Honours Algebra Notes

Leon Lee

March 21, 2024

Contents

1 Vector Spaces

1.1 Fields and Vector Spaces

Definition 1.1.1: Definition of a field

A **field** F is a set with functions

- Addition: $+ : F \times F \to F$, $(\lambda, \mu) \mapsto \lambda + \mu$
- Multiplication: $\cdot : F \times F$, $(\lambda, \mu) \mapsto \lambda\mu$

and two distinguished members 0_F, 1_F with $0_F \neq 1_F$ s.t. $(F, +)$ and $F \backslash \{0_F, \cdot\}$ are *abelian groups* whose neutral elements are 0_F and 1_F respectively, and which also satisifies

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu \in F$$

for any $\lambda, \mu, \nu \in F$. Additional Requirements: For all $\lambda, \mu \in F$,

- $\lambda + \mu = \mu + \lambda$
- $\lambda \cdot \mu = \mu \cdot \lambda$
- $\lambda + 0_F = \lambda$
- $\lambda \cdot 1_F = \lambda \in F$

For every $\lambda \in F$ there exists $-\lambda \in F$ such that

$$\lambda + (-\lambda) = 0_F \in F$$

For every $\lambda \neq 0 \in F$ there exists $\lambda^{-1} \neq 0 \in F$ such that

$$\lambda(\lambda^{-1}) = 1_F \in F$$

NOTE: This is a terrible definition of a field, just think of it as a group with two operations instead of one

Definition 1.1.2: Definition of a Vector Space

A **vector space** V **over a field** F is a pair consisting of an abelian group $V = (V, \dot{+})$ and a mapping

$$F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$$

such that for all $\lambda, \mu \in F$ and $\vec{v}, \vec{w} \in V$ the following identities hold:

$$\begin{aligned} \lambda(\vec{v}\dot{+}\vec{w}) &= (\lambda\vec{v})\dot{+}(\lambda\vec{w}) \\ (\lambda + \mu)\vec{v} &= (\lambda\vec{v})\dot{+}(\mu\vec{v}) \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1_F\vec{v} &= \vec{v} \end{aligned}$$

The first two laws are the **Distributive Laws**, the third law is called the **Associativity Law**. A vector field V over a field F is commonly called an F**-vector space**

1.1.3 Vector Space Terminology

- Elements of a vector space: **vectors**
- Elements of the field F: **scalars**
- The field F itself: **ground field**
- The map $(\lambda, \vec{v}) \mapsto \lambda\vec{v}$: **multiplication by scalars**, or the **action of the field F on V**

Notes:

- This is not the same as the "scalar product", as that produces a scalar from two vectors
- Let the zero element of the abelian group V be written as $\vec{0}$ and called the **zero vector**
- The use of $\dot{+}$ and 1_F is there for mostly pedantic rigorous reasons, and a much less confusing way of defining a vector field is defined below:

Definition 1.1.4: Alternative Vector Space definition

A **vector space V over a field F** is a pair consisting of an abelian group $V = (V, \dot{+})$ and a mapping

$$F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$$

such that for all $\lambda, \mu \in F$ and $\vec{v}, \vec{w} \in V$ the following identities hold:

$$\begin{aligned} \lambda(\vec{v}\dot{+}\vec{w}) &= \lambda\vec{v}\dot{+}\lambda\vec{w} \\ (\lambda + \mu)\vec{v} &= \lambda\vec{v}\dot{+}\mu\vec{v} \\ \lambda(\mu\vec{v}) &= (\lambda\mu)\vec{v} \\ 1\vec{v} &= \vec{v} \end{aligned}$$

1.1.5 Vector Space Lemmas

Product with the scalar zero: If V is a *vector space* and $\vec{v} \in V$, then $0\vec{v} = \vec{0}$, or in words "zero times a vector is the zero vector"
Product with the scalar (-1): If V is a *vector space* and $\vec{v} \in V$, then $(-1)\vec{v} = -\vec{v}$
Product with the zero vector: If V is a *vector space* over a field F, then $\lambda\vec{0} = \vec{0}$ for all $\lambda \in F$. Furthermore, if $\lambda\vec{v} = \vec{0}$ then either $\lambda = 0$ or @$\vec{v} = \vec{0}$

