

Algebra Lineal

Manuel Castillo-Lopez

manucalop@gmail.com

Copyright © (2018 - 2019) Manuel Castillo López.

GPL GNU General Public License

September 9, 2019

Abstract

The role of mathematics in science is about casting our concepts about the real world into rigorous mathematical form. But, science doesn't do that for its own sake. It does so, in order to fully explore the implications of what our concepts about the real world are. To certain extent, the spirit of science can be casted into the words of Ludwig Wittgenstein, who said: *What we cannot speak about clearly then we must pass over in silence.* Indeed, if we have concepts about the real world and it's not possible to cast them into precise mathematical language, that is usually an indicator that some aspects of these concepts have not been well understood. But then mathematics is just that, a language. And, if we want to extract physical conclusions from this formulation we must interpret that language. But again citing Wittgenstein: *The theorems of mathematics all say the same: namely nothing.* Obviously, he didn't mean that mathematics is useless. He just refers to the fact that if we have a theorem of the type: A if and only if B . A and B being propositions, then obviously B says nothing else than A does. And A says nothing else than B does. This is what is called in mathematics a tautology. However psychologically, for our understanding of A , it may be very useful to have a reformulation of A in terms of B .

Thus, with the understanding that mathematics just gives us a language for what we want to do, the objective of the course is to provide proper mathematical language to build the concepts addressed later on by the different sciences.

Contents

Abstract	iii
Index	v
1 Axiomatic set theory	1
1.1 Propositional logic	1
1.2 Predicate logic	3
1.3 Axiomatic System and theory of proofs	4
1.4 The \in -relation	5
1.5 Zermelo-Fraenkel axioms of set theory	5
1.5.1 Axiom on the \in -relation	5
1.5.2 Axiom on the existence of an empty set	5
1.5.3 Axiom on pair sets	6
1.5.4 Axiom on union sets	6
1.5.5 Axiom of replacement	6
1.5.6 Axiom on the existence of power sets	7
1.5.7 Axiom of infinity	7
1.5.8 Axiom of choice	7
2 Classification of sets	9
2.1 Maps	9
2.2 Equivalence relations	11
2.3 Construction of \mathbb{N} , \mathbb{Z} , \mathbb{Q} and \mathbb{R}	12
3 Algebraic structures	15
4 Conceptos básicos I	17
4.1 Conjuntos	17
4.2 Relaciones binarias	22
4.3 Principio de Inducción	27
4.4 Aplicaciones	28

2	Estructuras algebraicas	31
2.1	Operación interna	31
2.2	Operación externa	32
2.3	Homomorfismos	32
2.4	Grupo	33
2.5	Anillo	36
3	Espacios Vectoriales y Aplicaciones lineales	39
3.1	Espacio vectorial	39
3.2	Subespacio vectorial	41
3.3	Dependencia e independencia lineal	43
3.3.1	Sistema generador	43
3.3.2	Base	43
3.3.3	Base de un subespacio	43
3.3.4	Coordenadas y cambio de base	43
3.4	Operaciones con subespacios	43
3.5	Aplicación lineal	43
3.5.1	Matriz de una aplicación lineal	43
3.5.2	Matriz de una composición	43
3.5.3	Cambio de base en aplicaciones lineales	43
3.5.4	Núcleo e imagen de una aplicación lineal	43
3.6	Matrices y determinantes	43
3.7	Sistemas y ecuaciones lineales	43
3.7.1	Teorema de Rouché-Fröbenius	43
3.7.2	Regla de Cramer	43
3.7.3	Método de Gauss	43
3.7.4	Factorización LU	43
4	Formas bilineales y cuadráticas	49
4.1	Formas bilineales	49
4.2	Perpendicularidad u ortogonalidad	50
4.3	Matriz de una forma bilineal	50
4.4	Bases ortogonales	50
4.5	Formas bilineales simétricas	51
4.6	Formas cuadráticas	51
4.7	Matriz de una forma cuadrática	51
4.8	Isometrías	52
4.9	Transformaciones ortogonales	52

5	Espacio afín y euclídeo. Movimientos	53
5.1	Espacios afines	53
5.2	Transformaciones afines y afinidades	54
5.3	Matrices	54
5.4	Transformaciones ortogonales y movimientos	54
5.5	Orientación	55
5.6	Movimientos en el plano afín euclídeo	55
5.7	Movimientos en el espacio afín euclídeo	55
6	Cónicas y cuádricas	57
6.1	Estudio afín de las cónicas	57
6.2	Estudio afín de las cuádricas	57
7	Álgebra lineal numérica	59
7.1	Normas matriciales	59
7.2	Métodos de Jacobi y Gauss-Seidel	59
7.3	Factorización de matrices LU y QR	60
7.4	Estimación de errores	60
7.5	Implementación de algoritmos	60
7.6	Cálculo de autovalores y autovectores	61
8	Geometría diferencial	63
8.1	Curvas y superficies en el espacio	63
8.2	Triedro de Frenet	64
8.3	Curvatura de Gauss y media	64
	Bibliography	64

Chapter 1

Axiomatic set theory

Any space, such as the physical space, is a set "of points" equipped with further structure. But what precisely is a set? Well, one can think of a set as a collection of elements, but that raises the question of what a collection is and what elements are. So certainly we need to do better and, as a fundamental problem, if we start writing a book about mathematics whose pages are all empty yet, what could the first definition be? For a definition you need notions that you already have in order to define a new notion but, if you don't have any notion yet, how do you start? The trick is to start axiomatically, and to do so we will write axiomatic set theory. Again, this raises the question, in what language could you possibly do that? Then, we need another building block called propositional logic, which will allow us to write the axioms of set theory.

1.1 Propositional logic

The key notion of propositional logic is a proposition.

Definition 1. A **proposition** p is a variable¹ that can take the values true (T) or false (F). No other.

This is what a proposition is, from the point of view of propositional logic. In particular, it is not the task of propositional logic to decide whether a complex statement of the form: *there is extra-terrestrial life* is true or not. Propositional logic already deals with the complete proposition and it just assumes that is either true or false. Certainly, one can build new propositions from given ones by means of **logical operators**. The simplest kind of logical

¹By this we mean a formal expression, with no extra structure assumed.

operators are unary operators. A unary operator takes one proposition and makes from it a new proposition. We define them in the following table:

p	$\neg p$	$\text{id}(p)$	$\top p$	$\perp p$	
F	T	F	T	F	\neg NOT
T	F	T	T	F	id Identity
					\top Tautology
					\perp Contradiction

Table 1.1: Unary operators

One can quickly check that, if p can only be true or false, these operators cover all the possibilities to define a unary operator. The next step is to consider binary operators, i.e. operators that take two propositions and return a new one. We have 16 binary operators in total, but we draw some interesting ones in the following table:

p	q	$p \wedge q$	$p \vee q$	$p \underline{\vee} q$	$p \Rightarrow q$	$p \Leftrightarrow q$	
F	F	F	F	F	T	T	\wedge AND
F	T	F	T	T	T	F	\vee OR
T	F	F	T	T	F	F	$\underline{\vee}$ EX-OR
T	T	T	T	F	T	T	\uparrow NAND (not AND)
							\Rightarrow Implication
							\Leftrightarrow Equivalence

Table 1.2: Some binary operators

Remark 1. *All higher order operators can be constructed from the single NAND operator.*

We point out the importance of the implication arrow, which is frequently ill-understood. The implication arrow is a binary operator that takes two propositions and constructs a new one that, in total, is true or false, as defined in the previous table.

