9. Normal and Separable extensions

Now we turn to the question, given a field extension, when is there some polynomial for which it is a splitting field?

Definition 9.1. *Let L/K be an algebraic field extension. We say that L/K is* ***normal*** *if given any irreducible polynomial $f(x) \in K[x]$ such that $f(x)$ has at least one root in L then $f(x)$ splits in L.*

Proposition 9.2. *Let L/K be a field extension.*

Then L/K is a finite normal extension if and only if it is the splitting field of some polynomial $f(x) \in K[x]$.

Proof. Suppose that L/K is normal and finite. Pick $\alpha_1, \alpha_2, \dots, \alpha_n$ such that

$$L = K(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Let $m_i(x)$ be the minimum polynomial of α_i. Then $m_i(x)$ splits over L, as L/K is normal. Thus $f(x)$, the product of all the polynomials $m_i(x)$, splits over L/K. It follows that L/K is a splitting field for $f(x)$.

Now suppose that L/K is the splitting field for some polynomial $f(x)$. Pick a monic irreducible polynomial $m(x)$ with a root α in L (so that in fact $m(x)$ is the minimum polynomial of α over K). Let M/L be a splitting field for $m(x) \in L[x]$. It suffices to prove that $L = M$.

Pick any root $\beta \in M$ of $m(x)$. We have to prove that $\beta \in L$. Consider the following lattice of inclusions,

$$\begin{tikzcd}
 & M & \\
L(\alpha) \arrow[ur, hook] & & L(\beta) \arrow[ul, hook] \\
 & L \arrow[uu, hook] \arrow[ul, hook] \arrow[ur, hook] & \\
K(\alpha) \arrow[uu, hook] \arrow[ur, hook] & & K(\beta) \arrow[uu, hook] \\
 & K \arrow[uu, hook] \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Observe first that the extensions $K(\alpha)/K$ and $K(\beta)/K$ are isomorphic, as α and β have the same minimal polynomial. Similarly note that the extensions $L(\alpha)/K(\alpha)$ and $L(\beta)/K(\beta)$ are isomorphic, as both extensions are splitting fields for $f(x)$. It follows, by the tower law, that

$$[L(\alpha) : K] = [L(\beta) : K].$$

But by the tower Law again,

$$[L(\alpha) : K] = [L(\alpha) : L][L : K] \qquad \text{and} \qquad [L(\beta) : K] = [L(\beta) : L][L : K],$$

so that

$$[L(\alpha) : L] = [L(\beta) : L].$$

As $\alpha \in L$, the LHS is one. But then $\beta \in L$ as required. □

We note one rather easy consequence of (9.2),

Lemma 9.3. *Let L/K be a finite normal extension and let M be an intermediary field.*

Then L/M is normal.

Proof. By (9.2), L/K is the splitting field for some polynomial $f(x) \in K[x]$. But then L/M is a splitting field for the same polynomial and again by (9.2) it follows that L/M is normal.

Alternatively we could just prove this directly. Suppose that $\alpha \in L$ is a root of $f(x) \in M[x]$ an irreducible polynomial. Let $m(x)$ be the minimum polynomial of α over K. Then $f(x)$ divides $m(x)$ in $M[x]$. As $m(x)$ splits in L, then so does $f(x)$. □

Definition 9.4. *Let L/K be a field extension.*

*A **normal closure** for L/K is a field N/L such that N/K is normal, and there are no proper intermediary fields, between N and L, with this property.*

Lemma 9.5. *Let L/K be a finite extension.*

Then a normal closure for L/K exists and any two such are isomorphic over L.

Proof. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ generate L/K. Let N/L be a splitting field for the product of the minimum polynomials. Then N/L is a splitting field for the same polynomial, so that N/K is normal. But clearly any other normal closure must be a splitting field for the same polynomials. □

Example 9.6. *Consider the field extension $L = \mathbb{Q}(\alpha)/\mathbb{Q} = K$, where α is a real cube root of 2. This extension is not normal. Indeed the minimum polynomial of α is $x^3 - 2 \in \mathbb{Q}[x]$. But $x^3 - 2$ certainly does not split in this field, as the other two roots of this polynomial, considered as elements of $\mathbb{C}$, are not even real.*

In particular L/K is not the splitting field for any polynomial. Now suppose N/K is a normal closure for L/K. Then N/K is normal and

L is an intermediary field. Even though N/L is normal, in fact L/K is not.

