

Algebraic Extensions

1. Let K be a field and E an extension of K . One writes this assumption in short as

Let E/K be a field extension,

and the word “field” is often omitted when it can be inferred from the context.

An element α of E is called *algebraic over K* if there exists a polynomial $f(X) \neq 0$ in $K[X]$ such that

$$f(\alpha) = 0.$$

If α is not algebraic over K , we say that α is *transcendental over K* .

Remarks. (a) If $K = \mathbb{Q}$ and $E = \mathbb{C}$, the elements of E algebraic over K are called simply *algebraic numbers*, and the elements of E transcendental over K are called *transcendental numbers*. Example: $\alpha := \sqrt[3]{2}$ is an algebraic number, since α is a root of the polynomial $X^3 - 2 \in \mathbb{Q}[X]$.

(b) The set of algebraic numbers is countable (since $\mathbb{Q}[X]$ is countable and any nonzero polynomial in $\mathbb{Q}[X]$ has finitely many roots in \mathbb{C}). Therefore the set of transcendental numbers must be uncountable. To actually be able to exhibit a transcendental number is a different (and much harder) matter.

Theorem 1. *Let M be a subset of \mathbb{C} containing 0 and 1. Any point $z \in \Delta M$ is algebraic over $K := \mathbb{Q}(M \cup \overline{M})$.*

The proof will be given later in this chapter. But first we quote a famous result:

Theorem 2 (Lindemann 1882). *The number π is transcendental.*

Corollary. *The quadrature of the circle with ruler and compass is impossible.*

Proof. If it were possible, we would have $\pi \in \Delta\mathbb{Q}$; by Theorem 1 then π would be algebraic, which by Lindemann’s Theorem is not the case. \square

Lindemann’s Theorem can be proved using relatively elementary algebraic and analytic arguments, but the proof is on the whole quite intricate. We will go into it later on (Chapter 17).

2. Now we start our study of field theory with the following statement:

F1. Let E/K be a field extension. If $\alpha \in E$ is algebraic over K , then

$$K(\alpha):K < \infty.$$

Proof. Suppose there exists a nonzero polynomial

$$(1) \quad f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

such that $f(\alpha) = 0$; we have assumed without loss of generality that f is normalized (has leading coefficient 1). There exists a unique homomorphism of K -algebras φ from the polynomial ring $K[X]$ into E such that $\varphi(X) = \alpha$ (see page 21); its image

$$R = \text{im } \varphi \subset E$$

consists precisely of those elements of E that can be written as polynomial expressions $g(\alpha)$ in α with coefficients in K . But in writing such an expression we immediately see from the relation

$$(2) \quad \alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)$$

that only terms of degree less than n are needed, so in fact

$$(3) \quad R = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_i \in K\}.$$

Thus, as a vector space over K , the dimension of R is at most n . Since R , being a subring of E , has no zero-divisors, a simple argument (given a bit further down) shows that R is actually a field. It follows that $K(\alpha) \subseteq R$ (using the definition of $K(\alpha)$), and therefore that $R = K(\alpha)$. From (3) we then get

$$(4) \quad K(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_i \in K\}.$$

In particular,

$$(5) \quad K(\alpha):K \leq n. \quad \square$$

F2. Let R be an integral domain (that is, a commutative ring with no zero divisors and with $1 \neq 0$), and let K be a subfield of R . If R is finite-dimensional as a K -vector space, R is a field.

Proof. For a given $a \neq 0$ in R , consider the map $h: R \rightarrow R$ given by multiplication by a , namely, $h(x) = ax$ for all x in R . Then h is an endomorphism (linear map) of the K -vector space R . Since R has no zero-divisors, h is injective. Because R is assumed finite-dimensional over K , it is also surjective. In particular, there exists $b \in R$ such that $ab = 1$. \square

Remark. It can be proved in an analogous way that an integral domain that has finite cardinality is a field.

3. Let E/K be a field extension, and let $\alpha \in E$ be algebraic over K . Consider on the K -vector space $K(\alpha)$ the endomorphism h defined by multiplication by α . The minimal polynomial of h is called the *minimal polynomial of α over K* , and we denote it by

$$\text{MiPo}_K(\alpha).$$

This is the lowest-degree normalized polynomial in $K[X]$ that has α as a zero. (That there can be only one such polynomial is clear: if f, g are both normalized and of degree n , the degree of $f - g$ is less than n .) The degree of $f = \text{MiPo}_\alpha(K)$ is also called the *degree of α over K* , and is denoted by $[\alpha : K]$.

Example. Consider $E = \mathbb{C}$, $K = \mathbb{Q}$ and $\alpha = e^{2\pi i/3}$. Then α is a root of $X^3 - 1$. But $X^3 - 1 = (X - 1)g(X)$, with $g(X) = X^2 + X + 1$; since $\alpha \neq 1$, we have $g(\alpha) = 0$. Let $f = \text{MiPo}_K(\alpha)$; we claim that $f = g$. Otherwise necessarily $\deg f < \deg g$, so f could only be of the form $f(X) = X - \alpha$, which is impossible since $\alpha \notin \mathbb{R}$.

