Chapter 3. FIELDS AND VECTOR SPACES

§1T. Fields

(3.1.1) Definition.

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

$$x(y+z) = xy + xz.$$

- A **subfield** of a field F is a subset $K \subseteq F$ such that
  a) If $x, y \in K$ then $x+y \in K$.
  b) $0 \in K$.
  c) If $x \in K$ then $-x \in K$.
  d) If $x, y \in K$ then $xy \in K$.
  e) $1 \in K$.
  f) If $x \in K$ then $x^{-1} \in K$.

Note that every field is a commutative ring and the only conditions in the definition of a field that are not in the definition of a ring are f) and h).

Important examples of fields are:
a) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.
b) $\mathbb{Z}_p$ where p is a prime.

Homomorphisms

Field homomorphisms might be used to compare fields. The only problem is that there aren't many interesting field homomorphisms, as we show in Proposition 3.1.3. We shall study fields in more depth in Part V.

(3.1.2) Definition. Let K and F be fields with identities 1_K and 1_F respectively.

- A **field homomorphism** is a map $f\colon K \to F$ between fields K and F such that
  a) $f(x+y) = f(x)+f(y)$ for all $x, y \in F$.
  b) $f(xy) = f(x)f(y)$ for all $x, y \in F$.
  c) $f(1_K) = 1_F$.

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

HW: Explain why conditions a) and b) in the definition of a field homomorphism do not imply condition c).

(3.1.3) Proposition. *If $f\colon K \to F$ is a field homomorphism then f is injective.*

Proposition 3.1.3 stated another way, says that the kernel of any field homomorphism is $\{0\}$. This means that we cannot get an interesting analogue of Theorem 1.1.15 for fields. Proposition 3.1.3 also shows that if $f\colon K \to F$ is a field homomorphism then $\operatorname{im} f = f(K)$ is a subfield of F.

(3.2.1) Definition.

- A **vector space** over a field F is a set V with an addition operation $+: V \times V \to V$ and an action $\times: F \times V \to V$ $\big($we write $v + w$ instead of $+(v, w)$ and cv instead of $\times(c, v)\big)$ such that
  a) $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$ for all $v_1, v_2, v_3 \in V$.
  b) $v_1 + v_2 = v_2 + v_1$ for all $v_1, v_2 \in V$.
  c) There exists a **zero**, $0 \in V$, such that $0 + v = v$ for all $v \in V$.
  d) For each $v \in V$ there exists an **additive inverse**, $-v \in V$, such that $v + (-v) = 0$.
  e) $c_1(c_2 v) = (c_1 c_2)v$ for all $c_1, c_2 \in F$ and $v \in V$.
  f) $1 \cdot v = v$ for all $v \in V$.
  g) $c(v_1 + v_2) = cv_1 + cv_2$ for all $c \in F$ and $v_1, v_2 \in V$.
  h) $(c_1 + c_2)v = c_1 v + c_2 v$ for all $c_1, c_2 \in F$ and $v \in V$.

- A **subspace** W of a vector space V over a field F is a subset $W \subseteq V$ such that
  a) If $w_1, w_2 \in W$ then $w_1 + w_2 \in W$.
  b) $0 \in W$.
  c) If $w \in W$ then $-w \in W$.
  d) If $w \in W$ then $cw \in W$ for all $c \in F$.

- The **zero space**, (0), is the set containing only 0 with operations $0 + 0 = 0$ and $c \cdot 0 = 0$ for all $c \in F$.

Properties a), b), c), and d) in the definition of a vector space imply that a vector space is an abelian group with an action of the field F. A vector space is just a module over a field.

HW: Show that if V is a vector space over F then $0 \cdot v = 0$ for all $v \in V$. (Notice that the 0 on the left hand side of this equation is an element of F and the 0 on the right hand side is an element of V.)

HW: Show that if V is a vector space over F and if $c \in F$ and $v \in V$ then $c \cdot v = 0$ if and only if either $c = 0$ or $v = 0$.

Important examples of vector spaces are:
a) $\mathbb{R}^k$ and $\mathbb{C}^k$.
b) F^k for any field F.

Cosets

(3.2.2) Definition.

- A **subgroup** of a vector space V over a field F is a subset $W \subseteq V$ such that
  a) If $w_1, w_2 \in W$ then $w_1 + w_2 \in W$.
  b) $0 \in W$.
  c) If $w \in W$ then $-w \in W$.

Let V be a vector space over a field F and let W be a subgroup of V.

(3.2.3) Definition.

- A **coset** of W in V is a set $v + W = \{v + w \mid w \in W\}$ where $v \in V$.
- V/W (pronounced "V **mod** W") is the set of cosets of W in V.

(3.2.4) Proposition. *Let V be a vector space over a field F and let W be a subgroup of V. Then the cosets of W in V partition V.*

Notice that the proofs of Proposition 3.2.4 and Proposition 2.2.4 are essentially the same.

HW: Write a very short proof of Proposition 3.2.4 by using Proposition 2.2.4.

Quotient Spaces ↔ Subspaces

Let V be a vector space over F and let W be a subspace of V. We can try to make the set V/W of cosets of W in V into a vector space by defining an addition operation and an action of F.

(3.2.5) Theorem. *Let W be a subgroup of a vector space V over a field F. Then W is a subspace of V if and only if V/W with operations given by*

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W, \quad \textit{and}$$
$$c(v + W) = cv + W,$$

is a vector space over F.

