7 Fields and Vector Spaces

7.1 Review

Last time, we learned that we can quotient out a normal subgroup of N to make a new group, G/N.

7.2 Fields

Now, we will do a hard pivot to learning linear algebra, and then later we will begin to merge it with group theory in different ways. In order to define a vector space, the underlying *field* must be specified.

Definition 7.1
A **field** F is a set with the operations $(+, \times)$. It must satisfy that

- $(F, +)$ is an abelian group with the usual rules, and
- $(F^\times := F \setminus \{0\}, \times)$ is an abelian group.

Also, addition and multiplication must distribute over each other.[a]

[a] There is some compatibility required.

In essence, a field is a set with additive and multiplicative group structures that interact in nice ways.

Example 7.2
The sets $\mathbb{C}, \mathbb{R}$, and $\mathbb{Q}$ are fields, but not $\mathbb{Z}$, since it is not invertible under multiplication.

Since division does not exist in $\mathbb{Z}$, it is not a field. In fact, $\mathbb{Q}$ is essentially obtained from $\mathbb{Z}$ by making it into a field by adding division.

Example 7.2 gives us examples of fields with infinitely many elements, but fields can also be constructed that have finite order. Indeed, there is one for every prime number p.

Example 7.3 (Fields of prime order)
For a prime p,

$$(\mathbb{F}_p = \mathbb{Z}_p, +, \times)$$

is a field. If $a \neq 0 \mod p$, then $\gcd(a, p) = 1$ implies that $ar + ps = 1$, and so $ar \equiv 1 \mod p$, and thus a is invertible with multiplicative inverse r^{-1}.

However, $\mathbb{Z}_6$ is not a field; for example, $2 \mod 6$ has no inverse. In general, $\mathbb{Z}_n$ where n is not a prime is not a field, because there will exist some element that is not relatively prime to n, and it will not be invertible.

7.3 Vector Spaces

A vector space, which may be a familiar concept from learning about matrices, can be defined over any field.

Definition 7.4
A **vector space** V over a field F is a set V with some operation $+$ such that $(V, +)$ is an abelian group.

- We must be able to scale vectors:

$$F \times V \to V$$
$$(a, \vec{v}) \mapsto a\vec{v}.$$

- Addition and multiplication play nicely and satisfy the usual rules

$$(\cdots, a(b\vec{v}) = (ab) \cdot \vec{v}, \cdots).$$

Example 7.5
For a field F, F^n, column vectors with n components $(a_1, \cdots, a_n)^t$, form a vector space of dimension n.

Example 7.6
If A is an $m \times n$ matrix, then

$$\{\vec{v} \in F^n : A\vec{v} = (0, \cdots, 0)\}$$

is a vector space.

Example 7.7
For a homogeneous linear ODE, the solutions form a vector space.

7.4 Bases and Dimension

A basis of a vector space is a set of vectors providing a way of describing it without having to list every vector in the vector space.

Definition 7.8
Given $\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n \in V$, a **linear combination** is

$$\vec{v} = \sum a_i \vec{v}_i$$

for $a_i \in F$.

Definition 7.9
For $S = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$, the span

$$\text{Span}(S) = \{\vec{v} \in V : \vec{v} = \sum a_i \vec{v}_i\}$$

This is similar to generating subgroups using elements of a group G, except using the operations of vector spaces.

Artin likes to use the (nonstandard) notation

$$\begin{pmatrix} \vec{v}_1 & \cdots & \vec{v}_n \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \coloneqq \sum a_i \vec{v}_i$$

for a linear combination.

Definition 7.10
A set of vectors S **spans** V if $\text{Span}(S) = V$. [a]

[a] There is at least one way of writing $\vec{v}$ as a linear combination.

Definition 7.11
A set of vectors $\{\vec{v}_i\}$ is **linearly independent** if

$$\sum a_i \vec{v}_i = \vec{0}$$

if and only if $a_i = 0$ for all i.[a]

[a] There is at most one way of writing $\vec{v}$ as a linear combination.

A basis is both linearly independent and spans.

Definition 7.12
A set of vectors $S = \{\vec{v}_1, \cdots, \vec{v}_n\}$ is a **basis** if S spans V *and* is linearly independent. Equivalently, each $\vec{v} \in V$ can be written **uniquely** as $\vec{v} = a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$, where the a_i are called the **coordinates** of $\vec{v}$ in the basis S.

