2 Field Theory

This chapter loosely follows Chapter 13 of Dummit and Foote.

2.1 Field Extensions

We begin with a definition that you encountered on a previous homework problem.

Definition 2.1. Let R be a ring with $1 \neq 0$. We define the **characteristic** of R, denoted $\mathrm{Char}(R)$, to be the smallest positive integer n such that $n \cdot 1_R = 0$ if such an n exists and to be 0 otherwise.

Note that $n \cdot 1_R$ is an shorthand for

$$\underbrace{1_R + \cdots + 1_R}_{n \text{ terms}}.$$

The integer n may not even be in R.

Example 2.2. Here are a few quick examples.

(1) The characteristic of the ring $\mathbb{Z}/n\mathbb{Z}$ is n. In particular, if p is prime, then the field $\mathbb{Z}/p\mathbb{Z}$ has characteristic p. The polynomial ring $\mathbb{Z}/n\mathbb{Z}[x]$ also has characteristic n.

(2) The ring $\mathbb{Z}$ has characteristic 0.

(3) The fields $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ all have characteristic 0.

(4) If F is a field with characteristic 0, then $F[x]$ has characteristic 0.

The next theorem tells us what the possible characteristics are for integral domains.

Theorem 2.3. Let R be an integral domain. Then $\mathrm{Char}(R)$ is either 0 or a prime p.

Theorem 2.4. If R is an integral domain such that $\mathrm{Char}(R) = p$ (p prime), then

$$p \cdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{p \text{ terms}} = 0.$$

Theorem 2.5. The characteristic of an integral domain is the same as its field of fractions.

It turns out that if F is a field, F either contains a subfield isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ depending on whether $\mathrm{Char}(F)$ is 0 or p (for p prime). To see why this is true, define $\phi : \mathbb{Z} \to F$ via $\phi(n) = n \cdot 1_F$, where we interpret $(-n) \cdot 1_F = -(n \cdot 1_F)$ for positive n and $0 \cdot 1_F = 0$. Then $\ker(\phi) = \mathrm{Char}(F)\mathbb{Z}$. The First Isomorphism Theorem for Rings tells us that there is an injection of either $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ into F. This implies that F either contains a subfield isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, depending on the characteristic of F. In either case, this subfield is the smallest subfield containing 1_F, which we call the **subfield generated by** 1_F.

The next definition makes sense in light of the discussion above.

Definition 2.6. The **prime subfield** of a field F is the subfield generated by 1_F (i.e., the smallest subfield of F containing 1_F).

Note that the prime subfield of F is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$.

Example 2.7. Here are a couple quick examples.

(1) The prime subfield of both $\mathbb{Q}$ and $\mathbb{R}$ is $\mathbb{Q}$.

(2) The prime subfield of the field of rational functions with coefficients from the field $\mathbb{Z}/p\mathbb{Z}$ (denoted $\mathbb{Z}/p\mathbb{Z}(x)$) is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Definition 2.8. If K is a field containing the subfield F, then K is said to be an **extension field** (or simply an **extension**) of F, denoted K/F and read "K over F" (not be be confused with quotients!). The field F is called the **base field** of the extension.

Note that every field is an extension of its prime subfield.

Note 2.9. If K/F is a field extension, then we can interpret K as a vector space over F. In this case, K is the set of vectors and the scalars are coming from F.

Definition 2.10. The **degree** (or **index**) of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F (i.e., $[K : F] = \dim_F(K)$).

Example 2.11. For example, $[\mathbb{C} : \mathbb{R}] = 2$.

If we are given a polynomial $p(x)$ in $F[x]$, it is possible that $p(x)$ does not have any roots in F. It is natural to wonder if there is an extension K of F such that $p(x)$ has roots in K.

For example, consider the polynomial x^2+1 in $\mathbb{R}[x]$. We know that this polynomial does not have a root in $\mathbb{R}$. However, this polynomial has roots in $\mathbb{C}$.

