someone find a snappy cool title for this

A linear algebra book

Reblax

Contents

Preface

This book is intended to enable motivated students to self-study linear algebra. The point of view on the subject adopted here is the one a pure mathematician would have: computations are shunned to leave room for proofs, and the aim is to make the student feel the power of mathematical abstraction and linear algebra as well as learning how to use them as tools. The only assumed background is familiarity with proofs, proof methods, naive set theory, manipulation of real and complex numbers, and a bit of real analysis may sometimes be useful. In particular, no prior knowledge of abstract algebra is necessary. Thus, this book is intended to be an introduction to using abstract machinery in math. It is written in the author's usual style, giving lots of details in proofs and often taking a break from formal mathematical discussion to underline the intuition behind results, tell historical anecdotes, or little jokes. Read at your own risk.

How to read this book

In the text, there are some exercises that are usually meant to be easy and be done as you are reading, to check and solidify understanding. More challenging exercises can be found at the end of a chapter. You should do all the exercises in the text, and try some at the end of chapters.
The first chapter is not about linear algebra but about basic notions of abstract algebra that will be needed later. You can read only the first two sections, then move on to linear algebra, reading the other two sections (on quotients and polynomial rings) only when you need them, or you can read all of chapter 1 before the rest.

List of Symbols and Notations

$\mathbb{N}$	The natural numbers $\{0, 1, 2, \dots\}$
$\mathbb{Z}$	The integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Q}$	The rational numbers $\left\{ \frac{a}{b} \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{Z}^* \right\}$
$\mathbb{R}$	The real numbers
$\mathbb{C}$	The complex numbers $\{a + bi \mid a, b \in \mathbb{R}\}$
$\mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	The same sets as before with zero removed
$A \subset B, A \supset B$	set-theoretic containment (not necessarily proper)
$[a, b]$	the closed interval $\{x \in \mathbb{R} \mid a \leq x \leq b\}$
$]a, b[$	the open interval $\{x \in \mathbb{R} \mid a < x < b\}$
F^E	the set of all functions from E to F
$\lvert E \rvert$	cardinality (number of elements of) a finite set E
$f : E \to F$	function from E to F
$f_{\lvert A}$ for $A \subset E$	restriction of f to A, $f_{\lvert A} : A \to F$
$f^{\lvert G}$ for $G \subset F$	corestriction of f to G, $f^{\lvert G} : E \to G$; only defined if $f(E) \subset G$

Chapter 1

Prerequisites: what even is abstract algebra?

In this chapter, we introduce basic notions of abstract algebra. We discuss groups at large to introduce the notion of algebraic structure, substructures and morphisms (relations between them). Once these ideas have been developed, we see their analogues for rings and fields. We then introduce quotients which are a fundamental operation in nearly all of math. As an application, we prove some results on finite groups that are unimportant for later. Finally, we discuss properties of polynomials that will be of utmost important when discussing eigenvalues and eigenvectors.

1.1 Introduction: Groups

Abstract algebra, broadly speaking, is the study of algebraic structures. It is very different to the algebra you have learned in grade school, but it bears some similarities to it. It is worth explaining how this:

$$2x = 3$$

eventually becomes this:

$$(f : E \to F) \mapsto (f \otimes \mathrm{id} : E \otimes V \to F \otimes V)$$

A common idea in algebra (actually, math in general) is to notice similarities between different situations and abstract away the details, to prove more theorems, understand more about the underlying phenomena and overall think better. For instance, you can prove the following three theorems by hand:

$$1+1+1=1+2 \qquad 2+1+1=2+2 \qquad 3+1+1=3+2$$

but it is easier and faster to prove the more general theorem

$$\forall x \in \mathbb{R}, x+1+1=x+2$$

which can then be specialized to any situation by replacing x by a real number. The idea behind algebraic structures is similar, but more advanced and intricate.
Let's consider "operations" on different sets you already know of.

