7. Field Extensions

Suppose that we are interested in solving a polynomial equation. The natural place to look for solutions to equations is in a field and in field extensions.

Definition 7.1. *Let L be a field and let K be a subfield. Then we say that L/K is a **field extension**.*

Our aim then is to understand field extensions. Just as in the case of groups, rings and modules, we want to break up the problem of understanding the field extension L/K into parts.

Definition 7.2. *Let L/K be a field extension. If M is a subfield of L that contains K, then we say that M is an **intermediary field**.*

Thus an intermediary field is to a field extension as a subgroup (respectively subring, submodule) is to a group (respectively ring, module). As always in this situation, there is a notion of a subset generating an extension.

Definition 7.3. *Let L/K be a field extension. Let S be a subset of L. The **subfield generated by** S, denoted $K(S)$, is the smallest subfield of L that contains K and S.*

*We say that S **generates** L/K if $L = K(S)$. We say that L/K is **finitely generated** if we can find a finite set S that generates L/K. We say that L/K is* **primitive** *is there is a single element α of L that the generates L/K, so that $L = K(\alpha)$. In this case, we say that α is a **primitive generator**.*

As usual, to prove that (7.3) makes sense, it suffices to observe that the intersection of field extensions is a field extension. In contrast to the field generated by S, we will denote by $K[S]$, the smallest ring that contains K and S. Obviously we have $K[S] \subset K(S)$, and in many cases we won't have equality. For example, if x is an indeterminate, then $K(x)$ is the field of fractions of the polynomial ring $K[x]$.

Definition 7.4. *Let L be a field. The **prime subfield** of L is the smallest field containing the empty set.*

It is straightforward to list all possible prime subfields.

Proposition 7.5. *Let L be a field and let K be the prime subfield.*

If the characteristic is zero, then K is isomorphic to $\mathbb{Q}$. If the characteristic is p, then K is isomorphic to $\mathbb{F}_p$.

Proof. Let R be the smallest subring that contains the empty set. Clearly K is the field of fractions of R.

There are two cases. If the characteristic is p, then we have already seen that R is isomorphic to $\mathbb{Z}_p$. As this is isomorphic to $\mathbb{F}_p$, which is already a field, then K is isomorphic to $\mathbb{F}_p$.

Otherwise the characteristic is zero. In this case, R is isomorphic to $\mathbb{Z}$. In this case the field of fractions K of R is isomorphic to $\mathbb{Q}$. □

One particular consequence of (7.5) is that every field may be considered as a field extension over its prime field. Thus, since we understand the fields $\mathbb{Q}$ and $\mathbb{F}_p$ quite well, the study of fields is naturally subsumed in the study of field extensions.

The most basic observation, which in fact is really the main observation of field extensions, is that given a field extension L/K, L is a vector space over K, simply by restriction of scalars.

Definition 7.6. *Let L/K be a field extension. The* ***degree*** *of L/K, denoted $[L : K]$, is the dimension of L over K, considering L as a vector space over K.*

We say that L/K is finite, if L is a finite dimensional vector space over K.

Example 7.7. $\mathbb{C}/\mathbb{R}$ *has degree two. Indeed it is clear that* 1 *and i form a basis for $\mathbb{C}/\mathbb{R}$, as every complex number is, by definition, uniquely of the form $a + bi$.*

Lemma 7.8. *Let F be a finite field.*

Then the order q of F is a power of a prime.

Proof. Let p be the characteristic of F. p is not zero, as F cannot contain $\mathbb{Q}$, an infinite set. Thus p is a prime and F is a field extension of $\mathbb{F}_p$. As F is finite, the field extension $F/\mathbb{F}_p$ is finite. But every finite dimensional vector space over $\mathbb{F}_p$ is isomorphic, as a vector space, to a direct sum of copies of $\mathbb{F}_p$. In particular the cardinality of F is equal to the cardinality of the cartesian product of $\mathbb{F}_p$ with itself a finite number of times, and the cardinality of a product is the product of the cardinalities. Thus $q = p^d$, where d is the degree of the extension $F/\mathbb{F}_p$. □

Note that the proof of (7.8) gives us much more than simply the cardinality of F, in fact we know the additive structure of F (a product of d copies of the cyclic group of order p). We will see later that we can almost as explicitly determine the multiplicative structure as well.

