Topic 2: Algebra

Seppe Staelens

July 10, 2024

Introduction

Having studied sets and functions between them in the previous topic, we now move on to the topic of algebra. Algebra is the branch of mathematics that studies the structure of sets, and in particular the operations that can be defined on them. The most basic structure we will study is that of a group, which is a set equipped with an operation that satisfies certain properties. We discuss what an isomorphism is, and use this to show how some groups are in fact the same.

We will then move on to vector spaces, which are sets equipped with two operations, and study the concept of linear transformations between them. Afterwards, we will introduce the concept of matrices, which are ubiquitous in mathematics and physics. They can be used to solve systems of linear equations, and can be used to represent linear transformations between vector spaces. Finally, we bring together some of these concepts when we discuss the Google PageRank algorithm, which is based on the concept of eigenvectors of matrices.

1 Lecture 1: Groups

A **group** $(G, \circ)$ is a set G on which we define an operation $\circ$ that maps two elements of the group to another element in the same group. In mathematical notation this is written as

$$\circ : G \times G \to G : (g, h) \mapsto g \circ h \tag{1}$$

The group has to satisfy the following:

1. There must exist a **neutral element** of the group, which will here be indicated with e (or more specifically e_G), which satisfies: $\forall g \in G : g \circ e = e \circ g = g$.
2. The operation $\circ$ must be **associative**: $\forall f, g, h \in G : f \circ (g \circ h) = (f \circ g) \circ h$.
3. For each element $g \in G$, there must exist an **inverse** element h such that $g \circ h = h \circ g = e$.

Sometimes the group operation is written as $+$, in which case the neutral element is often denoted as 0. This is called the additive notation. Alternatively, the group operation can be written as $\cdot$, in which case the neutral element is often denoted as 1. This is called the multiplicative notation.

Proposition 1. *The neutral element of a group is necessarily unique.*

Proof. Suppose the group $(G, \circ)$ has two neutral elements for the operation $\circ$, e_A and e_B. By definition of the neutral element, we then must have the following sequence of equalities:

$$e_A = e_A \circ e_B = e_B \,.$$

So, we find that the two neutral elements must be in fact the same element, which is therefore unique. □

Similarly, we find that the inverse of an element is also unique.

Proposition 2. *The inverse of an element in a group is unique.*

Proof. The proof is left as an exercise to the reader. □

The inverse of an element g is often denoted as g^{-1} or $-g$ in the multiplicative and additive notation, respectively.

Exercise 1. *Let $(G, \circ)$ be a group. Show that $\forall g, h \in G$ we have $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$ and $(g^{-1})^{-1} = g$.*

An **Abelian group** is a group for which the operation is commutative, i.e.

$$\forall g, h \in G : g \circ h = h \circ g \,.$$

1.1 Examples

This section discusses some examples of well-known groups.

- $(\mathbb{N}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are all Abelian groups with neutral element 0.
- $(\mathbb{R}_0, \cdot)$ is an Abelian group with neutral element 1.
- The real matrices form an Abelian group with respect to the addition $(\mathbb{R}^{m \times n}, +)$.
- The real matrices do not form a group with respect to the multiplication $(\mathbb{R}^{m \times n}, \cdot)$. Why? Instead, the square invertible matrices form a group with respect to the multiplication. This group is denoted as $(GL(n, \mathbb{R}), \cdot)$.
- The linear functions with $f(x) = ax + b, a \neq 0$, form a group with respect to the composition of functions.
- The cyclic group $(\mathbb{Z}_n, +)$ is a group with n elements that contains a neutral element e and a *generator* a, which generates all the other elements as $a + a, a + a + a, \ldots$, i.e. by repeatedly adding a to itself. Denoting these elements as $e, a^1 \equiv a, a^2 \equiv a + a, \ldots, a^{n-1} \equiv a + a + \cdots + a$, we finally have that $a^{n-1} + a = e$. Often, the elements of this group are denoted $\{0, 1, 2, 3, \ldots, n-1\}$, and then the operation is the regular addition *modulo* n. We will come back to this concept, but for now it is enough to remember that $(n-1) + 1 \equiv 0$.
- The Klein four-group $(V, \oplus)$ is a group with four elements, defined by the following **Cayley table**:

$\oplus$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

  This table should be read as e.g.