Note that given any polynomial $p(x)$ in $F[x]$, any root of a factor of $p(x)$ is also a root of $p(x)$. It is enough to consider the case where $p(x)$ is irreducible.

Theorem 2.12. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.

In the proof of the above theorem, we took $K = F[x]/(p(x))$ (where $p(x)$ is irreducible). Since F is a subfield of K, there is a basis of K as a vector space over F. The next theorem makes this explicit.

Theorem 2.13. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial of degree n over F and let $K = F[x]/(p(x))$. Define $\theta = x \mod (p(x)) \in K$. Then the elements $1, \theta, \theta^2, \ldots, \theta^{n-1}$ are a basis for K as a vector space over F. In particular, $[K : F] = n$ and

$$K = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\},$$

which is the set of all polynomials of degree less than n in θ.

The previous theorem provides a nice description of the elements in $K = F[x]/(p(x))$ ($p(x)$ irreducible). Adding these elements is as simple as adding like terms. However, in order to be a ring, we also need to be able to multiply. The next corollary gives us some assistance in doing this.

Corollary 2.14. Let K be as in the previous theorem and let $a(\theta), b(\theta) \in K$ be two polynomials in θ of degree less than n. Then $a(\theta)b(\theta) = r(\theta)$, where $r(x)$ is the remainder of degree less than n obtained after dividing the polynomial $a(x)b(x)$ by $p(x)$ in $F[x]$.

Example 2.15. Here are a few examples.

(1) Let $p(x) = x^2 + 1$. Since $p(x)$ is irreducible over $\mathbb{R}$ and of degree 2, $\mathbb{R}[x]/(p(x))$ is a field extension of $\mathbb{R}$ of degree 2 by Theorem 2.13. In a recent homework assignment, you proved that $\mathbb{R}[x]/(p(x))$ is isomorphic to $\mathbb{C}$ (which has a basis of rank 2 over $\mathbb{R}$). As expected, $p(x)$ has a root in $\mathbb{C}$. The elements of $\mathbb{R}[x]/(p(x))$ are of the form $a + b\theta$ for $a, b \in \mathbb{R}$. Addition is defined by

$$(a + b\theta) + (c + d\theta) = (a + c) + (b + d)\theta.$$

To multiply, we use the fact that $\theta^2 + 1 = 0$, or equivalently $\theta^2 = -1$. Note that -1 is the remainder when x^2 is divided by $x^2 + 1$ in $\mathbb{R}[x]$. Then

$$\begin{aligned}(a + b\theta)(c + d\theta) &= ac + (ad + bc)\theta + bd\theta^2 \\ &= ac + (ad + bc)\theta - bd \\ &= (ac - bd) + (ad + bc)\theta\end{aligned}$$

This shouldn't come as a surprise as this is exactly how we add and multiply in $\mathbb{C}$ where we swap out θ for i. In other words, the map from $\mathbb{R}[x]/(p(x))$ to $\mathbb{C}$ defined by $a + b\theta \mapsto a + bi$ is an isomorphism. In fact, we could have defined $\mathbb{C}$ exactly as $\mathbb{R}[x]/(p(x))$ (which shows that imaginary numbers aren't so imaginary).

(2) In the example above, we could replace $\mathbb{R}$ with $\mathbb{Q}$ to obtain the field extension $\mathbb{Q}(i)$ of $\mathbb{Q}$ of degree 2 containing a root i of x^2+1.

(3) Let $p(x) = x^2 - 2$. Then $p(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (with prime 2). We obtain a field extension of $\mathbb{Q}$ of degree 2 containing a square root θ of 2, denoted $\mathbb{Q}(\theta)$. If we denote θ by $\sqrt{2}$, the elements of this field are of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. In this case, addition and multiplication are defined as expected.