Proposition 7.9 (Tower Law)**.** *Let L/K be a field extension and let M be an intermediary field.*

Then

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

Proof. Consider first the possibility that one of the two field extensions L/M or M/K is infinite. In this case L would contain infinitely many independent vectors over K and so it is clear that L/K is also infinite, and the equation comes out correctly in this case.

Otherwise we assume that both L/M and M/K are finite extensions. Suppose that $e_1, e_2, \dots, e_m$ is a basis for L/M and that $f_1, f_2, \dots, f_n$ is a basis for M/K. In this case,

$$[L : M] = m \qquad \text{and} \qquad [M : K] = n.$$

Clearly it suffices to prove that $e_i f_j$, $i = 1 \dots m$ and $j = 1 \dots n$ is a basis for $[L : K]$, since then

$$[L : K] = mn = [L : M][M : K].$$

We have to prove two things, that $\{e_i f_j\}$ spans and that it is independent. We first show that it spans. Pick $l \in L$. As $e_1, e_2, \dots, e_m$ is a basis for L/M, it follows that we may find $\alpha_1, \alpha_2, \dots, \alpha_m \in M$ such that

$$l = \sum_j \alpha_j e_.$$

On the other hand, as $\alpha_i \in M$ and $f_1, f_2, \dots, f_n$ is a basis for M/K, for each i, there are $\beta_{ij} \in K$ such that

$$\alpha_i = \sum \beta_{ij} f_j.$$

Putting all this together we have

$$\begin{aligned} l &= \sum_i \alpha_i e_i \\ &= \sum_i (\sum_j \beta_{ij} f_j) e_i \\ &= \sum_{i,j} \beta_{ij} (e_i f_j). \end{aligned}$$

Thus l is a linear combination of $e_i f_j$ over K and so $e_i f_j$ span L/K.

Now we turn to linear independence. Suppose that

$$\sum_{i,j} \beta_{ij} e_i f_j = 0.$$

We have to prove that

$$\beta_{ij} = 0.$$

Rearranging, we have

$$\sum_i (\sum_j \beta_{ij} f_j) e_i = 0.$$

Set $\alpha_i = \sum_j \beta_{ij} f_j$. Then $\alpha_i \in M$ and

$$\sum_i \alpha_i e_i = 0.$$

As $e_1, e_2, \dots, e_m$ are independent over M, it follows that

$$\sum_j \beta_{ij} f_j = \alpha_i = 0.$$

By independence of $f_1, f_2, \dots, f_n$ over K, we get $\beta_{ij} = 0$, for all i and j.

Thus $\{e_i f_j\}$ is indeed a basis for L/K. □

We say that a polynomial is *monic* if its leading coefficient is one.

Definition 7.10. *Let L/K be a field extension and let α be an element of K. We say that α is* ***algebraic*** *over K, if there is a polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. The minimum degree monic polynomial with this property is called the* ***minimum polynomial*** *of α over K. It will be denoted $m_\alpha(x)$.*

If there is no such polynomial we say that α is ***transcendental*** *over K.*

An extension L/K is called ***algebraic*** *if every element of L is algebraic over K.*

If $\alpha \in \mathbb{C}$ is a complex number, then we say that α is algebraic (respectively transcendental) if it is so over $\mathbb{Q}$.

Example 7.11. *$\alpha = \sqrt{2}$ is algebraic over $\mathbb{Q}$.*

Indeed α is a zero of $x^2 - 2 \in \mathbb{Q}[x]$. Of course $\sqrt{2}$ is not a rational number, that is, $\sqrt{2}$ is irrational. It follows that $x^2 - 2$ is the minimum polynomial of $\sqrt{2}$.

Similarly i is algebraic, as i is a zero of the polynomial x^2+1. Again, as $i \notin \mathbb{Q}$, it follows that x^2+1 is the minimum polynomial of i over $\mathbb{Q}$.

Consider the set $\overline{\mathbb{Q}}$ of all complex numbers that are algebraic over $\mathbb{Q}$. Since there are only countably many equations (the countable union of countable sets is countable), and each possible equation has only finitely many roots, then in fact there are only countably many algebraic numbers. As there are uncountably many irrational numbers, it follows that most numbers are transcendental. On the other hand, it is quite difficult to exhibit a single transcendental number and extremely difficult to prove the following, which is a deep result of analysis:

Theorem 7.12. *e and π are transcendental.*

What can we say about the structure of primitive extensions?