$\oplus$	b
a	$a \oplus b$

  This group can be thought of as the symmetry group of a non-square rectangle, as discussed in the lecture.

1.2 Isomorphisms

It is possible to construct larger groups from known smaller groups. A way to do this is by means of the direct product.

Definition 1. *The **direct product** of two groups $(G, \circ)$ and $(H, \star)$ is the group $(G \times H, \square)$, containing elements (g, h) with $g \in G, h \in H$ .The operation $\square$ is defined as*

$$(g_1, h_1)\square(g_2, h_2) = (g_1 \circ g_2, h_1 \star h_2)\,. \tag{2}$$

However, this does not always mean we are making a "new group". Consider the Cayley table of $\mathbb{Z}_2 \times \mathbb{Z}_2$, both equipped with the regular addition. This table is given by

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Comparing this to the Cayley table of the Klein four-group, we see that these have the same structure. This means that, in a way, these groups are the *same*, we just gave the elements different names. To make this more precise, we introduce the concept of an isomorphism.

Definition 2. *Let $(G, \circ)$ and $(H, \star)$ be two groups. A homomorphism from G to H is a map $\phi : G \to H$ that satisfies*

$$\forall g_1, g_2 \in G : \phi(g_1 \circ g_2) = \phi(g_1) \star \phi(g_2)\,. \tag{3}$$

An isomorphism is a homomorphism that is also bijective. In this case, the groups are said to be isomorphic, and we write $G \cong H$.

Note that in equation (3) the operation $\star$ is used for the objects $\phi(g_1)$ and $\phi(g_2)$, as by definition they are elements of H.

Exercise 2. *Given the Cayley tables of $(V, \oplus)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, show that these groups are the same by giving an explicit isomorphism between them.*

Theorem 1. *Given groups $(G, \circ)$ and $(H, \star)$ and a homomorphism $\phi : G \to H$. Denoting the neutral elements with e_G, e_H respectively, we have that*

1. $\phi(e_G) = e_H$,
2. $\phi(g^{-1}) = \phi(g)^{-1}$.

Furthermore, if ϕ is an isomorphism, then the inverse map $\phi^{-1} : H \to G$ is also an isomorphism.

Proof. The proof is left as an exercise to the reader. □

1.3 Subgroups

Definition 3. *A subset H of a group G is called a **subgroup** if it is itself a group with respect to the operation of G.*

Exercise 3. *Show that the set of even integers is a subgroup of the group of integers with respect to addition. Is the set of odd integers also a subgroup?*

Exercise 4. *Determine all subgroups of the cyclic group of order 12, $\mathbb{Z}_{12}$.*

Proposition 3. *Given two groups $(G, \circ)$ and $(H, \star)$, and a homomorphism $\phi : G \to H$. Given any subgroup K of G, the image of K under ϕ is a subgroup of H.*

Proof. We have to show that $\phi(K)$ is a subgroup of H, i.e. we have to show that it is a group. Since K is a group, $e_G \in K$, and therefore $e_H = \phi(e_G) \in \phi(K)$. Associativity of the operation $\star$ is inherited from the fact that H is a group. The set $\phi(K)$ is closed under the operation $\star$ as well: given any two elements of $\phi(K)$, say $\phi(k_1)$ and $\phi(k_2)$, we have that $\phi(k_1) \star \phi(k_2) = \phi(k_1 \circ k_2) \in \phi(K)$. Finally, we need to check that every element of $\phi(K)$ has an inverse in $\phi(K)$. Given an element $\phi(k) \in \phi(K)$, we have that $\phi(k^{-1}) \in \phi(K)$, as $k^{-1} \in K$ since K is a group. Therefore, $\phi(K)$ is a subgroup of H. □

Exercise 5. *Are the following groups isomorphic to $\mathbb{Z}_6$?*

- $\mathbb{Z}_2 \times \mathbb{Z}_3$
- $\mathbb{Z}_3 \times \mathbb{Z}_2$
- S_3. *This is the group of symmetries of an equilateral triangle. The elements of the groups are the reflections (around the axes of symmetry) and the rotations (by $120°$ and $240°$). Start by listing and labelling these basic elements, and form the Cayley table.*

2 Lecture 2: Linear algebra

Having studied groups, we will now impose additional structure on sets to turn them into vector spaces. This is one of the central concepts in the field of linear algebra, which in itself forms the basis of any scientific / engineering degree.

