

§49 Field Extensions (continued)

49.1 Definition: Let E be an extension field of K . If F is a field such that $K \subseteq F \subseteq E$, then F is said to be an *intermediate field of the extension E/K* .

49.2 Definition: Let E/K be a field extension and let S be a subset of E . The intersection of all subfields of E containing $K \cup S$, which is a subfield of E by Example 48.3(f), is called the *subfield of E generated by S over K* , and is denoted by $K(S)$.

It follows immediately from this definition that $K \subseteq K(S) \subseteq E$ so that $K(S)$ is an intermediate field of E/K . When S is a finite subset of E , say when $S = \{a_1, a_2, \dots, a_n\}$, we write $K(a_1, a_2, \dots, a_n)$ instead of $K(\{a_1, a_2, \dots, a_n\})$. In particular, if $a \in E$, then $K(a)$ is, by definition, the smallest subfield of E containing both K and a . Notice that $K(a_1, a_2, \dots, a_n) = K(a_{i_1}, a_{i_2}, \dots, a_{i_n})$ for any permutation $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ in S_n .

49.3 Definition: Let E/K be a field extension and let S be a subset of E . The intersection of all subrings of E containing $K \cup S$, which is a subring of E by Example 30.2'3(c), is called the *subring of E generated by S over K* , and is denoted by $K[S]$.

Since every subfield of E containing $K \cup S$ is also a subring of E containing $K \cup S$, we clearly have $K \subseteq K[S] \subseteq K(S) \subseteq E$. If S is a finite subset of E , say $S = \{a_1, a_2, \dots, a_n\}$, we write $K[a_1, a_2, \dots, a_n]$ instead of $K[\{a_1, a_2, \dots, a_n\}]$. In particular, if $a \in E$, then $K[a]$ is, by definition, the smallest subring of E containing both K and a . We have $K[a_1, a_2, \dots, a_n] = K[a_{i_1}, a_{i_2}, \dots, a_{i_n}]$ for any permutation $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ in S_n .

49.4 Example: In the extension \mathbb{C}/\mathbb{Q} , let us find the subfield of \mathbb{C} generated by i over \mathbb{Q} . Any subfield of \mathbb{C} containing both \mathbb{Q} and i contains complex numbers of the form $\frac{a + bi}{c + di}$, where $a, b, c, d \in \mathbb{Q}$ and $c + di \neq 0$. One verifies easily that $F = \left\{ \frac{a + bi}{c + di} \in \mathbb{C} : a, b, c, d \in \mathbb{Q}, c + di \neq 0 \right\}$ is a subfield of \mathbb{C} containing both \mathbb{Q} and i . Hence F is the subfield of \mathbb{C} generated by i over \mathbb{Q} .

Let us note that any element of F can be written in the form $x + yi$, with $x, y \in \mathbb{Q}$. Thus $\{x + yi \in \mathbb{C} : x, y \in \mathbb{Q}\} = F$ and F is equal to the field $\mathbb{Q}(i)$ defined in Example 48.3(c). So the notation of Example 48.3(c) is consistent with that of Definition 49.2.

The description of the elements in a field generated by a subset over a subfield resembles the preceding example.

49.5 Lemma: Let E/K be a field extension and $a_1, a_2, \dots, a_n \in E$. Then

$$(1) K[a_1, a_2, \dots, a_n] = \{f(a_1, a_2, \dots, a_n) \in E : f \in K[x_1, x_2, \dots, x_n]\};$$

$$(2) K(a_1, a_2, \dots, a_n)$$

$$= \left\{ \frac{f(a_1, a_2, \dots, a_n)}{g(a_1, a_2, \dots, a_n)} \in E : f, g \in K[x_1, x_2, \dots, x_n], g(a_1, a_2, \dots, a_n) \neq 0 \right\}.$$