Remark 2. *From the implication operator, one can conclude anything based on false assumptions, also known as "ex falso quodlibet".*

Then one may wonder why on Earth would you define the implication arrow like this. The answer is hidden in the following theorem:

Theorem 1.1.1. *Let p, q be propositions. Then $(p \Rightarrow q) \Leftrightarrow ((\neg q) \Rightarrow (\neg p))$.*

Proof. We need only to construct the truth table and see that the two last propositions are identical:

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$(\neg q) \Rightarrow (\neg p)$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	F	F
T	T	F	F	T	T

□

Corollary 1.1.1.1. *We can prove assertions by way of contradiction. E.g. assume that p is true and we want to prove that q is true. Then, what we can do instead, and is fully equivalent, is to assume that what we want to prove is not true, and then prove that the assumption is not true. Then we say we have a contradiction and q must have been true.*

1.2 Predicate logic

Definition 2. A **predicate** is (informally) a proposition-valued function of some variables(s). In particular, a predicate of two variables is called a *relation*.

For example, $Q(x, y)$ is a proposition which value depends on the variables x and y . Just like for propositional logic, it is not the task of predicate logic to examine how predicates are built from the variables on which they depend. Since the notions of set theory have not been yet defined, we leave it completely open, and simply consider x and y formal variables, with no extra conditions imposed. As with propositions, we can construct new predicates from given ones by means of the operators defined in the previous section. For example, we might have:

Example 1. $Q(x, y, z) :\Leftrightarrow P(x) \wedge R(y, z)$

More interestingly, we can construct a new proposition from a given predicate by using *quantifiers*². Let $P(x)$ be a predicate. Then, one can define the proposition

$$p :\Leftrightarrow \forall x : P(x)$$

²A quantifier is a language object that specify the elements that satisfy a given predicate.

by using the **universal quantifier** \forall . This means that the proposition p is true *iff*, for every preposition x , the predicate $P(x)$ is true. p is false otherwise.

Then, we can define the **existential quantifier** \exists and the **unique existential quantifier** $\exists!$ by:

$$\exists x : P(x) :\Leftrightarrow \neg(\forall x : \neg P(x)).$$

$$\exists! x : P(x) :\Leftrightarrow (\exists x : \forall y : P(y) \Leftrightarrow x = y)$$

1.3 Axiomatic System and theory of proofs

Definition 3. An **axiom** a or *assumption* is a proposition p taken to be true, i.e. a tautology of p ($a = T(p)$).

Definition 4. An **axiomatic system** is a finite sequence of axioms a_1, a_2, \dots, a_N .

Definition 5. A **proof** of a proposition p within an axiomatic system a_1, a_2, \dots, a_N is a finite sequence of propositions q_1, q_2, \dots, q_M such that $q_M = p$ and for any $1 \leq j \leq M$ one of the following is satisfied:

(A) q_j is a proposition from the list of axioms;

(T) q_j is a tautology;

(M) $\exists 1 \leq m, n < j : (q_m \wedge q_n \Rightarrow q_j)$ is true. This is called *modus ponens* or *deduction rule*.

Remark 3. If p can be proven within an axiomatic system a_1, a_2, \dots, a_N , we write:

$$a_1, a_2, \dots, a_N \vdash p$$

and we read “ a_1, a_2, \dots, a_N proves p ”.

Definition 6. An axiomatic system a_1, a_2, \dots, a_N is said to be *consistent* if there exists a proposition q which cannot be proven from the axioms.

$$\exists q : \neg(a_1, a_2, \dots, a_N \vdash q).$$

Theorem 1.3.1. Propositional logic is consistent.

Theorem 1.3.2 (Godel). Any axiomatic system powerful enough to encode elementary arithmetic is either inconsistent or contains an undecidable proposition, i.e. a proposition that can be neither proven nor disproven within the system.

1.4 The \in -relation

Set theory is built on the postulate that there is a fundamental relation (i.e. a predicate of two variables) denoted by \in . However, there is no definition of what \in is, or of what a set is. Instead, nine axioms concerning \in and sets formulate the set theory upon which all modern mathematics are built. This axiomatic system is called **Zermelo-Fraenkel set theory**. As an overview, we have:

- 2 basic existence axioms, one about the \in relation and the other about the existence of the empty set;
- 4 construction axioms, which establish rules for building new sets from given ones. They are the pair set axiom, the union set axiom, the replacement axiom and the power set axiom;
- 2 further existence/construction axioms, these are slightly more advanced and newer compared to the others;
- 1 axiom of foundation, excluding some constructions as not being sets.

Using the \in -relation we can immediately define the following relations:

- $x \notin y :\Leftrightarrow \neg(x \in y)$
- $x \subseteq y :\Leftrightarrow \forall a : (a \in x \Rightarrow a \in y)$
- $x = y :\Leftrightarrow (x \subseteq y) \wedge (y \subseteq x)$
- $x \subset y :\Leftrightarrow (x \subseteq y) \wedge \neg(x = y)$

1.5 Zermelo-Fraenkel axioms of set theory

1.5.1 Axiom on the \in -relation

The expression $x \in y$ is a proposition if, and only if, both x and y are sets.

$$\forall x : \forall y : (x \in y) \vee \neg(x \in y).$$

1.5.2 Axiom on the existence of an empty set

There exists a set that contains no elements.

$$\exists y : \forall x : x \notin y.$$

Theorem 1.5.1. *This set is unique and is called the empty set \emptyset .*

1.5.3 Axiom on pair sets

Let x and y be sets. Then there exists a set that contains as its elements precisely x and y

$$\forall x : \forall y : \exists m : \forall u : (u \in m \Leftrightarrow (u = x \vee u = y)).$$

The set m is called the *pair set* of x and y and it is denoted by $\{x, y\}$.

1.5.4 Axiom on union sets

Let x be a set. Then there exists a set whose elements are precisely the elements of the elements of x .

$$\forall x : \exists u : \forall y : (y \in u \Leftrightarrow \exists s : (y \in s \wedge s \in x))$$

The set u is denoted by $\bigcup x$, called union of the elements of x .

1.5.5 Axiom of replacement

Let R be a functional relation and let m be a set. Then the image of m under R , denoted by $\text{im}_R(m)$, is again a set.

Definition 7. A relation R is said to be **functional** if:

$$\forall x : \exists! y : R(x, y).$$

Definition 8. Let m be a set and let R be a functional relation. The **image** of m under R consists of all those y for which there is an $x \in m$ such that $R(x, y)$.

Theorem 1.5.2. Let $P(x)$ be a predicate and let m be a set. Then, $\{y \in m \mid P(y)\}$ is a set. This is called **principle of restricted comprehension** and is a consequence of the axiom of replacement.

The principle of restricted comprehension is not to be confused with the “principle” of universal comprehension which states that $\{y \mid P(y)\}$ is a set for any predicate. This has shown to be inconsistent by Russell. Observe that the $y \in m$ condition makes it so that $\{y \in m \mid P(y)\}$ cannot have more elements than m itself.

Definition 9. Let x be a set. Then we define the **intersection** of x by:

$$\bigcap x := \{a \in \bigcup x \mid \forall b \in x : a \in b\}.$$

If $a, b \in x$ and $\bigcap x = \emptyset$, then a and b are said to be *disjoint*.

Definition 10. Let u and m be sets such that $u \subseteq m$. Then the **complement** of u relative to m is defined as “ m without u ”:

$$m \setminus u := \{x \in m \mid x \notin u\}.$$

These are both sets by the principle of restricted comprehension, which is ultimately due to axiom of replacement.

1.5.6 Axiom on the existence of power sets

Let m be a set. Then there exists a set, denoted by $\mathcal{P}(m)$, whose elements are precisely the subsets of m .

Example 2. Let $m = \{a, b\}$. Then $\mathcal{P}(m) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

1.5.7 Axiom of infinity

There exists a set that contains the empty set and, together with every other element y , it also contains the set $\{y\}$ as an element.

$$\exists x : \emptyset \in x \wedge \forall y : (y \in x \Rightarrow \{y\} \in x).$$

Corollary 1.5.2.1. Let us consider one such set x . Then $\emptyset \in x$ and hence $\{\emptyset\} \in x$. Thus, we also have $\{\{\emptyset\}\} \in x$ and so on. Therefore:

$$x = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}.$$

We can introduce the following notation for the elements of x :

$$0 := \emptyset, \quad 1 := \{\emptyset\}, \quad 2 := \{\{\emptyset\}\}, \quad 3 := \{\{\{\emptyset\}\}\}, \quad \dots$$

to construct the set $\mathbb{N} := x$ and $\mathbb{R} := \mathcal{P}(\mathbb{N})$ as known as the set of natural and real numbers respectively.

