Chapter 1

Fields: Part I

§1.1 Introduction to Fields

Recall that in Chapter 3, we introduced fields as commutative rings with an additional property: every non-zero element had a multiplicative inverse. We extended this in Chapter 4 by building vector spaces with fields.

Definition 1.1.1: Fields

A **field** is a commutative ring F with the property that for every $a \in F$ with $a \neq 0$, there is a $b \in F$ such that $ab = 1$.

Now, we begin studying fields in their own right. First, we look at how fields fit into each other, how to construct new fields from old fields, and describe all fields with finitely many elements. Finite fields are not just a mathematical curiosity; they play important roles in pure and applied mathematics, as well as engineering; some applications include signal processing, error correcting codes, and cryptography.

Remark 1. *Field theory was originally developed to aid the study of polynomials, such as finding the roots of a certain polynomial. Interestingly, field theory and finite group theory both originated from the study of polynomials! For more history, Google Cardano's Formula.*

§1.2 Abstract Fields and Homomorphisms

Recall the definition of a unit group:

Definition 1.2.1: Unit Groups

Let R be a commutative ring. The **unit group** of R is the group

$$R^* = \{a \in R \mid \text{ there is some } b \in R \text{ such that } ab = 1\},$$

where the group law is ring multiplication.

Thus, a succinct way to characterize a field is that it is a commutative ring F satisfying

$$F^* = \{a \in F \mid a \neq 0\} = F \setminus \{0\}.$$

As for maps between fields, we obviously want them to preserve field properties. In particular, since fields are rings, we want our maps to *at least* be ring homomorphisms.

It turns out that it's enough to ensure that multiplicative inverses go to multiplicative inverses; moreover, somewhat surprisingly, maps between fields are always injective! Note that this statement is generally not true for rings; the ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is very non-injective.

Proposition 1.2.1

Let F, K be fields, and let $\phi : F \to K$ be a ring homomorphism.

- The map ϕ is injective.
- Let $a \in F^*$. Then $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof.

- From Theorem 3.31(b)ii, we need to show that $\ker(\phi)$ is the zero ideal, so suppose there is a non-zero element $a \in \ker(\phi)$. $a \neq 0$ in a field F implies that $ab = 1_F$ for some $b \in F$; thus

$$1_K = \phi(1_F) = \phi(ab) = \phi(a)\phi(b) = 0 \cdot \phi(b) = 0_K,$$

a contradiction (since ring axioms require $1 \neq 0$). Thus $\ker(\phi)$ is the zero ideal, and so ϕ is injective.

- By definition of multiplicative inverse, and since ϕ is a homomorphism, we have

$$1_K = \phi(1_F) = \phi(a \cdot a^{-1}) = \phi(a) \cdot \phi(a^{-1}).$$

Hence $\phi(a^{-1})$ is a multiplicative inverse for $\phi(a)$; i.e. $\phi(a^{-1}) = \phi(a)^{-1}$.

Alternatively, from (a) we know the map $\phi : F^* \to K^*$ is well-defined (by injectivity, since if $\phi(a) = \phi(a')$, then $a = a'$), and by the homomorphism property, it is a group homomorphism from F^* to K^*. Thus, the fact that ϕ sends multiplicative inverses to multiplicative inverses is a result of Proposition 2.20 (which states that for group homomorphisms, $\phi(a^{-1})$ is the inverse of $\phi(a)$).

□

§1.3 Interesting Examples of Fields

Example 1. *Three fields are already familiar:* $\mathbb{Q}, \mathbb{R}$, *and* $\mathbb{C}$. *Moreover, they fit into each other:*

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Example 2. *The following subset of* $\mathbb{C}$ *is a field:*

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

The multiplicative inverse of a non-zero element $a + bi$ *is obtained by "rationalizing the denominator:"*

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}.$$

In similar fashion, we can use $\sqrt{2}$ to describe a subfield of $\mathbb{R}$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

with a multiplicative inverse obtained again by rationalizing the denominator:

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.$$

This is well-defined, since $\sqrt{2}$ is not a rational number, so $a^2 - 2b^2 \neq 0$ for any $a, b \in \mathbb{Q}$ as long as they are non-zero as well.
What about the set

$$\{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}?$$

This is not even a ring, since one can see $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$, which is not in the set. The larger set

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

is a field. It's easy to see ring properties, but proving that non-zero elements have an inverse is not quite so easy. We'll see tools to help with this later.

Example 3. *In general, the ring $\mathbb{Z}/m\mathbb{Z}$ need not be a field. For example, $\mathbb{Z}/6\mathbb{Z}$ is not a field, since 2 does not have a multiplicative inverse. However, we've seen before that any ring $\mathbb{Z}/p\mathbb{Z}$, where p is a prime, is a field; we denote this $\mathbb{F}_p$. $\mathbb{F}_p$ is an example of a **finite field**; it turns out that there are other finite fields. Indeed, for every prime power p^k, there is exactly one (up to isomorphism) finite field containing p^k elements.*

Example 4. *A **skew field**, also called a **division ring**, is a ring in which every non-zero element has an inverse, but is no longer required to be commutative. Wedderburn's Theorem states that every finite skew field must be commutative (e.g. is a field), but there are also many interesting non-commutative infinite fields. One such example is $\mathbb{H}$, the ring of quaternions.*

§1.4 Subfields and Extension Fields

Definition 1.4.1: Subfields

Let K be a field. A **subfield of K** is a subset F of K that is itself a field using the addition and multiplication operations of K.