Proof: (1) Let A be the set on the right hand side of the equation in (1). Any subring of E containing K and $\{a_1, a_2, \dots, a_n\}$ will contain the elements of the form $ka_1^{m_1}a_2^{m_2}\dots a_n^{m_n}$, where $k \in K$ and m_1, m_2, \dots, m_n are nonnegative integers, hence also the elements of the form

$$\sum k_{m_1, m_2, \dots, m_n} a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \quad (*)$$

where $k_{m_1, m_2, \dots, m_n} \in K$ and m_1, m_2, \dots, m_n are nonnegative integers. Of course, (*) is nothing but the value of the polynomial

$$f(x_1, x_2, \dots, x_n) = \sum k_{m_1, m_2, \dots, m_n} x_1^{m_1} x_2^{m_2} \dots x_n^{m_n} \in K[x_1, x_2, \dots, x_n]$$

at (a_1, a_2, \dots, a_n) . So every element of A is in any subring of E containing K and $\{a_1, a_2, \dots, a_n\}$. This gives $A \subseteq K[a_1, a_2, \dots, a_n]$. To prove the reverse inclusion, it suffices, in view of $K \cup \{a_1, a_2, \dots, a_n\} \subseteq A \subseteq E$, to show that A is a subring of E . But this is immediate: given any $f(a_1, a_2, \dots, a_n)$ and $g(a_1, a_2, \dots, a_n) \in A$, where $f, g \in K[x_1, x_2, \dots, x_n]$, we have

$$\begin{aligned} f(a_1, a_2, \dots, a_n) + g(a_1, a_2, \dots, a_n) &= (f+g)(a_1, a_2, \dots, a_n) \in A \\ -g(a_1, a_2, \dots, a_n) &= (-g)(a_1, a_2, \dots, a_n) \in A \\ f(a_1, a_2, \dots, a_n)g(a_1, a_2, \dots, a_n) &= (fg)(a_1, a_2, \dots, a_n) \in A \end{aligned}$$

since $f+g, -g, fg$ belong to $[x_1, x_2, \dots, x_n]$ whenever f, g do. Thus A is a subring of E by the subring criterion (Lemma 30.2). This proves

$$K[a_1, a_2, \dots, a_n] = A.$$

(2) The reasoning is similar. Let B be the set on the right hand side of the equation in (2). Clearly $A \subseteq B$. Note that $B = \{b/c \in E: b, c \in A, c \neq 0\} = \{bc^{-1} \in E: b, c \in A, c \neq 0\}$. Any subfield of E containing K and $\{a_1, a_2, \dots, a_n\}$ will contain $K[a_1, a_2, \dots, a_n] = A$ and, since a subfield is closed under division, it will contain also the elements b/c , where $b, c \in A$ and $c \neq 0$. This means that B is contained in any subfield of E containing K and $\{a_1, a_2, \dots, a_n\}$. Hence $B \subseteq K(a_1, a_2, \dots, a_n)$. To prove the reverse inclusion, it suffices, in view of $K \cup \{a_1, a_2, \dots, a_n\} \subseteq B \subseteq E$, to show that B is a subfield of E . Indeed, given any $b/c, d/e \in B$, where $b, c, d, e \in A, c, e \neq 0$, we have

$$\begin{aligned} \frac{b}{c} + \frac{d}{e} &= \frac{be + dc}{ce} \in B \\ &\quad - \frac{d}{e} \in B \\ \frac{b}{c} \frac{d}{e} &= \frac{bd}{ce} \in B \\ \frac{1}{\frac{d}{e}} &= \frac{e}{d} \in B \quad (\text{provided } d/e \neq 0, \\ &\quad \text{i.e., } d \neq 0) \end{aligned}$$

i.e., $d \neq 0$)

since $be + dc, ce, -d, bd, ce$ belong to A whenever b, c, d, e do and $ce \neq 0$ whenever $c \neq 0 \neq e$ (A is a subring of the field E and has therefore no zero divisors). Thus B is a subfield of E by the subfield criterion (Lemma 48.2). This proves $K(a_1, a_2, \dots, a_n) = B$. \square

The proof of Lemma 49.5 can be somewhat simplified by referring to Theorem 31.8.

Let us take a new look at Example 49.4 under the light of Lemma 49.5. The field F in Example 49.4 is exactly the the field described in Lemma 49.5, with $K = \mathbb{Q}$, $n = 1$, $a_1 = i \in \mathbb{C}$. On the other hand, the field $\{x + yi \in \mathbb{C} : x, y \in \mathbb{Q}\}$ is exactly the subring of \mathbb{C} described in Lemma 49.5, with $K = \mathbb{Q}$, $n = 1$, $a_1 = i \in \mathbb{C}$. Thus we have $\mathbb{Q}(i) = \mathbb{Q}[i]$. The reader will easily verify that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ also (cf. Theorem 50.6).