1.5.8 Axiom of choice

Let x be a set whose elements are non-empty and mutually disjoint. Then there exists a set y which contains exactly one element of each element of x .

$$\forall x : P(x) \Rightarrow \exists y : \forall a \in x : \exists! b \in a : a \in y,$$

where $P(x) \Leftrightarrow (\exists a : a \in x) \wedge (\forall a : \forall b : (a \in x \wedge b \in x) \Rightarrow \bigcap \{a, b\} = \emptyset)$.

Remark 4. *The axiom of choice is independent of the other 8 axioms, which means that one could have set theory with or without the axiom of choice. However, there are important theorems that can only be proved by using the axiom of choice.*

Axiom of foundation. *Every non-empty set x contains an element y that has none of its elements in common with x . In symbols:*

$$\forall x : (\exists a : a \in x) \Rightarrow \exists y \in x : \bigcap \{x, y\} = \emptyset.$$

An immediate consequence of this axiom is that there is no set that contains itself as an element.

Chapter 2

Classification of sets

2.1 Maps

A recurrent theme in mathematics is the classification of *spaces* by means of structure-preserving *maps* between them.

Definition 11. Let A, B be sets. A **map** $\phi : A \rightarrow B$ is a relation such that for each $a \in A$ there exists exactly one $b \in B$ such that $\phi(a, b)$ holds.

The standard notation for a map is:

$$\begin{aligned}\phi : A &\rightarrow B \\ a &\mapsto \phi(a)\end{aligned}\tag{2.1}$$

The following is standard terminology for a map $\phi : A \rightarrow B$:

- the set A is called the **domain** of ϕ ;
- the set B is called the **target** of ϕ ;
- the set $\phi(A) \equiv \text{im}_\phi(A) := \{\phi(a) \mid a \in A\}$ is called the **image** of A under ϕ .

Definition 12. A **map** $\phi : A \rightarrow B$ is said to be:

- **injective** if $\forall a_1, a_2 \in A : \phi(a_1) = \phi(a_2) \Rightarrow a_1 = a_2$;
- **surjective** if $\text{im}_\phi(A) = B$;
- **bijective** if it is both injective and surjective.

Definition 13. Two sets A and B are called **(set-theoretic) isomorphic** if there exists a bijection $\phi : A \rightarrow B$. In this case, we write $A \cong_{\text{set}} B$.

Bijections are the “structure-preserving” maps for sets. Intuitively, they pair up the elements of A and B and a bijection between A and B exists only if A and B have the same “size”. This is clear for finite sets, but it can also be extended to infinite sets.

Definition 14 (Classification of sets). *A set A is:*

- **infinite** if there exists a proper subset $B \subset A$ such that $B \cong_{\text{set}} A$. In particular, if A is infinite, we further define A to be:
 - * **countably** infinite if $A \cong_{\text{set}} \mathbb{N}$;
 - * **uncountably** infinite otherwise.
- **finite** if it is not infinite. In this case, we have $A \cong_{\text{set}} \{1, 2, \dots, N\}$ for some $N \in \mathbb{N}$ and we say that the **cardinality** of A , denoted by $|A|$, is N .

Given two maps $\phi : A \rightarrow B$ and $\psi : B \rightarrow C$, we can construct a third map, called the **composition** of ϕ and ψ , denoted by $\psi \circ \phi$, defined by:

$$\begin{aligned} \psi \circ \phi : A &\rightarrow C \\ a &\mapsto \psi(\phi(a)). \end{aligned} \tag{2.2}$$

This is often represented by drawing the following diagram

$$\begin{array}{ccc} & B & \\ \phi \nearrow & & \searrow \psi \\ A & \xrightarrow{\psi \circ \phi} & C \end{array}$$

and by saying that “the diagram commutes” means that all paths connecting two nodes in the diagram are equivalent.

Proposition 1. *Composition of maps is associative.*

Definition 15. *Let $\phi : A \rightarrow B$ be a bijection. Then the **inverse** of ϕ , denoted ϕ^{-1} , is defined (uniquely) by:*

$$\phi^{-1} \circ \phi = id_A$$

$$\phi \circ \phi^{-1} = id_B.$$

Equivalently, we say that this diagram commutes:

$$\begin{array}{ccc} \text{id}_A \hookrightarrow A & \begin{array}{c} \xrightarrow{\phi} \\ \xleftarrow{\phi^{-1}} \end{array} & B \hookleftarrow \text{id}_B \end{array}$$

The inverse map is only defined for bijections. However, the following notion, which we will often meet in topology, is defined for any map.

Definition 16. Let $\phi : A \rightarrow B$ be a map and let $V \subseteq B$. Then we define the set:

$$\text{preim}_\phi(V) := \{a \in A \mid \phi(a) \in V\}$$

called the **pre-image** of V under ϕ .

Proposition 2. Let $\phi : A \rightarrow B$ be a map, let $U, V \subseteq B$ and $C = \{C_j \mid j \in J\} \subseteq \mathcal{P}(B)$. Then:

- i) $\text{preim}_\phi(\emptyset) = \emptyset$ and $\text{preim}_\phi(B) = A$;
- ii) $\text{preim}_\phi(U \setminus V) = \text{preim}_\phi(U) \setminus \text{preim}_\phi(V)$;
- iii) $\text{preim}_\phi(\bigcup C) = \bigcup_{j \in J} \text{preim}_\phi(C_j)$ and $\text{preim}_\phi(\bigcap C) = \bigcap_{j \in J} \text{preim}_\phi(C_j)$.

2.2 Equivalence relations

Definition 17. Let M be a set and let \sim be a relation such that the following conditions are satisfied:

- i) *reflexivity*: $\forall m \in M : m \sim m$;
- ii) *symmetry*: $\forall m, n \in M : m \sim n \Leftrightarrow n \sim m$;
- iii) *transitivity*: $\forall m, n, p \in M : (m \sim n \wedge n \sim p) \Rightarrow m \sim p$.

Then \sim is called an **equivalence relation** on M .

Example 3. Consider the following wordy examples.

- a) $p \sim q :\Leftrightarrow p$ is of the same opinion as q . This relation is reflexive, symmetric and transitive. Hence, it is an equivalence relation.
- b) $p \sim q :\Leftrightarrow p$ is a sibling of q . This relation is symmetric and transitive but not reflexive and hence, it is not an equivalence relation.

- c) $p \sim q :\Leftrightarrow p$ is taller q . This relation is transitive, but neither reflexive nor symmetric and hence, it is not an equivalence relation.

Definition 18. Let \sim be an equivalence relation on the set M . Then, for any $m \in M$, we define the set:

$$[m] := \{n \in M \mid m \sim n\}$$

called the **equivalence class** of m . Note that the condition $m \sim n$ is equivalent to $n \sim m$ since \sim is symmetric.

Proposition 3. Let \sim be an equivalence relation on M . Then:

- i) $a \in [m] \Rightarrow [a] = [m]$;
- ii) either $[m] = [n]$ or $[m] \cap [n] = \emptyset$.

Definition 19. Let \sim be an equivalence relation on M . Then we define the **quotient set** of M by \sim as:

$$M/\sim := \{[m] \mid m \in M\}.$$

This is indeed a set since $[m] \subseteq \mathcal{P}(M)$ and hence we can write more precisely:

$$M/\sim := \{[m] \in \mathcal{P}(M) \mid m \in M\}.$$

Then clearly M/\sim is a set by the power set axiom and the principle of restricted comprehension.

Remark 5. Due to the axiom of choice, there exists a complete system of representatives for \sim , i.e. a set R such that $R \cong_{\text{set}} M/\sim$.

Remark 6. Care must be taken when defining maps whose domain is a quotient set if one uses representatives to define the map. In order for the map to be **well-defined** one needs to show that the map is independent of the choice of representatives.