Lemma 7.13. *Let R be a PID and let I be a non-zero prime ideal of R.*

Then R/I is a field.

Proof. It suffices to prove that I is maximal. Suppose that $I \subset J \subset R$, where J is an ideal of R. As R is a PID, there are two elements a and b of R such that $I = \langle a \rangle$ and $J = \langle b \rangle$. As $a \in J$, b divides a. As I is prime, a is irreducible, and so either b is a unit, in which case $J = R$, or b is an associate of a, in which case $J = I$. Either way, I is maximal. □

Theorem 7.14. *Let L/K be a field extension, and let α be an element of L. Set $M = K(\alpha)$.*

If α is transcendental over K, then M is isomorphic to the field of rational functions of K, that is the field of fractions $K(x)$ of $K[x]$. In particular any two transcendental elements generate isomorphic extensions.

If α is algebraic over K, then

$$K(\alpha) = K[\alpha] \simeq K[x]/\langle m_\alpha(x) \rangle.$$

In particular any two elements of L with the same miminal polynomial generate isomorphic field extensions.

Proof. It is clear that $K(\alpha)$ is the smallest field that contains $K[\alpha]$, so that $K(\alpha)$ may be identified with the field of fractions of $K[\alpha]$.

We recall some of the theory of polynomial rings. Given any field extension L/K and an element α of L, there is a unique ring homomorphism

$$\phi = \mathrm{ev}_\alpha \colon K[x] \longrightarrow L,$$

which is defined by sending x to α. This follows by the universal property of polynomial rings. The kernel of ev_α is an ideal I in $K[x]$. It consists of all polynomials $f(x) \in K[x]$ which vanish at α.

The image of ϕ is clearly $K[\alpha]$. By the Isomorphism Theorem

$$K[\alpha] \simeq K[x]/I.$$

As $K[\alpha]$ is a subset of L, it follows that $K[\alpha]$ is an integral domain. But then I must be a prime ideal. If α is transcendental, then I is the zero ideal and we have an isomorphism $K[\alpha]$ with $K[x]$. The result follows in this case.

From now on, we suppose that α is algebraic, so that I is non-trivial. As K is a field, $K[x]$ is a Euclidean domain, and so $K[x]$ is a principal ideal domain. Thus there is a polynomial $f(x) \in K[x]$ such that $I = \langle f(x) \rangle$. Since K is field, if $f(x) \neq 0$, we can always normalise $f(x)$ so that it is monic. It is clear that in fact, in this case,

$f(x) = m_\alpha(x)$ (in fact this is a better way to define the minimum polynomial in the first place). As I is prime, f is irreducible. By (7.13) $K[x]/\langle f(x)\rangle$ is a field. Thus $K[\alpha]$ is a field and so by definition $K[\alpha] = K(\alpha)$. □

This innocent looking result will prove to be the linchpin of the whole Theory of field extensions. It has the following remarkable consequences.

Corollary 7.15. *The two fields $\mathbb{Q}(e)$ and $\mathbb{Q}(\pi)$ are isomorphic.*

Proof. Clear, since both e and π are transcendental over $\mathbb{Q}$. □

Example 7.16. (7.14) *gives a beautiful way to construct field extensions. For example, let us see how to construct the field $\mathbb{C}$, given the real numbers.*

We want to adjoin a square root of -1. So we consider the polynomial $x^2 + 1$. This is irreducible so that (7.14) tells us that

$$\mathbb{R}[x]/\langle x^2 + 1\rangle$$

is in fact a field, and that the coset generated by x is a square root of -1. Indeed put $\alpha = x + I$. Then

$$\begin{aligned} \alpha^2 &= (x+I)^2 \\ &= x^2 + I \\ &= x^2 + \langle x^2 + 1\rangle \\ &= -1 + \langle x^2 + 1\rangle \\ &= -1 + I \\ &= -1. \end{aligned}$$

Example 7.17. *Let ω be a primitive cube root of unity, so that $\omega^3 = 1$, but $\omega \neq 1$. Let α be a real root of $x^3 - 2$ (so that α is the cube root of 2). By Eisenstein, $x^3 - 2$ is irreducible over $\mathbb{Q}$. Then both α and $\omega\alpha$ have the same minimum polynomial, $x^3 - 2$. Thus*

$$\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\omega\alpha) \simeq \mathbb{Q}(\omega^2\alpha).$$

Of course, as subfields of $\mathbb{C}$, these fields are quite different.