F3. Let E/K be a field extension and let $\alpha \in E$ be algebraic over K , of degree $n := [\alpha : K]$. The elements

$$(6) \quad 1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

of E form a basis of $K(\alpha)$ over K . In particular,

$$(7) \quad K(\alpha) : K = [\alpha : K] = \deg \text{MiPo}_K(\alpha).$$

Proof. Let $f(X) = X^n + \dots + a_1 X + a_0$ the minimal polynomial of α over K . We know that

$$K(\alpha) : K \leq n;$$

see (5) in the proof of F1. There remains to show that $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are linearly independent over K . Suppose there is a relation

$$(8) \quad \sum_{i=0}^{n-1} c_i \alpha^i = 0 \quad \text{with } c_i \in K.$$

Set $g(X) := \sum_{i=0}^{n-1} c_i X^i$. If some c_i in (8) were nonzero, $g(X)$ would be a nonzero polynomial in $K[X]$ of degree less than n and vanishing at α . Contradiction! \square

4. Let E/K be a field extension and assume $\alpha \in E$ is algebraic over K . Is it the case that any $\beta \in K(\alpha)$ is also algebraic over K ?

Definition. An extension E/K is called *algebraic* if every element of E is algebraic over K . An extension E/K is called *finite* if $E : K < \infty$.

Remarks. \mathbb{C}/\mathbb{R} is a finite extension, since $\mathbb{C} : \mathbb{R} = 2$. The extension \mathbb{R}/\mathbb{Q} is not algebraic; see Remark (b) in Section 2.1.

An extension E/K is called *transcendental* if it is not algebraic.

F4. *If an extension E/K is finite, it is also algebraic; for each $\beta \in E$ the degree $[\beta : K]$ is a divisor of $E : K$.*

Proof. Let E/K be finite of degree n . Given $\beta \in E$, the $n + 1$ elements $1, \beta, \beta^2, \dots, \beta^n$ of the n -dimensional K -vector space E are linearly dependent. Therefore there exist $a_0, a_1, \dots, a_n \in K$, not all zero, such that

$$a_0 1 + a_1 \beta + \dots + a_n \beta^n = 0.$$

Thus β is algebraic over K . By F3, $[\beta : K] = K(\beta) : K$, and $K(\beta) : K$ is a divisor of $E : K$ by the degree formula (Chapter 1, F7). \square

We now can easily answer in the affirmative the question asked at the beginning of this section.

F5. *Let E/K be a field extension. If $\alpha \in E$ is algebraic over K , the extension $K(\alpha)/K$ is algebraic.*

Proof. If α is algebraic over K , we know from F1 that $K(\alpha)/K$ is finite. But every finite field extension is algebraic, by F4. \square

Together, F1 and F4 afford the following criterion:

F6. *Let E/K be a field extension. An element α of E is algebraic over K if and only if $K(\alpha)/K$ is finite.*

Now it is a cinch to prove Theorem 1, which we can reformulate as follows:

Theorem 1. *Let M be a subset of \mathbb{C} containing 0 and 1. Let $K = \mathbb{Q}(M \cup \overline{M})$. The field extension $\triangle M/K$ is algebraic.*

Proof. Take $z \in \triangle M$. From F9 of Chapter 1 we know that $K(z) : K < \infty$. Then F6 says that z is algebraic over K . \square

Remark. The converse of F4 is not true: Not every algebraic extension is finite. This will soon become obvious. In fact a counterexample comes up naturally in our context: If $E = \triangle\{0, 1\}$ is the field of all numbers constructible from $\{0, 1\}$ with ruler and compass, the field extension E/\mathbb{Q} is algebraic but not finite. (With what we know so far this is not very easy to prove, but it's worth thinking about; see §2.5 in the Appendix.)

Among algebraic extensions, finite extensions can be characterized thus:

F7. *Let E/K be a field extension. The following conditions are equivalent:*

- (i) *There are elements $\alpha_1, \dots, \alpha_m$ of E , finite in number and algebraic over K , such that $E = K(\alpha_1, \dots, \alpha_m)$.*
- (ii) *E/K is finite.*

Proof. (ii) \Rightarrow (i) is clear; all we need to do is choose a basis $\alpha_1, \dots, \alpha_m$ for E/K . Then we actually have $E = K\alpha_1 + \dots + K\alpha_m$, and by F4 all the α_i are algebraic over K .