Definition 1.4.2: Extension Fields

Let F be a field. An **extension field of $\mathbb{F}$** is a field K such that F is a subfield

of K. We write K/F to indicate that K is an extension field of F.[a]

[a]Note that K/F is just a piece of convenient notation. It doesn't mean that we're taking the quotient of K by F, despite its similarities to a quotient ring R/I.

Example 5. *The field $\mathbb{Q}$ is a subfield of $\mathbb{R}$, and thus $\mathbb{R}$ is an extension field of $\mathbb{Q}$; similarly with $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.*
The fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are extension fields of $\mathbb{Q}$. The former is a subfield of $\mathbb{C}$ but not $\mathbb{R}$, while the latter is a subfield of $\mathbb{R}$. Neither are subfields of each other.

The notation $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ is a special case of the following general construction.

Proposition 1.4.1

Let L/F be an extension of fields, and let $\alpha_1, \ldots, \alpha_n \in L$. Then there is a unique field K with the following properties:

1. $F \subseteq K \subseteq L$.
2. $\alpha_1, \ldots, \alpha_n \in K$.
3. If K' is a field satisfying $F \subseteq K' \subseteq L$ and $\alpha_1, \ldots, \alpha_n \in K'$, then $K \subseteq K'$.

The field K is denoted $F(\alpha_1, \ldots, \alpha_n)$ and is called the **extension field of F generated by** $a_1, \ldots, a_n$. Intuitively, it is the smallest subfield of L that contains both F and $\alpha_1, \ldots, \alpha_n$.

Proof. Let S be the set consisting of all subfields of L that contain F and $\alpha_1, \ldots, \alpha_n$. The set is not empty, since $L \in S$. Let K be the intersection of all of the fields in S. Then K is a field, since

$$\begin{aligned} \alpha, \beta \in K &\iff \alpha, \beta \in K' \text{ for every } K' \in S, \\ &\implies \alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K' \text{ for every } K' \in S, \quad \text{since } K' \text{ is a field }, \\ &\implies \alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K.. \end{aligned}$$

Clearly, K contains F and α_i, since it is the intersection of fields that contain both; and if $K' \subseteq L$ contains both, then $K' \in S$, so K' is one of the fields whose intersection forms K. Hence $K \subseteq K'$. □

Let K/F be an extension of fields. Observe that we can add elements of K, and multiply elements in K by elements in F; thus, the field K becomes an F-vector space. Essentially, we discard most of the multiplication operation in K, and restrict it solely to multiplication by elements in F. This allows us to use tools from linear algebra to study field extensions.

Definition 1.4.3: Degree of Field Extensions

Let K/F be an extension of fields. The **degree of K over F**, denoted $[K : F]$, is the dimension of K viewed as an F-vector space,

$$[K : F] = \dim_F(K).$$

If $[K : F]$ is finite, we say K/F is a **finite extension**; otherwise, we say K/F is an **infinite extension**.

Example 6. *The fields* $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ *have degree* 2 *over* $\mathbb{Q}$*:*

- $[\mathbb{Q}(i) : \mathbb{Q}] = 2$*, since* $\{1, i\}$ *is a* $\mathbb{Q}$*-basis for* $\mathbb{Q}(i)$*.*
- $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$*, since* $\{1, \sqrt{2}\}$ *is a* $\mathbb{Q}$*-basis for* $\mathbb{Q}(\sqrt{2})$*.*

Similarly, we have $[\mathbb{C} : \mathbb{R}] = 2$*, since* $\{1, i\}$ *is an* $\mathbb{R}$*-basis for* $\mathbb{C}$*. On the other hand,* $[\mathbb{R} : \mathbb{Q}] = \infty$*:*

Proof. Suppose that $\{a_1, \ldots, a_n\} \subset \mathbb{R}$ is a finite $\mathbb{Q}$-basis for $\mathbb{R}$. Then

$$\mathbb{R} = \{c_1 a_1 + \ldots + c_n a_n \in \mathbb{Q}\}.$$

But the set on the right is countable (since its cardinality is the same as the cardinality of the set of n-tuples of rational numbers), while $\mathbb{R}$ is uncountable. □

The next theorem is similar to the index multiplication rule, which counted cosets in a chain of groups.

Theorem 1.4.1

Let $L/K/F$ be an extension of fields (that is, L is a field extension of K, while K is a field extension of F). Then

$$[L : F] = [L : K] \cdot [K : F],$$

in the sense that one of the following is true:

- All of the degrees $[L : F], [L : K], [K : F]$ are finite, and the above equation is true.
- $[L : F] = \infty$, and either $[L : K] = \infty$ or $[K : F] = \infty$.