- Consider the integers $\mathbb{Z}$, and consider addition. We don't need parentheses: if $a, b, c \in \mathbb{Z}$, then

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

Plus, there is a special integer, namely 0, such that adding with it does nothing: $a + 0 = 0 + a = a$. Further, for any integer a, there is another integer $-a$ that takes a back to zero: $a + (-a) = (-a) + a = 0$. It is also worth noting that order does not matter: $a + b = b + a$.

- Now consider $\mathbb{Z}$ and multiplication. Again, we don't need parentheses :

$$(a \times b) \times c = a \times (b \times c)$$

and there is a special integer, 1, such that multiplying with it does nothing: $1 \times a = a \times 1 = a$. Again, order does not matter: $a \times b = b \times a$. However, notice that the number that when multiplied by 2 would give 1 is $\frac{1}{2}$, which is not in $\mathbb{Z}$. This means that we don't have an equivalent notion of "inverses" for multiplication in $\mathbb{Z}$ as we have for addition.

- When considering $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ with addition, we can say the exact same things as we did above with $\mathbb{Z}$ (check it!). With multiplication, something happens: nearly all numbers in $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ have multiplicative inverses. Precisely, if $x \in \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ and $x \neq 0$, then we have $\frac{1}{x}x = x\frac{1}{x} = 1$. So it's not quite like addition where all numbers have opposites, but it is worth nothing.

- Now consider $\mathbb{Z}$ again but with subtraction this time. None of the properties seen before work! Here are some counterexamples:

$$(1 - 0) - 1 \neq 1 - (0 - 1)$$
$$1 - 0 \neq 0 - 1$$

and there is no integer a such that for all b, $a - b = b - a = b$. Since we don't have such a "neutral" integer that does nothing, searching for "inverses" of elements does not even make sense.

- Consider $\mathbb{N}$ with addition. We have all the properties that $\mathbb{Z}$ with addition has, except the existence of opposites.

- Consider the set of all functions $\mathbb{R}^{\mathbb{R}}$. We can add and multiply functions together pointwise: if $f, g : \mathbb{R} \to \mathbb{R}$, we define new functions of $\mathbb{R}^{\mathbb{R}}$ by

$$f + g : x \mapsto f(x) + g(x) \qquad \text{and} \qquad fg : x \mapsto fg(x)$$

This addition of functions shares all the properties addition on $\mathbb{Z}$ does. Multiplication also shares numerous properties with the multiplication on $\mathbb{Z}$ (we will see more precisely which later).

- If you've done some analysis, convince yourself that the same things can be said about *continuous* functions from $\mathbb{R}$ to $\mathbb{R}$, and *differentiable* functions from $\mathbb{R}$ to $\mathbb{R}$ (you just need to check that adding/multiplying two continuous/differentiable functions gives a continuous/differentiable function).

- Consider the set $\{+1, -1\}$, together with multiplication. This makes sense, because $1 \times 1 = 1$, $1 \times (-1) = -1$ and $(-1) \times (-1) = 1$, so multiplying two elements of the set gives another element of the set. Since this multiplication is actually the one from $\mathbb{Z}$, we know it needs no parentheses and order does not matter. We still have the "neutral element" 1 in our set, and it turns out that since $(-1) \times (-1) = 1$, all elements of the set have multiplicative inverses.

Now, let's abstract these concepts. Recall that if E and F are two sets, $E \times F$ stands for the *cartesian product* of E and F, and is the set of all ordered pairs (x, y) with $x \in E$ and $y \in F$.

Definition 1.1.1. Let G be a set. A *binary operation* on G is a function $* : G \times G \to G$. For binary operations, we will use infix notation, that is instead of writing $*(x, y)$ like you would with a regular function, we write $x * y$.

Example 1.1.2. All operations discussed above are binary operations (on the appropriate sets).

This is powerful, because the concept of a binary operation allows us to talk about potentially very different operations simultaneously. Now let's abstract the properties we outlined above.

Definition 1.1.3. Let G be a set, and $*$ be a binary operation on G.