The standard basis for $\mathbb{R}^2$ is

$$\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}.$$

In general, when we write a vector $(a, b)^t$, it represents the linear combination $a(1, 0)^t + b(0, 1)^t$.

Example 7.13
Let $V = \mathbb{R}^2$. Then the set

$$S = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}\right\}$$

spans $\mathbb{R}^2$, but is linearly dependent: $\vec{v}_1 - \vec{v}_2 + \vec{v}_3 = \vec{0}$. But $\{\vec{v}_1, \vec{v}_2\}$ forms a basis.

A good choice of basis often makes problems easier.

Definition 7.14
A vector space V is **finite-dimensional** if $V = \text{Span}(\{\vec{v}_1, \cdots, \vec{v}_n\})$ for some $\vec{v}_i \in V$.[a]

[a] Infinite-dimensional vector spaces are super interesting, but not studied in this class. Real analysis can be used to study them!

Lemma 7.15
If $S = \{\vec{v}_1, \cdots, \vec{v}_r\}$ spans V, and $L = \{\vec{w}_1, \cdots, \vec{w}_s\}$ is linearly independent, then

1. Removing elements of S gets a basis of V.
2. Adding elements of S to L gets another basis of V.
3. $|S| \geq |L|$.

Corollary 7.16
If S and L are both bases for V, then $|S| = |L|$. Any two bases of V contain the same number of vectors.

Proof. Applying the lemma twice for S and L gives $|S| \geq |L|$ and $|L| \geq |S|$. □

Definition 7.17
The **dimension** of a vector space v is the size of any basis of V.

Proof of Lemma 7.15. We prove each point separately

1. If S is not linearly independent, then there are some a_i such that

$$\sum_{i=1}^{r} a_i \vec{v}_i = \vec{0}.$$

Suppose WLOG that $a_n \neq 0$. Then

$$\vec{v}_r = a_r^{-1}(-a_1\vec{v}_1 - \cdots - a_{r-1}\vec{v}_{r-1}) \in \text{Span}(\vec{v}_1, \cdots, \vec{v}_{r-1}).$$

If we take $S' = \{\vec{v}_1, \cdots, \vec{v}_{r-1}\}$, we have $\text{Span}(S') = \text{Span}(S) = V$. This is because if we have a linear combination using the vectors of S, we can use the equation above to turn it into a combination of vectors in S'. We can repeatedly remove until we have a basis of V.

2. If $S \subset \text{Span}(L)$, then $\text{Span}(L) = V$ so we are done. Otherwise, suppose $\vec{v}_i \notin \text{Span}(L)$. We can create $L' = \{\vec{w}_1, \ldots, \vec{w}_s, \vec{v}_i\}$. Then L' is still linearly independent. We can just keep adding vectors to L so that it stays linearly independent but eventually spans V.
3. Each $\vec{w}_j$ is a linear combination of $\vec{v}_1, \cdots, \vec{v}_r$. Then $\vec{w}_j = \sum_{i=1}^{r} a_{ij}\vec{v}_i$. Let A be the $r \times s$ matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rs} \end{pmatrix}.$$

Then $(\vec{w}_1, \cdots, \vec{w}_s) = (\vec{v}_1, \cdots, \vec{v}_r)A$. Suppose $r < s$. Then by row-reduction, there exists some nonzero vector $\vec{x}$ such that $A\vec{x} = \vec{0}$. Then $\sum x_i \vec{w}_i = (\vec{v}_1, \cdots, \vec{v}_r)A\vec{x} = \vec{0}$. This is a contradiction, since L is linearly independent, so $r \geq s$.

□

Definition 7.18

A **linear transformation** is a map

$$T : V \to W$$

such that

$$T(\vec{v}_1 + \vec{v}_2) = T(\vec{v}_1) + T(\vec{v}_2)$$

and

$$T(a\vec{v}) = aT(\vec{v}).$$

We say that T is an **isomorphism** if it is a bijection (T^{-1} is also an isomorphism).

For a vector space V over a field F and a set of vectors $S = \{\vec{v}_i \in V\}$, we can define the following linear transformation:

$$T_S : F^n \to V$$
$$(a_1, \cdots, a_n) \mapsto \sum a_i \vec{v}_i \in V.$$

If S is linearly independent, then T_S is injective; if $\text{Span}(S) = V$, then T_S is surjective, and if T_S is a basis, then T_S is an isomorphism.