Course: Linear Algebra(Preliminares)

Sebastián Caballero

December 1, 2022

A simple notes template. Inspired by Tufte-LaTeXclass and beautiful notes by

`https://github.com/abrandenberger/course-notes`

1 *Groups*

Let's start our study in algebra with the most basic, known but also powerful structure in mathematics. Groups are so useful because they generalize a lot of properties and allow the development of great theorems. Let's start by defining what is an operation.

Definition 1.1 (Operation). *An operation over G is a function*

$$\cdot : G \times G \to G$$

such that any pair of elements $(a, b) \mapsto \cdot(a, b)$(This image is noted as $a \cdot b$)

So, take for example the addition, the modular product or the symmetric difference over sets. Now, groups are literally the generalization of operations that "behave well".

Definition 1.2 (Group). *A group is a ordered pair $(G, \cdot)$ such that G is a set, $\cdot$ is an operation closed on G, that is, for any $a, b \in G$, $a \cdot b \in G$, and holds the next properties:*

1. ***Associativity:*** *For any $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$*
2. ***Identity element:*** *There is an element denoted as $e \in G$ such that $e \cdot a = a \cdot e = a$*
3. ***Inverse element:*** *For any $a \in G$, there is an element denoted as $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$*

Many of the properties given must be familiar with you for the work with real numbers. [1] Let's prove some statements basics in group theory.

[1] If for any $a, b \in G$, $a \cdot b = b \cdot a$ then G is called abelian.

Theroem 1.1 (Basic properties). *Let G be a group under $\cdot$. Then:*

1. *G has exactly one identity element, and every element of G has*

exactly one inverse element.

2. *For any $a, b, c \in G$, if $a \cdot b = a \cdot c$ then $b = c$*
3. *For any $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$*

Proof. For each of the properties, the trick is use the Associativity and the inverse elements.

1. Suppose e_1 and e_2 are identity elements of G. Then $e_1 \cdot e_2 = e_1$ because e_2 is an identity, but also $e_1 \cdot e_2 = e_2$ because e_1 is an identity. So, $e_1 = e_2$. Now suppose that for a, b and c are inverse elements. Manipulate the next expression with associativity law:

$$\begin{aligned} b \cdot a \cdot c &= (b \cdot a) \cdot c \\ &= e \cdot c \\ &= c \end{aligned}$$

   But also:

$$\begin{aligned} b \cdot a \cdot c &= b \cdot (a \cdot c) \\ &= b \cdot e \\ &= b \end{aligned}$$

   So $b = c$.

2. Just operate with the inverse of a by the left in both sides of the expression:

$$\begin{aligned} a \cdot b &= a \cdot c \\ a^{-1} \cdot a \cdot b &= a^{-1} \cdot a \cdot c \\ e \cdot b &= e \cdot c \\ b &= c \end{aligned}$$

3. Since the inverse element is unique, then if we prove that $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$ we can assure that $(a \cdot b)^{-1} = b^{-1}a^{-1}$. So:

$$\begin{aligned} (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) &= b^{-1} \cdot (a^{-1} \cdot a) \cdot b \\ &= b^{-1} \cdot e \cdot b \\ &= b^{-1} \cdot b \\ &= e \end{aligned}$$

   In a similar way, you can prove that $(a \cdot b) \cdot (b^{-1}a \cdot a^{-1}) = e$. So, it must be the inverse of $a \cdot b$.

□

2 Fields

Ok, now we are so far good. Our interest in groups is also because they let us define in an easier way a structure called *field*. Real numbers are such a good example of a field, when two operations are joined and "behave well" again.

Definition 2.1 (Field). *Let F be a set with two operations $+$ and $\cdot$. Then F is a field if:*

1. *$(F, +)$ is an abelian group. Its identity element is denoted as 0*
2. *$(F \setminus \{0\}, \cdot)$ forms an abelian group. Its identity element is denoted as 1*
3. *$+$ and $\cdot$ are related through the distributive law:*

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

In a field, the element 0 is called an annihilator since any element multiplied by 0, is 0. This is our next proof:[2]

[2] This is true even with special structures called *ring* that we will see later.