49.6 Lemma: *Let E/K be a field extension and $a, b, a_1, a_2, \dots, a_n \in E$.*

- (1) $K(a) = K$ if and only if $a \in K$.
- (2) $K(a_1, a_2, \dots, a_{n-1}, a_n) = (K(a_1, a_2, \dots, a_{n-1}))(a_n)$ and $K[a_1, a_2, \dots, a_{n-1}, a_n] = [K(a_1, a_2, \dots, a_{n-1})][a_n]$.
- (3) $K(a, b) = (K(a))(b) = (K(b))(a)$ and $K[a, b] = [K[a]][b] = [K[b]][a]$.

Proof: (1) $a \in K(a)$ by the definition of $K(a)$ and, if $K(a) = K$, we obtain $a \in K$. Conversely, if $a \in K$, then $K = K \cup \{a\}$ and K is the intersection of all subfields of E containing both K and a ; thus $K(a) = K$.

(2) Let us write $L = K(a_1, a_2, \dots, a_{n-1})$. Then L contains K and a_1, a_2, \dots, a_{n-1} . Now $L(a_n)$ is a subfield of E containing both L and a_n , so $L(a_n)$ is a subfield of E containing K and a_1, a_2, \dots, a_{n-1} and a_n . Then $K(a_1, a_2, \dots, a_{n-1}, a_n)$, being the intersection of all subfield of E containing K and $a_1, a_2, \dots, a_{n-1}, a_n$, is a subfield of $L(a_n)$. This gives $K(a_1, a_2, \dots, a_{n-1}, a_n) \subseteq L(a_n)$. On the other hand, $K(a_1, a_2, \dots, a_{n-1}, a_n)$ is a subfield of E containing K , a_1, a_2, \dots, a_{n-1} and also a_n . So $L \subseteq K(a_1, a_2, \dots, a_{n-1}, a_n)$ by the definition of $L = K(a_1, a_2, \dots, a_{n-1})$; and $a_n \in K(a_1, a_2, \dots, a_{n-1}, a_n)$. Hence $K(a_1, a_2, \dots, a_{n-1}, a_n)$ is a subfield of E containing both L and a_n . Then $L(a_n) \subseteq K(a_1, a_2, \dots, a_{n-1}, a_n)$ by the definition of $L(a_n)$. We obtain $K(a_1, a_2, \dots, a_{n-1}, a_n) = L(a_n)$, as was to be proved. The second assertion is proved in exactly the same way (read "subring" in place of "subfield" in the foregoing argument).

(3) Using part (2) twice, we get $(K(a))(b) = K(a, b) = K(b, a) = (K(b))(a)$ and similarly $[K[a]][b] = K[a, b] = K[b, a] = [K[b]][a]$.

□

We introduce a very important classification of field extensions: algebraic vs. transcendental extensions. They behave very differently.

49.7 Definition: Let E/K be a field extension. An element a of E is said to be *algebraic over K* if there is a nonzero polynomial f in $K[x]$ such that a is a root of f , i.e., $f(a) = 0$. An element a of E is said to be *transcendental over K* if a is not algebraic, that is to say, if there is no nonzero polynomial f in $K[x]$ with $f(a) = 0$.

If every element of E is algebraic over K , then E is called an *algebraic extension of K* and E/K is called an *algebraic extension*. In this case, E is said to be *algebraic over K* . If E is not an algebraic extension of K , then E is called a *transcendental extension of K* and E/K is called a *transcendental extension*. If so, that is to say, if E contains at least one element which is not algebraic over K , then E is said to be *transcendental over K* .

49.8 Examples: (a) Let K be any field. Then, for any element $a \in K$, the polynomial $f_a(x) := x - a$ is in $K[x]$, and a is a root of f_a . Thus any element of K is algebraic over K , and K is an algebraic extension of K .

