

§55 Separable Extensions

In §54, we established the foundations of Galois theory, but we have no handy criterion for determining whether a given field extension is Galois or not. Even in the quite simple cases such as in Example 54.18, we had to study the effects of automorphisms on the elements in the extension field, and this involved much calculation. The extension fields in Example 54.18 were seen to be splitting fields of certain polynomials over the base field. In this paragraph, we will learn that a finite dimensional extension is Galois if and only if the extension field is a splitting field of a polynomial whose irreducible factors have no multiple roots. We give a name to irreducible polynomials of this kind.

55.1 Definition: Let K be a field and $f(x) \in K[x]$. If $f(x)$ is irreducible over K and has no multiple roots (in any splitting field of $f(x)$ over K), then $f(x)$ is said to be *separable over K* .

Thus all the $\deg f(x)$ roots of a polynomial $f(x)$ separable over K are distinct and $f(x)$ splits into distinct linear factors in any splitting field of $f(x)$ over K .

The existence of multiple roots can be decided by means of the derivative. If K is a field, $f(x)$ an irreducible polynomial in $K[x]$ and E a splitting field of $f(x)$ over K , then Theorem 35.18 (5) and Theorem 35.18 (6) show that $f(x)$ is separable over K if and only if $f'(x) \neq 0$.

How can an irreducible polynomial $f(x)$ have a zero derivative? Now $f(x)$ is not 0 or a unit because of irreducibility, so $\deg f(x) =: m \geq 1$. Let $f(x) = \sum_{i=0}^m a_i x^i$, with $a_m \neq 0$. Then $f'(x) = \sum_{i=1}^m i a_i x^{i-1} = 0$ if and only if $i a_i = 0$ for all $i = 1, 2, \dots, m$. In particular, $(m1)a_m = m a_m = 0$. Since a field has no zero divisors and $a_m \neq 0$, this forces $m1 = 0$. This is impossible in case $\text{char } K = 0$ and is equivalent to $p|m$ in case $\text{char } K = p \neq 0$. Likewise, if $a_i \neq 0$, the

condition $ia_i = 0$ is equivalent to $p|i$ in case $\text{char } K = p$. So for terms $a_i x^i$ with $a_i \neq 0$, we have $i = pj$ for some j and we may write $f(x) = \sum_{j=0}^{\lfloor m/p \rfloor} a_{pj} x^{pj}$.

Putting $\lfloor m/p \rfloor = n$, $a_{pj} = b_j$ and $g(x) = \sum_{j=0}^n b_j x^j$, we obtain $f(x) = g(x^p)$. Thus

$f(x)$ is actually a polynomial in x^p . Conversely, if $f(x) = g(x^p)$, then $f'(x) = g'(x^p) \cdot px^{p-1} = g'(x^p) \cdot 0 = 0$ by Lemma 35.16. We summarize:

55.2 Lemma: *Let K be a field. If $\text{char } K = 0$, then any polynomial irreducible over K is separable over K . If $\text{char } K = p \neq 0$ and $f(x) \in K[x]$ is irreducible over K , then $f(x)$ is separable over K if and only if $f(x)$ is not a polynomial in x^p , i.e., $f(x)$ is not separable over K if and only if $f(x) = g(x^p)$ for some $g(x) \in K[x]$. \square*

In terms of separable polynomials we now define separable *elements* and separable field *extensions*.

55.3 Definition: Let E/K be a field extension and $a \in E$. If a is algebraic over K and the minimal polynomial of a over K is separable over K , then a is said to be *separable over K* .

Thus any element a of K is separable over K since the minimal polynomial of a over K is $x - a \in K[x]$ and $x - a$ is separable over K .

55.4 Definition: Let E/K be a field extension. If E is algebraic over K and if every element of E is separable over K , then E is said to be *separable over K* or a *separable extension of K* and E/K is called a *separable extension*.

The polynomial $x^2 + 1 \in \mathbb{Q}[x]$ is separable over \mathbb{Q} , because it is irreducible over \mathbb{Q} and $\text{char } \mathbb{Q} = 0$. On the other hand, $x^2 + 1 \in \mathbb{F}_2[x]$ is not separable over \mathbb{F}_2 because $x^2 + 1 = (x + 1)^2$ is not even irreducible over \mathbb{F}_2 .

If E/K is an extension of fields of characteristic 0, then any element of E that is algebraic over K is separable over K . Thus any algebraic extension of a field of characteristic 0 is a separable extension of that field.

We compare separability over a field with separability over an intermediate field.

54.5 Lemma: *Let E/K be a field extension and let L be an intermediate field of E/K . Let $a \in E$ be algebraic over K . If a is separable over K , then a is separable over L .*

Proof: Lemma 50.5 shows that a is algebraic over L . Let $f(x)$ be the minimal polynomial of a over K and $g(x)$ the minimal polynomial of a over L . By Lemma 50.5, $g(x)$ is a divisor of $f(x)$. Thus any root of $g(x)$ is a root of $f(x)$. Since a is separable over K , the roots of $f(x)$ are all simple, hence, all the more so, the roots of $g(x)$ are all simple and a is separable over L . \square

55.6 Lemma: *Let E/K be a field extension and let L be an intermediate field of E/K . Then E is separable over L and L is separable over K .*

Proof: Assume that E is separable over K . We are to show that (1) E is algebraic over L and L is algebraic over K and (2) any element of E is separable over L and any element of L is separable over K . Since E is separable over K , we deduce E is algebraic over L (Lemma 50.5) and any element of E , being (algebraic and) separable over K , is also separable over L (Lemma 55.5). Thus E/L is a separable extension. Moreover, all elements of E are separable over K , so, in particular, all elements in L are separable over K and L/K is a separable extension. \square

The converse of Lemma 55.6 is also true and will be proved later in this paragraph (Theorem 55.19). Our next goal is to characterize Galois extensions as splitting fields of separable polynomials.

55.7 Theorem: *Let E/K be a finite dimensional field extension. Then the following statements are equivalent.*

- (1) E is Galois over K .
- (2) E is a separable extension of K and the splitting field over K of a polynomial in $K[x]$.
- (3) E is the splitting field of a polynomial in $K[x]$ whose irreducible factors are separable over K .