Definition 4. *A **real vector space** is an Abelian group $(V, +)$ that is furthermore equipped with a scalar multiplication*

$$\cdot : \mathbb{R} \times V \to V : (\lambda, v) \mapsto \lambda \cdot v \,. \tag{4}$$

If the distinction between the scalars and group elements is clear, we will often simply denote $\lambda \cdot v$ as λv. The two operations have to satisfy the following properties $\forall v, w \in V, \lambda, \mu \in \mathbb{R}$:

1. *Identity element for scalar multiplication: $1v = v$ for all $v \in V$.*
2. *Distributivity w.r.t. the scalar multiplication: $\lambda \cdot (v + w) = \lambda v + \lambda w$.*
3. *Distributivity w.r.t. the vector addition: $(\lambda + \mu)v = \lambda v + \mu v$.*
4. *Compatibility of scalar multiplication with field multiplication: $(\lambda\mu)v = \lambda(\mu v)$.*

2.1 Examples

Some basic examples include:

- The set of real numbers $\mathbb{R}$ is a vector space with respect to the regular addition and multiplication.
- The set of real matrices $\mathbb{R}^{m\times n}$ is a vector space with respect to the regular matrix addition and scalar multiplication.
- The set of real functions $\mathcal{F}(\mathbb{R}, \mathbb{R})$ (i.e. functions $f : \mathbb{R} \to \mathbb{R}$) is a vector space with respect to the regular function addition and scalar multiplication, defined for all functions $f, g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ and $\lambda \in \mathbb{R}$ as
$$(f + g)(x) = f(x) + g(x)\,, \qquad (\lambda f)(x) = \lambda f(x)\,.$$
- In quantum mechanics, wave functions $|\psi\rangle$ are elements of a *Hilbert space*, which is a vector space with more structure added onto it. They can be added together and multiplied by complex numbers, as for example in the famous example of Schrödinger's cat who is "alive and dead" with wave function
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\text{alive}\rangle + |\text{dead}\rangle)\,.$$

2.2 Linear transformations

Much like we had homomorphisms between groups, we can define linear transformations between vector spaces.

Definition 5. *A **linear transformation** from a vector space V to a vector space W is a map $L : V \to W$ that satisfies the following:*

$$\forall \lambda, \mu \in \mathbb{R}, \forall v, w \in V : L(\lambda v + \mu w) = \lambda L(v) + \mu L(w)\,. \tag{5}$$

Exercise 6. *Show that the composition of two linear transformations is again a linear transformation.*

Theorem 2. *If $L : V \to W$ is a linear transformation, then the following statements are true:*

1. *$L(0_V) = 0_W$.*
2. *$L(-v) = -L(v)$.*

Proof. The first statement follows from the linearity of L:

$$L(0_V) = L(0_V + 0_V) = L(0_V) + L(0_V) \Rightarrow L(0_V) = 0_W \,.$$

The second statement follows from the first, as

$$0_W = L(0_V) = L(v + (-v)) = L(v) + L(-v) \Rightarrow L(-v) = -L(v) \,.$$

□

Exercise 7. *Show that the set of all linear transformations from a vector space V to itself forms a vector space under the regular addition and scalar multiplication of functions. This vector space is denoted as $\mathcal{L}(V)$.*

2.3 Bases of vector spaces

It turns out that vector spaces have a well defined structure, which can be described by a basis. We first need to define the concepts of linear independence and span.

Definition 6. *A set of vectors $\{v_1, \ldots, v_N\}$ is called **linearly independent** if the only way to write the zero vector as a linear combination of these vectors is by setting all the coefficients to zero, i.e.*

$$\sum_{i=1}^{N} \lambda^i v_i = 0 \Rightarrow \forall 1 \leq i \leq N : \lambda^i = 0 \,. \tag{6}$$

*If a set of vectors is not linearly independent, it is called **linearly dependent**.*

For example, the vectors $(1,0), (0,1) \in \mathbb{R}^2$ are linearly independent, as the only way to write the zero vector $(0,0)$ as a linear combination of these vectors is by setting both coefficients to zero. However, the vectors $(1,0), (2,0)$ are not linearly independent, as the zero vector can be written as $1 \cdot (2,0) + (-2) \cdot (1,0) = (0,0)$.