- We say $*$ is *associative* if for all $a, b, c \in G$, we have
$$a * (b * c) = (a * b) * c$$
- We say $*$ is *commutative* if for all $a, b \in G$, we have
$$a * b = b * a$$
- We say $e \in G$ is a *neutral element* for $*$ if for all $a \in G$, we have
$$a * e = e * a = a$$
- Assuming $*$ has an identity element $e \in G$, we say that $b \in G$ is an *inverse* of $a \in G$ if
$$a * b = b * a = e$$

Remark. Anglophones tend to call neutral elements "identity elements". The author learned with and prefers the terminology "neutral element" so it will be used here.

Exercise 1.1.A. Let E be a set, and consider the set E^E of functions from E to E. We define a binary operation called *function composition* on E^E by

$$\begin{array}{rccl} \circ : & E^E \times E^E & \to & E^E \\ & (g, f) & \mapsto & g \circ f : x \mapsto g(f(x)) \end{array}$$

1. Show that $\circ$ is associative.
2. Show that $\circ$ has a neutral element.
3. Show that if E has at least two different elements, $\circ$ is not commutative.

We can summarize what was discussed up until now in the following table:

	Associativity	Commutativity	Neutral element	Inverses
Addition $+$ on $\mathbb{Z}$ Addition $+$ on $\mathbb{R}^{\mathbb{R}}$	Yes	Yes	Yes	Yes
Multiplication $\times$ on $\mathbb{Z}$ Multiplication $\times$ on $\mathbb{R}^{\mathbb{R}}$ Addition $+$ on $\mathbb{N}$	Yes	Yes	Yes	No
Multiplication $\times$ on $\mathbb{Q}, \mathbb{R}, \mathbb{C}$	Yes	Yes	Yes	All except 0
Composition $\circ$ on E^E	Yes	No	Yes	Exercise 1.1.B
Composition $\circ$ on S_E (see exercise 1.1.B)	Yes	No	Yes	Yes

Remark. The above table shows we have not yet given an example of a non-associative binary operation. This is because such operations very rarely come up in practice. We will delve into an example here, but the interested reader may wish to look up what octonions are, and the motivated reader may try to come up with their own example of a non-associative binary operation on the set $\{1, 2, 3\}$ (hint: you can find such a binary operation that is commutative).

It is time to prove our two first propositions. These are about uniqueness of neutral elements and inverses.

Proposition 1.1.4. *If G is a set together with a binary operation $*$, then $*$ has at most one neutral element.*

Proof. Assume $e, f \in G$ be neutral elements for $*$. Then, since e is neutral, we have $e * f = f$. But since f is neutral, we also have $e * f = e$. Therefore we must have $e = f$, and this concludes. □

Proposition 1.1.5. *If G is a set together with an associative binary operation $*$ that has a neutral element $e \in G$, then inverses are unique. That is, if $a \in G$ has an inverse $b \in G$, then it is the only inverse of a.*

Proof. Assume $a \in G$ has an inverse $b \in G$. Let $c \in G$ be another inverse of a. Then, $a * b = e = a * c$, since b and c are both inverses of a. This implies that $b * (a * b) = b * (a * c)$. Since $*$ is associative, we have $(b * a) * b = (b * a) * c$. But b is an inverse of a, so $b * a = e$. We obtain $e * b = e * c$, which reduces to $b = c$ by neutrality of e. This proves b is the sole inverse of a. □

Notation. Since $a \in G$ has at most one inverse for $*$, we will usually denote it a^{-1}, without ambiguity. The main exception to this is when the operation is written $+$, then we write $-a$ for the inverse.

It is now time to define our very first algebraic structure.

Definition 1.1.6. A set G, together with a binary operation $*$ on it, is called a *group* if:

1. $*$ is associative,
2. $*$ has a neutral element $e \in G$,
3. All elements of G have an inverse for $*$.

If $*$ is commutative, we say G is *abelian*.

Notation. We usually write $(G, *)$ if we want to specify the operation. In practice, most of the time, the operation will be implicitly understood and we will write "G is a group".

Example 1.1.7. The integers $\mathbb{Z}$, rationals $\mathbb{Q}$, reals $\mathbb{R}$ and complex $\mathbb{C}$ are all abelian groups under addition. The set $\mathbb{C}^*$ is a group under multiplication.