Proof: (1) \Rightarrow (2) We prove E/K is a separable extension. Since E/K is a finite dimensional extension, E is algebraic over K . We have also to show that the minimal polynomial over K of any element u in E is separable over K . This follows immediately from Theorem 54.22. Hence E is a separable extension of K .

We must now show that there is a polynomial $g(x)$ in $K[x]$ such that E is a splitting field of $f(x)$ over K . Let $\{a_1, a_2, \dots, a_m\}$ be a K -basis of E and let $f_i(x) \in K[x]$ be the minimal polynomial of a_i over K ($i = 1, 2, \dots, m$). We put $g(x) = f_1(x)f_2(x) \dots f_m(x) \in K[x]$. From Theorem 54.22 again, we learn that each $f_i(x)$, hence also $g(x)$, splits in E . Moreover, $g(x)$ cannot split in any proper subfield L of E containing K for if L is an intermediate field of E/K and $g(x)$ splits in L , then L contains all roots of $g(x)$, hence L contains a_1, a_2, \dots, a_m and we have

$$E = s_K(a_1, a_2, \dots, a_m) \subseteq K(a_1, a_2, \dots, a_m) \subseteq L,$$

so $E = L$. Thus E is indeed a splitting field of $g(x)$ over K .

(2) \Rightarrow (3) Assume now E is separable over K and E is a splitting field over K of a polynomial $g(x)$ in $K[x]$. We are to prove that the irreducible factors of $g(x)$ in $K[x]$ are separable over K . Let $g(x) = f_1(x)f_2(x) \dots f_m(x)$ be the decomposition of $g(x)$ into irreducible factors $f_i(x)$ in $K[x]$. Since $g(x)$ splits in E , each $f_i(x)$ has a root $a_i \in E$. Here a_i is separable over K because E is separable over K . Thus the minimal polynomial of a_i over K is a separable polynomial over K . But the minimal polynomial of a_i over K is $c_i f_i(x)$ with some suitable $c_i \in K$, because a_i is a root of $f_i(x)$ and $f_i(x)$ is

irreducible in $K[x]$. So $c_i f_i(x)$ is separable over K and consequently $f_i(x)$ is also separable over K .

(3) \Rightarrow (1) Suppose now E is a splitting field of a polynomial $g(x) \in K[x]$ whose irreducible factors in $K[x]$ are separable over K . We put

$$K_0 = \{a \in E: a\varphi = a \text{ for all } \varphi \in \text{Aut}_K E\}.$$

Clearly $K_0 \subseteq K$. In fact K_0 is the fixed field of $\text{Aut}_K E$, hence K_0 is an intermediate field of the extension E/K . We prove that E is Galois over K by showing (i) E is Galois over K_0 ; (ii) $\text{Aut}_K E = \text{Aut}_{K_0} E$; (iii) $|E:K| = |\text{Aut}_K E|$. These will indeed imply

$$|E:K_0| = |\text{Aut}_{K_0} E| \quad (\text{by the fundamental theorem of Galois theory, since } E/K_0 \text{ is a finite dimensional Galois extension),}$$

$$|\text{Aut}_{K_0} E| = |\text{Aut}_K E| \quad (\text{by (ii)}),$$

$$|\text{Aut}_K E| = |E:K| \quad (\text{by (iii)}),$$

so $|E:K_0| = |E:K|,$

so $K_0 = K$

and E is Galois over K (by (i)).

Since, for any $\varphi \in \text{Aut}_K E$, there holds $a\varphi = a$ for all $a \in K_0$, we see that $\text{Aut}_K E \leq \text{Aut}_{K_0} E$.

(i) In order to show that E is Galois over K_0 , we have to find, for each $b \in E \setminus K_0$, an automorphism $\varphi \in \text{Aut}_{K_0} E$ such that $b\varphi \neq b$. If $b \in E \setminus K_0$, then, by definition of K_0 , there is a $\varphi \in \text{Aut}_K E$ such that $b\varphi \neq b$. From $\text{Aut}_K E \leq \text{Aut}_{K_0} E$, we see $\varphi \in \text{Aut}_{K_0} E$ and $b\varphi \neq b$. Thus E is Galois over K_0 .

(ii) E/K is a finite dimensional extension, hence E/K_0 is a finite dimensional extension and E/K_0 is Galois. Therefore, by the fundamental theorem of Galois theory, the subgroup $\text{Aut}_K E$ of $\text{Aut}_{K_0} E$ is a *closed* subgroup of $\text{Aut}_{K_0} E$. Hence $\text{Aut}_{K_0} E = K_0' = ((\text{Aut}_K E)^\wedge)' = (\text{Aut}_K E)'' = \text{Aut}_K E$.

(iii) We prove $|E:K| = |\text{Aut}_K E|$ by induction on $n = |E:K|$, the hypothesis being that E be a splitting field over K of a polynomial in $K[x]$ whose irreducible factors (in $K[x]$) are separable over K .

If $n = 1$, then $E = K$, so $\text{Aut}_K E = \text{Aut}_K K = \{I_K\}$ and $|E:K| = 1 = |\{I_K\}| = |\text{Aut}_K E|$.

Suppose now $n \geq 2$ and suppose that $|E_1:K_1| = |Aut_{K_1} E_1|$ whenever E_1/K_1 is a finite dimensional extension with $1 \leq |E_1:K_1| < n$ such that E_1 is a splitting field of a polynomial in $K_1[x]$ whose irreducible factors (in $K_1[x]$) are separable over K_1 .

Let $g(x) \in K[x]$ be the polynomial of which E is a splitting field over K and let $g(x) = f_1(x)f_2(x)\dots f_m(x)$ be the decomposition of $g(x)$ into irreducible polynomials $f_i(x)$ in $K[x]$. The polynomials $f_i(x)$ cannot all be of first degree, for then the roots of $f_i(x)$ would be in K and, as E is a splitting field of $g(x)$ over K , the field E would coincide with K , against the hypothesis $|E:K| = n > 1$. Thus at least one of $f_i(x)$ have degree > 1 . Let us assume $\deg f_1(x) = r > 1$ and let $a \in E$ be a root of $f_1(x)$. We put $L = K(a)$. Then $|L:K| = r$ and $|E:L| = n/r < n$.

Now E is a splitting field of $g(x) \in L[x]$ over L (Example 53.5(e)) and the irreducible factors (in $L[x]$) of $g(x)$, being divisors of $f_i(x)$, have no multiple roots and are therefore separable over L . Since $|E:L| = n/r < n$, we get $|E:L| = |Aut_L E| = |L'|$ by induction.

