Heads up on Advanced Linear Algebra

Optional, Time permitting

Satya Mandal
University of Kansas, Lawrence, Kansas 66045, USA

22 November 2024

Contents

Appendix A

Advanced Linear Algebra

A.1 Groups

Definition A.1.1. A nonempty set G with a binary operation

$$o : G \times G \longrightarrow G \quad \textit{sending} \quad (x, y) \mapsto xoy \ \ (\textit{or simply } xy)$$

is called a **group**, if the following conditions are satisfied:

1. (**Associativity:**) $\forall x, y, z \in G$ we have $(xy)z = x(yz)$
2. (**Identity:**) There is an element $\mathfrak{e} \in G$ such that $\mathfrak{e}x = x\mathfrak{e} = x \ \forall x \in G$.
3. (**Inverse:**) Given $x \in G$ there is an element $y \in G$ such that $xy = yx = \mathfrak{e}$.

Further, a group G is called a **commutative group**, if

$$xy = yx \qquad \forall x, y \in G$$

A commutative group is also called an **Abelian group** (after the name of Niels Henrik Abel). **Notations:** *The notation xy is called the multiplicative notation. Additive notation $x + y$ is also used, more often in the case of commutative groups. Other notations are also used, depending on the context.*

In the multiplicative notation, it is more customary to denote identity by $\mathfrak{e} = 1$. In the additive notation, it is more customary to denote identity by $\mathfrak{e} = 0$ (zero). However, all these depend on the context, textbook and the instructors.

Example A.1.2. Let $\mathbb{Z}$ be the set of integers. Then $\mathbb{Z}$ is a group under addition $+$.

Example A.1.3. Let $n \geq 1$ be an integers. Let $GL_n(\mathbb{R})$ be the set of all invertible matrices A of order n. Then we $GL_n(\mathbb{R})$ is a group under multiplication.

Example A.1.4. Let V be a vector space and $GL(V)$ be the set of all isomorphisms $\varphi : V \xrightarrow{\sim} V$. Then $GL(V)$ is a group under composition.

Example A.1.5. Let $X \subseteq \mathbb{R}^n$ be a subset of $\mathbb{R}^n$. Let $C(X)$ be the set of all real valued continuous functions $f : X \longrightarrow \mathbb{R}$. For $f, g \in C(X)$ define $f + g \in C(X)$, as follows

$$(f+g)(x) = f(x) + g(x) \qquad \forall x \in X$$

Then $C(X)$ is a commutative group under this addition.

Example A.1.6. Let $n \geq 1$ be an integers. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. For $x, y \in \mathbb{Z}_n$ define addition

$$x + y = \begin{cases} x + y & if\ x + y \leq n - 1 \\ x + y - n & if\ x + y \geq n \end{cases}$$

Then $\mathbb{Z}_n$ is a commutative group under this addition. This addition is called "*residue modulo n addition*". (*Ideally, we should use two different notations for + on two sides of the above equation.*)

Exercise A.1.7. Let G be a group. Prove that the identity $\mathfrak{e}$ is the definition is unique. In other words, if $\mathfrak{e}, e \in G$ are such that

$$\begin{cases} \mathfrak{e}x = x\mathfrak{e} & \forall x \in G \\ ex = xe & \forall x \in G \end{cases} \qquad Then \quad \mathfrak{e} = e.$$

Exercise A.1.8. Let G be a group. Let $x \in G$. Then x the inverse of x is unique. In other words, if $y_1, y_2 \in G$ such that

$$\begin{cases} y_1 x = x y_1 = \mathfrak{e} \\ y_2 x = x y_2 = \mathfrak{e} \end{cases} \qquad Then \quad y_1 = y_2.$$

In multiplicative notation, this unique inverse y is denoted by x^{-1}.
In Additive notation, this unique inverse y is denoted by $-x$.

A.2 Fields

In the context of Linear algebra, we are more interested in fields. The set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$, are the model of a field.

Definition A.2.1. Let $\mathbb{F}$ be a nonempty set, with two binary operations, to be called addition and multiplication:

$$\begin{cases} + : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} & (x, y) \mapsto x + y \\ \cdot : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} & (x, y) \mapsto xy \end{cases}$$

For $x, y \in \mathbb{F}$ the addition will be denoted by $x + y$ and multiplication will be denoted by xy or $x \cdot y$. We say that $\mathbb{F}$ is a **field**, if the addition and multiplication satisfy the following properties:

1. $(\mathbb{F}, +)$ is a commutative group. (*Zero* 0 *will denote the additive identiy. For* $x \in \mathbb{F}$, $-x$ *will denote the additive inverse.*)

2. Let $\mathbb{F}^\star = \{x \in \mathbb{F} : x \neq 0\}$. Then $(\mathbb{F}^\star, \cdot)$ a commutative group. The multiplicative identity is denoted by $1 \in \mathbb{F}^\star$. For any $x \in \mathbb{F}$, with $x \neq 0$, the multiplicative inverse is denoted by x^{-1} of $\frac{1}{x}$.