2.3 Construction of \mathbb{N} , \mathbb{Z} , \mathbb{Q} and \mathbb{R}

Recall that, invoking the axiom of infinity, we defined:

$$\mathbb{N} := \{0, 1, 2, 3, \dots\},$$

where:

$$0 := \emptyset, \quad 1 := \{\emptyset\}, \quad 2 := \{\{\emptyset\}\}, \quad 3 := \{\{\{\emptyset\}\}\}, \quad \dots$$

We would now like to define an addition operation on \mathbb{N} by using the axioms of set theory. We will need some preliminary definitions.

Definition 20. The successor map S on \mathbb{N} is defined by:

$$\begin{aligned} S : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto \{n\} \end{aligned}$$

Definition 21. The predecessor map S on $\mathbb{N}^* := \mathbb{N} \setminus \emptyset$ is defined by:

$$\begin{aligned} S : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto m \quad \text{such that } \{m\} = n \end{aligned}$$

Definition 22. Let $n \in \mathbb{N}$. The n -th power of S , denoted S^n , is defined recursively by:

$$\begin{aligned} S^n &:= S \circ S^{P(n)} && \text{if } n \in \mathbb{N}^* \\ S^0 &:= id_{\mathbb{N}} \end{aligned}$$

We are now ready to define addition.

Definition 23. The addition operation on \mathbb{N} is the map:

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \\ (m, n) &\mapsto m + n := S^n(m). \end{aligned}$$

Definition 24. Let \sim be the equivalence relation on $\mathbb{N} \times \mathbb{N}$ defined by:

$$(m, n) \sim (p, q) :\Leftrightarrow m + q = p + n.$$

Definition 25. We define the set of integers by:

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim.$$

The intuition behind this definition is that the pair (m, n) stands for “ $m - n$ ”. In other words, we represent each integer by a pair of natural numbers whose (yet to be defined) difference is precisely that integer. There are, of course, many ways to represent the same integer with a pair of natural numbers in this way. For instance, the integer -1 could be represented by $(1, 2)$, $(2, 3)$, $(112, 113)$, \dots

Remark 7. In a first introduction to set theory it is not unlikely to find the claim that the natural numbers are part of the integers, i.e. $\mathbb{N} \subseteq \mathbb{Z}$. However, according to our definition, this is obviously nonsense since \mathbb{N} and $\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim$ contain entirely different elements. What is true is that \mathbb{N} can be embedded into \mathbb{Z} , i.e. there exists an inclusion map ι , given by:

$$\begin{aligned} \iota : \mathbb{N} &\hookrightarrow \mathbb{Z} \\ n &\mapsto [(n, 0)] \end{aligned}$$

and it is in this sense that \mathbb{N} is included in \mathbb{Z} .

Definition 26. Let $n := [(n, 0)] \in \mathbb{Z}$. Then we define the inverse of n to be $-n := [(0, n)]$.

We would now like to inherit the $+$ operation from \mathbb{N} .

Definition 27. We define the addition of integers $+_{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ by:

$$[(m, n)] +_{\mathbb{Z}} [(p, q)] := [(m + p, n + q)].$$

Definition 28. In a similar fashion, we define the set of rational numbers by:

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*) / \sim,$$

where $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ and \sim is a relation on $\mathbb{Z} \times \mathbb{Z}^*$ given by:

$$(p, q) \sim (r, s) :\Leftrightarrow ps = qr,$$

assuming that a multiplication operation on the integers has already been defined.

We also have the *canonical embedding* of \mathbb{Z} into \mathbb{Q} :

$$\begin{aligned} \iota : \mathbb{Z} &\hookrightarrow \mathbb{Q} \\ p &\mapsto [(p, 1)] \end{aligned}$$

Definition 29. We define the addition of rational numbers $+_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ by:

$$[(p, q)] +_{\mathbb{Q}} [(r, s)] := [(ps + rq, qs)]$$

and multiplication of rational numbers by:

$$[(p, q)] \cdot_{\mathbb{Q}} [(r, s)] := [(pr, qs)],$$

where the operations of addition and multiplication that appear on the right hand sides are the ones defined on \mathbb{Z} . It is again necessary (but easy) to check that these operations are both well-defined.

There are many ways to construct the reals from the rationals. One is to define a set \mathcal{A} of *almost homomorphisms* on \mathbb{Z} and hence define:

$$\mathbb{R} := \mathcal{A} / \sim,$$

where \sim is a “suitable” equivalence relation on \mathcal{A} .

Chapter 3

Algebraic structures

Chapter 4

Conceptos básicos I

Para comenzar el estudio del álgebra lineal, es preciso introducir conceptos pertenecientes al álgebra abstracta:

4.1 Conjuntos

Un conjunto es una reunión de determinados objetos bien definidos y diferenciables los unos de los otros. A modo de ejemplo tenemos los siguientes conjuntos numéricos:

- Los números naturales: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- Los números enteros: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- Los números racionales: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$
- Los números irracionales: $\mathbb{I} = \{\sqrt{2}, \sqrt{5}, \pi, e, \dots\}$
- Los números reales: $\mathbb{R} = \{\mathbb{Q} \cup \mathbb{I}\}$
- Los números complejos: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$

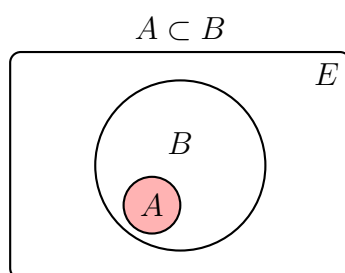
Sea A un conjunto numérico. Denotaremos por A^* al conjunto de elementos de A salvo el cero, mientras que A^+ y A^- designan a los elementos positivos y negativos de A respectivamente. Por ejemplo, $\mathbb{N}^* = \{1, 2, 3, \dots\} = \mathbb{Z}^+$, $\mathbb{Z}^- = \{\dots, -3, -2, -1\}$

Al número de elementos de A lo denominamos cardinal de A y se denota por $\text{card}(A)$

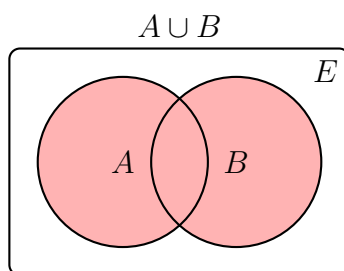
Operaciones entre conjuntos

Sean A y B como dos conjuntos contenidos en un tercero E . Las operaciones básicas que se pueden realizar entre ellos son las siguientes:

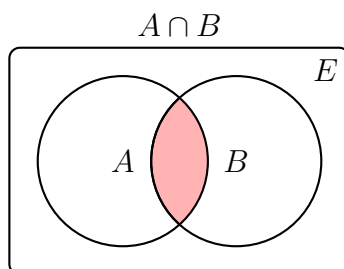
- Inclusión: $A \subset B \equiv \{x : x \in A \Rightarrow x \in B\}$



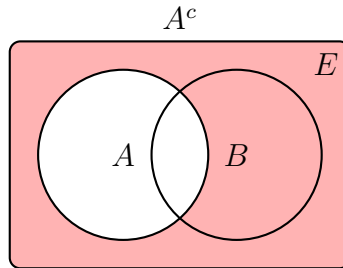
- Unión: $A \cup B \equiv \{x : x \in A \text{ ó } x \in B\}$



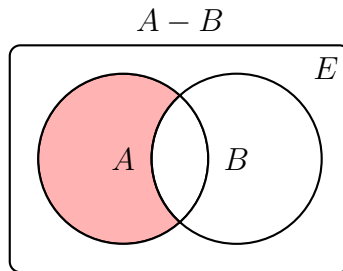
- Intersección: $A \cap B \equiv \{x : x \in A \text{ y } x \in B\}$



