

3. SPLITTING FIELDS

Definition 3.1. 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 intermediary subfield M in which $f(x)$ splits.

Example 3.2. 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.

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.

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 $\alpha, \omega\alpha, \omega^2\alpha, \omega^3\alpha, \omega^4\alpha$ 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 3.3. 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 3.4. Let $f(x) \in K[x]$ be a polynomial.

Then $f(x)$ has a splitting field.

Proof. By 3.3 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 $g(x) \in L[x]$.

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 . \square

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 3.5. We say that the two field extensions L/K and L'/K' are isomorphic if there are ring isomorphisms $\psi: L \rightarrow L'$ and $\phi: K \rightarrow K'$

K' such that the following diagram commutes,

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\phi} & K' \end{array}$$

In fact this gives us a category, the category of field extensions. The objects are field extensions L/K and the morphisms are pairs of ring maps, such that the given diagram commutes.

Lemma 3.6. *Let L/K be a primitive field extension, where $\alpha \in L$. Suppose we are given a ring homomorphism $\phi: K \rightarrow K'$ and a field extension L'/K' . Suppose $\beta \in L'$.*

Then we may find a ring homomorphism $\psi: L \rightarrow L'$ which sends α to β , iff 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

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

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

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

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 $f(x)$, 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

$$\psi: L \longrightarrow L'$$

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

Lemma 3.7. *Suppose we are given a ring homomorphism $\phi: K \longrightarrow K'$. 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 $\psi: L \longrightarrow L'$ such that the following diagram commutes,*

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\phi} & K' \end{array}$$

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 3.6 we may find a ring homomorphism π extending ϕ ,

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\pi} & K'(\beta) \\ \uparrow & & \uparrow \\ K & \xrightarrow{\phi} & K' \end{array}$$

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

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{\pi} & K'(\beta). \end{array}$$

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 π 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. \square

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

Definition 3.8. Let G be a group. The **exponent** of G is the least common multiple of the orders of the elements of G .

Lemma 3.9. Let G be a finite abelian group of order n .

Then the exponent m of G is smallest value of r such that $g^r = e$. In particular $m = n$ iff 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

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

where m_i divides m_{i+1} . In this case it is clear that $m = m_k$. \square

Lemma 3.10. 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 3.11. *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 $L = \mathbb{F}_p(\alpha)$. \square

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

Definition 3.12. *Let L/K be a 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 3.13. *Let L/K be a field extension.*

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

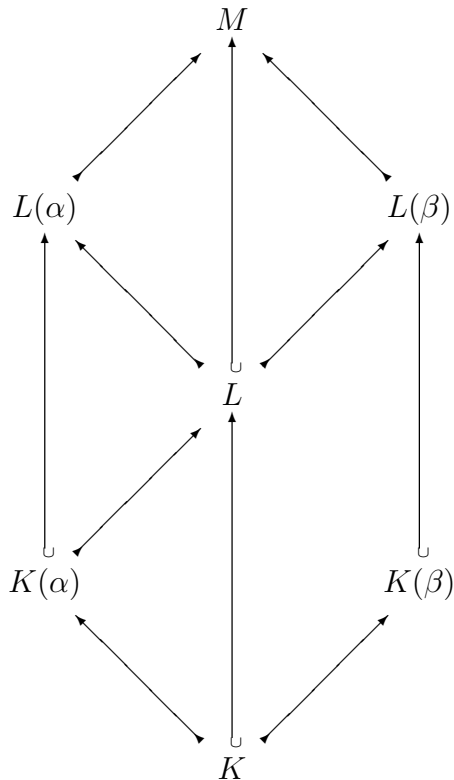
Proof. Suppose that L/K is normal and finite. Pick $\alpha_1, \alpha_2, \dots, \alpha_n$ such that

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

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 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 is clear that M/K is a splitting field for $m(x)$. It suffices then, 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,



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,

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

so that

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

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

We note one rather easy consequence of 3.13,

Lemma 3.14. *Let L/K be a finite normal extension and let M be an intermediary field.*

Then L/M is normal.

Proof. By 3.13, 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 3.13 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 $f(x)$. \square

Definition 3.15. 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 3.16. 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. \square

Example 3.17. 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 3.18. 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**, the minimum polynomial of every element of L is separable.