(4) Consider $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then $p(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (with prime 2). Let θ be a root of $p(x)$. Then

$$\mathbb{Q}[x]/(x^3 - 2) \cong \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\},$$

where $\theta^3 = 2$. This is an extension of degree 3. Let's find the inverse of $1+\theta$ in this field. Since $p(x)$ is irreducible, it is relatively prime to every polynomial of smaller degree. Thus, by the Euclidean Algorithm in $\mathbb{Q}[x]$, there are polynomials $a(x)$ and $b(x)$ in $\mathbb{Q}[x]$ such that

$$a(x)(1+x) + b(x)(x^3 - 2) = 1.$$

In the quotient field, this equation tells us that $a(\theta)$ is the inverse of $1+\theta$ (since $b(x)(x^3 - 2) \in (p(x))$). Actually carrying out the Euclidean Algorithm yields $a(x) = \frac{1}{3}(x^2 - x + 1)$ and $b(x) = -\frac{1}{3}$. This implies that

$$(1+\theta)^{-1} = \frac{\theta^2 - \theta + 1}{3}.$$

(5) Let $p(x) = p_n x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0$ be an irreducible polynomial over a field F. Suppose $\theta \in K$ is a root of $p(x)$. Notice that

$$\theta(p_n\theta^{n-1} + p_{n-1}\theta^{n-2} + \cdots + p_1) = -p_0.$$

Since $p(x)$ is irreducible, $p_0 \neq 0$. This implies that

$$\theta^{-1} = -\frac{1}{p_0}(p_n\theta^{n-1} + p_{n-1}\theta^{n-2} + \cdots + p_1) \in K.$$

(6) Consider $p(x) = x^2 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$. In Example 1.108(4), we verified that $p(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$. Then

$$\mathbb{Z}/2\mathbb{Z}[x]/(p(x)) \cong \{a + b\theta \mid a, b \in \mathbb{Z}/2\mathbb{Z}\} = \mathbb{Z}/2\mathbb{Z}(x),$$

where $\theta^2 = -\theta - 1 = \theta + 1$. This is extension of $\mathbb{Z}/2\mathbb{Z}$ of degree 2. The extension field contains 4 elements. Multiplication is defined by

$$\begin{aligned}(a + b\theta)(c + d\theta) &= ac + (ad + bc)\theta + bd\theta^2 \\ &= ac + (ad + bc)\theta + bd(\theta + 1) \\ &= (ac + bd) + (ad + bc + bad)\theta.\end{aligned}$$

Definition 2.16. Let K be an extension of the field F and let $\alpha, \beta, \ldots \in K$. Then the smallest subfield of K containing both F and the elements $\alpha, \beta, \ldots$, denoted $F(\alpha, \beta, \ldots)$ is called the field **generated by** $\alpha, \beta, \ldots$ **over** F.

Definition 2.17. If the field K is the generated by a single element α over F, $K = F(\alpha)$, then K is said to be a **simple extension** of F and the element α is called a **primitive element** for the extension.

Theorem 2.18. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then

$$F(\alpha) = F[x]/(p(x)).$$

Note 2.19. The previous theorem tells us that any field over F in which $p(x)$ contains a root contains a subfield isomorphic to the extension of F constructed in Theorem 2.12. In addition, this field is (up to isomorphism) the smallest extension of F containing such a root.

Corollary 2.20. Let F and $p(x)$ be as in the previous theorem and suppose $\deg(p(x)) = n$. Then

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\} \subseteq K.$$

Example 2.21. Here are two more examples.

(1) Since $\sqrt{2}, -\sqrt{2}$ are roots of $x^2 - 2$, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(-\sqrt{2})$. Note that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} + \mid a, b \in \mathbb{Q}\}$ as we saw in an earlier example.

