Chapter 4

Separability

The purpose of this chapter is to introduce a technical condition that appears within our main theorem. We shall observe that all extensions of a field of characteristic zero satisfy this condition (see Corollary 4.9 below), so the main purpose of introducing this condition is to ensure that the theory can be applied both in characteristic zero and in positive characteristic. The main result of this chapter is the Theorem of the Primitive Element that tells us that we can assume, under the technical condition provided, that a finite extension is actually a simple extension. This will enable us to establish later results more easily.

Separable polynomials

Definition 4.1 Let $f(X)$ be an irreducible polynomial over a field F. We say that $f(X)$ is *separable* over F if it has no multiple roots in a splitting field.

So this means that if $f(X)$ is a separable polynomial over a field F, then firstly it is irreducible over F and secondly, if K is a splitting field for $f(X)$ over F, then over K

$$f(X) = c(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$

where the elements α_1, α_2, …, α_n in K are distinct.

In order to interpret and make use of this definition, we introduce the concept of formal differentiation:

Definition 4.2 Let $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ be a polynomial over some field F. The *formal derivative* of $f(X)$ is the polynomial

$$Df(X) = a_1 + 2a_2X + 3a_3X^2 + \dots + na_nX^{n-1}.$$

Example 4.3 (i) When dealing with a polynomial over $\mathbb{C}$ (or indeed over any subfield of $\mathbb{C}$), the formal derivative D is simply the usual derivative of a complex-valued function.

(ii) If $f(X) = X^p + 1$ over some field of characteristic p, then

$$Df(X) = pX^{p-1} = 0.$$

Thus the formal derivative can behave somewhat unexpectedly when we work over a field of positive characteristic.

Despite the unusual behaviour just observed, formal differentiation does satisfy some familiar properties, namely it is linear and satisfies the usual product rule for differentiation.

Lemma 4.4 (Basic properties of formal differentiation) *Let $f(X)$ and $g(X)$ be polynomials in $F[X]$ and α and β be scalars in F. Then*

$$\begin{aligned} D\big(\alpha\, f(X) + \beta\, g(X)\big) &= \alpha\, Df(X) + \beta\, Dg(X) \\ D\big(f(X)\, g(X)\big) &= f(X) \cdot Dg(X) + Df(X) \cdot g(X) \end{aligned}$$

Proof: Suppose first that $f(X) = \sum a_i X^i$ and $g(X) = \sum b_i X^i$. Then

$$\alpha\, f(X) + \beta\, g(X) = \sum (\alpha a_i + \beta b_i) X^i,$$

so

$$\begin{aligned} D\big(\alpha\, f(X) + \beta\, g(X)\big) &= \sum_{i \geqslant 1} i(\alpha a_i + \beta b_i) X^{i-1} \\ &= \alpha \sum_{i \geqslant 1} i a_i X^{i-1} + \beta \sum_{i \geqslant 1} i b_i X^{i-1} \\ &= \alpha\, Df(X) + \beta\, Dg(X), \end{aligned}$$

as required.

Having shown that formal differentiation is linear, we shall now turn to the product rule. Consider first the case when $f(X) = X^m$ and $g(X) = X^n$ are powers of X. Then

$$D(f(X)\, g(X)) = D(X^{m+n}) = (m+n) X^{m+n-1},$$

while

$$\begin{aligned} f(X) \cdot Dg(X) + Df(X) \cdot g(X) &= X^m \cdot n X^{n-1} + m X^{m-1} \cdot X^n \\ &= n X^{m+n-1} + m X^{m+n-1} \\ &= (m+n) X^{m+n-1} \\ &= D(f(X)\, g(X)), \end{aligned}$$

in this special case.