3. (**Distributive:**) Further,

$$\forall x, y, z \in \mathbb{F} \qquad x(y + z) = xy + xz$$

More verbosely, without using the concept of Groups, most textbooks define a field (equivalently), as follows. We write it as a lemma:

Lemma A.2.2. Let $\mathbb{F}$ be a set with two binary operations $+$ and $\cdot$:

$$\begin{cases} + : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} & (x, y) \mapsto x + y \\ \cdot : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} & (x, y) \mapsto xy \end{cases}$$

Then $\mathbb{F}$, together with these two operations, is a field if and only if, the following properties are satisfied:

1. The additive properties:

   (a) (**Associativity of +:**) $\forall x, y, z \in \mathbb{F}$ we have

   $$(x + y) + z = x + (y + z)$$

   (b) (**Additive Identity:**) There is an element $0 \in \mathbb{F}$ such that

   $$0 + x = x + 0 = x \ \forall x \in \mathbb{F}$$

(c) (**Additive Inverse:**) Given $x \in \mathbb{F}$ there is an element $y \in \mathbb{F}$ such that

$$x + y = y + x = 0$$

(d) (**Additive Commutativity:**)

$$\forall x, y \in \mathbb{F} \qquad x + y = y + x$$

(*For* $x \in \mathbb{F}$, $-x$ *will denote the additive inverse.*)

2. Multiplicative properties:

(a) (**Associativity of ·:**) $\forall x, y, z \in \mathbb{F}$ we have

$$(xy)z = x(yz)$$

(b) (**Additive Identity:**) There is an element $1 \in \mathbb{F}$ such that

$$1 \cdot x = x \cdot 1 = x \ \forall x \in \mathbb{F}$$

(c) (**Multiplicative Inverse:**) Given $x \in \mathbb{F}$, with $x \neq 0$ there is an element $y \in \mathbb{F}$ such that

$$xy = yx = 1$$

This inverse y is denoted by x^{-1} or $\frac{1}{x}$.

(d) (**Multiplicative Commutativity:**)

$$\forall x, y \in \mathbb{F} \qquad xy = yx$$

3. (**Distributive:**) Further,

$$\forall x, y, z \in \mathbb{F} \qquad x(y + z) = xy + xz$$

Example A.2.3. Let

$$\begin{cases} \mathbb{R} = set\ of\ all\ real\ numbers \\ \mathbb{C} = set\ of\ all\ complex\ numbers \\ \mathbb{Q} = set\ of\ all\ rational\ numbers \\ \mathbb{I} = set\ of\ all\ irrational\ numbers \\ \mathbb{Z} = set\ of\ all\ integers \end{cases}$$

Then $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ are fields. But $\mathbb{Z}$ is not a field; nor is $\mathbb{I}$.

Example A.2.4. Let $p \geq 2$ be a prime number and

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}.$$

For $x, y \in \mathbb{Z}_p$, by division algorithm, we have

$$\begin{cases} x + y = pn_a + r_a & 0 \leq r_a \leq p-1, n_a \text{ integer} \\ xy = pn_m + r_m & 0 \leq r_m \leq p-1, n_m \text{ integer} \end{cases}$$

Define a (new) addition and multiplication on $\mathbb{Z}_p$ as follows:

$$x + y := r_a \qquad\qquad xy := r_m$$

(*Ideally, we should use a different notation for + and xy. These are called addition and multiplication modulo p.*)
Then, $\mathbb{Z}_p$ is a field under this addition and multiplication.

A.2.1 Vector spaces over fields $\mathbb{F}$

Recall that the set of real numbers $\mathbb{R}$, is a filed (under addition + and multiplication $\cdot$). In this course (Math 290/291) we discussed Vectors spaces over the field of real numbers $\mathbb{R}$. We can define vectors spaces over any field $\mathbb{F}$. So, we can talk about vector spaces over $\mathbb{C}$, over $\mathbb{Q}$, over $\mathbb{Z}_p$ and any other field. For completeness, I define vector spaces over any given field $\mathbb{F}$. (*The definition will be same as the vectors spaces over $\mathbb{R}$, by replacing $\mathbb{R}$ by $\mathbb{F}$.*)

Definition A.2.5. Let $\mathbb{F}$ be a field. Suppose V is a non empty, with a two operations (vector addition and scalar multiplication):

$$\begin{cases} + : V \times V \longrightarrow V & (\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} + \mathbf{v} & \textit{vector addition} \\ \cdot : \mathbb{F} \times V \longrightarrow V & (c, \mathbf{v}) \mapsto c\mathbf{v} & \textit{scalar multiplication} \end{cases} \tag{A.1}$$

(*So, we are dealing with two additions, one addition + on $\mathbb{F}$, one vector addition + on V. Further, there is a multiplication/product on $\mathbb{F}$ and a scalar multiplication on V. Any element $c \in \mathbb{F}$ will be called a* **scalar**.)