In order to prove $|E:K| = |Aut_K E|$, i.e., in order to prove $|E:L| |L:K| = |Aut_K E:L'| |L'|$, it will be thus sufficient to show that $r = |L:K| = |Aut_K E:L'|$.

We show $|Aut_K E:L'| = r$ by defining a one-to-one mapping A from the set \mathfrak{R} of right cosets of L' in $Aut_K E$ onto the set of distinct roots of $f_1(x)$ in E . Let $\{a = a_1, a_2, \dots, a_r\}$ be the distinct roots of $f_1(x)$ in E . We put

$$A: \mathfrak{R} \rightarrow \{a_1, a_2, \dots, a_r\}.$$

$$L'\varphi \rightarrow a\varphi$$

($\varphi \in Aut_K E$; we know $a\varphi \in E$ is a root of $f_1(x)$ from Lemma 54.5). This mapping A is well defined, for if $L'\varphi = L'\psi$, then

$$\varphi\psi^{-1} \in L'$$

$$\varphi\psi^{-1} \text{ fixes each element of } L = K(a)$$

$$\varphi\psi^{-1} \text{ fixes } a$$

$$a(\varphi\psi^{-1}) = a$$

$$(a\varphi)\psi^{-1} = a$$

$$a\varphi = a\psi$$

$$(L'\varphi)A = (L'\psi)A,$$

so A is well defined and, reading the lines backwards, we see that A is one-to-one as well. It remains to show that A is onto. Indeed, if a_i is any root of $f_1(x)$ in E , then there is a field homomorphism $\alpha_i: K(a) \rightarrow K(a_i)$

mapping a to a_i and fixing each element of K (Theorem 53.1) and α_i can be extended to a K -automorphism $\varphi_i: E \rightarrow E$ (Theorem 53.7). Then A sends the coset $L\varphi_i \in \mathfrak{R}$ to $a\varphi_i = a\alpha_i = a_i$. Hence A is onto. This gives $|Aut_K E:L| = |\mathfrak{R}| = |\{a_1, a_2, \dots, a_r\}| = r$. The proof is complete. \square

Thus for finite dimensional extensions, being Galois is equivalent to separability plus being a splitting field.

If E/K is a field extension and E is a splitting field of $f(x) \in K[x]$ over K , then all roots of the polynomial $f(x)$ are in E . We show more generally that, if there is a root in E of a polynomial over K , then all roots of that polynomial are in E . This gives a characterization of splitting fields without referring to any particular polynomial.

55.8 Theorem: *Let E/K be a finite dimensional field extension. The following statements are equivalent.*

- (1) *There is a polynomial $f(x) \in K[x]$ such that E is a splitting field of $f(x)$ over K .*
- (2) *If $g(x)$ is any irreducible polynomial in $K[x]$, and if $g(x)$ has a root in E , then $g(x)$ splits in E .*

Proof: (1) \Rightarrow (2) Assume that $g(x) \in K[x]$ is irreducible over K and that $g(x)$ has a root $u \in E$. We want to show that all irreducible factors of $g(x)$ in $E[x]$ have degree one. Suppose, on the contrary, that $h(x) \in E[x]$ is an irreducible (over E) factor of $g(x)$ with $\deg h(x) = n > 1$. We adjoin a root t of $h(x)$ to E and thereby construct the field $E(t)$.

Now u and t are roots of the irreducible polynomial $g(x)$ in $K[x]$, so there is a K -isomorphism $\varphi: K(u) \rightarrow K(t)$ (Theorem 53.2). Since E is a splitting field of $f(x)$ over $K(u)$ and $E(t)$ is a splitting field of $f(x)$ over $K(t)$ (Example 53.5(e)), the K -isomorphism φ can be extended to a K -isomorphism $\psi: E \rightarrow E(t)$ (Theorem 53.7). But then $|E:K| = |E(t):K| = |E(t):E||E:K| = n|E:K| > |E:K|$, a contradiction. Thus all irreducible factors of $g(x)$ in $E[x]$ have degree one and $g(x)$ splits in E .

(2) \Rightarrow (1) Suppose now that any irreducible polynomial in $K[x]$ splits in E whenever it has a root in E . Let $\{a_1, a_2, \dots, a_m\}$ be a K -basis of E and let

$f_i(x) \in K[x]$ be the minimal polynomial of a_i over K . We put $f(x) = f_1(x)f_2(x)\dots f_m(x)$. We claim E is a splitting field of $f(x)$ over K .

Each $f_i(x)$ has a root a_i in E , so each $f_i(x)$ splits in E by hypothesis, so $f(x)$ splits in E . Moreover, $f(x)$ cannot split in a proper subfield of E containing K for if L is an intermediate field of E/K and $f(x)$ splits in L , then all roots of $f(x)$ will be in L , in particular each a_i will be in L , thus $E = s_K(a_1, a_2, \dots, a_m) \subseteq K(a_1, a_2, \dots, a_m) \subseteq L$. Hence E is a splitting field of $f(x)$ over K . \square

Theorem 55.8 leads us to

55.9 Definition: Let E/K be a field extension. If E is algebraic over K and if every irreducible polynomial in $K[x]$ that has a root in E in fact splits in E , then E is said to be *normal over K* , and E/K is called a *normal extension*.

With this terminology, Theorem 55.8 reads as follows.

55.8 Theorem: A finite dimensional extension E/K is a normal extension if and only if E is a splitting field over K of a polynomial in $K[x]$. \square

55.10 Theorem: Let E/K be a finite dimensional field extension. E is Galois over K if and only if E is normal and separable over K .

Proof: This is immediate from Theorem 55.7(2) and Theorem 55.8. \square

55.11 Theorem: Let E/K be a finite dimensional field extension. There is an extension field N of E such that

- (i) N is normal over K ;
- (ii) no proper subfield of N containing E is normal over K ;
- (iii) $|N:K|$ is finite.
- (iv) N is Galois over K if and only if E is separable over K .

Moreover, if N' is another extension field of E with the same properties, then N and N' are E -isomorphic.