Notice that the proofs of Theorem 3.2.5 and Theorem 2.2.5 are essentially the same.

HW: Write a very short proof of Proposition 3.2.5 by using Proposition 2.2.5.

(3.2.6) Definition.

- The **quotient space** V/W is the vector space of cosets of a subspace W of a vector space V over a field F with operations given by $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$ and $c(v + W) = cv + W$.

We have made V/W into a vector space when W is a subspace of V.

Linear Transformations

Linear transformations are used to compare vector spaces.

(3.2.7) Definition.

- A **linear transformation** is a mapping $T: V \to W$ between vector spaces V and W over F such that
  a) $T(v_1 + v_2) = T(v_1) + T(v_2)$ for all $v_1, v_2 \in V$.
  b) $T(cv) = cT(v)$ for all $c \in F$ and $v \in V$.
- A **vector space isomorphism** is a bijective linear transformation.
- Two vector spaces V and W are **isomorphic**, $V \simeq W$, if there exists a vector space isomorphism $T: V \to W$ between them.

Two vector spaces are isomorphic if the elements of the vector spaces and the operations and the actions match up exactly. Think of two vector spaces that are isomorphic as being "the same".

(3.2.8) Proposition. *Let $T: V \to W$ be a linear transformation. Let 0_V and 0_W be the zeros for V and W respectively. Then*

a) $T(0_V) = 0_W$.
b) For any $v \in V$, $T(-v) = -T(v)$.

(3.2.9) Definition.

- The **null space** of a linear transformation $T: V \to W$ is the set

$$\ker T = \{v \in V \mid T(v) = 0_W\},$$

  where 0_W is the zero element of W.
- The **range** of a linear transformation $T: V \to W$ is the set

$$\operatorname{im} T = \{w \in W \mid T(v) = w \text{ for some } v \in V\}.$$

(3.2.10) Proposition. *Let $T: V \to W$ be a linear transformation. Then*

a) $\ker T$ is a subspace of V.
b) $\operatorname{im} T$ is a subspace of W.

(3.2.11) Proposition. *Let $T: V \to W$ be a linear transformation. Let 0_V be the zero in V. Then*

a) $\ker T = \{0_V\}$ *if and only if T is injective.*

b) $\operatorname{im} T = W$ *if and only if T is surjective.*

Notice that the proof of Proposition 3.2.11 b) does not use the fact that $T: V \to W$ is a linear transformation, only the fact that $T: V \to W$ is a function.

(3.2.12) Theorem.

a) Let $T: V \to W$ be a linear transformation and let $N = \ker T$. Define

$$\begin{array}{rccc} \hat{T}: & V/\ker T & \to & W \\ & v + N & \mapsto & f(v). \end{array}$$

Then $\hat{T}$ is a well defined injective linear transformation.

b) Let $T: V \to W$ be a linear transformation and define

$$\begin{array}{rccc} T': & V & \to & \operatorname{im} T \\ & v & \mapsto & T(v). \end{array}$$

Then T' is a well defined surjective linear transformation.

c) If $T: V \to W$ is a linear transformation, then

$$V/\ker T \simeq \operatorname{im} T,$$

where the isomorphism is a vector space isomorphism.

Direct Sums

Suppose V and W are vector spaces over a field F. The idea is to make $V \times W$ into a vector space.

(3.2.13) Definition.

- The **direct sum** of $V \oplus W$ of two vector spaces V and W over a field F is the set $V \times W$ with operations given by
$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$$
$$c(v, w) = (cv, cw)$$
for all $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ and $c \in F$. The operations in $V \oplus W$ are **componentwise**.
- More generally, given vector spaces $V_1, V_2, \ldots, V_n$ over F the **direct sum** $V_1 \oplus \cdots \oplus V_n$ is the set given by $V_1 \times \cdots \times V_n$ with the operations given by
$$(v_1, \ldots, v_i, \ldots, v_n) + (w_1, \ldots, w_i, \ldots, w_n) = (v_1 + w_1, \ldots, v_i + w_i, \ldots, v_n + w_n)$$
$$c(v_1, \ldots, v_i, \ldots, v_n) = (cv_1, \ldots, cv_i, \ldots, cv_n)$$
where $v_i, w_i \in V_i$, $c \in F$, and $v_i + w_i$ and cv_i are given by the operations in V_i.

HW: Show that these are good definitions, i.e., that as defined above, $V \oplus W$ and $V_1 \oplus \cdots \oplus V_n$ are vector spaces over F with zeros given by $(0_V, 0_W)$ and $(0_{V_1}, \ldots, 0_{V_n})$ respectively. (0_{V_i} denotes the zero element in V_i.)

Further Definitions

(3.2.14) Definition.

- Let V be a vector space and let S be a subset of V. The **span of** S, $\operatorname{span}(S)$, or the **subspace generated by** S, is the subspace of V such that
  a) $S \subseteq \operatorname{span}(S)$,
  b) If W is a subspace of V and $S \subseteq W$ then $\operatorname{span}(S) \subseteq W$.

The subspace $\operatorname{span}(S)$ is the smallest subspace of V containing S. Think of $\operatorname{span}(S)$ as gotten by adding to S exactly those elements of V that are needed to make a subspace.