8. Splitting Fields

Definition 8.1. *Let K be a field and let $f(x)$ be a polynomial in $K[x]$. We say that $f(x)$* ***splits*** *in K if there are elements $\alpha_1, \alpha_2, \dots, \alpha_n$ of K such that*

$$f(x) = \lambda(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\dots(x-\alpha_n).$$

We say that a field extension L/K is a ***splitting field*** *if $f(x)$ splits in L and there is no proper intermediary subfield M in which $f(x)$ splits.*

Example 8.2. *Let $f(x) = x^2 - 5x + 6$. Then $\mathbb{Q}$ is a splitting field for f.*

Indeed

$$f(x) = (x-2)(x-3),$$

and $\mathbb{Q}$ does not contain any proper fields whatsoever, let alone smaller fields in which $f(x)$ would split.

Example 8.3. *Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Then $f(x)$ splits in $\mathbb{C}$, as*

$$f(x) = (x-i)(x+i).$$

But $\mathbb{C}$ is not a splitting field. Indeed f splits inside $\mathbb{Q}(i)$, and this is much smaller than $\mathbb{C}$. In fact this field is a splitting field, almost by definition.

Example 8.4. *Finally consider $x^6 - 2$.*

Let $\alpha = \sqrt[6]{2}$, be the unique positive real root, and let ω be a primitive sixth root of unity, so that $\omega^6 = 1$, but no smaller power of ω is equal to one. Then a splitting field is given by

$$\mathbb{Q}(\alpha, \omega).$$

Indeed the six roots of $x^6 - 2$ are α, $\omega\alpha$, $\omega^2\alpha$, $\omega^3\alpha$, $\omega^4\alpha$ and $\omega^5\alpha$. It follows that $x^6 - 2$ does split in this field. On the other hand, we must include α and

$$\omega = \frac{\omega\alpha}{\alpha}.$$

Lemma 8.5. *Let $f(x) \in K[x]$ and suppose that L/K is an extension of K over which $f(x)$ splits,*

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\dots(x-\alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in L$.

Then $M = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ is a splitting field of f.

Proof. Clear. □

Lemma 8.6. *Let $f(x) \in K[x]$ be a polynomial.*
Then $f(x)$ has a splitting field.

Proof. By (8.5) it suffices to find a field extension L/K in which $f(x)$ splits. The proof is by induction on the degree d of $f(x)$. If $d = 1$, then $f(x)$ is a linear polynomial,

$$ax + b = a(x - \alpha),$$

where $\alpha = -b/a \in K$. Thus K/K is a splitting field for f in this case.

Now suppose that the result is true for any field extension of degree less than n.

Suppose that $f(x)$ is irreducible. In this case $f(x)$ is also prime, as $K[x]$ is a UFD. But then $\langle f(x) \rangle$ is a prime ideal and the quotient ring

$$\frac{K[x]}{\langle f(x) \rangle}.$$

is in fact a field L, an extension of K. Further if α denotes the left coset $x + \langle f(x) \rangle$, then $L = K(\alpha)$, and α is a root of $f(x)$. Thus we may factor $f(x)$ as

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

where $g(x) \in L[x]$ has degree $n - 1$.

Replacing K by L we may assume that $f(x)$ is reducible. Suppose that

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

where both $g(x)$ and $h(x)$ have degree at least one. We proceed in two steps. First we find a field extension, M/K in which $g(x)$ splits. Then we find a field extension L/M for which $h(x)$ splits. It is clear that we are able to do this, as both $g(x)$ and $h(x)$ have degree smaller than n. In this case $f(x)$ clearly splits in L/K. □

Now we know that splitting fields exist, we turn to the problem of showing that they are unique. At this point there arises a small problem. The idea is to apply the same argument as the one above. The problem is that when we carry out our inductive step, in the case that $f(x)$ is reducible, we will have two intermediate field extensions M/K and M'/K. We then we want to argue that L/M and L'/M' are isomorphic extensions. In fact we want to slightly enlarge our notion of two isomorphic field extensions.

Definition 8.7. *The category of field extensions has as objects field extensions L/K and as morphisms between objects L/K and L'/K'*

pairs of ring homomorphisms $\phi\colon K \longrightarrow K'$ and $\psi\colon L \longrightarrow L'$ such that the following diagram commutes,

$$\begin{tikzcd} L \arrow[r, "\psi"] & L' \\ K \arrow[u, hook] \arrow[r, "\phi"] & K'. \arrow[u, hook] \end{tikzcd}$$

Of course, once we have a category, we have a notion of isomorphism; this translates to the condition that both ϕ and ψ are isomorphisms.

Lemma 8.8. *Let L/K be a primitive field extension, where $\alpha \in L$. Suppose we are given a ring homomorphism $\phi\colon K \longrightarrow K'$ and a field extension L'/K'. Suppose $\beta \in L'$.*

Then we may find a ring homomorphism $\psi\colon L \longrightarrow L'$ extending ϕ which sends α to β, if and only if β is a root of the image of the minimum polynomial of α.