Proof: Let $\{a_1, a_2, \dots, a_m\}$ be a K -basis of E and let $f_i(x) \in K[x]$ be the minimal polynomial of a_i over K . We put $f(x) = f_1(x)f_2(x) \dots f_m(x) \in K[x]$. Let N be a splitting field of $f(x)$ over E , with $|N:E|$ finite (Theorem 53.6). We claim N has the properties stated above. Since $|N:E|$ and $|E:K|$ are both finite, $|N:K|$ is finite. This proves (iii).

To establish (i), we show that N is a splitting field of $f(x)$ over K (Theorem 55.8). Certainly $f(x)$ splits in N , because N is a splitting field of $f(x)$ over E . Now we have to prove that $f(x)$ does not split in any proper subfield of N containing K . If L is an intermediate field of N/K in which $f(x)$ splits, then L contains all roots of $f(x)$, hence $\{a_1, a_2, \dots, a_m\} \subseteq L$, hence $E = s_K(a_1, a_2, \dots, a_m) \subseteq K(a_1, a_2, \dots, a_m)L \subseteq N$; so L , in which $f(x)$ splits, is an intermediate field of N/E ; so $L = E$ since N is a splitting field of $f(x)$ over E . Thus N is indeed a splitting field of $f(x)$ over K .

Now (ii). If L is a proper subfield of N containing E , then L cannot be normal over K . Otherwise L , containing a root a_i of $f_i(x)$, would in fact contain all roots of $f_i(x)$ by normality, hence L would contain all the roots of $f(x)$, thus L would contain E and all roots of $f(x)$. Then L would contain H , where H is the subfield of N generated by the roots of $f(x)$ over E . But H is the unique splitting field of $f(x)$ which is an intermediate field of N/E (Example 53.5(d)), so $N = H \subseteq L$ and this forces $L = N$. This establishes (ii).

(iv) If N is Galois over K , then N is separable over K and the intermediate field E of N/K is also separable over K (Lemma 55.6). Conversely, if E is separable over K , then a_i are separable over K , so $f_i(x)$ are separable over K and N' is a splitting field over K of a polynomial $f(x)$ whose irreducible divisors are separable over K . Thus N is Galois over K (Theorem 55.7).

Finally, let N' be any extension field satisfying (i),(ii),(iii). As $a_i \in E \subseteq N'$ and N' is normal over K , the field N' contains all roots of the minimal polynomial $f_i(x)$ over K , hence N' contains all roots of $f(x)$, hence N' contains a splitting field H' of $f(x)$ over K . Then H' is normal over K (Theorem 55.8). Because of the condition (ii), we get $H' = N'$. Hence N' is a splitting field of $f(x)$ over K . From Example 53.5(e), we deduce that N' is also a splitting field of $f(x)$ over E . Thus both N and N' are splitting fields of $f(x)$ over E and therefore N and N' are E -isomorphic (Theorem 53.8). \square

55.12 Definition: Let E/K be a finite dimensional field extension. An extension field N of E as in Theorem 55.11 is called a *normal closure of E over K* .

Since a normal closure of E over K is unique to within an E -isomorphism, we sometimes speak of *the* normal closure of E over K .

The field $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a normal closure of $\mathbb{Q}(\sqrt[3]{2})$ over \mathbb{Q} . Likewise $\mathbb{Q}(\sqrt[4]{2}, i)$ is a normal closure of $\mathbb{Q}(\sqrt[4]{2})$ over \mathbb{Q} .

Our next topic is the so-called primitive element theorem which states that a finitely generated separable extension is in fact a simple extension. This theorem is due to Abel, but the first complete proof was given by Galois. The elements of a finitely generated separable extension can therefore be expressed in the extremely convenient form $\sum_i a_i u^i$, where u is a primitive element of the extension and a_i are in the base field.

55.13 Theorem: Let E/K be an algebraic separable extension of fields and $a, b \in E$. Then there is an element c in $K(a, b)$ such that $K(a, b) = K(c)$.

Proof: We distinguish two cases according as K is a finite or an infinite field.

If K is finite, then $K(a, b)$ is finite dimensional over K (Theorem 50.12) and has $|K|^{[K(a, b):K]}$ elements. Hence $K(a, b)$ is finite and its characteristic is $p \neq 0$, thus $\mathbb{F}_p \subseteq K(a, b)$ and $K(a, b) = \mathbb{F}_p(c)$ for some c in $K(a, b)$ (Theorem 52.19(1); c can be chosen as a generator of the cyclic group $K(a, b)^\times$). Then $K(a, b) = K(c)$.

Assume now K is infinite. Let N be a normal closure of E over K (Theorem 55.11). Let $f(x) \in K[x]$ be the minimal polynomial of a over K and $g(x) \in K[x]$ the minimal polynomial of b over K . Since $a, b \in E \subseteq N$ and N is normal over K , all roots of $f(x)$ and $g(x)$ lie in N .

Let $a = a_1, a_2, \dots, a_n \in N$ be the roots of $f(x)$ and $b = b_1, b_2, \dots, b_m \in N$ be the roots of $g(x)$. Since E is separable over K , a and b are separable over K , so $f(x)$ and $g(x)$ are separable over K , so $a_i \neq a_j$ when $i \neq j$ ($i, j = 1, 2, \dots, n$) and $b_k \neq b_l$ when $k \neq l$ ($k, l = 1, 2, \dots, m$).

There are finitely many elements in N of the form

$$\frac{b_k - b_l}{a_i - a_j} \quad (i, j = 1, 2, \dots, n; k, l = 1, 2, \dots, m; i \neq j).$$

Since K is assumed to be infinite, there is a $u \in K$ which is distinct from all these $(b_k - b_l)/(a_i - a_j)$. Hence

$$a_i u + b_l \neq a_j u + b_k \quad \text{unless } i = j \text{ and } k = l. \quad (*)$$

With this u , we put $c = au + b = a_1 u + b_1$. We claim $K(a, b) = K(c)$. Certainly $K(c) \subseteq K(a, b)$. In order to prove $K(a, b) \subseteq K(c)$, we must show $a, b \in K(c)$. Since $b = c - au$, the relation $a \in K(c)$ implies $b \in K(c)$. Hence we need only prove $a \in K(c)$. We do this by showing $x - a \in K(c)[x]$. We shall see that $x - a$ is a greatest common divisor of two polynomials in $K(c)[x]$.