We now use linearity to deal with arbitrary polynomials: for $f(X) = \sum a_i X^i$ and $g(X) = \sum b_i X^i$, observe

$$\begin{aligned} D\big(f(X)\, g(X)\big) &= D\Big(\Big(\sum a_i X^i\Big)\Big(\sum b_j X^j\Big)\Big) \\ &= D\Big(\sum_{i,j} a_i b_j X^i X^j\Big) \\ &= \sum_{i,j} a_i b_j D(X^i X^j) \\ &= \sum_{i,j} a_i b_j (X^i \cdot D(X^j) + D(X^i) \cdot X^j) \\ &= \Big(\sum_i a_i X^i\Big)\Big(\sum_j b_j D(X^j)\Big) + \Big(\sum_i a_i D(X^i)\Big)\Big(\sum_j b_j X^j\Big) \\ &= \Big(\sum_i a_i X^i\Big) \cdot D\Big(\sum_j b_j X^j\Big) + D\Big(\sum_i a_i X^i\Big) \cdot \Big(\sum_j b_j X^j\Big) \\ &= f(X) \cdot Dg(X) + Df(X) \cdot g(X), \end{aligned}$$

as claimed. □

We have now shown that formal differentiation satisfies familiar properties of "normal" differentiation. We are also only using it with polynomials, which were the easiest functions that we first learnt to differentiate anyway. One just simply needs to be careful with polynomials over fields of positive characteristic, where some unusual things happen (as observed in Example 4.3(ii) above). The crucial link between formal differentiation and the concept of separability is the following:

Lemma 4.5 *Let $f(X)$ be a polynomial over a field F. Then $f(X)$ has a repeated root in a splitting field if and only if $f(X)$ and the formal derivative $Df(X)$ have a common factor of degree at least one.*

PROOF: Suppose first that $f(X)$ has a repeated root in a splitting field K for $f(X)$. Then

$$f(X) = (X - \alpha)^2 g(X)$$

where $\alpha \in K$ and $g(X) \in K[X]$ is some polynomial. Hence, using the basic properties of formal differentiation,

$$Df(X) = (X - \alpha)^2 \cdot Dg(X) + 2(X - \alpha)\, g(X)$$

over K. In particular, $f(\alpha) = Df(\alpha) = 0$; that is, $f(X)$ and $Df(X)$ are polynomials over F which vanish when evaluated at α in K. Therefore, by Lemma 2.11(iv), they are both divisible by the minimum polynomial of α. Thus they have a common factor of degree at least one.

Conversely, suppose $f(X)$ has no repeated root in a splitting field K. Over the majority of the rest of this proof, we forget about the original field F and instead work over the splitting field K. We shall show, by induction on the degree n of $f(X)$, that $f(X)$ and $Df(X)$ are coprime in $K[X]$. If $n = 1$, then $Df(X)$ is a non-zero constant (even over a field of positive characteristic), so the highest common factor is also a constant (that is, a unit in $F[X]$) and hence $f(X)$ and $Df(X)$ are indeed coprime.

Suppose that that $n > 1$ and, over the splitting field K, write

$$f(X) = (X - \alpha)\, g(X)$$

where $\alpha \in K$ and $g(X) \in K[X]$. Our hypothesis tells us that $g(X)$ has no repeated roots in K and that $X - \alpha$ does not divide $g(X)$. Then, by the basic properties of formal differentiation,

$$Df(X) = (X - \alpha) \cdot Dg(X) + g(X). \tag{4.1}$$

Suppose that $f(X)$ and $Df(X)$ are not coprime over K. As K is a splitting field for $f(X)$ over F, any polynomial that divides $f(X)$ in $K[X]$ can be factorized into linear factors and we conclude that there exists some linear factor of $f(X)$ in $K[X]$ that also divides $Df(X)$. Now, by hypothesis, $X - \alpha$ does not divide $g(X)$ and hence, by Equation (4.1), it does not divide $Df(X)$. Thus any linear factor dividing both $f(X)$ and $Df(X)$ is not $X - \alpha$. Hence there is a linear factor of $g(X)$ that divides $Df(X)$ and, from Equation (4.1), this linear factor divides $Dg(X)$. However, by induction, $g(X)$ and $Dg(X)$ are coprime in K, so we have a contradiction. This establishes the claim.