Definition 7. *The **span** of a set of vectors $\{v_1, \ldots, v_N\}$ is the set of all possible linear combinations of these vectors, i.e.*

$$\operatorname{span}\{v_1, \ldots, v_N\} = \left\{ \sum_{i=1}^{N} \lambda^i v_i \mid \lambda^i \in \mathbb{R} \right\} \,. \tag{7}$$

For example, in $\mathbb{R}^3$, the span of the vectors $(1,0,0), (0,1,0)$ is the xy-plane, as any vector in the xy-plane can be written as a linear combination of these two vectors:

$$(x, y, 0) = x \cdot (1,0,0) + y \cdot (0,1,0) \,.$$

Exercise 8. *Show that the span of a set of vectors is a vector space.*

Definition 8. *A set of vectors $\{e_1, \ldots, e_N\}$ is called a **basis** of a vector space V if they are linearly independent and span V.*

Such a basis is in general not unique. However, it turns out that the number of basis vectors is fixed for a given vector space. Once a basis is chosen, any vector in the vector space can be written as a linear combination of the basis vectors, and this representation is unique.

Theorem 3. *Given a basis $\{e_1, \ldots, e_N\}$ of a vector space V, any vector $v \in V$ can be written as*

$$v = \sum_{i=1}^{N} v^i e_i \tag{8}$$

in a unique way.

Proof. Suppose that v can be written in two ways, i.e.

$$v = \sum_{i=1}^{N} v^i e_i \,,$$
$$v = \sum_{i=1}^{N} w^i e_i \,.$$

Subtracting the two expressions, we find that

$$0 = \sum_{i=1}^{N} (v^i - w^i) e_i \,.$$

Since the basis vectors are linearly independent, we must have that $v^i - w^i = 0$ for all i. □

The proof of the following theorem would take us too far, but forms a cornerstone of the field of linear algebra.

Theorem 4. *Every vector space V admits a basis. The **dimension** of a vector space V is the number of basis vectors in any basis of V. This number is denoted as $\dim(V)$. If the dimension is finite, we say that the vector space is **finite-dimensional**.*

The following theorem is a direct consequence of the definition of a basis.

Theorem 5. *A linear transformation $L : V \to W$ is completely determined by its action on the basis vectors.*

Proof. Take a basis of the N-dimensional vector space V, $\{e_1, \ldots, e_N\}$. Then any vector $v \in V$ can be written as $v = \sum_{i=1}^{N} v^i e_i$. The linear transformation acting on v then satisfies

$$L(v) = \sum_{i=1}^{N} v^i L(e_i)$$

Therefore, once the linear transformation of the basis vectors is known, it is known for all the vectors. □

We can also create linear maps between different vector spaces.

Theorem 6. *Any vector space V is isomorphic to $\mathbb{R}^N$ for $N = \dim(V)$.*

Proof. Take a basis of V, $\{e_1, \ldots, e_N\}$. Then any vector $v \in V$ can be written as $v = \sum_{i=1}^{N} v^i e_i$. The map $\phi : V \to \mathbb{R}^N$ that sends v to the vector $(v^1, \ldots, v^N)$ is an isomorphism. This means we implicitly take the standard basis of $\mathbb{R}^N$, which is the set of vectors $(1, 0, 0, \ldots), (0, 1, 0, \ldots), \ldots$. □

3 References

These notes are based on my own knowledge of these basic mathematical concepts, and the writing has been accelerated by the use of *Github copilot* and its implementation in VSCode. Inspiration has been taken from the course notes for *"Algebraische Structuren"* (Algebraic Structures), used in the first year of the Bachelor of Mathematics at the KU Leuven, at the time taught by Prof. Raf Cluckers - also the author of the lecture notes. The section on PageRank has been based on (among others) this and this link. Proofs with respect to the spectrum of the linking matrix have been inspired by this link.