$ is an algebraic extension of K . So every element of $L(u)$ is algebraic over K . In particular, since $u \in L(u)$, we see that u is algebraic over K . Since u is an arbitrary element of F , we conclude that F is an algebraic extension of K . \square

50.17 Definition: Let K and L be subfields of a field E . The subfield of E generated by $K \cup L$ over P , where P is the prime subfield of E , is called the *compositum* of K and L , and denoted by KL .

So $KL = P(K \cup L)$ by definition. It follows immediately from this definition that $KL = LK$. The compositum KL is the smallest subfield of E containing both K and L , whence $KL = K(L) = L(K)$.

In order to define the compositum of two fields K and L , it is necessary that these be contained in a larger field. If K and L are not subfields of a common field, we cannot define the compositum KL .

If E/K is a field extension and $a, b \in E$, then the compositum $K(a)K(b)$ of $K(a)$ and $K(b)$ is $K(P \cup \{a, b\}) = K(a, b)$.

Exercises

1. Find the minimal polynomials of the following numbers over the fields indicated.

- | | |
|---|---|
| (a) $\sqrt{2}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$. |
| (b) $\sqrt{3} - \sqrt{2}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$. |
| (c) $\sqrt{2} + \sqrt{3} + \sqrt{5}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2} + \sqrt{5})$. |
| (d) $\sqrt[3]{2} + \sqrt{2}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[4]{2})$. |
| (e) $\sqrt[3]{2} + \sqrt{3}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt{2} + \sqrt{3})$. |
| (f) $\sqrt{3 + \sqrt{2}}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2})$. |
| (g) $\sqrt[3]{-1 + \sqrt{2}}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$. |
| (h) $\sqrt[3]{-1 - \sqrt{2}}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$. |
| (j) $\sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}}$ | over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$. |

2. Let E/K be an extension of fields and let D be an integral domain such that $K \subseteq D \subseteq E$. Prove that, if E is algebraic over K , then D is a field.

3. Let E/K be an extension of fields and a_1, a_2, \dots, a_m elements of E which are algebraic over K . Prove that $K[a_1, a_2, \dots, a_m] = K(a_1, a_2, \dots, a_m)$.

4. Let E/K be a field extension and $a, b \in E$. If a is algebraic of degree m over K and b is algebraic of degree n over K , show that $K(a, b)$ is an algebraic extension of K and that $|K(a, b):K| \leq mn$. If, in addition, m and n are relatively prime, then in fact $|K(a, b):K| = mn$.

5. Let E/K be a field extension and L, M intermediate fields. Prove the following statements.

- $|LM:K|$ is finite if and only if both $|L:K|$ and $|M:K|$ are finite.
- If $|LM:K|$ is finite, then $|L:K|$ and $|M:K|$ divide $|LM:K|$.
- If $|L:K|$ and $|M:K|$ are finite and relatively prime, then $|LM:K|$ is equal to $|L:K||M:K|$.
- If L and M are algebraic over K , then LM is algebraic over K .
- If L is algebraic over K , then LM is algebraic over M .

6. A complex number u is said to be an algebraic integer if u is the root of a monic polynomial in $\mathbb{Z}[x]$. Prove the following statements.

- If $c \in \mathbb{C}$ is algebraic over \mathbb{Q} , then there is a natural number n such that nc is an algebraic integer.
- If $u \in \mathbb{Q}$ and u is an algebraic integer, then $u \in \mathbb{Z}$.

(c) Let $f(x)$ and $g(x)$ be monic polynomials in $\mathbb{Q}[x]$. If $f(x)g(x) \in \mathbb{Z}[x]$, then $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$. (Hint: consider contents.)

(d) If $u \in \mathbb{C}$ is an algebraic integer, then the minimal polynomial of u over \mathbb{Q} is in fact a polynomial in $\mathbb{Z}[x]$.