CHAPTER F

STRUCTURE AND ACTION: FIELDS AND VECTOR SPACES

The standard abstract algebra course presents the basic properties of groups, rings, and fields. The motivation is to study the properties of the number systems that we use, some of these being:

(a) the positive integers, $\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$,
(b) the integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
(c) the rational numbers, $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}_{>0} \right\}$,
(d) the real numbers, $\mathbb{R}$,

with the operations of addition and multiplication. We need to find exactly what properties these structures have and what the implications of these properties are.

F.1. Fields

We start by identifying the key properties of the favorite number systems $\mathbb{Q}$ and $\mathbb{R}$.

Definition F.1.1. —

- A **field** is a set $\mathbb{F}$ with two operations, **addition** $+ \colon \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and **multiplication** $\times \colon \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ $\big($we write $a + b$ instead of $+(a, b)$ and ab or $a \cdot b$ instead of $\times(a, b)\big)$, such that
  (a) If $x, y, z \in \mathbb{F}$ then $(x + y) + z = x + (y + z)$.
  (b) If $x, y \in \mathbb{F}$ then $x + y = y + x$.
  (c) There exists a **zero**, or **additive identity**, $0 \in \mathbb{F}$ such that if $x \in \mathbb{F}$ then $0 + x = x$.
  (d) If $x \in \mathbb{F}$ then there is an **additive inverse**, $-x \in \mathbb{F}$, such that $x + (-x) = 0$.
  (e) If $x, y, z \in \mathbb{F}$ then $x(yz) = (xy)z$.
  (f) If $x, y \in \mathbb{F}$ then $xy = yx$.
  (g) There exists an **identity**, or **multiplicative identity**, $1 \in F$ such that $1 \neq 0$ and if $x \in \mathbb{F}$ then $1 \cdot x = x$.
  (h) If $x \in \mathbb{F}$ and $x \neq 0$ then there exists an **inverse** (sometimes called a **multiplicative inverse**), $x^{-1} \in \mathbb{F}$ such that $xx^{-1} = 1$.
  (i) If $x, y, z \in \mathbb{F}$ then
  $$x(y + z) = xy + xz.$$
- A **subfield** of a field $\mathbb{F}$ is a subset $\mathbb{K} \subseteq \mathbb{F}$ such that
  (a) If $x, y \in \mathbb{K}$ then $x + y \in \mathbb{K}$.
  (b) $0 \in \mathbb{K}$.
  (c) If $x \in \mathbb{K}$ then $-x \in \mathbb{K}$.
  (d) If $x, y \in \mathbb{K}$ then $xy \in \mathbb{K}$.

(e) $1 \in \mathbb{K}$.
(f) If $x \in \mathbb{K}$ and $x \neq 0$ then $x^{-1} \in \mathbb{K}$.

A *commutative ring* has the same definition as a field except that condition (h) is not required and the definition of a *ring* is the same as the definition of a field excpet that (f) and (h) are not required.

Important examples of fields are:

(a) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.
(b) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where $p \in \mathbb{Z}_{>0}$ is a prime.

F.1.1. Homomorphisms. — Field homomorphisms might be used to compare fields except that there aren't many field homomorphisms, see Proposition F.1.1.

Definition F.1.2. — Let $\mathbb{K}$ and $\mathbb{F}$ be fields with identities $1_{\mathbb{K}}$ and $1_{\mathbb{F}}$ respectively.
• A **field homomorphism from $\mathbb{K}$ to $\mathbb{F}$** is a function $f\colon \mathbb{K} \to \mathbb{F}$ such that
(a) If $x, y \in \mathbb{F}$ then $f(x+y) = f(x) + f(y)$,
(b) If $x, y \in \mathbb{F}$ then $f(xy) = f(x)f(y)$,
(c) $f(1_{\mathbb{K}}) = 1_{\mathbb{F}}$.

HW: Show that if $f\colon \mathbb{K} \to \mathbb{F}$ is a field homomorphism then $f(0_{\mathbb{K}}) = 0_{\mathbb{F}}$, where $0_{\mathbb{K}}$ and $0_{\mathbb{F}}$ are the zeros in $\mathbb{K}$ and $\mathbb{F}$ respectively.

HW: Let $\mathbb{F}$ be a field. Show that function $f\colon \mathbb{F} \to \mathbb{F}$ given by $f(x) = 0$ satisfies conditions (a) and (b) in the definition of a field homomorphism but does not satisfy (c).

Proposition F.1.1. — *If $f\colon \mathbb{K} \to \mathbb{F}$ is a field homomorphism then f is injective.*

Proposition F.1.1, stated another way, says that the kernel of any field homomorphism is $\{0\}$. This means that any analogue of Theorem R.1.6 for fields always has $\ker f = 0$. Proposition F.1.1 also shows that if $f\colon \mathbb{K} \to \mathbb{F}$ is a field homomorphism then $\operatorname{im} f = f(\mathbb{K})$ is a subfield of $\mathbb{F}$ isomorphic to $\mathbb{K}$.