Definition 3.19. Let R be a commutative ring. The **formal derivative** is a function

$$d : R[x] \longrightarrow R[x]$$

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

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

Lemma 3.20. 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 $\phi: R \longrightarrow S$, 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 . \square

Lemma 3.21. Let $f(x)$ be a polynomial over K . Then f has a repeated root iff $f(x)$ and $f'(x)$ have a common zero in some splitting field.

Proof. By the last statement of 3.20, 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 $g(x)$. \square

Lemma 3.22. *Let $m(x) \in K[x]$ be an irreducible polynomial over a field K .*

Then $m(x)$ has a repeated root iff $m'(x) = 0$.

In particular $m(x)$ is inseparable iff

$$m(x) = \sum a_i x^{p^i}.$$

Proof. By 3.21 $m(x)$ has a repeated root iff $m(x)$ and $m'(x)$ have a common root α . As $m(x)$ is irreducible, it follows that $m(x)$ would be the minimum polynomial of α and so either $m(x)$ would divide $m'(x)$ or $m'(x)$ is the zero polynomial. As $m'(x)$ has degree one less than $m(x)$, the latter is the only possibility. \square

Proposition 3.23. *Let L/K be a finite field extension.*

Then L/K is separable if $[L : K]$ is coprime to the characteristic. In particular every field extension in characteristic zero is separable.

Proof. Suppose that L/K is not separable. Pick $\alpha \in L$ such that $m(x)$ the minimum polynomial of α is inseparable. By 3.22 m has degree a multiple of p . In particular p would divide the LHS of

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

at it divides the RHS, a contradiction. \square

Definition-Lemma 3.24. \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 3.11 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 . \square

Example 3.25. 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 3.26. (Einstein's Criteria: Bis) Let

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

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 F 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

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

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 $a_0 = b_0c_0$. \square

Definition 3.27. *Let K be a field. The algebraic closure of K , denoted \bar{K} , is an algebraic field extension L/K , such that every polynomial in $K[x]$ splits in L .*

*We say that K is **algebraically closed** if $K = \bar{K}$.*

Lemma 3.28. *Let L/K be an extension of fields.*

TFAE

- (1) L/K is algebraic and L is algebraically closed.
- (2) $L = \bar{K}$ is an algebraic closure of K .
- (3) L/K is algebraic and for every finite extension N/L , $N = L$.

Proof. (1) clearly implies (2).

Suppose that (2) holds. Let N/L be a finite extension. Passing to a normal closure, we may as well assume that N/L is a splitting field for $f(x) \in L[x]$. Let $L/M/K$ be the intermediary field generated by the coefficients of $f(x)$. Then $f(x) \in M[x]$.

As $f(x)$ splits in N , we may find an intermediary field $N/N'/M$ which is a splitting field for $f(x)$ over M . As $M \subset L$ and L/K , M/K is algebraic. As it is also finitely generated, M/K is finite. Similarly for N'/M . By the tower law N'/K is finite. Pick $\alpha \in N'$. Then α is algebraic over K . Let $m(x) \in K[x]$ be the minimum polynomial of α . By assumption $m(x)$ splits in L . As α is a root of $m(x)$, and $m(x)$ splits in L , it follows that $\alpha \in L$. But then $N' \subset L$. But then $N = L$, as we have shown that $f(x)$ splits in L . Hence (3).

Now suppose that (3) holds. Let $f(x) \in L[x]$. We have to show that $f(x)$ splits in L . Let N/L be a splitting field for $f(x)$. Then N/L is finite. But then $N = L$, and $f(x)$ splits in L . \square

We now turn to the proof of existence and uniqueness. Unfortunately to prove either of these, we need to confront a highly non-trivial logical issue.

Axiom 3.29. (*Axiom of Choice*) For every set x , which does not contain the empty set, we may find a set y and a function $f: x \rightarrow y$ such that

$$f(z) \in z,$$

for every $z \in x$.

In other words, the axiom of choice states that given a collection of sets x (for example $x = \{A_i \mid i \in I\}$) for every element z of x , we may pick an element $f(z)$ of z (for the example before, we would have $a_i \in A_i$). Note that if the set x is finite, there is no issue here at all. The problem is when x is a very big set (equivalently the indexing set I is very big), since in this case we are supposed to be making infinitely many choices. In fact there could be a problem, even when every element of x has only finitely many elements.

There are many axioms in set theory, all of which are equivalent to the axiom of choice.

Definition 3.30. Let $(x, <)$ be a total order. We say that x is well-ordered if every subset of x has a smallest element.