(2) Similarly, since $\sqrt[3]{2}$ is a root of $x^3 - 2$, $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$. Note that $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^3 \mid a, b, c \in \mathbb{Q}\}$. The only real root of $x^3 - 2$ is $\sqrt[3]{2}$, but there are two other roots of

$x^3 - 2$, namely

$$\sqrt[3]{2}\left(\frac{-1 \pm i\sqrt{3}}{2}\right).$$

The fields generated by these two roots are subfields of $\mathbb{C}$ but not $\mathbb{R}$. In both cases, the fields are isomorphic to $\mathbb{Q}[x]/(x^3 - 2)$.

Theorem 2.22. Let $\phi : F \to F'$ be an isomorphism of fields. Then we can extend ϕ to an isomorphism from $F[x]$ to $F'[x]$. Let $p(x)$ be an irreducible polynomial in $F[x]$ and let $p'(x)$ be the corresponding irreducible polynomial in $F'[x]$. Let α be a root of $p(x)$ (in some extension of F) and let β be any root of $p'(x)$ (in some extension of F'). Then there exists an isomorphism of fields $\sigma : F(\alpha) \to F'(\beta)$ such that $\sigma(\alpha) = \beta$.

2.2 Algebraic Extensions

Throughout this section, assume F is a field and let K be an extension of F.

Definition 2.23. The element $\alpha \in K$ is said to be **algebraic** over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, then α is called **transcendental** over F. The extension K/F is called **algebraic** if every element of K is algebraic over F.

Example 2.24. Here are a few short examples.

(1) Every field F is algebraic over itself. For $\alpha \in F$, α is a root of the polynomial $x - \alpha \in F[x]$.

(2) The real number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$.

(3) The complex number i is algebraic over $\mathbb{Q}$ since it is a root of the polynomial $x^2+1 \in \mathbb{Q}[x]$.

(4) It turns out that the real number π is transcendental over $\mathbb{Q}$ since there is no polynomial in $\mathbb{Q}[x]$ having π as a root. However, π is algebraic over $\mathbb{R}$ since it is a root of $x - \pi \in \mathbb{R}[x]$.

Theorem 2.25. Let α be algebraic over F. Then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ that has α as a root. Moreover, a polynomial $f(x) \in F[x]$ has α as a root iff $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Definition 2.26. The polynomial $m_{\alpha,F}(x)$ is called the **minimal polynomial** for α over F. The degree of $m_{\alpha,F}(x)$ is called the **degree** of α.

The next theorem follows immediately from 2.18.

Theorem 2.27. Let α be algebraic over F. Then

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$$

and $[F(\alpha) : F] = \deg(m_{\alpha,F}(x)) = \deg(\alpha)$.

Theorem 2.28. This got combined with Theorem 2.25.

Corollary 2.29. If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

Corollary 2.30. A monic polynomial $f(x) \in F[x]$ with α as a root is equal to $m_{\alpha,F}(x)$ iff $f(x)$ is irreducible over F.

Example 2.31. Here are a couple of examples.

(1) Consider the polynomial $x^n - 2 \in \mathbb{Q}[x]$ with $n > 1$. This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's Criteria (with prime 2). Then the positive nth root of 2, denoted by $\sqrt[n]{2}$ in $\mathbb{R}$, is a root. By Corollary 2.30, $x^n - 2$ is the minimal polynomial of $\sqrt[n]{2}$ and by Theorem 2.27, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. In particular, the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ and $\sqrt{2}$ is of degree 2.

(2) Consider the polynomial $x^3 - 3x - 1 \in \mathbb{Q}[x]$. By the Rational Root Test, the only possible roots of this polynomial are ± 1. However, neither of these numbers are roots. Since the polynomial is of degree 3, it must be irreducible over $\mathbb{Q}$. This implies that if α is a root of $x^3 - 3x - 1$, then $x^3 - 3x - 1$ is the minimal polynomial of α and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Theorem 2.32. The element α is algebraic over F iff the simple field extension $F(\alpha)/F$ is finite. More specifically, if α is an element of an extension of degree n over F, then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F, then the degree of $F(\alpha)$ over F is at most n.

Corollary 2.33. If the extension K/F is finite, then it is algebraic.