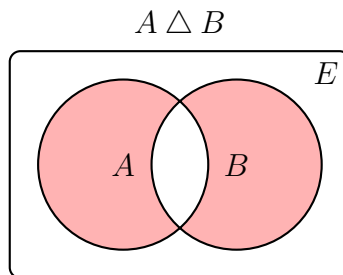
- Contrario o complementario: $A^c = \overline{A} \equiv \{x : x \notin A\}$



- Diferencia: $A - B = A \setminus B = A \cap B^c = A - (A \cap B) \equiv \{x \in A : x \notin B\}$



- Diferencia simétrica: $A \triangle B = (A - B) \cup (B - A)$



Para operar con n conjuntos emplearemos las siguientes notaciones:

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup \dots \cup A_n \quad \forall i \neq j$$

$$\bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap \dots \cap A_n$$

Ejemplo:

Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{1, 3, 6, 7, 9\}$ y $B = \{2, 3, 5, 7, 10\}$.
Entonces:

- $A \cup B = \{1, 2, 3, 5, 6, 7, 9, 10\}$
- $A \cap B = \{3, 7\}$
- $A^c = \{2, 4, 5, 8, 10\}$, $B^c = \{1, 4, 6, 8, 9\}$
- $A - B = \{1, 6, 9\}$, $B - A = \{2, 5, 10\}$
- $A \triangle B = \{1, 2, 5, 6, 9, 10\}$

Partición de un conjunto

Particionar un conjunto E consiste en dividirlo en subconjuntos tales que:

1.

$$A_i \cap A_j = \emptyset$$

2.

$$E = \bigcup_{i=1}^n A_i$$

Ejemplo:

Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ podemos partitionarlo, por ejemplo, en tres subconjuntos de diferentes tamaños: $A = \{1, 2\}$, $B = \{3, 5, 7\}$ y $C = \{4, 6, 8, 9, 10\}$. De ésta manera se cumple que:

- $A \cap B = \emptyset$, $A \cap C = \emptyset$ y $B \cap C = \emptyset$
- $E = A \cup B \cup C$

También podemos comprobar que el cardinal de un conjunto es la suma del cardinal de sus particiones: $\text{card}(E) = \text{card}(A) + \text{card}(B) + \text{card}(C) = 2 + 3 + 5 = 10$.

Producto cartesiano

Sean dos conjuntos A y B . Se define el producto cartesiano $A \times B$ al conjunto de todos los pares ordenados (a, b) en los que el primer componente pertenece a A y el segundo a B , es decir:

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Ejemplo:

Sean dos conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3, 4\}$. Entonces:

$$A \times B = \left\{ \begin{pmatrix} (a, 1) & (a, 2) & (a, 3) & (a, 4) \\ (b, 1) & (b, 2) & (b, 3) & (b, 4) \\ (c, 1) & (c, 2) & (c, 3) & (c, 4) \end{pmatrix} \right\}$$

Propiedades de los conjuntos

Para facilitar la comprensión de algunas de las siguientes propiedades podemos utilizar las semejanzas entre las propiedades de las operaciones de conjuntos y las operaciones numéricas. Así, la unión se asemeja a la suma numérica, la intersección al producto, el conjunto vacío sería el equivalente del cero y el complementario equivaldría a un cambio de signo.

Sean dos subconjuntos A , B y C pertenecientes al conjunto E . Se dice que las partes de E $P(E)$ forman un Álgebra de Boole si se cumplen las siguientes propiedades.

1. Idempotente: $A \cap A = A$ $A \cup A = A$
2. De complemento: $A \cap A^c = \emptyset$ $A \cup A^c = E$
3. Conmutativa: $A \cap B = B \cap A$ $A \cup B = B \cup A$
4. Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$
5. Distributiva: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. Elemento absorbente: $A \cap \emptyset = \emptyset$ $A \cup E = E$
7. Elemento neutro: $A \cup \emptyset = A$ $A \cap E = A$
8. Simplificativa: $A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$
9. Leyes de Morgan: $(A \cup B)^c = A^c \cap B^c$ $(A \cap B)^c = A^c \cup B^c$

El lector puede comprobar el cumplimiento de todas estas propiedades gráficamente o numéricamente definiendo los conjuntos A , B , C y E .

4.2 Relaciones binarias

Se denomina relación binaria a la vinculación de dos elementos (a y b por ejemplo) y se denota por aRb .

Sean dos conjuntos A y B . Se llama grafo a cualquier subconjunto G del producto cartesiano $A \times B$.

$$G \subset A \times B$$

Se dirá que $a \in A$ está relacionado con $b \in B$ a través de G ($aR_G b$) si el par ordenado (a, b) pertenece a G .

$$aR_G b \Leftrightarrow (a, b) \in G$$

Ejemplo:

Tomemos el mismo ejemplo que usamos para el producto cartesiano. Sean dos conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3, 4\}$. Definiremos el grafo

$$G = \{(a, 1), (b, 2), (b, 3), (c, 3), (c, 4)\}$$

De ésta manera, tenemos en G qué elementos de A que están relacionados con qué elementos de B mediante pares ordenados (a, b) . Así tenemos, por ejemplo, que $bR_G 2$ y que $cR_G 3$.

Otra forma de establecer una relación es mediante una propiedad p . Así diremos que

$$aRb \Leftrightarrow p(a, b) \text{ es cierta}$$

Ejemplo:

Sean los conjuntos $A = \{1, 3, 5, 7\}$ y $B = \{2, 4, 6, 8\}$ y tomemos como propiedad $p(a, b) = a > b$. De ésta manera podemos construir el grafo donde quedan incluidas todas las relaciones que cumplen dicha propiedad:

$$aRb \Leftrightarrow a > b \Rightarrow G = \{(3, 2), (5, 2), (5, 4), (7, 2), (7, 4), (7, 6)\}$$

Propiedades de las relaciones binarias

- Reflexiva: $aRa, \forall a \in A$
- Simétrica: $aRb \Rightarrow bRa$
- Antisimétrica: aRb y $bRa \Rightarrow a = b$
- Transitiva: aRb y $bRc \Rightarrow aRc$
- Antirreflexiva: $a \not R a, \forall a \in A$
- Conexa: aRb ó $bRa, \forall (a, b) \in A \times A, a \neq b$
- Euclídea: aRb y $aRc \Rightarrow bRc$

Relaciones binarias de equivalencia

Se dice que una relación binaria es de equivalencia si verifica las propiedades reflexiva, simétrica y transitiva. Se denota por $a \sim b$.

$$R \text{ es de equivalencia} \Leftrightarrow R \text{ es } \begin{cases} \text{Reflexiva} \\ \text{Simétrica} \\ \text{Transitiva} \end{cases}$$

Clase de equivalencia

Sea A un conjunto y \sim una relación binaria de equivalencia definida en A . Se denomina clase de equivalencia del elemento $a \in A$, denotada por $[a]$ o por \bar{a} , al subconjunto de A formado por todos los elementos relacionados con a , es decir,

$$[a] \equiv \{b \in A : a \sim b\}$$

Puesto que las relaciones de equivalencia, por definición, son transitivas y simétricas podemos afirmar que la clase de equivalencia de dos elementos relacionados es la misma y, por tanto, cualquiera de los elementos puede representar a dicha clase.

$$a \sim b \Leftrightarrow [a] = [b] \quad (4.1)$$

Además podemos afirmar que dos elementos no relacionados pertenecen a distintas clases de equivalencia.

$$a \not\sim b \Leftrightarrow [a] \cap [b] = \emptyset \quad (4.2)$$

Basándonos en lo deducido en las expresiones 4.1 y 4.2, podemos afirmar que cada clase de equivalencia define una partición del conjunto A ya que se cumplen las expresiones 4.3 y 4.4.

$$A = \bigcup_{i=1}^n [a_i] \quad (4.3)$$

$$[a_i] \cap [a_j] = \emptyset \quad \text{si} \quad a_i \not\sim a_j \quad (4.4)$$

Conjunto cociente

Al conjunto de todas las clases de equivalencia del conjunto A se le llama conjunto cociente, y se representa por A/\sim .

$$A/\sim \equiv \{[a_i] : a_i \in A\}$$

Ejemplo:

Sea $A = \{1, 2, 3, 4, 5\}$ y el grafo

$$G = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (3, 1), (2, 4), (4, 2)\}$$

Apoyándonos en la Figura 4.1, comprobamos que es relación binaria de equivalencia ya que es reflexiva, simétrica y transitiva.