In Galois Theory, the main idea is to relate the structure of the intermediate fields to the group of automorphisms of the field extension. In practice the main issue is to establish that there are enough automorphisms to start with. In turn the only issue is to show that there are enough roots.

Definition 9.7. *Let K be a field and let $m(x) \in K[x]$ be an irreducible polynomial.*

*We say that $m(x)$ is **separable** if $m(x)$ does not have any repeated roots in a splitting field. We say that an arbitrary polynomial is **separable**, if every irreducible factor is separable.*

*Let L/K be a field extension. We say that L/K is a **separable extension**, if the minimum polynomial of every element of L is separable.*

Definition 9.8. *Let R be a commutative ring. The **formal derivative** is a function*

$$D \colon R[x] \longrightarrow R[x]$$

such that if $f(x) \in R[x]$, with

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

then $f'(x) = D(f(x))$, the formal derivative of $f(x)$, is defined as

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots a_1.$$

Lemma 9.9. *The formal derivative is an R-linear map (considering $R[x]$ as a module over R, by restriction of scalars) which satisfies Leibniz's rule, that is,*

$$D(fg) = D(f)g + fD(g).$$

Further if we are given a ring homomorphism $\phi \colon R \longrightarrow S$, then the formal derivative $S[x] \longrightarrow S[x]$ is nothing but the map obtained by extending scalars.

Proof. Linearity is easy to check. Now consider the equation

$$D(fg) = D(f)g + fD(g).$$

Fixing g, note that both sides are linear functions $R[x] \longrightarrow R[x]$, of f. Indeed the LHS is the composition of the two linear maps, multiplication by g and D, and composition of linear maps, is linear. Similarly the RHS is a sum of two linear maps, where one map is the composition the other way. As $R[x]$ is freely generated by the powers of x, we may as well suppose that $f(x) = x^m$. Similarly we may suppose that $g(x) = x^n$. In this case the LHS is

$$D(x^{m+n}) = (m+n)x^{m+n-1},$$

and the RHS is

$$\begin{aligned} D(x^m)x^n + x^m D(x^n) &= (mx^{m-1})x^n + x^m(nx^{n-1}) \\ &= (m+n)x^{m+n-1}, \end{aligned}$$

as required.

The last statement is clear, since both functions are linear and have the same effect on x^n. □

Lemma 9.10. *Let $f(x)$ be a polynomial over K. Then f has a repeated root if and only if $f(x)$ and $f'(x)$ have a common zero in some splitting field.*

Proof. By the last statement of (9.9), passing to a splitting field of $f(x)$, we may as well suppose that $f(x)$ splits in K.

Suppose that $f(x)$ has a repeated root. Then $f(x) = (x-\alpha)^2 g(x)$, for some polynomial $g(x)$. In this case,

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x),$$

so that α is a common root of $f(x)$ and $f'(x)$.

Now suppose that α is a common root of $f(x)$ and $f'(x)$. Then we may write

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

so that

$$f'(x) = g(x) + (x-\alpha)g'(x).$$

Thus α must be a root of $g(x)$. But then $x-\alpha$ divides $g(x)$ and α is a repeated root of $f(x)$. □

Lemma 9.11. *Let $m(x) \in K[x]$ be an irreducible polynomial over a field K.*

Then $m(x)$ has a repeated root if and only if $m'(x) = 0$.

In particular $m(x)$ is inseparable if and only if

$$m(x) = \sum a_i x^{pi},$$

where p is the characteristic.