1.2 Product of Sets and of Vector Spaces

Definition 1.2.1: Cartesian Product of n sets

Trivially: $X \times Y = \{(x, y) : x \in X,\ y \in Y\}$
Just extend this to n numbers

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_i \in X_i \text{ for } 1 \leq i \leq n\}$$

The elements of a product are called **n-tuples**. An individual entry $x_i = (x_1, \ldots, x_n)$ is called a **component**.
There are special mappings called **projections** for a cartesian product:

$$\begin{aligned} \mathrm{pr}_i : X_1 \times \cdots \times X_n &\to X_i \\ (x_1, \ldots, x_n) &\mapsto x_i \end{aligned}$$

The cartesian product of n copies of a set X is written in short as: X^n

The elements of X^n are n-tuples of elements from X. In the special case $n = 0$ we use the general convention that X^0 is "the" one element set, so that for all $n, m \geq 0$, we then have the canonical bijection

$$\begin{aligned} X^n \times X^m &\to X^{n+m} \\ ((x_1, x_2, \ldots, x_n),\ (x_{n+1}, x_{n+2}, \ldots, x_{n+m})) &\mapsto (x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m}) \end{aligned}$$

Note: the $\to$ should have a tilde but idk how to typeset it like that
[Bunch of examples: check LN 1.3]

1.3 Vector Subspaces

Definition 1.3.1: Vector Subspace

A subset U of a vector space V is called a **vector subspace** or **subspace** if U contains the zero vector, and whenever $\vec{u}, \vec{v} \in U$ and $\lambda \in F$ we have $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$

Note There is a more generalized definition using concepts we haven't learned yet, it is as follows: Let F be a field. A subset of an F-vector space is called a vector subspace if it can be given the structure of an F-vector space such that the embedding is a "homomorphism of F-vector spaces". This definition is a lot more general since it also applies to subgroups, subfields, sub-"any structure", etc

Definition 1.3.2: Spanning Subspace

Let T be a subset of a vector space V over a field F. Then amongst all vector subspaces of V that include T there is a smallest vector subspace

$$\langle T \rangle = \langle T \rangle_F \subseteq V$$

It can be described as the set of all vectors $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ with $\alpha_1, \ldots, \alpha_r \in F$ and $\vec{v}_1, \ldots, \vec{v}_r \in T$, together with the zero vector in the case $T = \emptyset$

1.3.3 Subspace terminology

- An expression of the form $a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r$ is called a **linear combination** of vectors $\vec{v}_1, \ldots, \vec{v}_r$.
- The smallest vector subspace $\langle T\rangle \subseteq V$ containing T is called the **vector subspace generated by** T or the vector subspace **spanned by** T or even the **span of** T
- If we allow the zero vector to be the "empty linear combination of $r = 0$ vectors", which is what we will mean from hereon, then the span of T is exactly the set of all linear combinations of vectors from T

Definition Number: Generating Subspace

A subset of a vector space is called a **generating** or **spanning set** of our vector space if its span is all of the vector space. A vector space that has a finite generating set is said to be **finitely generated**.

1.4 Linear Independence and Bases

Definition 1.4.1: Linear Independence

A subset L of a vector space V is called **linearly independent** if for all pairwise different vectors $\vec{v}_1, \ldots, \vec{v}_r \in L$ and arbitrary scalars $\alpha, \ldots, \alpha_r \in F$,

$$a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r = \vec{0} \implies a_1 = \cdots = \alpha_r = 0$$

Definition 1.4.2: Linear Dependence

A subset L of a vector space V is called **ilnearly dependent** if it is not linearly independent (duh..). This means there exists pairwise different vectors $\vec{v}j_1, \ldots, \vec{v}_r \in L$ and scalars $\alpha_1, \ldots, \alpha_r \in F$, not all zero, such that $\alpha_1\vec{v}_1 + \cdots \alpha_r\vec{v}_r = \vec{0}$

Definition 1.4.3: Basis of a Vector Space

A **basis of a vector space** V is a linearly independent generating set in V

1.4.4 Family notation

Let A and I be sets. We will refer to a mapping $I \to A$ as a **family of elements of** A **indexed by** I and use the notation

$$(a_i)i \in I$$

This is used mainly when I plays a secondary role to A. In the case $I = \emptyset$, we will talk about the **empty family** of elements of A.
Random facts:

- The family $(\vec{v}_i)_{i\in I}$ would be called a generating set if the set $\{\vec{v}_i : i \in I\}$ is a generating set.
- It would be called **linearly independent** or a **linearly independent family** if, for pairwise distinct indices $i(1), \ldots, i(r) \in I$ and arbitrary scalars $a_1, \ldots, a_r \in F$,

$$a_1\vec{v}_{i(1)} + \cdots + a_r\vec{v}_{i(r)} = \vec{0} \to \alpha_1 = \cdots = a_r = 0$$

A difference between families and subsets is that the same vector can be represented by different indices in a family, in which case linear independence as a family is not possible. A family of vectors that is not linearly independent is called a **linearly dependent family**. A family of vectors that is a generating set and linearly independent is called either a **basis** or a **basis indexed by** $i \in I$

Example 1.4.5: Standard Basis

Let F be a field and $n \in \mathbb{N}$. We consider the following vectors in F^n

$$\vec{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$$

with one 1 in the i-th place and zero everywhere else. Then $\vec{e}_1, \dots, \vec{e}_n$ form an ordered basis of F^n, the so-called **standard basis of** F^n

Theorem 1.4.6: Linear combinations of basis elements

Let F be a field, V a vector space over F and $\vec{v}_1, \dots, \vec{v}_r \in V$ vectors. The family $(\vec{v}_i)_{1 \leq i \leq r}$ is a basis of V if and only if the following "evaluation" mapping

$$\begin{aligned} \psi : F^r &\to V \\ (\alpha_1, \dots, a_r) &\mapsto a_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r \end{aligned}$$

is a bijection
If we label our ordered family by $\mathcal{A} = (\vec{v}_1, \dots, \vec{v}_r)$, then we done the above mapping by

$$\psi = \psi_{\mathcal{A}} : F^r \to V$$

2 Rings

I can't be bothered doing changes of basis and stuff, time for something more interesting :D

2.1 Ring basics

Definition 2.1.1: Definition of a Ring

A **ring** is a set with two operations $(\mathbb{R}, +, \cdot)$ that satisfy:

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is a **monoid** - this means that the second operation $\cdot : R \times R \to R$ is associative and that there is an **identity element** $1 = 1_R \in R$, often just called the identity, with the property that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
3. The distributive laws hold, meaning that for all $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c))$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

The two operations are called **addition** and **multiplication** in our ring. A ring in which multiplication, that is $a \cdot b = b \cdot a$ for all $a, b \in R$, is a **commutative ring**

Note: We'll call the element $1 \in R$ as the identity element of the monoid $(R, \cdot)$, and we call the additive identity of $(R, +)$ zero, written as 0_R or 0

Example: We can define the **null ring** or **zero ring** as a ring where R is a single ement set, e.g. $\{0\}$, with the operations $0 + 0 = 0$ and $0 \times 0 = 0$. We will call any ring that isn't the zero ring a **non-zero ring**

Example 2.1.2: Modulo Rings

Let $m \in \mathbb{Z}$ be an integer. Then the set of **integers modulo** m, written

$$\mathbb{Z}/m\mathbb{Z}$$

is a ring. The elements of $\mathbb{Z}/m\mathbb{Z}$ consist of **congruence classes** of integers modulo m - that is the elements are the subsets T of $\mathbb{Z}$ of the form $T = a + m\mathbb{Z}$ with $a \in \mathbb{Z}$. Think of these as the set of integers that have the same remainder when you divide them by m. I denote the above congruence class by $\overline{a}$. Obviously $\overline{a} = \overline{b}$ is the same as $a - b \in m\mathbb{Z}$, and often I'll write

$$a \equiv b \mod m$$

If $m \in \mathbb{N}_{\geq 0}$ then there are m congruence classes modulo m, in other words, $|\mathbb{Z}/m\mathbb{Z}| = m$, and I could write out the set as

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

To define addition and multiplication, set

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

Distributivity for $\mathbb{Z}/m\mathbb{Z}$ then follows from distributivity for $\mathbb{Z}$.