Exercise 1.1.B (Symmetric group)**.** Let E be a set. Recall we have composition $\circ$ on E^E.

1. Show that $f : E \to E$ has an inverse for composition if and only if f is bijective.
2. Let $S_E = \{f : E \to E \mid f \text{ is bijective}\}$. Show that S_E is a group under $\circ$. Notice that you need to show that composing two bijections gives a bijection for $\circ$ to be a binary operation on S_E.
3. Show that $S_{\{1,2,3\}}$ is not abelian.
4. Show that S_E is finite if and only if E is finite, and in that case $|S_E| = |E|!$.

Remark. The group constructed in the previous exercise is called *the symmetric group on* E and such groups are very important in group theory and math in general. In fact, they will show up again much later in chapter 6 when we seek to understand multilinearity and determinants.

Exercise 1.1.C. We define $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ the set of complex numbers of module 1.

1. Check that $(\mathbb{U}, \times)$ is a group.
2. Make a picture. What is the geometric interpretation of $\times$?
3. Let $n \in \mathbb{N}^*$ be a positive integer. Let
$$\mathbb{U}_n = \{e^{\frac{2i\pi k}{n}} \mid 0 \leq k < n\}$$
   (a) Check that $\mathbb{U}_n$ is precisely the complex solutions to the equation $z^n = 1$. For this reason we call elements of $\mathbb{U}_n$ the *n-th roots of unity*.
   (b) Check that $(\mathbb{U}_n, \times)$ is a group.

Remark. You may notice that $(\mathbb{N}, +)$ and $(\mathbb{Z}, \times)$ are almost groups: they only lack the assumption that all elements have an inverse. This is made precise by the notion of a *monoid*: a set together with an associative binary operation that has a neutral element. Monoids are also useful but we won't elaborate on them here.

We now give one more example of a group, that comes from geometry. **TODO**

Remark. **TODO**

Notation. From now on, we will call the binary operation of a group $\cdot$, and omit writing it, which means we will write ab instead of $a \cdot b$ for convenience.

We now introduce the notion of a subgroup, which roughly speaking is a smaller group inside a bigger group. As we will see, smaller structures existing inside bigger structures is recurrent in abstract algebra.

Definition 1.1.8. Let $(G, \cdot)$ be a group. We say that $H \subset G$ is a *subgroup of* G if :

- For all $x, y \in H$, we have $xy \in H$,
- We have $e \in H$,
- For any $x \in H$, we have $x^{-1} \in H$.

Example 1.1.9. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$. If G is any group, G is a subgroup of G, and $\{e\}$ is a subgroup of G.

Exercise 1.1.D. Let E be a non-empty set, and consider the symmetric group S_E. Let $x \in E$. Show that $\{f \in S_E \mid f(x) = x\}$ is a subgroup of S_E.

Notation. Let g be an element of a group. For $n \in \mathbb{N}^*$, we will write

$$g^n = \underbrace{gg\cdots g}_{n \text{ times}} \qquad g^{-n} = \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{n \text{ times}}$$

and $g^0 = e$ is the neutral element. Using this notation, we have $g^{n+m} = g^n g^m$ for all $n, m \in \mathbb{Z}$.

A particularly interesting and relevant example of a subgroup is the following:

Proposition 1.1.10. *Let G be a group and $g \in G$. Then $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ is an abelian subgroup of G.*

Proof. We check the three properties we need. If $g^n, g^m \in \langle g \rangle$, then $g^n g^m = g^{n+m} \in \langle g \rangle$. We have $e = g^0 \in \langle g \rangle$. The inverse of $g^n \in \langle g \rangle$ is $g^{-n} \in \langle g \rangle$. This shows $\langle g \rangle$ is a subgroup. Since

$$g^n g^m = g^{m+n} = g^m g^n$$

The group $\langle g \rangle$ is abelian. □

Definition 1.1.11. Let G be a group and $g \in G$. The subgroup $\langle g \rangle$ is called the *subgroup generated by g*.