We now return to the base field F. If $f(X)$ and $Df(X)$ have a common factor $h(X)$ in $F[X]$, then it also divides these two polynomials in $K[X]$, so it is constant by what we have just established. This shows that, under the assumption that $f(X)$ has no repeated root in K, we can conclude $f(X)$ and $Df(X)$ have only constants as factors. This establishes the required converse. □

Proposition 4.6 *Let $f(X)$ be an irreducible polynomial over a field F of characteristic zero. Then $f(X)$ is separable.*

PROOF: Let $f(X)$ be an irreducible polynomial over a field F. Necessarily $f(X)$ is not constant, so using the fact that F has characteristic zero,

$$Df(X) \neq 0.$$

(If the leading term of $f(X)$ is $a_n X^n$ with $a_n \neq 0$, then the leading term of $Df(X)$ is $na_n X^{n-1}$ and $na_n \neq 0$ in F.) Suppose that $f(X)$ is not separable. Then, by Lemma 4.5, $f(X)$ and $Df(X)$ have a common factor $g(X)$ of degree at least one. Now

$$\deg g(X) \leqslant \deg Df(X) = \deg f(X) - 1,$$

yet $f(X)$ is irreducible so has no non-constant divisors of degree less than $\deg f(X)$. This is a contradiction and we conclude that $f(X)$ is indeed separable. □

The same result is not true over a field of characteristic p. The proof above breaks down since possible $Df(X) = 0$ even when $f(X)$ is an irreducible polynomial over a field of characteristic p. To construct a counterexample requires a bit of work. We shall state the construction here, but defer the details to Problem Sheet IV, Question 5, since this is not central to the theory we develop.

Example 4.7 Let t be an indeterminate and consider the field $F = \mathbb{F}_p(t)$ of rational functions over the finite field $\mathbb{F}_p$ in the indeterminate t. Define

$$f(X) = X^p - t,$$

a polynomial in the indeterminate X with coefficients in the field F. One can establish the following facts:

(i) $f(X) = 0$ has no roots in F;

(ii) if α is any root of $f(X)$ in a splitting field, then $f(X) = (X - \alpha)^p$;

(iii) $f(X)$ is irreducible over F.

Hence $f(X)$ is an inseparable polynomial over the field F.

Separable extensions and the Theorem of the Primitive Element

We shall now extend the concept of separability to extensions. Since it relates to the minimum polynomials of elements in the extension, this definition relates to algebraic extensions.

Definition 4.8 Let K be an algebraic extension of a field F. We say that K is a *separable extension* of F if the minimum polynomial of every element of K over F is separable over F.

In view of Proposition 4.6, we conclude:

Corollary 4.9 *Every algebraic extension of a field of characteristic zero is a separable extension.* □

We now turn to establish the Theorem of the Primitive Element concerning finite separable extensions. This will enable us to assume that we are working with a simple extension; that is, an extension of the form $F(\alpha)$ for some algebraic element α.

Lemma 4.10 *Let L be a separable extension of an infinite field F and let $\beta, \gamma \in L$. Then there exists some $\alpha \in F(\beta, \gamma)$ such that*

$$F(\beta, \gamma) = F(\alpha).$$

PROOF: Recall that a separable extension is, in particular, an algebraic extension. Let $f(X)$ be the minimum polynomial of β over F and $g(X)$ be the minimum polynomial of γ over F. Let K be a splitting field for the polynomial $f(X)\,g(X)$ over F. Let

$$\beta_1, \beta_2, \dots, \beta_m \qquad \text{and} \qquad \gamma_1, \gamma_2, \dots, \gamma_n$$

be the roots of $f(X)$ and $g(X)$, respectively, in K, where $\beta_1 = \beta$ and $\gamma_1 = \gamma$, without loss of generality. The assumption that L is a separable extension ensures that the β_i are distinct and the γ_i are distinct.

Since F is an infinite field, we can choose $c \in F$ such that $c \neq 0$ and

$$c \neq \frac{\beta_1 - \beta_i}{\gamma_1 - \gamma_j}$$

for all $i \geqslant 2$ and $j \geqslant 2$. Put $\alpha = \beta_1 - c\gamma_1$. The purpose of our choice of c is to achieve the following claim:

Claim:

$$\beta_i - c\gamma_j = \alpha \qquad \text{if and only if} \qquad i = j = 1. \tag{4.2}$$

Certainly if $i = j = 1$, then $\beta_i - c\gamma_i = \beta_1 - c\gamma_1 = \alpha$. Conversely, suppose $\beta_i - c\gamma_j = \beta_1 - c\gamma_1$. Then $c(\gamma_1 - \gamma_j) = \beta_1 - \beta_i$. If $j \neq 1$, then $c = (\beta_1 - \beta_i)/(\gamma_1 - \gamma_j)$ which is impossible since if $i = 1$, it says $c = 0$, and if $i \geqslant 2$ then we have contradicted the definition of c. Hence $j = 1$ and now $\beta_1 - \beta_i = 0$, which gives $i = 1$ since the roots of $f(X)$ are distinct.