We say V is a vector space over $\mathbb{F}$, if the following holds:

1. The equation (A.1) can be alternately restated as: V is closed under addition and scalar multiplication.

2. Additive properties of V:

(a) (**Associativity:**) For $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, we have

$$(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$$

(b) (**Additive identity:**) There is an element $\mathbf{0} \in V$ such that

$$\forall\ \mathbf{u} \in V \qquad \mathbf{0}+\mathbf{u}=\mathbf{u}$$

(c) (**Additive Inverse:**) Given any element $\mathbf{u} \in V$ there is an element $\mathbf{y} \in V$ such that

$$\mathbf{u}+\mathbf{y}=\mathbf{0}$$

(d) (**Commutativity:**)

$$\forall\ \mathbf{u}, \mathbf{v} \in V \qquad \mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$$

3. Scalar multiplication properties:

$$\begin{cases} c\,(\mathbf{u}+\mathbf{v})=c\mathbf{u}+c\mathbf{v} & \forall c \in \mathbb{F}; \forall \mathbf{u}, \mathbf{v} \in V & \textbf{Distributivity} \\ (c+d)\mathbf{u}=c\mathbf{u}+d\mathbf{u} & \forall c, d \in \mathbb{F}; \forall \mathbf{u} \in V & \textbf{Distributivity} \\ (cd)\mathbf{u}=c\,(d\mathbf{u}) & \forall c, d \in \mathbb{F}; \forall \mathbf{u} \in V & \textbf{Associativity} \\ 1 \cdot \mathbf{u}=\mathbf{u} & \forall \mathbf{u} \in V & \textbf{scalar Identity} \end{cases}$$

Exercise A.2.6. Let $\mathbb{F}$ be a field and V be a nonempty set with a addition $+$ and a scaler multiplication, as in (A.1). The V is a vector space over $\mathbb{F}$ if and only if

1. V is a commutative group under vector addition $+$.

2. Scalar multiplication properties:

$$\begin{cases} c\,(\mathbf{u}+\mathbf{v})=c\mathbf{u}+c\mathbf{v} & \forall c \in \mathbb{F}; \forall \mathbf{u}, \mathbf{v} \in V & \textbf{Distributivity} \\ (c+d)\mathbf{u}=c\mathbf{u}+d\mathbf{u} & \forall c, d \in \mathbb{F}; \forall \mathbf{u} \in V & \textbf{Distributivity} \\ (cd)\mathbf{u}=c\,(d\mathbf{u}) & \forall c, d \in \mathbb{F}; \forall \mathbf{u} \in V & \textbf{Associativity} \\ 1 \cdot \mathbf{u}=\mathbf{u} & \forall \mathbf{u} \in V & \textbf{scalar Identity} \end{cases}$$

Remark A.2.7. We extend most of what I did in Math 290/291 as follows:

1. Barring the chapter on Inner product spaces, almost everything I said about vector spaces over $\mathbb{R}$, works for vector spaces over any field $\mathbb{F}$. This includes vector spaces over $\mathbb{C}$.

2. Almost anything I said about Matrices, with real entries, works for matrices with entries in a field $\mathbb{F}$. Let $\mathbb{M}_{m\times n}(\mathbb{F})$ denote the set of all matrices with entries in $\mathbb{F}$. For square matrices $A \in \mathbb{M}_{n\times n}(\mathbb{F})$, we define determinant $|A|$ in the same way. We can define adjoint $Adj(A)$ in the same way. It follows, in the same way

$$A\left(Adj(A)\right) = \left(Adj(A)\right)A = |A|I_n$$

If $|A| \neq 0$ then the inverse

$$A^{-1} = \frac{1}{|A|}\left(Adj(A)\right)$$

3. The idea of inner product does not extend, because $\mathbb{R}$ has a order relationship $a \leq b$, while that is absent in other fields $\mathbb{F}$. We can talk about length of vector in a meaningful way, for vectors over $\mathbb{R}$.

   While the idea of vector spaces works for vector spaces over $\mathbb{C}$, the definitions need to be fine tuned a little.

Example A.2.8. Here are some examples.

1. Let $\mathbb{F}$ be a field. Then $\mathbb{F}^n$ is a vector space over $\mathbb{F}$.

2. $\mathbb{F}$ be a field. Let X be an indeterminate (symbol). For integers $n \geq 1$ let X^n is also a symbol, Let

$$\mathbb{F}[X] = \left\{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n : a_i \in \mathbb{F}, n \geq 0\right\}$$

   (*We say* $\mathbb{F}[X]$ *is the set of all polynomials over* $\mathbb{F}$.)
   Then $\mathbb{F}[X]$ is a vector space over $\mathbb{F}$.