Lemma 7.18. *Let L/K be a field extension and let α be algebraic over K.*

Then the minimum polynomial of α divides every polynomial that has α as a root. In particular a monic polynomial which has α as a root, is the minimum polynomial of α if and only if it is irreducible.

Proof. Follows from the fact that in the proof of (7.14), it is proved that the minimum polynomial generates the ideal of all functions that have α as a root and the fact that this ideal is prime. □

Corollary 7.19. *Let L/K be a field extension, let α be an algebraic element of L. Let d be the degree of the minimum polynomial of α.*

Then $[K(\alpha) : K] = d$.

Proof. It clearly suffices to prove that $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ form a basis for $K(\alpha)$. We have to show that these elements both span and are independent.

First we prove that they span. Suppose the minimal polynomial is

$$x^d + a_{d-1}x^{d-1} + \cdots + a_0,$$

so that

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0.$$

As $K(\alpha) = K[\alpha]$ and the latter is generated by the powers of α, it suffices to prove that α^n is a linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$. If $n < d$ there is nothing to prove. Otherwise, by induction, it suffices to prove that α^n is a linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. But

$$\begin{aligned} \alpha^n &= \alpha^{n-d}\alpha^d \\ &= \alpha^{n-d}(-a_{d-1}\alpha^{d-1} - \cdots - a_0) \\ &= -a_{d-1}\alpha^{n-1} - \cdots - a_0\alpha^{n-d}. \end{aligned}$$

Thus $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ span $K(\alpha)/K$.

Now we turn to linear independence. Suppose that

$$\sum b_i\alpha^i = 0.$$

Let $g(x) = \sum b_i x^i$. Then α is a zero of $g(x)$. As the degree of g is less than the degree of $m_\alpha(x)$, the mininum polynomial of α, it follows that $g(x)$ is the zero polynomial. But then each $b_i = 0$ and we also have linear independence.

Thus $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ do indeed form a basis. □

Example 7.20. *Let us calculate the degree of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.*

The minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. Similarly the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$. Thus

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2.$$

However, by the tower law,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

So we want to calculate

$$[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})].$$

Now $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$, and $\sqrt{3}$ is a zero of this, so the latter is either 1 or 2, depending on whether $x^2 - 3$ is irreducible, when considered as a polynomial over $\mathbb{Q}(\sqrt{2})$. Since $x^2 - 3$ is quadratic, this is the same as to ask whether or not $x^2 - 3$ has a root in $\mathbb{Q}(\sqrt{2})$.

Suppose it does. Let $\beta \in \mathbb{Q}(\sqrt{2})$ be a root of $x^2 - 3$. It helps to rename $\sqrt{2}$ as α. As $\mathbb{Q}(\alpha)$ is quadratic over $\mathbb{Q}$, 1 and α are a basis. Thus there are rational numbers a and b such that

$$\beta = a + b\alpha.$$

Squaring both sides, we get

$$3 + 0\alpha = 3 = \beta^2 = a^2 + 2ab\alpha + b^2\alpha^2 = (a^2 + 2b^2) + 2ab\alpha.$$

Comparing like terms, and using the fact that $1, \alpha$ is a basis, we get

$$a^2 + 2b^2 = 3$$

and

$$2ab = 0.$$

Thus either $b = 0$ and $a^2 = 3$ or $a = 0$ and $2b^2 = 3$, either of which are clearly impossible, since a and b are rational numbers.

Thus, by the Tower law, the extension has degree four.

Lemma 7.21. *Let L/K be a field extension.*

Then L/K is finite if and only if $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where each α_i is algebraic over K.

Proof. Easy consequence of (7.9) and (7.14). □

Lemma 7.22. *Let L/K be a field extension. Let M be the subset of L consisting of all elements of L that are algebraic over K.*

Then M is an intermediary field.