Now $a = a_1$ is a root of $f(x)$ and of $g(c - ux)$. These are polynomials in $K(c)[x]$. Thus $x - a$ is a divisor of the greatest common divisor of $f(x)$ and $g(c - ux)$. On the other hand, any root a_i of $f(x)$ distinct from a_1 cannot be a root of $g(c - ux)$, because then $c - ua_i$ would be a root of $g(x)$, hence a_i would be equal to one of $b = b_1, b_2, \dots, b_m$, contrary to (*). Thus $a = a_1$ is the only common root of $f(x)$ and $g(c - ux)$. Thus $x - a$ is a greatest common divisor of the polynomials $f(x)$ and $g(c - ux)$ in $K(c)[x]$ and $x - a$ itself is in $K(c)[x]$. This gives $a \in K(c)$ and completes the proof. \square

We can now prove that every finitely generated algebraic separable extension is a simple extension.

55.14 Theorem: *Let E/K be an algebraic separable extension of fields and assume $E = K(a_1, a_2, \dots, a_m)$. Then there is an element c in E such that $E = K(c)$.*

Proof: We make induction on m . The claim is true when $m = 2$ by Theorem 55.13 (with $E = K(a, b)$). If the assertion is proved for $m - 1$,

then $K(a_1, a_2, \dots, a_{m-1}) = K(c_1)$ for some c_1 and therefore we have $K(a_1, a_2, \dots, a_m) = K(a_1, a_2, \dots, a_{m-1})(a_m) = K(c_1)(a_m) = K(c_1, a_m) = K(c)$ for some $c \in E$.

□

We give a useful characterization of simple algebraic extensions. This yields an alternative proof of Theorem 55.14.

55.15 Theorem: *Let E/K be a finite dimensional extension of fields. E is a simple extension of K if and only if there are only finitely many intermediate fields of E/K .*

Proof: Assume first that E is a simple extension of K , say $E = K(c)$. We want to show that there are finitely many intermediate fields. We will show that each intermediate field of E/K is uniquely determined by a divisor of the minimal polynomial of c over K .

Let $f(x) \in K[x]$ be the minimal polynomial of c over K . Let L be an intermediate field of E/K and let $g(x) \in L[x]$ be the minimal polynomial of c over L . The field L is generated over K by the coefficients of $g(x)$. To see this, let $g(x) = \sum_{i=0}^m a_i x^i$ (with $a_m = 1$) and $M = K(a_1, a_2, \dots, a_m)$. Since $g(x)$ is in $L[x]$, we have $\{a_1, a_2, \dots, a_m\} \subseteq L$ and $K(a_1, a_2, \dots, a_m) \subseteq L$. Thus $M \subseteq L$ and $|E:M| \geq |E:L| = |K(c):L| = |L(c):L| = \deg g(x) = m$. On the other hand, c is a root of a polynomial $g(x)$ in $M[x]$ of degree m , so the degree of the minimal polynomial of c over M is at most m , so $|E:M| = |K(c):M| = |M(c):M| \leq m$ (Theorem 50.7). Therefore $|E:M| = m = |L(c):L| = |E:L|$ and consequently $|L:K| = |M:K|$. Together with $M \subseteq L$, this gives $M = L$ (Lemma 42.15(2)).

Therefore each intermediate field L of E/K is uniquely determined by the minimal polynomial $g(x)$ of the primitive element c over that intermediate field L . We know $g(x)$ divides $f(x)$ in $L[x]$ (Lemma 50.5). Let N be a normal closure of E over K . Then N contains all roots of $f(x)$ and $f(x)$ splits in N . Of course $g(x)$ divides $f(x)$ in $N[x]$ and, since $N[x]$ is a unique factorization domain, $g(x)$ is a product of some of the linear factors of $f(x)$ in $N[x]$. Since, in $N[x]$, there are only finitely many monic divisors of

$f(x)$, there is only a finite number of possibilities for $g(x)$ and there are only a finite number of intermediate fields L .

Assume conversely that there is only a finite number of intermediate fields of E/K . If K is finite, so is E and E is a simple extension of its prime subfield and of K (Theorem 52.19(1)). So we may suppose K is infinite. We choose an element c in E such that $|K(c):K|$ is as large as possible. In other words, $|K(c):K| \geq |K(b):K|$ for any $b \in E$. With this c , we claim $E = K(c)$. Otherwise, there is an $e \in E \setminus K(c)$. As k ranges through the infinite set K , we get finitely many intermediate fields $K(c + ek)$. Thus there are k and k' in K such that $k \neq k'$ and $K(c + ek) = K(c + ek')$. Then $c + ek$ and $c + ek'$ are in $K(c + ek')$, then their difference $e(k - k')$ is in $K(c + ek)$, then e is in $K(c + ek)$, hence ek is also in $K(c + ek)$ and finally $c = (c + ek) - ek$ is in $K(c + ek)$. Thus $e, c \in K(c + ek)$. So $K(c) \subseteq K(c + ek)$. Since $e \in K(c + ek)$ and $e \notin K(c)$, we get $K(c) \subset K(c + ek)$ and thus $|K(c):K| < |K(c + ek):K|$ (Lemma 42.15(2)), a contradiction. Hence $E = K(c)$.

□

Theorem 55.14 follows very easily from Theorem 55.15. Suppose $E = K(a_1, a_2, \dots, a_m)$ is an algebraic separable extension of K . We find a normal closure N of K over E . Then N is Galois over K and finite dimensional over K (Theorem 55.11). The Galois group of the extension N/K is thus finite and it has finitely many subgroups. By the fundamental theorem of Galois theory, there are finitely many intermediate fields of N/K and so finitely many intermediate fields of E/K . Theorem 55.15 states that E is a simple extension of K .

We proceed to prove the converse of Lemma 55.6. We need some preparatory lemmas, which are of intrinsic interest as well.

55.16 Lemma: *Let E/K be an extension of fields of characteristic $p \neq 0$ and let $a \in E$. Assume a is algebraic over K . Then a is separable over K if and only if $K(a) = K(a^p)$.*

Proof: Suppose first that a is separable over K . Then a is also separable over $K(a^p)$ by Lemma 55.5. Let $g(x) \in K(a^p)[x]$ be the minimal polynomial of a over $K(a^p)$. Thus all roots of $g(x)$ are simple. Since a is a root of the

polynomial $x^p - a^p \in K(a^p)[x]$, we have $g(x)|x^p - a^p$ in $K(a^p)[x]$. Therefore $g(x)|x^p - a^p$ and $g(x)|(x - a)^p$ in $E[x]$. So $g(x) = (x - a)^m$ for some m such that $1 \leq m \leq p$. Since $g(x)$ has no multiple roots, we get $m = 1$. Then $g(x) = x - a \in K(a^p)[x]$ and consequently $a \in K(a^p)$. This gives $K(a) \subseteq K(a^p)$ and, since $K(a^p) \subseteq K(a)$ in any case, we obtain $K(a) = K(a^p)$.