2.2 Linking Rings to Fields and Further Properties

Definition 2.2.1: Ring definition of a field

A **field** is a non-zero commutative ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$, that is an element a^{-1} with the property that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Example: The ring $\mathbb{Z}/3\mathbb{Z}$ is a field, which we have been calling $\mathbb{F}_3$. The ring $\mathbb{Z}/12\mathbb{Z}$ is not a field, because neither $\overline{3}$ or $\overline{8}$ are invertible, since $\overline{3} \cdot \overline{8} = \overline{0}$.

Theorem 2.2.2: Prime property of fields

Let m be a positive integer. The commutative ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

Theorem 2.2.3: Lemmas for multiplying by zero and negatives

Let R be a ring and let $a, b \in R$. Then

1. $0a = 0 = a0$
2. $(-a)b = -(ab) = a(-b)$
3. $(-a)(-b) = ab$

Note: The distributive axiom for rings has familiar properties such as

$$(a+b)(c+d) = ac + ad + bc + bd$$
$$a(b-c) = ab - ac$$

But remember that multiplication is not always commutative, so multiplicative factors must be kept in the correct order - ac may not equal ca

---

Suppose we have a ring R such that $1_R = 0_R$, then R must be the zero ring. 3.2.2 in notes for proof

Definition 2.2.4: Multiples of an abelian group

Let $m \in \mathbb{Z}$. The m**-th multiple** ma **of an element** $a$in an abelian group R is:

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ terms}} \quad \text{if} m > 0$$

$0a = 0$ and negative multiples are defined by $(-m)a = -(ma)$

Theorem 2.2.5: Lemmas for multiples

Let R be a ring, let $a, b \in R$ and let $m, n \in \mathbb{Z}$. Then:

1. $m(a+b) = ma + mb$
2. $(m+n)a = ma + na$
3. $m(na) = (mn)a$
4. $m(ab) = (ma)b = a(mb)$
5. $(ma)(nb) = (mn)(ab)$

Proof. (in the lecturer's words) This is trivial and boring, so I will leave the details up to you. $\square$

Definition 2.2.6: Unit of a ring

Let R be a ring. An element $a \in R$ is called a **unit** if it is *invertible* in R or in other words *has a multiplicative inverse in* R, meaning that there exists $a^{-1} \in R$ such that

$$aa^{-1} = 1 = a^{-1}a$$

Example: In a field, such as $\mathbb{R}, \mathbb{R}, \mathbb{C}$, every non-zero element is a unit. In $\mathbb{Z}$, only 1 and -1 are units

Theorem 2.2.7: The subset of units in a ring forms a group

The set $R^\times$ of units in a ring R forms a group under multiplication

I will call $R^\times$ the **group of units of the ring** R

Definition 2.2.8: zero-divisors of a ring

In a ring R, a non-zero element a is called a **zero-divisor** or **divisor of zero** if there exists a non-zero element b such that either $ab = 0$ or $ba = 0$.

Example: In $\mathrm{Mat}(2; \mathbb{R})$,

$$\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

So, both $\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ are zero-divisors

Definition 2.2.9: Integral Domain

An **integral domain** is a non-zero commutative ring that has no zero-divisors.
In an integral domain there are no zero-divisors and therefore the following laws will hold:

1. $ab = 0 \implies a = 0$ or $b = 0$, and
2. $a \neq 0$ and $b \neq 0 \implies ab \neq 0$

Example: $\mathbb{Z}$ is an integral domain. Any field is an integral domain, since a unit in a ring R cannot be a zero-divisor. To see this, let R be a non-zero ring and let $a \in R^\times$ be a unit. Suppose that $ab = 0$ or $ba = 0$ for some $b \in R$. Multiplying on the left or on the right respectively by a^{-1} shows that $a^{-1}ab = a^{-1}0$ or $baa^{-1} = 0a^{-1}$, so in both cases, $b = 0$

Theorem 2.2.10: Cancellation Law for Integral Domains

Let R be an *integral domain* and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$

We will now reprove 2.2.2 as a special case of a general theorem

Theorem 2.2.11: Prime Property for Integral Domains

Let m be a natural number. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.

Theorem 2.2.12: Finite Integral Domains are Fields

Every **finite** integral domain is a field.

2.3 Polynomials