Proof. Suppose that $\alpha \in K$. Then α is a root of the polynomial $x - \alpha$. Thus α is algebraic over K and so $K \subset M$.

Note that $\gamma \in M$ if and only if γ is algebraic over K if and only if $K(\gamma)/K$ is a finite extension.

Suppose that α and β are in M. It suffices to prove that $\alpha + \beta$, $-\alpha$, $\alpha\beta$ and $1/\alpha$ are in M. All of these are elements of the field $K(\alpha, \beta)$. Thus it suffices to prove that $K(\alpha, \beta) \subset M$. As α and β are in M, $K(\alpha)/K$ and $K(\beta)/K$ are finite. Thus $K(\alpha, \beta)/K(\beta)$ is certainly finite and so, by the Tower Law,

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\beta)][K(\beta) : K]$$

it follows that $K(\alpha, \beta)/K$ is finite. Let $\gamma \in K(\alpha, \beta)$. Then by the Tower Law

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\gamma)][K(\gamma) : K],$$

so that $K(\gamma)/K$ is finite. But then γ is algebraic over K and $\gamma \in M$. Thus $K(\alpha, \beta) \subset M$ as required. □

Theorem 7.23. *Let L/K be a finite field extension.*

Then L/K is primitive if and only if there are only finitely many intermediary fields.

Proof. Suppose that L/K is primitive. Let α be a primitive generator, so that $L = K(\alpha)$. Let M be an intermediary field. Clearly $L = M(\alpha)$. Attach to M the data $f_M(x)$ of the minimum polynomial of α over M.

I claim that f_M determines M. Indeed first note that $f_M(x) \in M[x]$ and that $f_M(x)$ is monic and irreducible. Let M' be the subfield of M generated by the coefficients of f_M. By definition of M', $f_M(x) \in M'[x]$. As $f_{M'}$ is the minimal polynomial of α over M', it follows that $f_{M'}$ divides f_M. As f_M is irreducible in $M[x]$, it is certainly irreducible in $M'[x]$. Thus $f_M = f_{M'}$. Thus

$$[L : M] = [L : M']$$

as both are equal to the degree of f_M. On the other hand,

$$[L : K] = [L : M][M : K] = [L : M'][M' : K],$$

by the tower law applied to both $L/M/K$ and $L/M'/K$. Thus

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

Now consider the extensions $M/M'/K$. We have

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

We conclude that $[M : M'] = 1$. Thus $M = M'$. But clearly M' is determined by f_M so that M is also determined by f_M.

Now observe that there are only finitely many possibilities for f_M. In fact f_M divides f_K over L, and as $L[x]$ is a UFD, there are only finitely many ways to factor f_K. Thus there are only finitely many intermediate fields.

Suppose that there are only finitely many intermediary fields. We want to prove that L/K is primitive. We will prove this for now only in the case that L is infinite; we defer the case of finite fields to later on in the course.

Suppose not. Let α be an element of L such that $[K(\alpha) : K]$ is maximal. By assumption we may pick $\beta \in L$ not in $K(\alpha)$. Consider the intermediary fields, $K(\alpha+\lambda\beta)$, where λ ranges over K. As there are infinitely many different values for λ and only finitely many intermediary fields, there are $\lambda \neq \mu \in K$ such that

$$K(\alpha + \lambda\beta) = K(\alpha + \mu\beta) = M.$$

Clearly $\alpha + \lambda\beta$ and $\alpha + \mu\beta \in M$. Thus

$$\begin{aligned}(\alpha + \lambda\beta) - (\alpha + \mu\beta) &= \lambda\beta - \mu\beta \\ &= (\lambda - \mu)\beta,\end{aligned}$$

lies in M. As $\lambda \neq \mu$, we can divide by $\lambda - \mu$, to conclude that $\beta \in M$. Thus

$$(\alpha + \lambda\beta) - \lambda\beta = \alpha \in M.$$

Thus α and β lie in M. As $\alpha \in M$, $K(\alpha) \subset M$. As $\beta \notin K(\alpha)$, this inclusion is strict. Thus the degree of M over K is greater than the degree of $K(\alpha)$ over K. As $M = K(\gamma)$, for $\gamma = \alpha+\lambda\beta$, this contradicts our choice of α. Thus L/K is primitive. □