3. Here are some more:

   (a) $\mathbb{C}$ is vector space over $\mathbb{Q}$.

   (b) $\mathbb{C}$ is vector space over $\mathbb{R}$.

   (c) $\mathbb{R}$ is vector space over $\mathbb{Q}$.

A.2.2 Division Algebra and Quaternions

In a field $\mathbb{F}$ product is commutative $xy = yx$. By relaxing the definition of field, by removing the condition on commutativity $xy = yx$, we obtain the definition of Devision Algebra, as follows.

Definition A.2.9. Let $\mathbb{D}$ be a nonempty set, with two binary operations, to be called addition and multiplication:

$$\begin{cases} + : \mathbb{D} \times \mathbb{D} \longrightarrow \mathbb{D} & (x, y) \mapsto x + y \\ \cdot : \mathbb{D} \times \mathbb{D} \longrightarrow \mathbb{D} & (x, y) \mapsto xy \end{cases}$$

For $x, y \in \mathbb{D}$ the addition will be denoted by $x+y$ and multiplication will be denoted by xy or $x \cdot y$. We say that $\mathbb{D}$ is a **Division Algebra**, if the addition and multiplication satisfy the following properties:

1. $(\mathbb{D}, +)$ is a commutative group. (*Zero* 0 *will denote the additive identiy. For* $x \in \mathbb{F}$, $-x$ *will denote the additive inverse.*)

2. Let $\mathbb{D}^\star = \{x \in \mathbb{D} : x \neq 0\}$. Then $(\mathbb{D}^\star, \cdot)$ a group (*not necessarily commutative*). The multiplicative identity is denoted by $1 \in \mathbb{D}^\star$. For any $x \in \mathbb{D}$, with $x \neq 0$, the multiplicative inverse is denoted by x^{-1} of $\frac{1}{x}$.

3. (**Distributive:**) Further,

$$\forall x, y, z \in \mathbb{F} \qquad \begin{cases} x(y+z) = xy + xz \\ (x+y)z = xz + yz \end{cases}$$

The most important example of Division algebra is the **Quaternion Algebra**, defined as follows.

Definition A.2.10. Let $\mathcal{Q} = \mathbb{R}^4$. Write

$$\begin{cases} \mathbb{1} = (1,0,0,0) \\ i = (0,1,0,0) \\ j = (0,0,1,0) \\ k = (0,0,0,1) \end{cases} \qquad \textit{They form a basis of } \mathcal{Q}$$

Given $\mathbf{x} = (x_1, x_2, x_3, x_4) \in \mathcal{Q}$, we can write

$$\mathbf{x} = x_1\mathbb{1} + x_2 i + x_3 j + x_4 k \quad \textit{Likewise, let} \quad \mathbf{y} = y_1\mathbb{1} + y_2 i + y_3 j + y_4 k$$

Usually, $\mathbb{1}$ is omitted and we write $1 = \mathbb{1}$ and i, j, k are treated as symbols. So, one writes

$$\mathbf{x} = x_1 + x_2 i + x_3 j + x_4 k \qquad \textit{Likewise} \quad \mathbf{y} = y_1 + y_2 i + y_3 j + y_4 k$$

Define

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1) + (x_2 + y_2)i + (x_3 + y_3)j + (x_4 + y_4)k$$

This addition is same as sum is $\mathcal{Q} = \mathbb{R}^4$.

A product is defined by the following multiplication table:

	$\mathbb{1}$	i	j	k
$\mathbb{1}$	$\mathbb{1}$	i	j	k
i	i	$-\mathbb{1}$	k	$-j$
j	j	$-k$	$-\mathbb{1}$	i
k	k	j	$-i$	$-\mathbb{1}$

So, for $\mathbf{x}, \mathbf{y} \in \mathcal{Q}$, as above

$$\mathbf{x} \cdot \mathbf{y} = \begin{cases} (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4) + \\ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)i + \\ (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)j + \\ (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)k \end{cases}$$

Note, the product is not commutative $ij \neq ji$. Then $\mathcal{Q}$ is a Division Algebra.

$$\mathbf{x}^{-1} = (x_1 + x_2i + x_3j + x_4k)^{-1} = \frac{x_1 - x_2i - x_3j - x_4k}{x_1^2 + x_2^2 + x_3^2 + x_4^2}$$

Thuis $\mathcal{Q}$ is known as the **Quaternion Algebra**.

Appendix B

Rings and Modules

Rings are extension of the idea of Division algebras or fields. The modules are similar to vectors spaces over rings.

