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 $\phi : \mathbb{Z} \to F$ 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 $\ker(\phi) = \text{Char}(F)\mathbb{Z}$. 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 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.