Theorem 2.34. Let K/F and L/K be field extensions. Then $[L : K][K : F] = [L : F]$.

Corollary 2.35. Suppose L/F is a finite field extension and let K be any subfield of L containing F ($F \subseteq K \subseteq L$). Then $[K : F]$ divides $[L : F]$.

Example 2.36. Here are two examples.

(1) By the Intermediate Value Theorem, the polynomial $p(x) = x^3 - 3x - 1$ has a real root between 0 and 2. Actually, it has one such root. Let's call it α.

In Example 2.31(b), we argued that $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$ and that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Is it possible that $\sqrt{2}$ is an element of $\mathbb{Q}(\alpha)$? The answer is no.

Arguing that $\sqrt{2}$ is not equal to a linear combination of $1, \alpha, \alpha^2$ would be annoying. Thankfully, there is an easier way.

We already know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (since $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$). If $\sqrt{2}$ is an element of $\mathbb{Q}(\alpha)$, then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$. However, 2 does not divide 3, which implies that $\mathbb{Q}(\sqrt{2}) \nsubseteq \mathbb{Q}(\alpha)$.

(2) Let $\sqrt[6]{2}$ be the positive real 6th root of 2. It is quickly seen that $x^6 - 2$ is the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}$. This implies that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$.

Notice that $(\sqrt[6]{2})^3 = \sqrt{2}$. Then $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$. By the multiplicity of the degrees of the extensions, it must be the case that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$. This implies that the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ is of degree 3. We see that the polynomial $x^3 - \sqrt{2}$ is a monic polynomial of degree 3 over $\mathbb{Q}(\sqrt{2})$ that has $\sqrt[6]{2}$ as a root. It follows that $x^3 - \sqrt{2}$ is the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ (and hence irreducible).

Observe that showing $x^3 - \sqrt{2}$ is irreducible directly would not be an easy task.

Definition 2.37. A field extension K/F is **finitely generated** if there are elements $\alpha_1, \ldots, \alpha_k \in K$ such that $K = F(\alpha_1, \ldots, \alpha_k)$.

Theorem 2.38. Let F be a field. Then $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Example 2.39. Consider the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Since $\sqrt{3}$ is of degree 2 over $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$ is at most 2. In fact, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ iff $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. But x^2-3 is irreducible iff it does not have a root in $\mathbb{Q}(\sqrt{2})$. That is, x^2-3 is reducible iff $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

Suppose $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Squaring both sides, we obtain $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. We consider 3 cases. First, suppose $ab \neq 0$. In this case, we can write $\sqrt{2}$ as a rational number, which is impossible. Now, assume $b = 0$. Then we have $\sqrt{3} = a \in \mathbb{Q}$, which is absurd. Lastly, assume $a = 0$. Then $\sqrt{3} = b\sqrt{2}$. This implies that $\sqrt{6} = 2b \in \mathbb{Q}$, which is a contradiction since $\sqrt{6}$ is not rational.

We have shown that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Thus, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and so $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. It follows that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$. We have also shown that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.

Theorem 2.40. The field extension K/F is finite iff K is generated by a finite number of algebraic elements over F. More precisely, a field generated over F by a finite number of algebraic elements of degrees $n_1, \ldots, n_k$ is algebraic of degree less than or equal to $n_1 \cdots n_k$.

Corollary 2.41. Suppose α and β are algebraic over F. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (for $\beta \neq 0$), and α^{-1} (for $\alpha \neq 0$) are all algebraic.

Corollary 2.42. Let L/F be an arbitrary field extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.