B.1 Rings

Definition B.1.1. Let R be a nonempty set, with two binary operations, to be called addition and multiplication:

$$\begin{cases} + : R \times R \longrightarrow R & (x, y) \mapsto x + y \\ \cdot : R \times R \longrightarrow R & (x, y) \mapsto xy \end{cases}$$

For $x, y \in R$ the addition will be denoted by $x + y$ and multiplication will be denoted by xy or $x \cdot y$. We say that R is a **Ring**, if the addition and multiplication satisfy the following properties:

1. $(R, +)$ is a commutative group.
   (*Zero* 0 *will denote the additive identiy. For* $x \in R$, $-x$ *will denote the additive inverse.*)
2. (**Multiplicative Associativity:**)
   $$\forall x, y, z \in R \qquad (xy)z = x(yz)$$
3. (**Distributive:**)
   $$\forall x, y, z \in R \qquad \begin{cases} x(y + z) = xy + xz \\ (x + y)z = xz + yz \end{cases}$$

4. There is a multiplicative identity, denoted by $1 \in R$, such that

$$0 \neq 1 \qquad \forall x \in R \qquad x \cdot 1 = 1 \cdot x = x$$

Definition B.1.2. Suppose R is a ring, and $x \in R$. We say, x has an inverse, if there in an element $y \in R$ such that $xy = yx = 1$.

Exercise B.1.3. Suppose R is a ring.

1. Let $x \in R$. If x has an inverse, then the inverse is unique. The inverse is denoted by x^{-1} or $\frac{1}{x}$.

2. Let $x \in R$ then $0 \cdot x = 0$ and $x \cdot 0 = 0$.

3. Prove 0 does not have a multiplicative inverse.

Example B.1.4. Every Division Algebra is a ring.

As in the definition of Fields, more verbosely, without using the concept of Groups, most textbooks define a ring (equivalently), as follows. We write it as a lemma:

Lemma B.1.5. Let R be a non empty set with two binary operations $+$ and $\cdot$:

$$\begin{cases} + : R \times R \longrightarrow R & (x, y) \mapsto x + y \\ \cdot : R \times R \longrightarrow R & (x, y) \mapsto xy \end{cases}$$

Then R, together with these two operations, is a field if and only if, the following properties are satisfied:

1. The additive properties:

   (a) (**Associativity of +:**) $\forall x, y, z \in R$ we have

   $$(x + y) + z = x + (y + z)$$

   (b) (**Additive Identity:**) There is an element $0 \in R$ such that

   $$0 + x = x + 0 = x \ \forall x \in R$$

   (c) (**Additive Inverse:**) Given $x \in R$ there is an element $y \in R$ such that

   $$x + y = y + x = 0$$

(d) (**Additive Commutativity:**)

$$\forall x, y \in R \qquad x + y = y + x$$

(*For $x \in R$, $-x$ will denote the additive inverse.*)

2. Multiplicative properties:

(a) (**Associativity of $\cdot$:**) $\forall x, y, z \in R$ we have

$$(xy)z = x(yz)$$

(b) (**Additive Identity:**) There is an element $1 \in R$ such that

$$0 \neq 1 \qquad and \qquad 1 \cdot x = x \cdot 1 = x \ \forall x \in R$$

3. (**Distributive:**) Further,

$$\forall x, y, z \in R \qquad \begin{cases} x(y+z) = xy + xz \\ (x+y)z = xz + yz \end{cases}$$

Remark B.1.6. Suppose R is a ring. Note that not all non zero $x \in R$ has an inverse. But if x has an inverse, then it is unique and is denoted by x^1 or $\frac{1}{x}$. Ans invertible elements $x \in R$, are called units of R.

Remark B.1.7. Let R be a ring. Let $U(R) = \{x \in R : x \text{ is invertible.}\}$. Prove $U(R)$ is a group, under multiplication.

Example B.1.8. Let $n \geq 1$ be an integer. Let $R = \mathbb{M}_{n \times n}(\mathbb{R})$. Then R is a ring.

Definition B.1.9. Let R be a ring. We say R is a commutative ring is the multiplication is commutative. This means

$$xy = yx \qquad \forall x, y \in R.$$

Note, $R = \mathbb{M}_{n \times n}(R)$ is not commutative.

Example B.1.10. The set of integers $\mathbb{Z}$ is a commutative ring, under usual addition $+$ and multiplication. Note $U(\mathbb{Z}) = \{-1, 1\}$.

I believe, motivation to define rings, came from the examples, similar to the following.

Example B.1.11. Let $[0,1]$ denote the unit interval. Let $R = C([0,1])$ denote the set of continuous function $f : [0,1] \longrightarrow \mathbb{R}$. Notionally,

$$R = \{f : [0,1] \longrightarrow \mathbb{R} : f \textit{ is continuous}\}$$

For $f, g \in R$ define addition and multiplication

$$\begin{cases} (f+g)(t) = f(t) + g(t) & t \in [0,1] \\ (fg)(t) = f(t)g(t) & t \in [0,1] \end{cases}$$

Then R is commutative ring. Resolve the following questions:

1. What is the additive zero of R.

2. What is the multiplicative identity of R.

3. Given $f \in R$, give a conditions when f has multiplicative inverse. Further, describe, f^{-1}, when exists.

4. Given as subset $X \subseteq \mathbb{R}^n$, we can define $R = C(X)$, as above. Convince yourself!

Exercise B.1.12. Let $\mathbb{F}$ be a field and $\mathbb{F}[X]$ be the set of all polynomials, with coefficients in $\mathbb{F}$ (see example A.2.8). Addition was defined in (A.2.8). Define multiplication on $\mathbb{F}[X]$. Prove $F[X]$ is a ring. Resolve the following:

1. What is the additive zero of $\mathbb{F}[X]$.

2. What is the multiplicative identity of $\mathbb{F}[X]$.

3. Describe the units $U(\mathbb{F}[X])$ of $\mathbb{F}[X]$.

B.2 Modules

A module M over a ring R, extends the idea vector spaces over a field. In order to avoid defining right-modules and left-modules, I will assume R is a commutative ring, in the section. We imitate (*literal copy and paste*) the definition of vector spaces.

Definition B.2.1. Suppose R is a commutative ring. Suppose M is a non empty set, with two operations (vector addition and scalar multiplication):

$$\begin{cases} + : M \times M \longrightarrow M & (\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} + \mathbf{v} & \textit{vector addition} \\ \cdot : R \times M \longrightarrow M & (c, \mathbf{v}) \mapsto c\mathbf{v} & \textit{scalar multiplication} \end{cases} \tag{B.1}$$

(*So, we are dealing with two additions, one addition* $+$ *on* R*, one vector addition* $+$ *on* M*. Further, there is a multiplication/product on* R *and a scalar multiplication on* M*.*)

We say M is a module over R, if the following holds:

1. The equation (B.1) can be alternately restated as: M is closed under addition and scalar multiplication.
2. Additive properties of M:
   (a) (**Associativity:**) For $\mathbf{u}, \mathbf{v}, \mathbf{w} \in M$, we have
   $$(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$$
   (b) (**Additive identity:**) There is an element $\mathbf{0} \in M$ such that
   $$\forall\ \mathbf{u} \in M \qquad \mathbf{0} + \mathbf{u} = \mathbf{u}$$
   (c) (**Additive Inverse:**) Given any element $\mathbf{u} \in M$ there is an element $\mathbf{y} \in M$ such that
   $$\mathbf{u} + \mathbf{y} = \mathbf{0}$$
   (*This* $\mathbf{y}$ *is unique and is denoted by* $-\mathbf{u}$.)
   (d) (**Commutativity:**)
   $$\forall\ \mathbf{u}, \mathbf{v} \in M \qquad \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$$
3. Scalar multiplication properties:

$$\begin{cases} c\,(\mathbf{u} + \mathbf{v}) = c\mathbf{u} + c\mathbf{v} & \forall c \in R; \forall \mathbf{u}, \mathbf{v} \in M \quad \textbf{Distributivity} \\ (c + d)\mathbf{u} = c\mathbf{u} + d\mathbf{u} & \forall c, d \in R; \forall \mathbf{u} \in M \quad \textbf{Distributivity} \\ (cd)\mathbf{u} = c\,(d\mathbf{u}) & \forall c, d \in R; \forall \mathbf{u} \in M \quad \textbf{Associativity} \\ 1 \cdot \mathbf{u} = \mathbf{u} & \forall \mathbf{u} \in M \quad \textbf{scalar Identity} \end{cases}$$

A module M *over* R *is also called an R-module.*

Exercise B.2.2. Let R be a commutative ring and M be a nonempty set with a addition $+$ and a scaler multiplication, as in (B.1). Then M is a module over R if and only if

1. M is a commutative group under vector addition $+$.

2. Scalar multiplication properties:

$$\begin{cases} c(\mathbf{u}+\mathbf{v}) = c\mathbf{u}+c\mathbf{v} & \forall c \in R; \forall \mathbf{u}, \mathbf{v} \in M & \textbf{Distributivity} \\ (c+d)\mathbf{u} = c\mathbf{u}+d\mathbf{u} & \forall c, d \in R; \forall \mathbf{u} \in M & \textbf{Distributivity} \\ (cd)\mathbf{u} = c(d\mathbf{u}) & \forall c, d \in R; \forall \mathbf{u} \in M & \textbf{Associativity} \\ 1 \cdot \mathbf{u} = \mathbf{u} & \forall \mathbf{u} \in M & \textbf{scalar Identity} \end{cases}$$

Remark B.2.3. I have tacitly continued with the terminologies of vector spaces. However, terminologies change a little, which you need to worry at this point.

The elements $c \in R$ are thought of as functions; not so much as a scalars.

Remark B.2.4. Let R be a commutative ring. Since there are non-zero non-units $x \neq 0$, in R, unlike in a field, a lot of vector space like properties fail for modules M over R. (*This gives us a lot of opportunity for research.*) We list a few:

1. Let M be an R-module. Then M need not have a basis.

2. If M has a basis, we say that M is a **Free** R-module.

3. (**Example:**) For any commutative ring R, easiest example of an R-module is $M = R^n$. Actually, $M = R^n$ is a free module.