Let $E = F(\alpha)$, which is some subfield of $F(\beta, \gamma)$ since $\alpha = \beta_1 - c\gamma_1 \in F(\beta, \gamma)$. We must establish the reverse inclusion.

Consider the two polynomials

$$h(X) = f(cX + \alpha) \qquad \text{and} \qquad g(X),$$

which are polynomials over E. Observe that

$$h(\gamma_1) = f(c\gamma_1 + \alpha) = f(\beta_1) = 0,$$

while $g(\gamma_1) = 0$. Our goal is to determine the greatest common divisor of these two polynomials in $E[X]$. However, we first work over the splitting field K. Indeed, over K, we know

$$g(X) = (X - \gamma_1)(X - \gamma_2) \dots (X - \gamma_n)$$

and so the greatest common divisor $k(X)$ of $h(X)$ and $g(X)$ in $K[X]$ is a product of some of these factors $X - \gamma_j$. If $X - \gamma_j$ is a divisor of $h(X)$, then $h(\gamma_j) = 0$; that is,

$$f(c\gamma_j + \gamma) = 0.$$

This $c\gamma_j + \gamma = \beta_i$ for some i and, as noted above in Equation (4.2), this forces $i = j = 1$. Hence any such common factor of $h(X)$ and $g(X)$ could only be $X - \gamma_1$ and this is indeed a factor since $h(\gamma_1) = g(\gamma_1) = 0$. Hence

the greatest common divisor of $h(X)$ and $g(X)$ in $K[X]$ is $k(X) = X - \gamma_1$.

Now consider the highest common factor of $h(X)$ and $g(X)$ in $E[X]$. It is certainly a factor of $h(X)$ and $g(X)$ in the larger ring $K[X]$, so divides $k(X) = X - \gamma_1$. However, if $h(X)$ and $g(X)$ were coprime in $E[X]$, we would be able to find $u(X), v(X) \in E[X]$ such that

$$1 = u(X)\,h(X) + v(X)\,g(X),$$

but this would give a contradiction since the right-hand side evaluates to 0 when we substite the element γ_1 for X. We conclude that the highest common factor of $h(X)$ and $g(X)$ in $E[X]$ must also be $X - \gamma_1$ and hence the coefficient $\gamma = \gamma_1 \in E$. Finally

$$\beta = \beta_1 = \alpha + c\gamma_1 \in E$$

and we deduce $F(\beta, \gamma) \subseteq E = F(\alpha)$.

From this we conclude the claimed equality: $F(\alpha) = F(\beta, \gamma)$. □

Theorem 4.11 (Theorem of the Primitive Element) *Let K be a finite separable extension of an infinite field F. Then $K = F(\alpha)$ for some $\alpha \in K$.*

PROOF: By Theorem 2.17, we know that $K = F(\beta_1, \beta_2, \ldots, \beta_n)$ for some $\beta_1, \beta_2, \ldots, \beta_n \in K$. If $n = 1$, then certainly the claim holds.

If $n > 1$, we now apply induction. Since every element of K has separable minimum polynomial over F, we conclude that $F(\beta_1, \ldots, \beta_{n-1})$ is also a finite separable extension of F. Hence, by induction,

$$F(\beta_1, \ldots, \beta_{n-1}) = F(\gamma)$$

for some γ. Now $K = F(\gamma, \beta_n)$ and, by Lemma 4.10, we now conclude $K = F(\alpha)$ for some $\alpha \in K$, as required. □

Corollary 4.12 *Every finite extension of a field of characteristic zero can be expressed as a simple extension.*

As we mentioned at the start of the chapter, separable extensions will appear in our main theorem. We still need to understand finite separable extensions of finite fields, since Theorem 4.11 does not apply. Accordingly, we study finite fields in the next chapter to establish, in particular, an analogous result upon which we can rely in that case.