Conversely, suppose that $K(a) = K(a^p)$. We want to show that a is separable over K . Let $f(x)$ be the minimal polynomial of a over K . If a is not separable over K , then $f(x)$ has the form $f(x) = g(x^p)$ for some $g(x) \in K[x]$. Here $g(x)$ is irreducible over K because $g(x)$ is not a unit in $K[x]$ (for $f(x)$, being irreducible over K , is not a unit in $K[x]$) and any factorization $g(x) = r(x)s(x)$ with $\deg r(x) \neq 0 \neq \deg s(x)$ would give a proper factorization $f(x) = r(x^p)s(x^p)$ with $\deg r(x^p) \neq 0 \neq \deg s(x^p)$, contrary to the irreducibility of $f(x)$ over K . Clearly $g(x)$ is a monic polynomial and, since $0 = f(a) = g(a^p)$, we see that a^p is a root of $g(x)$. Thus $g(x)$ is the minimal polynomial of a^p over K (Theorem 50.3). Of course $\deg f(x) = p \cdot \deg g(x)$ and

$$|K(a):K| = \deg f(x) = p(\deg g(x)) > \deg g(x) = |K(a^p):K|.$$

Hence $K(a^p)$ is a *proper* subspace of the K -vector space $K(a)$ (Lemma 42.15(2)), contrary to the hypothesis $K(a) = K(a^p)$. Consequently, $K(a) = K(a^p)$ implies that a is separable over K . \square

55.17 Lemma: *Let E/K be a finite dimensional extension of fields of characteristic $p \neq 0$, say $|E:K| = n$. Then the following are equivalent.*

- (1) *There is a K -basis $\{u_1, u_2, \dots, u_n\}$ of E such that $\{u_1^p, u_2^p, \dots, u_n^p\}$ is also a K -basis of E .*
- (2) *For all K -bases $\{t_1, t_2, \dots, t_n\}$ of E , $\{t_1^p, t_2^p, \dots, t_n^p\}$ is also a K -basis of E .*
- (3) *E is a separable extension of K .*

Proof: (1) \implies (2) Let $\{u_1, u_2, \dots, u_n\}$ be a such a K -basis of E that $\{u_1^p, u_2^p, \dots, u_n^p\}$ is also a K -basis of E and let $\{t_1, t_2, \dots, t_n\}$ be an arbitrary K -basis of E . In order to show that $\{t_1^p, t_2^p, \dots, t_n^p\}$ is a K -basis of E , it suffices to prove that $\{t_1^p, t_2^p, \dots, t_n^p\}$ spans E over K (Lemma 42.13(2); t_i^p are mutually distinct since $t_i^p - t_j^p = (t_i - t_j)^p \neq 0$ for $i \neq j$) and thus it suffices to prove that $u_i^p \in s_K(t_1^p, t_2^p, \dots, t_n^p)$ for all $i = 1, 2, \dots, n$. But this is obvious: we have

$$u_i \in s_K(t_1, t_2, \dots, t_n),$$

$$\begin{aligned}
u_i &= k_1 t_1 + k_2 t_2 + \cdots + k_n t_n && \text{for some } k_j \in K, \\
u_i^p &= k_1^p t_1^p + k_2^p t_2^p + \cdots + k_n^p t_n^p && \text{for some } k_j^p \in K, \\
u_i^p &\in s_K(t_1^p, t_2^p, \dots, t_n^p).
\end{aligned}$$

(2) \Rightarrow (1) This is trivial.

(2) \Rightarrow (3) Suppose now that $\{t_1^p, t_2^p, \dots, t_n^p\}$ is a K -basis of E whenever $\{t_1, t_2, \dots, t_n\}$ is. Every element in E is algebraic over K because E/K is a finite dimensional extension (Theorem 50.10). Thus we are to show that every element b of E is separable over K . We do this by proving $K(b) = K(b^p)$ (Lemma 55.16).

Let $b \in E$. We put $r = |K(b):K|$. Then $r \leq n$ and $\{1, b, b^2, \dots, b^{r-1}\}$ is a K -basis of $K(b)$. We extend the K -linearly independent subset $\{1, b, b^2, \dots, b^{r-1}\}$ of E to a K -basis $\{1, b, b^2, \dots, b^{r-1}, c_{r+1}, \dots, c_n\}$ of E , as is possible by virtue of Theorem 42.14. Then $\{1, b^p, (b^p)^2, \dots, (b^p)^{r-1}, c_{r+1}^p, \dots, c_n^p\}$ is also a K -basis of E by hypothesis and so $\{1, b^p, (b^p)^2, \dots, (b^p)^{r-1}\}$ is a K -linearly independent subset of $K(b)$. Lemma 42.13(1) states that $\{1, b^p, (b^p)^2, \dots, (b^p)^{r-1}\}$ spans $K(b)$ over K . So $K(b) \subseteq s_K(1, b^p, (b^p)^2, \dots, (b^p)^{r-1}) \subseteq K(b^p)$. This proves $K(b) = K(b^p)$. Hence b is separable over K .

(3) \Rightarrow (2) We assume E is separable over K and $\{t_1, t_2, \dots, t_n\}$ is a K -basis of E . We want to show that $\{t_1^p, t_2^p, \dots, t_n^p\}$ is a K -basis of E . Since $t_i^p \neq t_j^p$ for $i \neq j$, the set $\{t_1^p, t_2^p, \dots, t_n^p\}$ has exactly $n = |E:K|$ elements and, in view of Lemma 42.13, it suffices to prove that $\{t_1^p, t_2^p, \dots, t_n^p\}$ spans E over K . So we put $L = s_K(t_1^p, t_2^p, \dots, t_n^p)$ and try to show $L = E$.