To show (i) \Rightarrow (ii) we use induction over m . For $m = 0$ there is nothing to prove. Assume that (i) holds for some $m \geq 1$ and set

$$K' = K(\alpha_1, \dots, \alpha_{m-1}).$$

Then $E = K'(\alpha_m)$. Since α_m is algebraic over K , it is *a fortiori* algebraic over the larger field K' . By F1 this implies $E:K' < \infty$. But by the induction hypothesis, K'/K is finite. The degree formula (Chapter 1, F7) then implies that E/K is finite. \square

5. Let E/K be a field extension. A subfield L of E containing K is called an *intermediate field* of the extension E/K .

F8. Let E/K be a field extension. The subset

$$F = \{\alpha \in E \mid \alpha \text{ is algebraic over } K\}$$

is an intermediate field of E/K . It is called the *algebraic closure of K in E* . In particular, the set of all algebraic numbers is a subfield of \mathbb{C} .

Proof. Take $\alpha, \beta \in F$. Consider the subfield $K(\alpha, \beta)$ of E . By F7 the extension $K(\alpha, \beta)/K$ is finite (prove this again for practice). Now apply F4; all elements of $K(\alpha, \beta)$ are algebraic over K , so

$$K(\alpha, \beta) \subseteq F.$$

The elements $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and $1/\alpha$ (if $\alpha \neq 0$) lie in $K(\alpha, \beta)$, and thus also in F . So F really is a subfield of E . Clearly $K \subseteq F$, since any $\alpha \in K$ is a zero of a polynomial $X - \alpha \in K[X]$ and therefore algebraic over K . This completes the proof. \square

This proof qualifies as easy, but it's only easy because we have the right notions at our disposal. Otherwise, would you be able to write down, at the drop of a hat, a nontrivial rational polynomial that vanishes at the sum of two numbers, given only rational polynomials vanishing at one and the other number respectively?

F9 (Transitivity of algebraicness). Let L be an intermediate field of the extension E/K . If E/L and L/K are algebraic, so is E/K (and vice versa).

Proof. Take $\beta \in E$. By assumption β is algebraic over L . Let $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ be the coefficients of $\text{MiPo}_L(\beta)$; then β is also algebraic over the subfield $F := K(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$. By assumption all the α_i are algebraic over K . Therefore we can apply F7 to conclude that $F:K$ is finite. But $F(\beta):F$ is also finite, by F6; therefore the degree formula gives

$$F(\beta):K < \infty.$$

Using F4 we see in particular that β is algebraic over K . \square

F10. Let E/K be a field extension and A a subset of E . If all elements of A are algebraic over K , the extension $K(A)/K$ is algebraic.

Proof. Clearly $K(A)$ is the union of all subfields of the form $K(M)$, where M ranges over finite subsets of A . By F7, each $K(M)/K$ is finite and therefore also algebraic. Thus $K(A)$ contains only elements algebraic over K . (Of course F10 also follows directly from F8.) \square

F11. Let E/K be a field extension, and L_1, L_2 intermediate fields of E/K . The field

$$(9) \quad L_1 L_2 := L_1(L_2) = L_2(L_1)$$

is called the **composite** of L_1 and L_2 in E .

- (a) If L_1/K is algebraic, so is $L_1 L_2/L_2$.
- (b) If L_1/K is finite, so is $L_1 L_2/L_2$; moreover $L_1 L_2 : L_2 \leq L_1 : K$.
- (c) If L_1/K and L_2/K are algebraic, so is $L_1 L_2/K$.
- (d) If L_1/K and L_2/K are finite, so is $L_1 L_2/K$; if, moreover, the extension degrees $n_1 = L_1 : K$ and $n_2 = L_2 : K$ are relatively prime, we have $L_1 L_2 : K = n_1 n_2$.

Proof. Part (a) follows from F10, taking (9) into account. Part (c) therefore also follows, thanks to F9. Let L_1/K and L_2/K be finite. Assuming (b) already proved, we see from the degree formula that

$$(10) \quad L_1 L_2 : K = (L_1 L_2 : L_2)(L_2 : K) \leq (L_1 : K)(L_2 : K),$$

which is the first part of (d). Again from the degree formula we obtain that $L_1 L_2 : K$ is divisible by n_1 and by n_2 . If n_1, n_2 are relatively prime, $L_1 L_2 : K$ is divisible by $n_1 n_2$, which together with (10) gives the second part of (d).

There remains to prove (b). Consider the set R of all finite sums of products ab with $a \in L_1, b \in L_2$. Clearly R is a subring of E containing L_1 and L_2 . It is also clear that any basis of L_1/K generates R as an L_2 -vector space R , so in particular $R : L_2 \leq L_1 : K$. If $L_1 : K < \infty$, this implies that R is a field (see F2). It follows that $R = L_1 L_2$, which concludes the proof. \square



<http://www.springer.com/978-0-387-28930-4>

Algebra

Volume I: Fields and Galois Theory

Lorenz, F.

2006, VIII, 296 p. 6 illus., Softcover

ISBN: 978-0-387-28930-4