

# 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  $\text{Char}(R)$ , 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  $\text{Char}(R)$  is either 0 or a prime  $p$ .

**Theorem 2.4.** If  $R$  is an integral domain such that  $\text{Char}(R) = p$  ( $p$  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  $\text{Char}(F)$  is 0 or  $p$  (for  $p$  prime). To see why this is true, define  $\phi : \mathbb{Z} \rightarrow F$  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  $\ker(\phi) = \text{Char}(F)\mathbb{Z}$ . 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 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  $\theta = x \bmod (p(x)) \in K$ . Then the elements  $1, \theta, \theta^2, \dots, \theta^{n-1}$  are a basis for  $K$  as a vector space over  $F$ . In particular,  $[K : F] = n$  and

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

which is the set of all polynomials of degree less than  $n$  in  $\theta$ .

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  $\theta$  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  $\theta$  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  $\theta$  of 2, denoted  $\mathbb{Q}(\theta)$ . If we denote  $\theta$  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  $\theta$  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

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

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  $\alpha, \beta, \dots \in K$ . Then the smallest subfield of  $K$  containing both  $F$  and the elements  $\alpha, \beta, \dots$ , denoted  $F(\alpha, \beta, \dots)$  is called the field **generated by  $\alpha, \beta, \dots$  over  $F$** .

**Definition 2.17.** If the field  $K$  is generated by a single element  $\alpha$  over  $F$ ,  $K = F(\alpha)$ , then  $K$  is said to be a **simple extension** of  $F$  and the element  $\alpha$  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  $\alpha$  of  $p(x)$ . Let  $F(\alpha)$  denote the subfield of  $K$  generated over  $F$  by  $\alpha$ . 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

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

**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  $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ . 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  $\phi : F \rightarrow F'$  be an isomorphism of fields. Then we can extend  $\phi$  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  $\alpha$  be a root of  $p(x)$  (in some extension of  $F$ ) and let  $\beta$  be any root of  $p'(x)$  (in some extension of  $F'$ ). Then there exists an isomorphism of fields  $\sigma : F(\alpha) \rightarrow F'(\beta)$  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  $\alpha$  is a root of some nonzero polynomial  $f(x) \in F[x]$ . If  $\alpha$  is not algebraic over  $F$ , then  $\alpha$  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  $\alpha \in F$ ,  $\alpha$  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  $\pi$  is transcendental over  $\mathbb{Q}$  since there is no polynomial in  $\mathbb{Q}[x]$  having  $\pi$  as a root. However,  $\pi$  is algebraic over  $\mathbb{R}$  since it is a root of  $x - \pi \in \mathbb{R}[x]$ .

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

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

The next theorem follows immediately from [2.18](#).

**Theorem 2.27.** Let  $\alpha$  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.** Let  $\alpha$  be algebraic over  $F$ . A polynomial  $f(x) \in F[x]$  has  $\alpha$  as a root iff  $m_{\alpha,F}(x)$  divides  $f(x)$  in  $F[x]$ .

**Corollary 2.29.** If  $L/F$  is an extension of fields and  $\alpha$  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  $\alpha$  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  $n$ th 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  $\pm 1$ . 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  $\alpha$  is a root of  $x^3 - 3x - 1$ , then  $x^3 - 3x - 1$  is the minimal polynomial of  $\alpha$  and  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ .

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