(b) $i \in \mathbb{C}$ is a root of the polynomial $x^2 + 1 \in \mathbb{Q}[x]$. Hence i is algebraic over \mathbb{Q} . Also, any element $a + bi$ of $\mathbb{Q}(i)$, where $a, b \in \mathbb{Q}$, is a root of

$$[x - (a + bi)][x - (a - bi)] = x^2 - 2ax + (a^2 + b^2) \in \mathbb{Q}[x]$$

and is therefore algebraic over \mathbb{Q} . Hence $\mathbb{Q}(i)/\mathbb{Q}$ is an algebraic extension.

(c) $\sqrt{2} \in \mathbb{R}$ is a root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$. Hence $\sqrt{2}$ is algebraic over \mathbb{Q} . Also, any element $a + b\sqrt{2}$ of $\mathbb{Q}(\sqrt{2})$, where $a, b \in \mathbb{Q}$, is a root of

$$[x - (a + b\sqrt{2})][x - (a - b\sqrt{2})] = x^2 - 2ax + (a^2 - 2b^2) \in \mathbb{Q}[x]$$

and is therefore algebraic over \mathbb{Q} . Hence $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is an algebraic extension.

(d) It is a fact that $\pi \in \mathbb{R}$ and $e \in \mathbb{R}$ are transcendental over \mathbb{Q} . We borrow this fact from number theory without proof. Thus \mathbb{R}/\mathbb{Q} is a transcendental extension. $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are also transcendental extensions of \mathbb{Q} .

(e) Let K be a field and x an indeterminate over K . Then $K(x)$ is an extension field of K and $x \in K(x)$. If f is any nonzero polynomial in $K[x]$, then $f(x) = f \neq 0$ (Example 35.2(d)). Thus x is transcendental over K and $K(x)/K$ is a transcendental extension.

Likewise $f(x^2) \neq 0$ for any nonzero polynomial f in $K[x]$ and x^2 is transcendental over K . On the other hand, if y is another indeterminate over K , then x is the root of the polynomial $y^2 - x^2 \in (K(x^2))[y]$, so x is algebraic over $K(x^2)$. Thus an element may be transcendental over a field and algebraic over another field.

49.9 Definition: Let E/K be a field extension. If there is an element a in E such that $E = K(a)$, then E is called a *simple extension of K* . In this case, any element a of E satisfying $E = K(a)$ is called a *primitive element of the extension E/K* . If there are finitely many elements a_1, a_2, \dots, a_n in E such that $E = K(a_1, a_2, \dots, a_n)$, then E is said to be *finitely generated over K* .

The reader should clearly distinguish between finite dimensional extensions and finitely generated extensions.

We close this paragraph with a theorem that describes all simple transcendental extensions up to isomorphism. Simple algebraic extensions will be treated in the next paragraph.

49.10 Theorem: Let E/K be a field extension and let $a \in E$ be transcendental over K . Then $K(a) \cong K(x)$, where x is an indeterminate over K .

Proof: We wish to find an isomorphism from $K(x)$ onto $K(a)$. What is more natural than the extension

$$\begin{aligned} \varphi: K(x) &\rightarrow K(a) \\ \frac{f}{g} &\rightarrow \frac{f(a)}{g(a)} \end{aligned}$$

of the substitution homomorphism? In any case, Lemma 49.5(2) suggests that we try this mapping. Now φ is meaningful, for, given any $f/g \in K(x)$ with $f, g \in K[x]$, $g \neq 0$, we have $g(a) \neq 0$ (a is transcendental over K) and so $(f/g)\varphi = f(a)/g(a)$ is a perfectly definite element of $K(a)$.

We claim that φ is well defined. Indeed, if $f/g = f_1/g_1$ in $K(x)$, where $f, g, f_1, g_1 \in K[x]$ and $g \neq 0 \neq g_1$, then $fg_1 = f_1g$ in $K[x]$ and, by Lemma 35.3, $f(a)g_1(a) = f_1(a)g(a)$ in E , with $g_1(a) \neq 0 \neq g(a)$; multiplying this equation by $1/g_1(a)g(a)$, we obtain

$$\left(\frac{f}{g}\right)\varphi = \frac{f(a)}{g(a)} = \frac{f_1(a)}{g_1(a)} = \left(\frac{f_1}{g_1}\right)\varphi,$$

which shows that φ is well defined.