Our first step will be to establish that L is a subring of E . In order to prove this, we must only show that L is closed under multiplication. If a

$$= \sum_{i=1}^n a_i t_i^p \text{ and } b = \sum_{j=1}^n b_j t_j^p \text{ are elements of } L \text{ (} a_i, b_j \in K \text{), then } ab = \sum_{i,j=1}^n a_i b_j t_i^p t_j^p,$$

and L will be closed under multiplication provided $t_i^p t_j^p \in L$. As $\{t_1, t_2, \dots, t_n\}$

is a K -basis of E , there are elements c_{ijk} in K with $t_i t_j = \sum_{k=1}^n c_{ijk} t_k$ and so

$$t_i^p t_j^p = \sum_{k=1}^n c_{ijk}^p t_k^p \in s_K(t_1^p, t_2^p, \dots, t_n^p) = L. \text{ Thus } L \text{ is a subring of } E.$$

Since L contains K and $\{t_1^p, t_2^p, \dots, t_n^p\}$, and L is contained in the ring $K[t_1^p, t_2^p, \dots, t_n^p]$, we get $L = K[t_1^p, t_2^p, \dots, t_n^p]$. Now for each $i = 2, \dots, n$, the element t_i^p is algebraic over K , so algebraic over $K(t_1^p, \dots, t_{i-1}^p)$ and so $K(t_1^p, \dots, t_{i-1}^p)[t_i] = K(t_1^p, \dots, t_{i-1}^p)(t_i)$ (Theorem 50.6) and repeated application of Lemma 49.6(2), Lemma 49.6(3) gives $L = K[t_1^p, t_2^p, \dots, t_n^p] = K(t_1^p, t_2^p, \dots, t_n^p)$. Thus $L = K(t_1^p, t_2^p, \dots, t_n^p)$ and L is in fact a field.

We now prove $E = K(t_1^p, t_2^p, \dots, t_n^p)$. Let a be an arbitrary element of E . Then a is algebraic over K and over L (Lemma 50.5). Let $f(x) \in L[x]$ be the minimal polynomial of a over L . Since $a \in s_K(t_1^p, t_2^p, \dots, t_n^p)$ and therefore $a^p \in s_K(t_1^p, t_2^p, \dots, t_n^p) = L$, we see $x^p - a^p \in L[x]$ and a is a root of $x^p - a^p$. Thus $f(x)$ divides $x^p - a^p$ in $L[x]$. We put $x^p - a^p = f(x)^e g(x)$, where $e \geq 1$, $g(x) \in L[x] \setminus \{0\}$ and $(f(x), g(x)) \approx 1$ in $L[x]$. Taking derivatives, we obtain

$$\begin{aligned} 0 &= ef(x)^{e-1}f'(x)g(x) + f(x)g'(x), \\ g(x) &\text{ divides } f(x)g'(x) \text{ in } L[x], \\ g(x) &\text{ divides } g'(x) \text{ in } L[x], \\ g'(x) &= 0, \\ 0 &= ef(x)^{e-1}f'(x)g(x), \end{aligned}$$

and since E is separable over K , here $f'(x) \neq 0$, so $f(x)^{e-1}f'(x)g(x) \neq 0$ and

$$\begin{aligned} e &= 0 \text{ in } L, \\ p|e &\text{ in } \mathbb{Z}, \\ e &= pm \text{ for some } m \in \mathbb{N}, \\ p &= \deg(x^p - a^p) = pm(\deg f(x)) + \deg g(x), \\ m &= 1, \deg f(x) = 1 \text{ and } g(x) = 0, \\ e &= p \text{ and } g(x) = 1 \text{ (comparing leading coefficients),} \\ (x - a)^p &= x^p - a^p = f(x)^p, \\ x - a &= f(x) \in L[x], \end{aligned}$$

and $a \in L$. This proves $E \subseteq L$. Hence $E = L = s_K(t_1^p, t_2^p, \dots, t_n^p)$ and thus $\{t_1^p, t_2^p, \dots, t_n^p\}$ is a K -basis of E , as was to be proved. \square

55.18 Lemma: *Let E/K be a field extension and $a \in E$. Then $K(a)$ is a separable extension of K if and only if a is separable over K .*

Proof: If $K(a)$ is separable over K , then every element of $K(a)$ is separable over K , in particular a is separable over K . Suppose now a is separable (thus algebraic) over K . We wish to prove that $K(a)$ is separable

over K . The case $\text{char } K = 0$ being trivial, we may assume $\text{char } K = p \neq 0$. Let $n = |K(a):K|$. Then $\{1, a, a^2, \dots, a^{n-1}\}$ is a K -basis of $K(a)$ (Theorem 50.7). Likewise $\{1, a^p, (a^p)^2, \dots, (a^p)^{m-1}\}$ is a K -basis of $K(a^p)$, where $m = |K(a^p):K|$. Since a is separable over K , we have $K(a^p) = K(a)$ (Lemma 55.16) and $m = |K(a^p):K| = |K(a):K| = n$. Thus $\{1, a^p, (a^p)^2, \dots, (a^p)^{n-1}\} = \{1^p, (a^p)^p, (a^2)^p, \dots, (a^{n-1})^p\}$ is also a K -basis of $K(a)$. Thus $K(a)$ is separable over K by Lemma 55.17. \square

55.19 Theorem: *Let E/K be a finite dimensional field extension and let L be an intermediate field of E/K . Then E is separable over K if and only if E is separable over L and L is separable over K .*

Proof: If E is separable over K , then E is separable over L and L is separable over K (Lemma 55.6). Conversely, suppose that E is separable over L and L is separable over K . We are to show that (1) E is algebraic over K and that (2) any element in E is separable over K . Since E/L and L/K are separable extensions, they are algebraic extensions and E/K is also algebraic by Theorem 50.16. Now the separability of E over K . The case $\text{char } K = 0$ being trivial, we assume $\text{char } K = p \neq 0$. As E/K is a finite dimensional extension by hypothesis, $|E:L|$ and $|L:K|$ are finite (Lemma 48.14). Let $|E:L| = n$ and $|L:K| = m$.