4. (**Example:**) The set of real numbers $\mathbb{R}$ is a $\mathbb{Z}$-module.
   The set of complex numbers $\mathbb{C}$ is a $\mathbb{Z}$-module.

B.3 Polynomial rings

Unless we know more rings, we would not know better examples of modules. So, we define polynomial rings over commutative rings.

Definition B.3.1. Suppose R is a commutative ring. Let $\{X^n : n = 1, 2, \ldots\}$ be set of symbols. We write $X^1 = X$ and $X^0 = 1$.

1. A polynomial $f(X)$ with coefficients in R is a formal finite linear combination:

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \qquad \ni \qquad a_i \in R \;\; \forall \;\; i = 0, 1, \ldots, n$$

It is possible some $a_i = 0$. If some the a_iX^i is omitted. So,

$$f(X) = \begin{cases} a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \\ a_0 + a_1X + a_2X^2 + \cdots + a_nX^n + 0 \cdot X^{n+1} + 0 \cdot X^{n+2} + \cdots \end{cases}$$

A polynomial $f(X) = a_0$ is called a **constant polynomial** (meaning coefficients $a_i = 0 \ \forall i \neq 0$).

2. Let $R[X]$ denote the set of all polynomials, with coefficients in R.

3. We define addition and multiplications on $R[X]$. Consider two polynomials

$$\begin{cases} f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \\ g(X) = b_0 + n_1X + b_2X^2 + \cdots + b_nX^n \end{cases}$$

By including $0 \cdot X^k$ we can assume $f(X)$ and $g(X)$ have same number of terms. Define

$$\begin{cases} (f+g)(X) = f(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots + (a_n + b_n)X^n \\ (fg)(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + a_nb_nX^{2n} \end{cases}$$

Lemma B.3.2. The set $R[X]$ is commutative ring, under the addition and multiplication defined above. The zero of the ring is the $\mathbf{0} = 0 + 0 \cdot X + \cdots$ (the constant polynomial 0). The Multiplicative identity is $1 = 1 + 0 \cdot X + \cdots$ (the constant polynomial 1) *We say $R[X]$ is the polynomial ring, in one variable X.*

Proof. Exercise! ■

Definition B.3.3. Let R be a commutative ring. Let $X_1, X_2, \ldots, X_n$ be symbols (variables). Inductively, define the polynomial ring in these variables

$$R[X_1, X_2, \ldots, X_n] = R[X_1, X_2, \ldots, X_{n-1}][X_n]$$

Alternate way to define this is as follows:

1. For integers, $r_1 \geq 0, r_2 \geq 0, \ldots, r_n \geq 0$, the following expression

$$X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n}$$

is called a **monomial** . Here if $r_i = 0$ then $X_i^0 := 1$ is omitted. We consider $X_i^0 = 1$. A polynomial $f(X_1, X_2, \ldots, X_n)$ is a sum

$$f(X_1, X_2, \ldots, X_n) = \sum a_{r_1, r_2, \ldots, r_n} X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n} \tag{B.2}$$

where

(a) $a_{r_1,r_2,\ldots,r_n} \in R$

(b) **Only finitely many** $a_{r_1,r_2,\ldots,r_n} \neq 0$. So, the above sum is a finite sum. it is a formal sum.

2. Given two polynomials

$$\begin{cases} f(X_1, X_2, \ldots, X_n) = \sum a_{r_1,r_2,\ldots,r_n} X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n} \\ g(X_1, X_2, \ldots, X_n) = \sum b_{r_1,r_2,\ldots,r_n} X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n} \end{cases}$$

Define sum

$$(f+g)(X_1, X_2, \ldots, X_n) = \sum \left(a_{r_1,r_2,\ldots,r_n} + b_{r_1,r_2,\ldots,r_n}\right) X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n}$$

Define product

$$(fg)(X_1, X_2, \ldots, X_n) = \sum_{r_1 \geq 0,\ldots,r_n \geq 0} \left(\sum_{s_1+t_1=r_1,\ldots,s_n+t_n=r_n} a_{s_1,s_2,\ldots,s_n} b_{t_1,t_2,\ldots,t_n} \right) X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n}$$

3. With this sum and product $R[X_1, X_2, \ldots, X_n]$ is commutative ring.

(a) A polynomial f as in (B.2) is called **constant polynomial** , if

$$a_{r_1,r_2,\ldots,r_n} = 0 \quad unless \quad r_1 = r_2 = \cdots = r_n = 0$$

(b) The constant polynomial $f = 0$ is the zero of addition.

(c) The constant polynomial $f = 1$ is the multiplicative identity.