φ is a ring homomorphism because, from Lemma 35.3, we have

$$\begin{aligned} \left(\frac{f}{g} + \frac{p}{q}\right)\varphi &= \frac{fq + pg}{gq} \varphi = \frac{(fq + pg)(a)}{(gq)(a)} = \frac{f(a)q(a) + p(a)g(a)}{g(a)q(a)} \\ &= \frac{f(a)}{g(a)} + \frac{p(a)}{q(a)} = \left(\frac{f}{g}\right)\varphi + \left(\frac{p}{q}\right)\varphi \end{aligned}$$

$$\text{and } \left(\frac{f}{g} \frac{p}{q}\right)\varphi = \frac{fp}{gq} \varphi = \frac{f(a)p(a)}{g(a)q(a)} = \frac{f(a)}{g(a)} \frac{p(a)}{q(a)} = \left(\frac{f}{g}\right)\varphi \left(\frac{p}{q}\right)\varphi$$

for any $f/g, p/q \in K(x)$, where $f, g, p, q \in K[x]$ and $g \neq 0 \neq q$, the last condition ensuring $g(a) \neq 0 \neq q(a)$.

$$\begin{aligned} \text{Since } \text{Ker } \varphi &= \{f/g \in K(x): f, g \in K[x], g \neq 0 \text{ in } K[x], f(a)/g(a) = 0\} \\ &= \{f/g \in K(x): f, g \in K[x], g \neq 0, f(a) = 0\} \\ &= \{f/g \in K(x): f, g \in K[x], g \neq 0, f = 0\} \\ &= \{0\}, \end{aligned}$$

φ is one-to-one. Hence φ is a field homomorphism. Lemma 49.5(2) states that φ is onto $K(a)$. So $\varphi: K(x) \rightarrow K(a)$ is a field isomorphism: $K(x) \cong K(a)$. \square

Exercises

1. Let E/K be a field extension and $S \subseteq E$, $S \neq \emptyset$. Show that $K[S] = \{f(s_1, s_2, \dots, s_n) \in E: n \in \mathbb{N}, f \in K[x_1, x_2, \dots, x_n] \text{ and } s_1, s_2, \dots, s_n \in S\}$;

and $K(S) =$

$$= \left\{ \frac{f(s_1, s_2, \dots, s_n)}{g(s_1, s_2, \dots, s_n)} \in E: n \in \mathbb{N}, f, g \in K[x_1, x_2, \dots, x_n] \text{ and } g(s_1, s_2, \dots, s_n) \neq 0 \right\}.$$

2. Let E/K be a field extension and $S \subseteq E$, $S \neq \emptyset$. Using the definition of $K[S]$ and $K(S)$ only (in particular, without using Ex. 1), prove that $K(S)$ is the field of fractions of $K[S]$.

3. Let E/K be a field extension and $S \subseteq E$. Show that $K(S) = K$ if and only if $S \subseteq K$.
4. Let E/K be a field extension and $a_1, a_2, \dots, a_n \in E$. Prove that $(K(a_1, \dots, a_k))(a_{k+1}, \dots, a_n)$ for any $k = 1, 2, \dots, n - 1$.
5. Let a, b be arbitrary rational numbers. Find a polynomial in $\mathbb{Q}[x]$ which admits $a + b\sqrt{5}$ as a root. Conclude that $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is an algebraic extension.
6. Show that $\sqrt{2} + i$, $\sqrt{2} + \sqrt{3}$, $\sqrt{2} + \sqrt{3} + i$ are algebraic over \mathbb{Q} by exhibiting polynomials in $\mathbb{Q}[x]$ having these numbers among their roots.
7. Let K be a field. Prove that every element in $K(x) \setminus K$ is transcendental over K .
8. Let E/K be a simple field extension and let a be a primitive element of this extension. Let $k, k' \in K$, with $k \neq 0$. Show that $ka + k'$ is also a primitive element of E/K .
9. Find a finitely generated field extension which is not finite dimensional. Prove that every finite dimensional extension is finitely generated.
10. Prove or disprove: if E/K is a field extension and $a, b \in E$ are transcendental over K , then $K(a, b) \cong K(x, y)$, where x, y are indeterminates over K .