Proof. There is no harm in assuming that $m(x)$ is monic. By (9.10) $m(x)$ has a repeated root if and only if $m(x)$ and $m'(x)$ have a common root α. As $m(x)$ is irreducible, it follows that $m(x)$ is he minimum polynomial of α and so $m(x)$ divides $m'(x)$. As $m'(x)$ has degree one less than $m(x)$, $m'(x) = 0$. □

Proposition 9.12. *Let L/K be a finite field extension.*

If L/K is not separable then $[L : K]$ is divisible by the characteristic. In particular every field extension in characteristic zero is separable.

Proof. Pick $\alpha \in L$ such that $m(x)$, the minimum polynomial of α, is inseparable. By (9.11) m has degree a multiple of p. In particular p divides divide the LHS of

$$[L : K] = [L : K(\alpha)][K(\alpha) : K]$$

at it divides the RHS. □

Definition-Lemma 9.13. *$\mathbb{F}_q$ denotes the unique field of order q, where q is a power of a prime.*

Proof. Suppose that F is a finite field of order $q = p^n$. Then by (8.13) L is the splitting field of $x^q - x$. It follows that F is unique, by uniqueness of the splitting field.

Now we turn to existence. Let F be the splitting field of $x^q - x$. As

$$D(x^q - x) = qx^{q-1} - 1 = -1$$

has no zeroes whatsoever, it certainly has no zeroes in common with $x^q - x$. Thus $x^q - x$ has q distinct zeroes in F and so F has at least q elements. But we have already seen that this implies that F has order q. □

Example 9.14. *Let $L = \mathbb{F}_p(t)$ and let K be the subfield $\mathbb{F}_p(t^p) = \mathbb{F}_p(s)$, where $s = t^p$.*

Then L/K is a primitive extension, generated by t. Consider the polynomial

$$m(x) = x^p - s \in K[x].$$

Then t is a root of $m(x)$. On the other hand, we have

$$\begin{aligned} m(x) &= x^p - s \\ &= x^p - t^p \\ &= (x - t)^p \in L[x]. \end{aligned}$$

Thus if we can show that $m(x)$ is irreducible, it would follow that the extension L/K is inseparable of degree p. This follows easily from the result below.

Theorem 9.15 (Einstein's Criteria: Bis)**.** *Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x] = \mathbb{F}_p[s][x],$$

be a polynomial, and fix an irreducible polynomial $p = p(s) \in R$. Suppose that p does not divide the leading coefficient a_n of $f(x)$, but it does divide the rest, whilst p^2 does not divide a_0.

Then $f(x) \in K[x] = \mathbb{F}_p(s)[x]$ is irreducible.

Proof. We first apply Gauss' Lemma. If we let $R = \mathbb{F}_p[s]$ then the field of fractions of R is K. As $f(x) \in R[x]$, Gauss' Lemma informs us that it is sufficient to prove that $f(x)$ is irreducible in $R[x]$.

Suppose not. Then we could find $g(x)$ and $h(x) \in R[x]$ such that

$$f(x) = g(x)h(x).$$

Suppose that

$$g(x) = b_l x^l + b_{l-1} x^{l-1} + \cdots + b_0 \qquad \text{and} \qquad h(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_0$$

Let

$$R \longrightarrow R/\langle p \rangle = F,$$

denote reduction modulo p. As R is the polynomial ring over a field and p is irreducible, we have already seen that F is a field. In fact F is also finite, of characteristic p, so in fact it is isomorphic to $\mathbb{F}_q$, where q is a power of a prime. We will not need this.

As with the proof of Eisenstein's criteria, this map determines, by the universal property of a polynomial ring, a map

$$R[x] \longrightarrow F[x]$$

In both maps, reduction modulo p, is denoted by a bar. We have

$$\begin{aligned} x^n &= \bar{m}(x) \\ &= \bar{f}(x)\bar{g}(x). \end{aligned}$$

As $F[x]$ is a UFD and $x \in F[x]$ is prime, in fact $\bar{f}(x) = x^l$ and $\bar{g}(x) = x^m$. But then $\bar{b}_0 = \bar{c}_0 = 0$. Thus p divides both b_0 and c_0. But then p^2 divides $a_0 = b_0 c_0$. □