A classic example of a well-ordered set is the set of natural numbers, under the natural ordering.

Axiom 3.31. (*Well-Ordering Principle*). For every set x , we may find a total ordering of the elements of x , such that the resulting order is a well-ordering.

For example, the well-ordering principle states that the real numbers can be well-ordered. Clearly the usual ordering is not a well-ordering.

One of the most useful equivalent ways to state the axiom of choice, is the following:

Axiom 3.32. (*Zorn's Lemma*) Let $(P, <)$ be a partially-ordered set.

Suppose that for totally-ordered subset Q of P we may find an element of P such that $a \leq b$, for all $a \in Q$.

Then P has an element m , which is not smaller than any other element.

The element m is sometimes called a maximal element. Note that it does not have the property that it is bigger than every other element of P , just that if we can compare m with another element n , then $n \leq m$.

Here are some other equivalent formulations of the axiom of choice.

Axiom 3.33. (*Tychonov's Theorem*) *The product of compact topological spaces is compact.*

The issue with Tychonov's Theorem, as with the axiom of choice, is that no restriction on the number of factors in the product is given.

Axiom 3.34. *Every vector space has a basis.*

Axiom 3.35. *Every ring has a maximal ideal.*

Axiom 3.36. *Every field has an algebraic closure.*

Let us practice using Zorn's Lemma, with some baby applications.

Lemma 3.37. *Let R be a ring and let I be an ideal, $I \neq R$.*

Zorn's Lemma implies that R contains a maximal ideal which contains I .

Proof. Let P be the partially ordered set of all ideals, not equal to R , that contain I , with the order given by inclusion. We want to apply Zorn's Lemma.

Let Q be a totally ordered subset of P . Let J be the union of all the elements of Q . I claim that J is an ideal of R , which contains I . Clearly J contains I and so it is definitely non-empty. We have to prove that J is closed under addition and scalar multiplication.

Pick a and $b \in J$. Then there are K and L in Q with $a \in K$ and $b \in L$. As Q is totally-ordered, possibly switching K and L , $K \subset L$ and so we may assume that a and $b \in L$. In this case $a + b \in L$ and so $a + b \in J$. Similarly $ra \in L$, for all $r \in R$, so that $ra \in J$. On the other hand, note that $1 \notin J$. Thus $J \in P$ and J dominates every element of Q .

By Zorn's Lemma P contains a maximal element, call it M and we are done. \square

Lemma 3.38. *Zorn's Lemma implies that every vector space has a basis.*

Proof. Let V be a vector space over a field F . Let P denote the subset of the power set of V , consisting of all independent subsets of V . The relation on V is the natural one given by inclusion.

To apply Zorn's Lemma, we need to check that every totally-ordered subset Q of P , is dominated by an element of P . Given a totally-ordered subset Q of P , set

$$B = \bigcup_{C \in Q} C.$$

Clearly $C \subset B$, for every $C \in Q$. Suppose that we may find $v_1, v_2, \dots, v_n \in B$ and $a_1, a_2, \dots, a_n \in F$, such that

$$\sum a_i v_i = 0.$$

For every i , there is a $C_i \in Q$, such that $v_i \in B_{k_i}$. Let C be the maximum of the C_i . Then $v_i \in C$, as Q is well-ordered. As C is a collection of independent vectors, we have $a_i = 0$, for all i . But then B is a collection of independent vectors, that is $B \in P$.

As every totally-ordered subset in P is dominated by an element of P , by Zorn's Lemma it follows that there is an element B of P , such that B is not smaller than any other element of P .

I claim that B is a basis of V . As $B \in P$, B is an independent set. Suppose that $v \in V$. The set $A = B \cup \{v\}$ strictly contains B . As B is maximal in P , A must be a dependent set, so that v must be a linear combination of the elements of B . Thus B spans V , and B is a basis of V . \square

We now show that the axiom of choice, Zorn's Lemma and the well-ordering principle are equivalent.

Theorem 3.39. *TFAE*

- (1) *Well-ordering principle.*
- (2) *Axiom of Choice.*
- (3) *Zorn's Lemma.*

Proof. Suppose that the well-ordering principle holds. Let x be a set and let x' be the disjoint union of the elements of x . Well-order the elements of x' . Then every element z of x is a subset of x' and we define a function

$$f: x \longrightarrow y$$

by the simple prescription, $f(z)$ is the smallest element of z . Thus (1) implies (2).

We skip the proof that (2) implies (3).