Theroem 2.1 (Zero cancellation). *In a field F, for any $a \in F$,*

$$a \cdot 0 = 0$$

Proof. Operate the expression like follows:

$$a \cdot 0 = a \cdot (0 + 0)$$
$$a \cdot 0 = a \cdot 0 + a \cdot 0$$

And if you add the additive inverse of $a \cdot 0$ in both sides we have:

$$a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0)$$
$$0 = a \cdot 0$$

□

Note that fields have at least two elements: 1 and 0. If it's not true, then $\cdot$ would be an empty group in F. But groups have at least the identity element, so it can't be empty.

We will prove one property that should be very familiar with you at this point. If you have two real numbers and their product is zero, then one of them must be zero. This is a general property of fields.

Theroem 2.2 (No divisors of zero). *In a field F, if $a, b \in F$ are such that $a \cdot b = 0$ then $a = 0$ or $b = 0$.*

Proof. Suppose $a \cdot b = 0$ but $a \neq 0$. Then we want to prove that $b = 0$. So, begin with the original expression:

$$\begin{aligned} a \cdot b &= 0 \\ a^{-1} \cdot a \cdot b &= a^{-1} \cdot 0 \\ b &= 0 \end{aligned}$$

□

The fields could also have a property called *torsion*. For example, if F has only 1 and 0 and the operation are modular addition and product, then $1 + 1 = 0$. This is also a characteristic of fields!(Bad prank).

Definition 2.2 (Characteristic of a field). *In a field F, the number λ is called a characteristic of the field if λ is the least natural number such that:*

$$\underbrace{1 + 1 + \cdots + 1}_{\lambda \text{ times}} = 0$$

if such number doesn't exists, then the field has characteristic zero.

And since we are talking about equations, we should think about equations in fields. So, similarly to what we see in calculus, we define a polynomial with coefficients in F as a function $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ where $a_i \in F$ with $0 \leq i \leq n$.

If you are familiar with math, you should be familiar that most problems in high school is solve a equation of the form $p(x) = 0$. If for any combinations of coefficients in polynomials of a field F, you can find at least one $a \in F$ such that $p(a) = 0$, then F is said to be algebraically closed.

For example, $\mathbb{R}$ is not algebraically closed, because $p(x) = x^2 + 1$ has no real solutions. There is a fact, called *the fundamental theorem of algebra* that assures that $\mathbb{C}$ is algebraically closed.

Before we continue in a development of algebra, let's announce a definition important in fields.

Definition 2.3 (Subfield). *Let F be a field. If K is a subset of F such that K forms a field under the same operations of F, then K is called a subfield of K and F is called an extension field of K.*

3 Construction of $\mathbb{C}$ from $\mathbb{R}$

The next construction is introduced in order to explain and development the exercises with fields. So, consider in general $\mathbb{R}^n$ as the $n-$tuples of real numbers. If you take $n = 2$ we define the sum of tuples as:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

for all $x = (x_1, y_1)$ and $y = (x_2, y_2)$ tuples on $\mathbb{R}^2$. It is easy to verify that since $\mathbb{R}$ is a field, then $\mathbb{R}^2$ forms a group under $+$. And what if we want to create a field? How we should define the product? Well, the first approach that one can think is:

$$(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$$

But this approach has a lot of drawbacks. Even when it commutes and associate, the existence of neutral element, no zero divisors and inverse elements is a big problem here! As long as we advanced in the development of algebra, it will become evident that is is convenient to define it as:

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$$

4 Exercises

The next exercises are taken from the book *Abstract Linear Algebra* by *Morton L. Curtis*.

Problem 1. *A subset H of a group G is a subgroup of G if the operation on G makes H into a group. Prove that $H \subseteq G$ is a subgroup if and only if:*

1. $e \in H$
2. *if $a, b \in H$, then $ab^{-1} \in H$*

Proof. Suppose $H \subseteq G$ and let's prove a double implication:

$\Rightarrow$) Suppose that H is a subgroup. Then by definition H must have an identity element, but since G has only one identity element, then it must be the same in H. We conclude that $e \in H$. Now, since H is a group, then b must be an inverse element in H and since the operation must be closed then $ab^{-1} \in H$.