Proof. One direction is clear. Suppose that we can find such a ψ. Then

$$\begin{aligned} \phi(m_\alpha)(\beta) &= \psi(m_\alpha)(\psi(\alpha)) \\ &= \psi(m_\alpha(\alpha)) \\ &= 0. \end{aligned}$$

Now suppose that the converse is true. We may as well suppose that $L' = K'(\beta)$. Then

$$L \simeq \frac{K[x]}{\langle m_\alpha(x)\rangle} \qquad \text{and} \qquad L' \simeq \frac{K'[x]}{\langle m_\beta(x)\rangle}.$$

But as β is a root of $\phi(m_\alpha(x))$, it follows that $m_\beta(x)$ divides $\phi(m_\alpha(x))$. Define a ring homomorphism

$$f\colon K[x] \longrightarrow \frac{K'[x]}{\langle m_\beta(x)\rangle}$$

as the composition of the ring homomorphism

$$K[x] \longrightarrow K'[x]$$

whose existence is guaranteed by the universal property of a polynomial ring, and the canonical projection,

$$K'[x] \longrightarrow \frac{K'[x]}{\langle m_\beta(x)\rangle}.$$

We have already seen that $m_\alpha(x)$ is in the kernel I of f, so that $\langle m_\alpha(x)\rangle \subset I$. Thus by the universal property of the quotient map, there is an induced map

$$\frac{K[x]}{\langle m_\alpha(x)\rangle} \longrightarrow \frac{K'[x]}{\langle m_\beta(x)\rangle}.$$

Via the two isomorphisms above, this induces a ring homomorphism

$$\psi \colon L \longrightarrow L'$$

which extends ϕ and sends α (corresponding to $x + \langle m_\alpha(x)\rangle$) to β. $\square$

Lemma 8.9. *Suppose we are given a ring homomorphism $\phi \colon K \longrightarrow K'$. Let $f(x) \in K[x]$ be a polynomial and let $f'(x)$ be the corresponding polynomial in $K'[x]$. Let L/K be a splitting field for $f(x)$ and let L'/K' be a field in which $f'(x)$ splits. Then there is an induced morphism (ϕ, ψ), in the category of field extensions, that is, there is a ring homomorphism $\psi \colon L \longrightarrow L'$ such that the following diagram commutes,*

$$\begin{tikzcd} L \arrow[r, "\psi"] & L' \\ K \arrow[u, hook] \arrow[r, "\phi"] & K'. \arrow[u, hook] \end{tikzcd}$$

If further ϕ is an isomorphism and L'/K' is a splitting field for $f'(x)$, then so is ψ.

Proof. The proof proceeds by induction on the degree n of the field extension L/K. If the degree is one, then there is nothing to prove, as in this case $L = K$ and we make take $\psi = \phi$.

So suppose that the result is true for any field extension of degree less than n. Pick a root $\alpha \in L$ of $f(x)$, which is not in K. Let $m(x)$ be the minimum polynomial of α. Then $m(x)$ divides $f(x)$, as α is a root of $f(x)$. Let $m'(x) \in K'[x]$ be the polynomial corresponding to $m(x)$. As $f'(x)$ splits in L', it follows that there is an element $\beta \in L'$, which is a root of $m'(x)$. By (8.8) we may find a ring homomorphism π extending ϕ,

$$\begin{tikzcd} K(\alpha) \arrow[r, "\pi"] & K'(\beta) \\ K \arrow[u, hook] \arrow[r, "\phi"] & K'. \arrow[u, hook] \end{tikzcd}$$

As $[K(\alpha) : K] > 1$, it follows by the Tower Law that $[L : K(\alpha)] < [L : K]$. By induction, we can find ψ extending π,

$$\begin{tikzcd}
L \arrow[r, "\psi"] & L' \\
K(\alpha) \arrow[u, hook] \arrow[r, "\pi"] & K'(\beta). \arrow[u, hook]
\end{tikzcd}$$

Since ψ extends π and π extends ϕ, it follows that ψ extends ϕ, as required.

Now suppose that L'/K' is a splitting field for $f'(x)$ and that ϕ is an isomorphism. As ψ is a ring homomorphism between fields, it follows that ψ is injective. It follows that

$$[L : K] \leq [L' : K'].$$

Replacing ϕ by its inverse, by symmetry we also get

$$[L' : K'] \leq [L : K].$$

Thus

$$[L : K] = [L' : K'].$$

But any linear injective map between two finite dimensional vector spaces of the same dimension is automatically a bijection, so that ψ is in fact an isomorphism. □

We can use the result above to give a complete description of finite fields. First a couple of useful results.

Definition 8.10. *Let G be a group. The **exponent** of G is the least common multiple of the orders of the elements of G.*

Lemma 8.11. *Let G be a finite abelian group of order n.*

Then G has an element of order the exponent m of G. In particular $m = n$ if and only if G is cyclic.

Proof. By the classification of finitely generated abelian groups, we may find integers $m_1, m_2, \dots, m_k$ such that

$$G \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k},$$

where m_i divides m_{i+1}. In this case $m = m_k$ and so it is clear that there are elements of order $m =$. □

Lemma 8.12. *Let G be a finite subgroup of the multiplicative group of a field F.*

Then G is cyclic.

Proof. Let m be the exponent of G and let n be the order of G. Now G is abelian as F is a field. Thus $m \leq n$ and for every element α of G, $\alpha^m = 1$, so that every element of G is a root of the polynomial

$$x^m - 1 \in F[x].$$

But a polynomial of degree m has at most m roots, and so $n \leq m$. But then $m = n$ and G is cyclic. $\square$

Theorem 8.13. *Let L be a finite field of order $q = p^n$.*

Then the elements of L are the q roots of the polynomial $x^q - x$. In particular L is the splitting field of the polynomial $x^q - x$. Furthermore there is an element $\alpha \in L$ such that $L = \mathbb{F}_p(\alpha)$.

Proof. Let G be the set of non-zero elements of L. Then G is a finite subgroup of the multiplicative group. Thus the elements of G are precisely the $q - 1$ roots of the polynomial

$$x^{q-1} - 1.$$

Thus the elements of L are indeed the roots of the polynomial

$$x^q - x.$$

Let α be a generator of the cyclic group G. Then $G = \langle \alpha \rangle$, so that certainly $L = \mathbb{F}(\alpha)$. $\square$