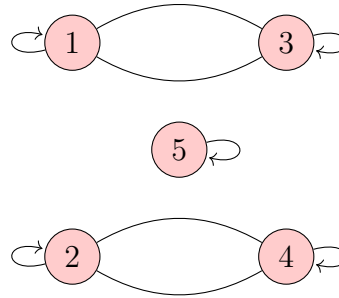


Figure 4.1: Diagrama sagital de las relaciones binarias

Las clases de equivalencia son:

$$\begin{aligned} [1] &= \{1, 3\} = [3] \\ [2] &= \{2, 4\} = [4] \\ [5] &= \{5\} \end{aligned}$$

Por tanto, el conjunto cociente será:

$$A/\sim = \{[1], [2], [5]\}$$

Relaciones binarias de orden

Se dice que una relación binaria es de orden si verifica las propiedades reflexiva, antisimétrica y transitiva. Se denota por $a \leq b$. Si $a \leq b$ se dice que a es anterior a b o que b es posterior a a .

$$R \text{ es de equivalencia} \Leftrightarrow R \text{ es } \begin{cases} \text{Reflexiva} \\ \text{Antisimétrica} \\ \text{Transitiva} \end{cases}$$

Una relación es de **orden total** si además es conexa, es decir, todos los elementos están relacionados. Si no es conexa será relación de **orden parcial**. Se dirá entonces que A está totalmente o parcialmente ordenado si en él hay definida una relación de orden total o parcial respectivamente. Se llama cadena a un subconjunto no vacío totalmente ordenado.

Sean (A, \leq) un conjunto ordenado y B un subconjunto no vacío de A .

Llamamos **cota superior** de B a cualquier elemento de A que es posterior a todo elemento de B . Si existe alguna cota superior, se dice que B está acotado superiormente.

Llamamos **cota inferior** de B a cualquier elemento de A que es anterior a todo elemento de B . Si existe alguna cota inferior, se dice que B está acotado inferiormente.

Si B está acotado inferiormente y superiormente, se dirá simplemente que está acotado.

Extremo superior de B o **supremo** de B es la menor de las cotas superiores de B . Se denota por $\sup_A(B)$. Si el supremo pertenece a B , se llama **máximo**.

Extremo inferior de B o **ínfimo** de B es la mayor de las cotas inferiores de B . Se denota por $\inf_A(B)$. Si el ínfimo pertenece a B , se llama **mínimo**.

Un conjunto se dice que está **bien ordenado** si todo subconjunto suyo no vacío tiene mínimo.

Elemento maximal de B es cualquier elemento de B tal que no existe un elemento posterior a él.

Elemento minimal de B es cualquier elemento de B tal que no existe un elemento anterior a él.

Un conjunto A ordenado se llamará **retículo** si todo subconjunto suyo formado por dos elementos posee ínfimo y supremo.

Ejemplo:

Sea $A = \{2, 3, 5, 6, 8, 16, 18\}$ y consideremos en A la relación de divisibilidad.

$$\forall x, y \in A \quad xRy \Leftrightarrow x|y$$

Inciso: El término $x|y$ significa x divide a y . Ésto se cumple cuando el resto de la división y/x es cero y, por tanto, y es un múltiplo de x . En notación matemática sería:

$$\forall x, y \in \mathbb{Z} \quad x|y \Leftrightarrow \exists k \in \mathbb{Z} : y = kx$$

Puede comprobarse fácilmente que ésta relación es reflexiva, antisimétrica y transitiva. Además, no todos los elementos están relacionados por lo que es de orden parcial.

Una herramienta gráfica empleada para las relaciones de orden es el diagrama de Hasse. Está estructurado de abajo a arriba en niveles en función de la anterioridad o posterioridad de cada elemento.

Podemos observar, en la figura 4.2, el diagrama de Hasse de nuestro ejemplo. Comprobamos que los elementos 2 y 3 son minimales y los elementos 16 y 18 son maximales. El 5 es minimal y maximal a la vez.

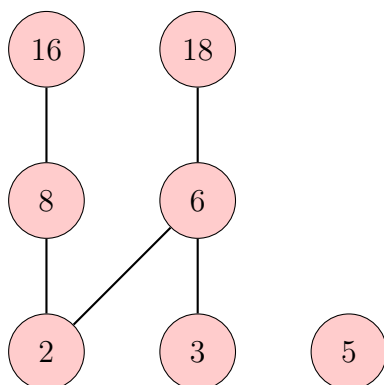


Figure 4.2: Diagrama de Hasse

En éste caso, no tenemos ni máximo ni mínimo ya que no hay ningún elemento de A que acote superior o inferiormente al resto. Puesto que $A \subset \mathbb{N}$ podemos encontrar cotas superiores e inferiores naturales. El 1 divide al resto, por lo que es una cota inferior de A_R . El 720 es múltiplo de los tres maximales, por lo que es cota superior de A_R .

4.3 Principio de Inducción

Sea $P(n)$ una proposición matemática en función de un número entero positivo $n \in \mathbb{Z}^+$. Si $P(n)$ puede ser únicamente verdadera o falsa, entonces podemos emplear el principio de inducción:

Si $P(1)$ es cierta, y si suponiendo que $P(k)$ es verdadera se puede demostrar que $P(k+1)$ también lo es, entonces $P(n)$ es cierta para todo $n \in \mathbb{Z}^+$.

Ejemplo:

Demostrar que la siguiente ecuación es cierta:

$$\sum_{i=1}^n i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}^*$$

Comprobamos que para $n = 1$ es cierto.

$$\sum_{i=1}^1 i = 1 = \frac{1(1+1)}{2}$$

Supongamos que para $n = k$ es cierto.

$$\sum_{i=1}^k i = \frac{k(k+1)}{2}$$

Para $n = k + 1$ tenemos que:

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^k i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

4.4 Aplicaciones

Dados dos conjuntos A y B , una función o aplicación $f : A \rightarrow B$ es un caso particular de relación binaria que asocia a cada $a \in A$ un único objeto $b \in B$, que se denomina imagen de a y se denota por $b = f(a)$.

Al conjunto de los elementos de A para los cuales existe imagen se denomina dominio de la función y se denota por $Dom(f)$.

Al conjunto de todas las imágenes de A se denomina imagen de la función y se denota por $Im(f)$.

$$Im(f) = f(A) = B$$

Se define la imagen recíproca de $b \in B$ como el conjunto de los elementos de A cuya imagen es b . Se denota por $f^{-1}(b)$.

$$f^{-1}(b) := \{a \in A : f(a) = b\}$$

Tipos de aplicaciones

- **Aplicación inyectiva:** Una aplicación es inyectiva si no hay dos objetos del dominio con la misma imagen.

$$f(x) = f(y) \iff x = y$$

- **Aplicación sobreyectiva:** Una aplicación es sobreyectiva si todos los objetos de B son imagen de al menos un objeto de A :

$$\forall b \in B \exists a \in A / f(a) = b \iff Im(f) = B$$

- **Aplicación biyectiva:** Una función es biyectiva si es sobreyectiva e inyectiva a la vez. Por tanto, todos los elementos de A tienen una imagen distinta en B y a cada $b \in B$ le corresponde un único elemento $a \in A$.

Para las aplicaciones biyectivas existe una aplicación o **función inversa**, denotada por f^{-1} , tal que

$$f^{-1}(b) = a$$

Composición de aplicaciones

Sean $f : A \rightarrow B$ y $g : C \rightarrow D$ dos aplicaciones con $B \subset C$. Se denomina función o aplicación compuesta a

$$(g \circ f)(a) \equiv g(f(a))$$

Propiedades:

- Asociativa: $h \circ (g \circ f) = (h \circ g) \circ f$
- No conmutativa en general.
- La composición de aplicaciones inyectivas es una aplicación inyectiva.
- La composición de aplicaciones sobreyectivas es una aplicación sobreyectiva.
- La composición de aplicaciones biyectivas es una aplicación biyectiva.