$\Leftarrow$) Suppose H is a subset of G such that $e \in H$ and for any $a, b \in H$, then $ab^{-1} \in H$. We want to prove that H is a group. Note that

since $e \in H$, we have already the identity element. The associativity property is given because G is a group. Now, if $a \in H$, we already have that $a^{-1} \in H$, because the second property given and the fact that $ea^{-1} = a^{-1}$. To prove that H is closed under the same operation, take that $a \in H$ and $b \in H$. We know that $b^{-1} \in H$ and by the second property we can assure that $a(b^{-1})^{-1} \in H$, but it means that $ab \in H$.

□

Problem 2. *For $n \in \mathbb{Z}^+$ define:*

$$\begin{aligned} \mathbb{Z}_n &:= \{0, 1, \ldots, n-1\} \\ a \oplus b &:= (a + b) \mod n \\ a \otimes b &:= (a \cdot b) \mod n \end{aligned}$$

Prove that $\mathbb{Z}_n$ has no divisors of zero if and only if n is prime

Proof. $\Rightarrow$) Suppose n no is prime. Then there are two numbers x, y different from 1 and 0 such that $x \cdot y = n$. Then:

$$\begin{aligned} x \otimes y &= (x \cdot y) \mod n \\ &= n \mod n \\ &= 0 \end{aligned}$$

So $x \otimes y = 0$ but $x \neq 0$ and $y \neq 0$. So, $\mathbb{Z}_n$ has divisors of 0.

$\Leftarrow$) Suppose n is a prime number. Now, suppose that exists $a, b \in \mathbb{Z}_n$ such that $a \otimes b = 0$ but $a \neq 0$ and $b \neq 0$. So, $(a \cdot b) \mod n = 0$. Now, we can make:

$$\begin{aligned} n \otimes (a \otimes b) &= (n \cdot a \cdot b) \mod n \\ &= n \mod n \cdot (a \cdot b) \mod n \\ &= n \mod n \cdot 0 \\ &= 0 \end{aligned}$$

So we conclude that $n | n(ab)$ but it contradicts the hypotesis that n is a prime number since ab cannot be 1.

□

Problem 3. *Show that $(1, 0)$ acts as identity for $\mathbb{C}$ with the defined multiplication*

Proof. Let $(a,b) \in \mathbb{R}^2$, then its product with $(1,0)$ is defined as:

$$\begin{aligned}(a,b)(1,0) &= (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1)\\ &= (a\cdot 1, b\cdot 1)\\ &= (a,b)\end{aligned}$$

□

Problem 4. *Show that the product defined for $\mathbb{C}$ extends the multiplication for $\mathbb{R}$ if $\mathbb{R}$ is defined as $\{(r,0) \in \mathbb{R}^2 : r \in \mathbb{R}\}$*

Proof. Take $a, b \in R$. Then their product is:

$$\begin{aligned}(a,0)(b,0) &= (a\cdot b - 0\cdot 0, a\cdot 0 - b\cdot 0)\\ &= (a\cdot b - 0, 0 - 0)\\ &= (a\cdot b, 0)\end{aligned}$$

Which is the representation for $a \cdot b$ in $\mathbb{C}$ □

Problem 5. *Show that the operations defined before makes $\mathbb{C}$ a field.*

Proof. □

Problem 6. *Write (a,b) as $a + bi$ and treat these as polynomials in i with the condition that $i^2 = -1$. Show this generates our definition of product.*

Proof. Take two complex numbers, named $x_1 + y_1 i$ and $x_2 + y_2 i$, if you multiply them:

$$\begin{aligned}(x_1 + y_1 i)(x_2 + y_2 i) &= (x_1 + y_1 i)x_2 + (x_1 + y_1 i)y_2 i\\ &= x_1x_2 + y_1x_2 i + x_1y_2 i + y_1y_2 i^2\\ &= x_1x_2 - y_1y_2 + x_1y_2 i + y_1x_2 i\\ &= (x_1x_2 - y_1y_2) + (x_1y_2 + y_1x_2)i\end{aligned}$$

And that is represented as $(x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$ □

Problem 7. *Define the conjugate of $\alpha = a + bi \in \mathbb{C}$ to be $\overline{\alpha} = a - bi$. Prove that for $\alpha, \beta \in \mathbb{C}$ we have:*

1. $\overline{(\alpha+\beta)} = \overline{\alpha}+\overline{\beta}$
2. $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$

Also show that $\alpha\overline{\alpha}$ is a nonnegative real number, and $\alpha\overline{\alpha} = 0$ exactly when $\alpha = 0$.