Example 2.43. Consider the field extension $\mathbb{C}/\mathbb{Q}$. Recall that the degree of this extension is the dimension of $\mathbb{C}$ as a vector space over $\mathbb{Q}$. We will argue that this degree is infinite. Let $\overline{\mathbb{Q}}$

be the subfield of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. Notice that for each $n > 1$, the positive nth root of 2, namely $\sqrt[n]{2}$, is an element of $\overline{\mathbb{Q}}$. Recall that the minimal polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$ is $x^n - 2$, and hence $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q} = n$. This implies that $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all $n > 1$. But then $\overline{\mathbb{Q}}$ is an infinite algebraic extension of $\mathbb{Q}$, called the field of **algebraic numbers**. It follows that $[\mathbb{C} : \mathbb{Q}]$ is infinite.

Consider the subfield $\overline{\mathbb{Q}} \cap \mathbb{R}$, which is the set of all real numbers that are algebraic over $\mathbb{Q}$. Since $\mathbb{Q}$ is countable, the number of polynomials of degree n is countable. This implies that the number of algebraic elements of $\mathbb{R}$ of degree n is countable, and hence the number of real numbers that are algebraic over $\mathbb{Q}$ is countable. Since $\mathbb{R}$ is uncountable, there must be uncountably many real numbers that are transcendental over $\mathbb{Q}$.

In general, it is difficult to determine whether a given real number is algebraic (over $\mathbb{Q}$). It is know that π and e are transcendental (over $\mathbb{Q}$).

Theorem 2.44. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

Definition 2.45. Let K_1 and K_2 be two subfields of a field K. Then the **composite field** of K_1 and K_2, denoted K_1K_2 is the smallest subfield of K containing both K_1 and K_2. Similarly, we can define the composite of any collection of subfields of K.

Theorem 2.46. Let K_1 and K_2 be two finite extensions of a field F contained in field K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality iff an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ are bases of K_1 and K_2 over F, respectively, then the elements $\alpha_i \beta_j$ span $K_1 K_2$ over F.

Corollary 2.47. Suppose $[K_1 : F] = n, [K_2 : F] = m$ in the previous theorem, where m and n are relatively prime. Then $[K_1 K_2 : F] = [K_1 : F][K_2 : F] = nm$.

2.3 Splitting Fields

Throughout this section, assume F is a field.
In Section 2.2, we saw that given any polynomial $f(x) \in F[x]$, there exists a field K containing an isomorphic copy of F in which $f(x)$ has a root, say α. The upshot is that $f(x)$ has a linear factor $x - \alpha$ in $K[x]$. This idea motivates the following definition.

Definition 2.48. The extension field K of F is called **splitting field** for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (i.e., **splits completely**) in $K[x]$ and $f(x)$ does not factor completely into linear factor over any proper subfield of K containing F.

By Theorem 1.115, if $f(x)$ is of degree n, then $f(x)$ has at most n roots in K. This polynomial will have exactly n roots (counting multiplicities) in K iff $f(x)$ splits completely in $K[x]$.

Theorem 2.49. If $f(x) \in F[x]$, then there exists an extension K of F that is a splitting field for $f(x)$.

The previous theorem guarantees that splitting fields exist for all polynomials (over fields). Later in this section, we will see that any two splitting fields for the same polynomial are isomorphic, which allows us to refer to *the* splitting field of a polynomial.

Definition 2.50. If K is an algebraic extension of F that is the splitting field over F for a collection of polynomials $f(x) \in F[x]$, then K is called a **normal extension** of F.

Example 2.51. Here are a few short examples.

(1) The splitting field of $x^2 - 4$ over $\mathbb{Q}$ is $\mathbb{Q}$ itself.

(2) The field $\mathbb{Q}(\sqrt{2})$ is the splitting for $x^2 - 2$ over $\mathbb{Q}$ since the two roots $\pm\sqrt{2}$ are in $\mathbb{Q}$ and no proper $\mathbb{Q}(\sqrt{2})$ contains these two roots.

(3) Consider the polynomial $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$. The roots of this polynomial are $\pm\sqrt{2}, \pm\sqrt{3}$. The corresponding splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is an extension of degree 4 over $\mathbb{Q}$. Let's draw the corresponding lattice of know subfields. Does it look like anything we've seen before?