(d) A polynomial f as in (B.2), is an unit (invertible) if and only if (1) $f = a$ is a constant polynomial and a is unit in R. (*Needs a proof.*)

Remark B.3.4. Some remarks:

1. Most basic case of such polynomial rings, is when $R = \mathbb{F}$ is a field, and we consider the polynomial ring

$$\mathbb{F}[X_1, X_2, \ldots, X_n]$$

2. Main usefulness of such polynomials $f(X_1, X_2, \ldots, X_n)$ is that, for $x_1, x_2, \ldots, x_n \in R$, we can substitute

$$X_1 = x_1, \cdots, X_n = x_n \quad and\ get\ a\ value \quad f(x_1, x_2, \ldots, x_n) \in R.$$

3. Then, given $f \in R[X_1, X_2, \ldots, X_n]$ you can look at the **zero set**

$$Z(f) = \{(x_1, x_2, \ldots, x_n) \in R^n : f(x_1, x_2, \ldots, x_n) = 0\}$$

We can do the same with more than one polynomials. Let $f_1, f_2, \ldots, f_k \in R[X_1, X_2, \ldots, X_n]$. Then look at the common zero set

$$Z(f_1, f_2, \ldots, f_k) = \left\{ (x_1, x_2, \ldots, x_n) \in R^n : \begin{array}{c} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \cdots \\ f_k(x_1, x_2, \ldots, x_n) = 0 \end{array} \right\}$$

These are called Algebraic sets or spaces.

B.4 Division Algorithm and Euclidean rings

We start with two lemmas that are referred to as Division Algorithms.

Lemma B.4.1 (Euclid's Algorithms)**.** Fix an integer $n \geq 2$. Given a integer $m \in \mathbb{Z}$, we can write

$$m = nq + r \qquad where \begin{cases} q \in \mathbb{Z} & unique\ integer \\ r \in \mathbb{Z}, \quad 0 \leq r \leq n-1 & unique\ integer \end{cases}$$

Proof. Do we need one? It follows from, so called, Well Ordering Principle. ■

Lemma B.4.2 (Division Algorithms of polynomials)**.** Let $\mathbb{F}$ be a field and $\mathbb{F}[X]$ be the polynomial ring, in one variable X. Let $f(X) \in \mathbb{F}[X]$ be a polynomial, such that $f(X) \neq 0$. Given a polynomial $g(X) \in \mathbb{Z}$, there are two unique polynomials $q(X), r(X) \in \mathbb{F}[X]$, such that

$$g(X) = f(X)q(X) + r(X) \qquad such\ that \quad r(X) = 0\ or\ \deg(r(X)) < \deg(f(X))$$

Proof. Try it! Use degree! ■

These lead to the following definition.

Definition B.4.3 (Euclidean Ring)**.** Let R be ring. Assume R has no zero divisors

$$(\textbf{Meaning} \qquad \forall a, b \in R, \quad ab = 0 \Longrightarrow a = 0\ or\ b = 0)$$

Write $\hat{R} = \{x \in R : x \neq 0\}$, the set of non zero elements in R.
We say R is a **Euclidean Ring** if there is a function

$$d : \hat{R} \longrightarrow \{0, 1, 2, \ldots\}$$

such that

1. $d(1) = 0$.

2. $\forall a, b \in \hat{R} \;\; d(a) \leq d(ab)$

3. Let $a \in \hat{R}$. Then, for any $b \in \hat{R}$ there are $q, r \in R$ such that

$$b = qa + r \qquad \ni \qquad r = 0 \quad or \quad d(r) < d(a)$$

The function d will be referred to as the division algorithm.

Exercise B.4.4. Let R be an Euclidean ring, with the division algorithm d. Prove that an element $a \in R$, with $a \neq 0$ is a unit in R if and only if $d(a) = 0$.

Proof. Suppose $d(a) = 0$. If we divide 1 by a, then

$$1 = qa + r \qquad r = 0 \quad or \quad d(r) < d(q) = 0$$

So, $r = 0$ and $1 = qa$. So, a is a unit.

Conversely, assume a is unit. Then $1 = aa^{-1}$. So, $d(a) \leq d(1) = 0$. So, $d(a) = 0$.

Example B.4.5. For integers $n \in \mathbb{Z}$, with $n \neq 0$ define $d(n) = |n|$, the absolute value. Then $\mathbb{Z}$ is an Euclidean ring.

Example B.4.6. Let $\mathbb{F}$ be a field. For $x \in \mathbb{F}$, with $x \neq 0$ define $d(x) = 0$. Then $\mathbb{F}$ is an Euclidean ring.

Example B.4.7. Let $\mathbb{F}$ be a field and $R = \mathbb{F}[X]$ be the polynomial ring. For $f(X) \in \mathbb{F}[X]$, with $f(X) \neq 0$ define $d(f) = \deg(f)$, the degree. Then $\mathbb{F}[X]$ is an Euclidean ring.

Index