Since E is separable over L , there is an L -basis $\{a_1, a_2, \dots, a_n\}$ of E such that $\{a_1^p, a_2^p, \dots, a_n^p\}$ is also an L -basis of E and, since L is separable over K , there is a K -basis $\{b_1, b_2, \dots, b_m\}$ of L such that $\{b_1^p, b_2^p, \dots, b_m^p\}$ is also a K -basis of L (Lemma 55.17). Then $\{a_i b_j\}$ is a K -basis of E by the proof of Theorem 48.13, and likewise $\{a_i^p b_j^p\}$ is a K -basis of E . Hence $\{a_i b_j\}$ is a K -basis of E such that $\{(a_i b_j)^p\}$ is also a K -basis of E . From Lemma 55.17, it follows that E is separable over K . \square

We close this paragraph with a brief discussion of perfect fields.

55.20 Definition: Let K be a field. If $\text{char } K = 0$ or if $\text{char } K = p \neq 0$ and for each $a \in K$, there is a $b \in K$ such that $a = b^p$, then K is said to be *perfect*.

Thus in case $\text{char } K = p \neq 0$, K is a perfect field if and only if the field homomorphism $\varphi: K \rightarrow K$ is onto K . Then for each $a \in K$, there is a

$$u \rightarrow u^p$$

unique $b \in K$ such that $a = b^p$, for φ is one-to-one. This unique b will be denoted by $\sqrt[p]{a}$.

For example, every finite field is perfect, for if \mathbb{F}_q is a finite field and $\text{char } \mathbb{F}_q = p \neq 0$, then the one-to-one homomorphism $\varphi: \mathbb{F}_q \rightarrow \mathbb{F}_q$ ($u \rightarrow u^p$) is \mathbb{F}_p -linear and thus onto \mathbb{F}_q by Theorem 42.22 (or, more simply, because the one-to-one mapping from the finite set \mathbb{F}_q into \mathbb{F}_q must be onto \mathbb{F}_q).

55.21 Theorem: *Let K be a field. K is perfect if and only if every irreducible polynomial in $K[x]$ is separable over K .*

Proof: The assertion is trivial in case $\text{char } K = 0$, so assume that $\text{char } K = p \neq 0$.

Suppose first that K is perfect. Now, if $f(x) \in K[x]$ is not separable over K ,

then $f(x) = g(x^p)$ for some $g(x) \in K[x]$, say $g(x) = \sum_{i=0}^m a_i x^i$ and

$$f(x) = g(x^p) = \sum_{i=0}^m a_i x^{ip} = \sum_{i=0}^m (\sqrt[p]{a_i})^p x^{ip} = \left(\sum_{i=0}^m \sqrt[p]{a_i} x^i \right)^p,$$

$f(x)$ cannot be irreducible over K . Thus, if K is a perfect field, then every irreducible polynomial in $K[x]$ is separable over K .

Conversely, suppose that every irreducible polynomial in $K[x]$ is separable over K . We want to show that K is perfect. Let $a \in K$. We must find a b in K with $b^p = a$. So we consider the polynomial $x^p - a \in K[x]$. We adjoin a root $\sqrt[p]{a}$ of $x^p - a$ to K and obtain the field $K(\sqrt[p]{a})$ (possibly $K \subset K(\sqrt[p]{a})$). Then, in $K(\sqrt[p]{a})[x]$, we have the factorization $x^p - a = (x - \sqrt[p]{a})^p$. The minimal polynomial of $\sqrt[p]{a}$ over K is thus $(x - \sqrt[p]{a})^k$ for some $k \in \{1, 2, \dots, p\}$. So $(x - \sqrt[p]{a})^k$ is necessarily irreducible and, by hypothesis, separable over K and has therefore no multiple roots. This forces $k = 1$. So the minimal polynomial of $\sqrt[p]{a}$ is $x - \sqrt[p]{a} \in K[x]$, which gives $\sqrt[p]{a} \in K$, as was to be proved. \square

Consequently every algebraic extension of a perfect field K is separable over K . Theorem 55.21 yields the corollary that every algebraically closed field is perfect, since any irreducible polynomial in an algebraically closed field is of first degree and has therefore no multiple roots (is separable over that field).

Exercises

1. Find a normal closure of $\mathbb{Q}(\sqrt{3}, \sqrt[5]{7})$ over \mathbb{Q} .
2. If E/K is a field extension and $|E:K| = 2$, show that E is normal over K .
3. Let E/K be a field extension with $|E:K| = 3$ and assume that E is not normal over K . Let N be a normal closure of E over K . Show that $|N:K| = 6$ and that there is a unique intermediate field L of N/K satisfying $|L:K| = 2$.
4. Let N/K be a field extension and assume that N is normal over K . Let L be an intermediate field of N/K . Prove that L is normal over K if and only if E is (K, N) -stable.
5. Find fields $K \subseteq L \subseteq N$ such that N is normal over L , L is normal over K but N is not normal over K .
6. Find fields $K \subseteq L \subseteq N$ such that $|N:K| = 6$, N is Galois over K but L is not Galois over K .
7. Find fields $K \subseteq L \subseteq N$ such that $|N:K|$ is finite, N is normal over K but L is not normal over K .
8. Find primitive elements for the extensions $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ of \mathbb{Q} .
9. Find a splitting field K over \mathbb{F}_3 of $(x^2 + 1)(x^2 + x + 2) \in \mathbb{F}_3[x]$ and a primitive element of K .

10. Let p be a prime number and x, y two distinct indeterminates over \mathbb{F}_p . Let $E = \mathbb{F}_p(x, y)$ and $K = \mathbb{F}_p(x^p, y^p)$. Show that E is not a simple extension of K and find infinitely many intermediate fields of E/K .
11. Prove the following generalization of Theorem 55.14. If K is a field, $K(a_1, a_2, \dots, a_m)$ is an algebraic extension of K and a_2, \dots, a_m are separable over K , then $K(a_1, a_2, \dots, a_m)$ is a simple extension of K .
12. Let K be a field and $K(a_1, a_2, \dots, a_m)$ a finitely generated extension of K . Show that $K(a_1, a_2, \dots, a_m)$ is separable over K if and only if all a_1, a_2, \dots, a_m are separable over K .
13. Prove that Theorem 55.19 is valid without the hypothesis that E be finite dimensional over K . (Hint: Reduce the general case to the finite dimensional case.)
14. Let L and M be intermediate fields of a field extension E/K . Prove that, if L is separable over K , then LM is separable over M .
15. Prove that every finite dimensional extension of a perfect field is perfect.
16. Let E/K be a finite dimensional field extension. If E is perfect, show that K is also perfect.