Example 1.1.12. Even integers, denoted by $2\mathbb{Z}$, are the subgroup of $\mathbb{Z}$ generated by 2.

Exercise 1.1.E. Consider the group $(\mathbb{U}, \times)$.

1. Let $n \in \mathbb{N}^*$ be a positive integer. Find $z \in \mathbb{U}$ such that $\langle z \rangle = \mathbb{U}_n$.
2. Find $z \in \mathbb{U}$ such that $\langle z \rangle$ is infinite (this one is trickier).

If $G = \langle g \rangle$ for some $g \in G$, we say the group G is cyclic. Cyclic groups are quite easy to completely classify. Their classification is established in section 1.3 as an application of quotients.

Exercise 1.1.F. Let G be a group and $H, K \subset G$ be subgroups of G.

1. Show that $H \cap K$ is again a subgroup of G.
2. Show that $H \cup K$ is a subgroup of G if and only if $H \subset K$ or $K \subset H$.

We now move on to morphisms. A fundamental idea in algebra is that while objects are important, relations between objects are at least as important if not even more. To motivate this, notice that as a group, $(2\mathbb{Z}, +)$ is really similar to $(\mathbb{Z}, +)$. Indeed, if we replace some integer x by $2x$, we notice that addition in $\mathbb{Z}$ becomes addition in $2\mathbb{Z}$: $z = x + y$ becomes $2z = 2x + 2y$. To make this precise, we need a way to assign one value to another value, so a function.

Definition 1.1.13. Let $(G, *)$ and $(H, \star)$ be two groups. A *group homomorphism* from G to H is a function $f : G \to H$, such that

$$\forall x, y \in G, f(x * y) = f(x) \star f(y)$$

Example 1.1.14. We have a group homomorphism $f : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & 2n \end{array}$, because $2(n+m) = 2n + 2m$.

Example 1.1.15. The exponential $\exp : \mathbb{R} \to \mathbb{R}^{+*}$ is a group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^{+*}, \times)$:

$$\exp(x+y) = \exp(x)\exp(y)$$

From now on we fix two groups G and H that we both note multiplicatively (omitting the operation).

Proposition 1.1.16. *A group homomorphism $f : G \to H$ takes the neutral element to the neutral element and inverses to inverses:*

$$f(e_G) = e_H \qquad \forall x \in G, f(x^{-1}) = f(x)^{-1}$$

Proof. We have $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. Multiplying by the inverse of $f(e_G)$, we obtain $e_H = f(e_G)$, as desired. If $x \in G$, then $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$. Similarly, one shows $f(x^{-1})f(x) = e_H$. This proves that $f(x^{-1})$ is the inverse of $f(x)$ in H. □

1.2 Rings and Fields

1.3 Quotients

Quotients are a basic, fundamental construction in algebra. Here we introduce quotients of sets, use them to prove Lagrange's theorem on finite groups, and then show how quotients of abelian groups are again groups. Later, we will introduce quotients of vector spaces, which are often useful.

1.4 Polynomial rings

1.5 More exercises

Chapter 2

Vector spaces

We now begin our study of linear algebra with the definition of vector spaces, the main algebraic structures of interest in linear algebra.

2.1 The definition of vector spaces

2.2 Constructing new vector spaces out of old

2.3 Families of vectors: linear independence and span

Chapter 3

Linear maps

Chapter 4

Dimension

4.1 Technicalities: defining dimension

4.2 Finite-dimensional vector spaces and their consequences

4.3 Applications to field theory

Chapter 5

Matrices

5.1 Matrices done right

5.2 Change of basis, equivalence, similarity, trace

Chapter 6

Multilinearity and Determinants

Chapter 7

Inner product Spaces

7.1 Inner products and norms

7.2 Orthogonality

7.3 Orthogonal complements, and minimisation problems

Chapter 8

Eigenvalues and Eigenvectors

Chapter 9

Adjoints and Spectral Theorems

9.1 Adjoints, self-adjoint and normal operators

9.2 Spectral theorems

9.3 Isometries and unitary operators

Epilogue: what next?

Appendix A

Spooky scary set-theoretic stuff