Chapter 2

Estructuras algebraicas

2.1 Operación interna

Sea A un conjunto no vacío. Se llama operación interna definida en A a cualquier aplicación de $A \times A$ en A que asocia a cada par (a, b) de elementos de A un único elemento c , resultado de operar a con b . Matemáticamente, para el operador " $*$ ", se expresa de la siguiente forma:

$$\begin{array}{l} A \times A \xrightarrow{*} A \\ (a, b) \rightarrow c := a * b \end{array} \quad \text{con } a, b, c \in A$$

Ejemplo:

El producto de números reales (\mathbb{R}, \cdot) es una operación interna del conjunto de los números reales, ya que cualquier producto de números reales da como resultado otro número real.

$$x \cdot y \in \mathbb{R} \quad \forall x, y \in \mathbb{R}$$

Propiedades

Sea $(A, *)$ un conjunto no vacío (A) donde hay definida una operación interna $(*)$. Diremos que la operación es:

- **Asociativa** $\Leftrightarrow a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$
- **Conmutativa** $\Leftrightarrow a * b = b * a \quad \forall a, b \in A$

Añadamos una nueva operación interna a nuestro par, obteniendo $(A, *, \circ)$. Diremos que \circ es **distributiva** respecto de $*$ si

$$\forall a, b, c \in A, \begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c), \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

Elementos particulares

- Elemento neutro e : $a * e = e * a = a$
- Elemento simétrico a' : $a * a' = a' * a = e$

Ejemplo:

Sea $(\mathbb{R}, +, \cdot)$ el conjunto de los números reales con las operaciones internas de producto y suma. Podemos comprobar que tanto el producto como la suma son asociativos y conmutativos. Además el producto es distributivo respecto de la suma ya que:

$$\forall a, b, c \in \mathbb{R}, \begin{cases} a \cdot (b + c) = (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c = (a \cdot c) + (b \cdot c) \end{cases}$$

2.2 Operación externa

Dados dos conjuntos A y K , se llama operación externa definida en A y con dominio de escalares K , a cualquier aplicación:

$$\begin{array}{ccc} K \times A & \xrightarrow{\perp} & A \\ (k, a) \rightarrow b & := & k \perp a \end{array} \quad \text{con} \quad \begin{array}{l} k \in K \\ a \in A \end{array}$$

Ejemplo:

Sea $V_3 \equiv \{v = (x, y, z) \mid \forall x, y, z \in \mathbb{R}\}$ el conjunto de los vectores reales de tres dimensiones y el conjunto de los escalares enteros $K \equiv \{k \mid \forall k \in \mathbb{Z}\}$. El producto de escalares por vectores es operación externa ya que $k \cdot v \in V_3$.

2.3 Homomorfismos

Sean $(A, *)$ y (B, \circ) dos conjuntos con operaciones internas definidas. Una aplicación $f : A \rightarrow B$ es un **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in A$$

Si f es un homomorfismo y además

- es inyectivo se llamará **monomorfismo**.
- es sobreyectivo se llamará **epimorfismo**.
- es biyectivo se llamará **isomorfismo**.
- $A = B$ se llamará **endomorfismo**.
- es endomorfismo biyectivo se llamará **automorfismo**

Ejemplo:

Sean $G = (\mathbb{R}, +)$ y $H = (\mathbb{R}^+, \cdot)$. Definamos una aplicación

$$\begin{aligned} f : G &\leftarrow H \\ x &\mapsto e^x \end{aligned}$$

Podemos afirmar que se trata de un homomorfismo ya que

$$\begin{aligned} f(x + y) &= f(x) \cdot f(y) \\ e^{x+y} &= e^x + e^y \end{aligned}$$

2.4 Grupo

Un **grupo** es una pareja $(G, *)$, donde G es un conjunto en el que está definida una operación interna $*$ que verifica:

1. Asociativa.
2. Existencia de elemento neutro e , es decir, $g * e = g$
3. Todo elemento g posee simétrico g' , es decir, $g * g' = e$

Si además la operación interna $*$ es conmutativa, el grupo se llamara **abeliano**.

Propiedades de un grupo

- El elemento neutro es único
- $(a * b)' = b' * a'$
- $(a')' = a$
- $a * x = a * y \Rightarrow x = y$

Orden de un grupo

Sea $(G, *)$ un grupo. El **orden** de un elemento $a \in G$ es el menor entero positivo $k \in \mathbb{N}^*$ para el que $a^k = e$. Si no existe k , el orden es infinito o cero.

Al número de elementos de un grupo se le llama **orden** de G y se denota por $|G|$.

Ejemplo:

El conjunto de los números enteros con la suma $(\mathbb{Z}, +)$ es un grupo abeliano ya que:

1. La suma de numeros enteros es otro número entero.
2. El elemento neutro de los enteros con la suma es el cero: $z + 0 = z$.
3. Todo z posee un simétrico $-z$: $z + (-z) = 0$.
4. La suma de enteros es conmutativa: $z_1 + z_2 = z_2 + z_1$.

A modo de ejemplo diremos que el orden del grupo es infinito $|\mathbb{Z}| = \infty$. El orden de los elementos son

$$\begin{aligned} |1| &= 1 \\ |-1| &= 2 \\ |z| &= \infty \quad \forall z \in \mathbb{Z} - \{-1, 1\} \end{aligned}$$

Subgrupo

Sea $(G, *)$ un grupo y $H \subset G$, un subconjunto suyo no vacío. $(H, *)$ es **subgrupo** si también posee estructura de grupo.

Caracterización

Un subconjunto H es subgrupo si se cumple que

$$\forall a, b \in H \Rightarrow a * b \in H \tag{2.1}$$

$$\forall a \in H \Rightarrow a' \in H \tag{2.2}$$

Las ecuaciones 2.1 y 2.2 se pueden resumir en la siguiente

$$\forall a, b \in H \Rightarrow a * b' \in H$$

Clases de un grupo

Dado un grupo G , un subgrupo H y un elemento $a \in G$ arbitrario fijo, a los conjuntos

$$\begin{aligned} aH &= \{x/x \in G, x = a * h, h \in H\} \\ Ha &= \{x/x \in G, x = h * a, h \in H\} \end{aligned}$$

se les denomina respectivamente **clases** del grupo G a la izquierda y a la derecha módulo el subgrupo H . Se les llama así por ser clases de cierta relación de equivalencia¹ y, por tanto, forman particiones del grupo G .

Si $aH = Ha$ entonces, H es un subgrupo **normal o invariante**.

Supongamos que el grupo G es finito y que posee n clases a la izquierda módulo H . Entonces,

$$G = a_1H \cup a_2H \cup \dots \cup a_nH$$

$$|G| = |a_1H| + |a_2H| + \dots + |a_nH| = n|H|$$

por lo que el orden de un grupo finito G será múltiplo del orden de cualquier subgrupo suyo (**teorema de Lagrange**).

Al cociente $n = |G|/|H|$ se le denomina **índice del subgrupo H** .

Un grupo G se dice **finitamente generado** si existe una parte finita A de G que engendra todo G . Si A se reduce a un elemento, el grupo G se llama **monógeno**.

El grupo G es **cíclico** si es monógeno y finito.

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

Nota: Con a^n nos referimos a aplicar n veces el operador $*$ sobre a . Ésto coincidirá con la potencia en el caso de que la operación sea el producto pero, en general, no es así.

¹La relación es $x \sim y \Leftrightarrow x' * y \in H$, aunque no es de interés para ésta explicación.