Proof. Take $\alpha = a + bi$ and $\beta = c + di$ then:

$$\begin{aligned}
\overline{(\alpha+\beta)} &= \overline{(a+bi+c+di)} \\
&= \overline{(a+c+bi+di)} \\
&= \overline{((a+c)+(b+d)i)} \\
&= (a+c)-(b+d)i \\
&= a+c+(-b-d)i \\
&= a+c-bi-di \\
&= a-bi+c-di \\
&= (a-bi)+(c-di) \\
&= \overline{\alpha}+\overline{\beta}
\end{aligned}$$

Also, if you multiply them we would have by our representation of tuples of $\mathbb{R}^2$:

$$\begin{aligned}
\overline{(a,b)(c,d)} &= \overline{(ac-bd, ad+bc)} \\
&= (ac-bd, -ad-bc) \\
&= (a,-b)(c,-d)
\end{aligned}$$

And the last property is a consequence that $\mathbb{C}$ is a field, since a field has no divirsos of 0, then if $\alpha\overline{\alpha} = 0$ implies that $\alpha = 0$ or $\overline{\alpha} = 0$, but if $\alpha = 0$ then $\alpha = \overline{\alpha}$ and in the other way. □

Problem 8. *Let $p(x)$ be a polynomial in the indeterminate x with real coefficients. Show that for any $\alpha \in \mathbb{C}$ we have*

$$\overline{p(\alpha)} = p(\overline{\alpha})$$

and use this to prove that if α is a complex root of p, the $\overline{\alpha}$ is also a root.

Proof. Take $p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 x + a_0$. Remember that $a_i \in \mathbb{R}$, and remember that if $r \in \mathbb{R}$ then $\overline{r} = r$. So, for p, we have:

$$\begin{aligned}
\overline{p(\alpha)} &= \overline{(a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \cdots + a_1\alpha + a_0)} \\
&= \overline{a_n \cdot \alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \cdots + \overline{a_1\alpha} + \overline{a_0}
\end{aligned}$$

Note that $\overline{a_0} = a_0$. Now:

$$\begin{aligned}\overline{a_i\alpha^i} &= \overline{a_i} \cdot \overline{\alpha^i} \\ &= a_i \cdot \overline{\alpha^i}\end{aligned}$$

And if you apply inductively the second property of the previous problem, then $\overline{\alpha^i} = \overline{\alpha}^i$. Therefore:

$$\overline{a_n \cdot \alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \cdots + \overline{a_1\alpha} + \overline{a_0} = a_n \cdot \overline{a}^n + a_{n-1} \cdot \overline{\alpha}^{n-1} + \cdots + a_1\overline{\alpha} + a_0$$

But it implies that $\overline{p(\alpha)} = p(\overline{\alpha})$. Now, suppose that α is a complex root of p, then:

$$p(\alpha) = 0$$

If you apply the conjugate of both expression:

$$\overline{p(\alpha)} = 0$$

And by the proposition we just have proved:

$$p(\overline{\alpha}) = 0$$

So $\overline{\alpha}$ is a complex root of p. □

Problem 9. *A polynomial $p(x)$ over a field k is monic if the highest power of x has coefficient 1. Let $p(x)$ be monic and let $r \in k$. Show that if $p(x)$ is divided by $x - r$, then the remainder is $p(r)$. Show that this remains true if $p(x)$ has coefficients in $\mathbb{R}$ and $r \in \mathbb{C}$.*

Problem 10. *From the previous problem, we see that if $p(x)$ is monic with real coefficients and $\alpha \in \mathbb{C}$ is a root of $p(x)$, then $x - a$ divides $p(x)$. Now prove that a monic polynomial $p(x)$ with real coefficients can be factored into linear and quadratic factors.*