(4) Next, consider the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. You might think that $\mathbb{Q}(\sqrt[3]{2})$ is the splitting field. However, as we saw in Example 2.21(2), $x^3 - 2$ also has two non-real roots, namely

$$\sqrt[3]{2}\left(\frac{-1 + i\sqrt{3}}{2}\right) \text{ and } \sqrt[3]{2}\left(\frac{-1 - i\sqrt{3}}{2}\right).$$

But $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of $\mathbb{R}$, so it cannot be the splitting field of $x^3 - 2$. In fact, the splitting field of $x^3 - 2$, call it K, is obtained by adjoining all three roots to $\mathbb{Q}$.

Note that since K contains $\sqrt[3]{2}$ and the first complex root above, K contains their quotient

$$\frac{-1 + \sqrt{-3}}{2},$$

which implies that K contains the element $\sqrt{-3}$. On the other hand, if K contains $\sqrt[3]{2}$ and $\sqrt{-3}$, then certainly K contains the three roots of $x^3 - 2$. We have argued that $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

We claim that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = 6$. To see why this is true, notice that $\sqrt{-3}$ is a root of $x^2 + 3$, which implies that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[3]{2})]$ is at most 2. But since $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of $x^3 - 2$ over $\mathbb{Q}$, it must be the case that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$. By Theorem 2.34, we have

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Let's draw the corresponding lattice of known subfields. Any observations?

(5) In the previous example, the degree of the splitting field might have been larger than what you expected. Here's an example that has degree smaller than what you might expect. Consider the polynomial $x^4 + 4$ over $\mathbb{Q}$. It turns out that

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2),$$

which shows that $x^4 + 4$ is not irreducible over $\mathbb{Q}$. However, since the two quadratic factors above are irreducible over $\mathbb{Q}$ (by Eisenstein's Criterion), none of the roots of $x^4 + 4$ lie in $\mathbb{Q}$. Using the quadratic formula, we find that the roots are $\pm 1 \pm i$. It follows that the splitting field for $x^4 + 4$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$, which is an extension of degree 2.

Theorem 2.52. A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.

Example 2.53. Let's explore the splitting field of $x^n - 1$ over $\mathbb{Q}$.

In the example above, we introduced the following definitions.

Definition 2.54. The roots of $x^n - 1$ are called the **nth roots of unity**. A generator of the cyclic group of all nth roots of unity is called a **primitive** nth root of unity. We often use ζ_n to represent a primitive nth root of unity. The field $\mathbb{Q}(\zeta_n)$ is called the **cyclotomic field of nth roots of unity**.

Example 2.55. Let's explore the splitting field of $x^p - 2$ over $\mathbb{Q}$, where p is a prime.

Theorem 2.56. Let $\phi : F \to F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ and let $f'(x) \in F'[x]$ be the polynomial obtained by applying ϕ to the coefficients of $f(x)$. Let E be the splitting field of $f(x)$ over F and let E' be the splitting field of $f'(x)$ over F'. Then the isomorphism of ϕ extends to an isomorphism $\sigma : E \to E'$ (i.e., $\sigma|_F = \phi$).

Corollary 2.57 (Uniqueness of Splitting Fields)**.** Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

The rest of this section is devoted to discussion of field extensions of a field F that contain *all* the roots of *all* polynomials over F. We state a few results without proof (see Section 13.4 of Dummit and Foote if you are interested in the details).

Definition 2.58. A field $\overline{F}$ is called an **algebraic closure** of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$ (i.e., $\overline{F}$ contains all the elements that are algebraic over F).

Definition 2.59. A field K is said to be **algebraically closed** if every polynomial with coefficients in K has a root in K.

It isn't obvious that algebraically closed fields should even exist nor that there exists an algebraic closure of a given field.

Theorem 2.60. Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ is algebraically closed.

All known proofs of the following result use Zorn's Lemma.

Theorem 2.61. For any field F, there exists an algebraically closed field K containing F.