Homomorfismo de grupos

Al igual que en la sección anterior, dos grupos $(G_1, *)$, (G_2, \circ) y una aplicación $f : G_1 \rightarrow G_2$ es **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in G_1$$

Llamamos **núcleo** de f , representándose por $Ker(f)$, al conjunto de los elementos del dominio cuya imagen es el elemento neutro de G_2 .

$$Ker(f) = \{x \in G_1 : f(x) = e_2\} = f^{-1}(e_2)$$

Llamamos **imagen** de f , denotándose por $Im(f)$, como el subconjunto de G_2 formado por aquellos elementos que son imagen de algún elemento de G_1 . Es decir,

$$Im(f) = \{y \in G_2 : \exists x \in G_1, f(x) = y\}$$

Por tanto, podemos decir que

$$\begin{aligned} f \text{ es inyectiva} &\Leftrightarrow Ker(f) = \{e_1\} \\ f \text{ es sobreyectiva} &\Leftrightarrow Im(f) = G_2 \end{aligned}$$

2.5 Anillo

Un anillo es un conjunto dotado con dos operaciones internas llamadas suma y producto. El anillo $(R, +, \cdot)$ cumple que:

1. $(R, +)$ es un grupo abeliano.
2. El producto es asociativo.
3. Existe un elemento neutro para la multiplicación.
4. El producto es distributivo respecto a la suma.

Si el producto es conmutativo se dice que el anillo es conmutativo. Si el producto posee elemento neutro es unitario.

El elemento neutro de la suma será 0 y el del producto 1.

Subanillo

Cuerpo

Un cuerpo es un anillo conmutativo y unitario en el que todo elemento distinto de cero es invertible respecto del producto, es decir, un anillo de división conmutativo.

Por ejemplo, los números reales con la suma y el producto algebraicos $(\mathbb{R}, +, \cdot)$ es un cuerpo ya que:

1. $(\mathbb{R}, +)$ es un grupo abeliano (siendo 0 el elemento neutro de la suma)
2. El producto de números reales es asociativo.
3. El elemento neutro de la multiplicación es el 1.
4. El producto es distributivo respecto de la suma (propiedades de anillo cumplidas).
5. El anillo es conmutativo, ya que el producto de números reales lo es.
6. El anillo es unitario ya que el neutro de la multiplicación es distinto del de la suma.
7. Todo elemento distinto de cero es invertible respecto del producto: Sea $r \in \mathbb{R}$ y $r \neq 0$, entonces $\frac{1}{r} \in \mathbb{R}$.

Así lo serían también $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{Q}, +, \cdot)$.

Chapter 3

Espacios Vectoriales y Aplicaciones lineales

3.1 Espacio vectorial

Un espacio vectorial sobre un cuerpo $(K, +, \cdot)$ es un grupo abeliano $(V, +)$ dotado con una operación externa $K \times V \rightarrow V$, que verifica las siguientes propiedades:

1. Distributiva respecto a escalares $\rightarrow \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$
2. Distributiva respecto a vectores $\rightarrow (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
3. Asociativa $\rightarrow \lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$
4. Modular $\rightarrow 1 \cdot v = v$

Con $\lambda, \mu \in K$ y $v, w \in V$.

Si el espacio vectorial en cuestión tiene como cuerpo a los números reales será un espacio vectorial real, mientras que si tiene a los números complejos se denotará como espacio vectorial complejo.

Veamos a continuación un ejemplo práctico para su mejor comprensión:

Ejemplo 1

Demostrar que el conjunto \mathbb{C} de los números complejos, con las operaciones suma y producto usuales, tiene estructura de espacio vectorial sobre el cuerpo de los números reales:

Demostremos que $(\mathbb{C}(\mathbb{R}), +, \cdot)$ tiene estructura de espacio vectorial:

Partiendo de que $(\mathbb{R}, +, \cdot)$ es un cuerpo, comprobamos que $(\mathbb{C}, +)$ es grupo abeliano:

1. Operación interna: La suma de números complejos es una operación interna ya que da como resultado otro número complejo:

$$(a + bi) + (c + di) = (a + b) + (c + d)i \in \mathbb{C}$$

2. Propiedad asociativa: La suma de números complejos es asociativa, ya que:

$$(a+bi)+[(c+di)+(e+fi)] = [(a+bi)+(c+di)]+(e+fi) = (a+c+e)+(b+d+f)i$$

3. Existencia de elemento neutro $(0 + 0i)$, ya que:

$$(a + bi) + (0 + 0i) = a + bi$$

4. Existencia de elemento simétrico $[(-a) + (-b)i]$, ya que:

$$(a + bi) + [(-a) + (-b)i] = (0 + 0i)$$

5. Propiedad conmutativa: La suma de números complejos es conmutativa, ya que:

$$(a + bi) + (c + di) = (c + di) + (a + bi) = (a + b) + (c + d)i$$

Es trivial demostrar que el producto de escalares reales con números complejos es operación externa, ya que el producto de un número real por un número complejo sigue siendo un número complejo:

$$r * (a + bi) = ra + rbi \in \mathbb{C} \quad \text{con } r, a, b \in \mathbb{R}$$

Por lo que $\mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}$.

Para terminar demostramos las cuatro propiedades que hacen que un grupo abeliano con operación externa e interna sea un espacio vectorial sobre el cuerpo, en este caso, de los números reales:

1. Distributiva respecto a escalares:

$$r[(a + bi) + (c + di)] = r(a + bi) + r(c + di) = (ra + rc) + (rb + rd)i$$

2. Distributiva respecto a vectores:

$$(r + s)(a + bi) = r(a + bi) + s(a + bi) = (ra + sa) + (rb + sb)i$$

3. Asociativa:

$$r[(a + bi)(c + di)] = [r(a + bi)](c + di) = (rac - rbd) + (rad + rbc)i$$

4. Modular:

$$1 \cdot (a + bi) = a + bi$$

Con $r, s, a, b, c, d \in \mathbb{R}$

Y así queda demostrado que el cuerpo de los números complejos, con las operaciones de suma y producto, tiene estructura de espacio vectorial sobre el cuerpo de los números reales.

3.2 Subespacio vectorial







3.3 Dependencia e independencia lineal

3.3.1 Sistema generador

3.3.2 Base

3.3.3 Base de un subespacio

3.3.4 Cooredenadas y cambio de base

3.4 Operaciones con subespacios

3.5 Aplicación lineal

3.5.1 Matriz de una aplicación lineal

3.5.2 Matriz de una composición

3.5.3 Cambio de base en aplicaciones lineales

3.5.4 Núcleo e imagen de una aplicación lineal

3.6 Matrices y determinantes

3.7 Sistemas y ecuaciones lineales

3.7.1 Teorema de Rouché-Fröbenius

3.7.2 Regla de Cramer

3.7.3 Método de Gauss

3.7.4 Factorización LU









Chapter 4

Formas bilineales y cuadráticas



4.1 Formas bilineales





4.2 Perpendicularidad u ortogonalidad

4.3 Matriz de una forma bilineal



4.4 Bases ortogonales





4.5 Formas bilineales simétricas

4.6 Formas cuadráticas



4.7 Matriz de una forma cuadrática





4.8 Isometrías

4.9 Transformaciones ortogonales



Chapter 5

Espacio afín y euclídeo. Movimientos



5.1 Espacios afines



5.2 Transformaciones afines y afinidades



5.3 Matrices



5.4 Transformaciones ortogonales y movimientos



5.5 Orientación



5.6 Movimientos en el plano afín euclídeo



5.7 Movimientos en el espacio afín euclídeo



Chapter 6

Cónicas y cuádricas



6.1 Estudio afín de las cónicas



6.2 Estudio afín de las cuádricas



Chapter 7

Álgebra lineal numérica

7.1 Normas matriciales



7.2 Métodos de Jacobi y Gauss-Seidel



7.3 Factorización de matrices LU y QR



7.4 Estimación de errores



7.5 Implementación de algoritmos



7.6 Cálculo de autovalores y autovectores



Chapter 8

Geometría diferencial



8.1 Curvas y superficies en el espacio





8.2 Triedro de Frenet

8.3 Curvatura de Gauss y media



Bibliography