Finally suppose that Zorn's Lemma holds. Let x be any set. Let P be the set of all well-orderings induced on a subset y of x (note that P is a subset of the power set of x Cartesian product the power set of the Cartesian product of x with itself). Define a relation $<$ on P , if given two elements $a_1 = (y_1, r_1)$, $a_2 = (y_2, r_2)$, we say that $a_1 < a_2$ if y_1 is a subset of y_2 and the well-ordering r_2 extends r_1 .

Let Q be a totally-ordered subset of P . Define an element $b = (y, r) \in P$ as follows. Let y be the union of all the subsets y' , where for some r' , $(y', r') \in Q$.

Given l_1 and $l_2 \in y$, there exists y_1 and y_2 in Q such that $l_i \in y_i$. As Q is well-ordered, we may suppose that $y_1 \subset y_2$. Thus we may put l_1 and l_2 in the same order in y , as they are in y_2 . It is easy to check that r is a well-ordering of y . Thus b dominates Q .

By Zorn's Lemma, P contains a maximal element $(y, <)$. Suppose $y \neq x$. Let $l \in x - y$. Define an ordering on $y \cup \{l\}$ by decreeing that l is bigger than every element of y . It is clear that this ordering is a well-ordering. In this way we get an element b of P that is bigger than y , a contradiction. \square

In practice we assume the Axiom of Choice holds, so that we are free to apply Zorn's Lemma.

We now return to the existence and uniqueness of an algebraic closure. First uniqueness.

Lemma 3.40. *The algebraic closure of a field is unique.*

Proof. Let K be a field and suppose that L_1 and L_2 are two algebraic closures of K . We want to exhibit an isomorphism of L_1 with L_2 .

Let P be denote the set of all triples $a = (M_1, M_2, \phi)$, where ϕ is an isomorphism of $M_1 \subset L_1$ with $M_2 \subset L_2$. We say that the triple $a < b = (N_1, N_2, \psi)$ if $M_1 \subset N_1$, $M_2 \subset N_2$ and ψ extends ϕ .

We want to apply Zorn's Lemma. Let Q be a totally-ordered subset of P .

Let N_1 be the union of the M_1 and let N_2 be the union of the M_2 . Define $\psi: N_1 \rightarrow N_2$ in the obvious way. Given $m \in N_1$, pick $a \in Q$, such that $m \in M_1$. Then set $\psi(m) = \phi(m)$. ψ is well-defined as Q is totally-ordered. It is easy to check that ψ is an automorphism. Thus Q is dominated by the triple (M, N, ψ) .

By Zorn's Lemma, there is a maximal triple a . Suppose that $M_1 \neq L_1$. Pick $\alpha \in L_1 - M_1$. Let $N_1 = M_1(\alpha)$. Let $m(x)$ be the minimum polynomial of α over K . Then $m(x)$ splits in L_2 . Pick $\beta \in L_2$. Then we may extend ϕ to $\psi: N_1 \rightarrow N_2 = M_2(\beta)$, a contradiction. \square

A similar proof ought to work to establish existence. However there are some subtleties. Here is one way to proceed.

Lemma 3.41. *The algebraic closure of a field exists.*

Proof. Let K be a field. If K is finite, then let E be any countable set. Otherwise let E be the power set of K . Note that the collection P' of all fields structures on all subsets of E is naturally a set (indeed note that the operations of addition, inverses and multiplication are all functions on the given subset of E). There is a natural order on P' . Given two subsets A and B , we say that $A < B$, if A is a subset of

B and B/A is a field extension, with the two sets of operations on A and B . We will abuse notation and identify an element of P' with the corresponding field. Fix an element K' of P' which is isomorphic to K and let P be subset of P' consisting of all fields that contain this copy K' of K and which are algebraic over K' .

The key point, is that given any finite field extension L/K , we may find $L' \in P$ such that the corresponding extension L'/K' is isomorphic to L/K . Indeed the point is that L has the same cardinality as K and so this is clear.

By a now standard argument, it is clear that given a chain Q in P , we may find an element L/K that dominates Q . The union of the corresponding subsets with the induced operations is obviously a field, which dominates every element of Q .

By Zorn's Lemma, it follows that P has a maximal element, call it L . I claim that L is algebraically closed. Suppose not. Then there would be a non-trivial finite extension N/L . By what we just said, we may assume that $N \in P$, by reasons of cardinality, so that $L < N$. But this contradicts our choice of L . \square