Theorem 2.62. Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to isomorphism.

The hope is that we will prove the following result later in the course. Purely analytic proofs exist.

Theorem 2.63 (Fundamental Theorem of Algebra)**.** The field $\mathbb{C}$ is algebraically closed.

Corollary 2.64. The field $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\overline{\mathbb{Q}}$ is the collection of complex numbers algebraic over $\mathbb{Q}$.

2.4 Separable and Inseparable Extensions

Throughout this section, assume F is a field.

Let $f(x) \in F[x]$ be a polynomial with leading coefficient a_n. Over a splitting field for $f(x)$ we have the factorization

$$f(x) = a_n(x-\alpha_1)^{n_1}(x-\alpha_1)^{n_2}\cdots(x-\alpha_k)^{n_k},$$

where $\alpha_1,\ldots,\alpha_k$ are distinct elements of the splitting field and $n_i \geq 1$ for all i. A root α_i is called a **multiple root** if $n_i > 1$ and is called a **simple root** if $n_i = 1$. The integer n_i is called **multiplicity** of the root α_i.

Definition 2.65. A polynomial over F is called **separable** if it has no multiple roots (i.e., all roots are distinct). A polynomial that is not separable is called **inseparable**.

Example 2.66. The polynomial x^2-3 is separable over $\mathbb{Q}$ while the polynomial x^2+2x+1 is inseparable over $\mathbb{Q}$.

Definition 2.67. The **derivative** of the polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

is defined to be the polynomial

$$D_x[f(x)] = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

This definition agrees with the ordinary notion of a derivative from calculus. However, it is purely algebraic and be applied to a polynomial over an arbitrary field F. The usual derivative formulas hold:

- $D_x[f(x)+g(x)] = D_x[f(x)] + D_x[g(x)]$
- $D_x[c \cdot f(x)] = c \cdot D_x[f(x)]$
- $D_x[f(x)g(x)] = D_x[f(x)]g(x) + f(x)D_x[g(x)]$

Theorem 2.68. A polynomial $f(x)$ has a multiple root α iff α is also a root of $D_x[f(x)]$, i.e., $f(x)$ and $D_x[f(x)]$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable iff $\gcd(f(x), D_x[f(x)]) = 1$.

Example 2.69. Here are two quick examples.

(1) The polynomial $x^n - 1$ has derivative nx^{n-1}. Over any field of characteristic not dividing n, including characteristic 0, this polynomial has only the root 0 (of multiplicity $n-1$), which is not a root of $x^n - 1$. This implies that $x^n - 1$ is separable and there are n distinct nth roots of unity, which we already saw in the case $F = \mathbb{Q}$.

(2) If F is of characteristic p and p divides n, then there are fewer than n distinct roots of unity over F. In this case, the derivative is identically 0 since $n = 0$ in F. In fact, every root of $x^n - 1$ is multiple in this case.

Corollary 2.70. Every irreducible polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable iff it is the product of distinct irreducible polynomials.

Theorem 2.71. Suppose $f(x) \in F[x]$ is irreducible over F. Then the polynomial $f(x)$ is inseparable iff $D_x[f(x)] = 0$.

Theorem 2.72. Let F be a field of characteristic p. Then for any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$. Moreover, the map $\phi : F \to F$ given by $\phi(a) = a^p$ is an injective field homomorphism.

The map ϕ defined in the previous theorem is called the **Frobenius endomorphism** (which means that it better be onto).

Corollary 2.73. Suppose F is a finite field of characteristic p. Then every element of F is a pth power in F.

Theorem 2.74. Every irreducible polynomial over a finite field F of characteristic p is separable. A polynomial in $F[x]$ is separable iff it si the product of distinct irreducible polynomials in $F[x]$.

The proof of the previous theorem suggests the following definition.

Definition 2.75. A field K of characteristic p is called **perfect** if every element of K is a pth power in K. Any field of characteristic 0 is also called perfect.