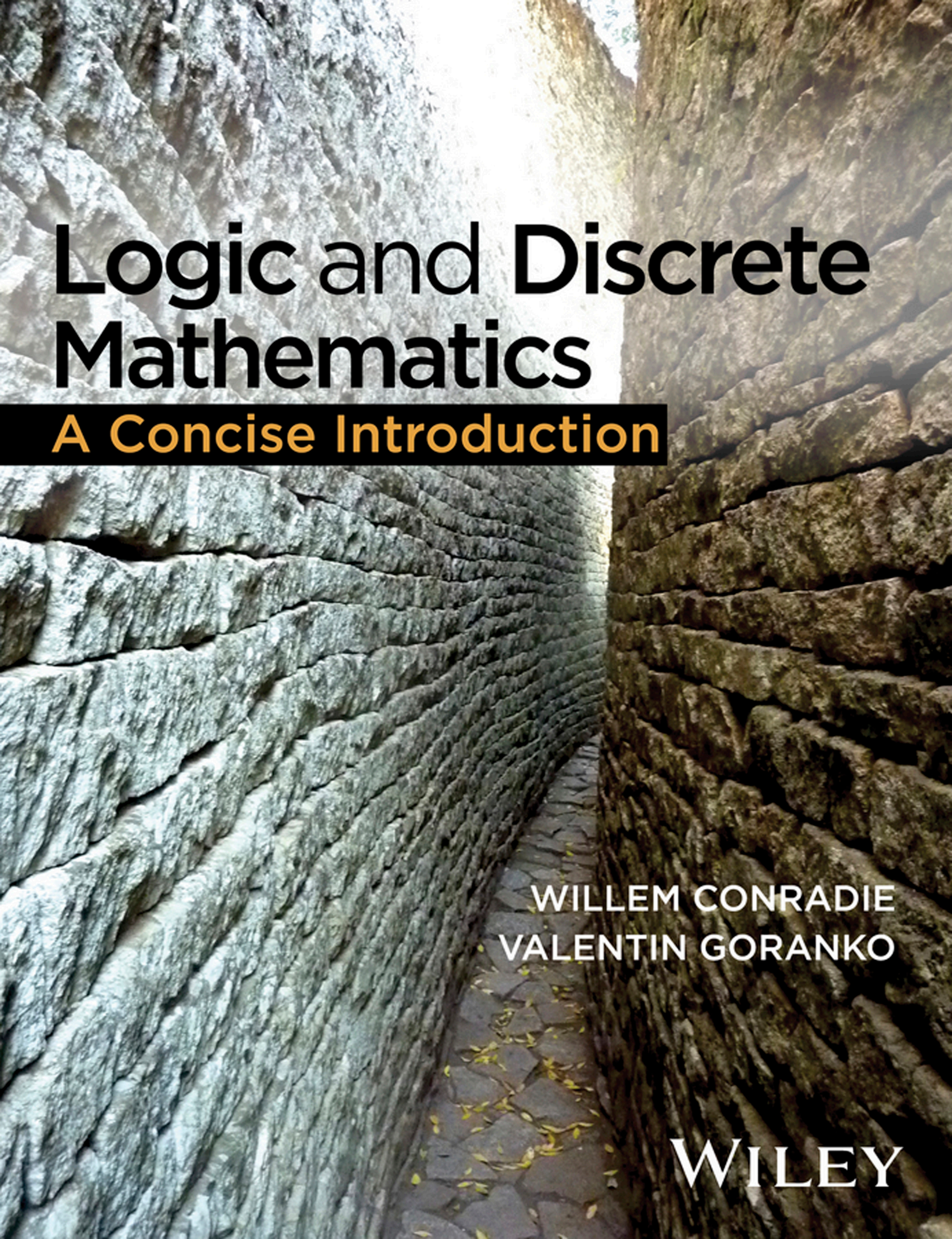

Logic and Discrete Mathematics

A Concise Introduction

WILLEM CONRADIE
VALENTIN GORANKO

WILEY

Logic and Discrete Mathematics

Logic and Discrete Mathematics

A Concise Introduction

Willem Conradie
University of Johannesburg,
South Africa

Valentin Goranko
Stockholm University, Sweden

WILEY

This edition first published 2015

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Conradie, Willem, 1978- author.
Logic and discrete mathematics : a concise introduction / Willem Conradie, Valentin Goranko.
pages cm
Includes index.
ISBN 978-1-118-75127-5 (pbk.)
1. Logic, Symbolic and mathematical–Textbooks. 2. Computer science–Mathematics–Textbooks.
I. Goranko, Valentin, author. II. Title.
QA9.C7423 2015
511.3–dc23
2014035964

A catalogue record for this book is available from the British Library.

Front cover image: Narrow walkway inside the Great Enclosure at the Great Zimbabwe ruins. Reproduced by kind permission of Kenneth Meeks.

Set in 9/11pt, PalatinoLTStd by Laserwords Private Limited, Chennai, India

1 2015

Contents

List of Boxes

Preface

Discrete Mathematics[1] refers to a range of mathematical disciplines that study discrete structures and phenomena, unlike other classical fields of mathematics, such as analysis, geometry and topology, which study continuous structures, processes and transformations. Intuitively put, discrete structures – such as the linear order of natural numbers or the set of cities and towns in a country together with the roads between them – consists of separable, discretely arranged objects, whereas continuous structures – such as the trajectory of a moving object, the real line, the Euclidian plane or a sphere – are densely filled, with no "gaps". The more important distinction, however, is between the types of problems studied and solved in discrete and continuous mathematics and also between the main ideas and techniques that underly and characterize these two branches of mathematics. Nevertheless, this distinction is often blurred and many ideas, methods and results from each of these branches have been fruitfully applied to the other.

The intuitive explanation above is not meant to define what should be classified as Discrete Mathematics, as every such definition would be incomplete or debatable. A more useful description would be to list what we consider to be the basic mathematical disciplines traditionally classified as Discrete Mathematics and included in most university courses on that subject: the Theory of Sets and Relations, Mathematical Logic, Number Theory, Graph Theory and Combinatorics. These are the topics covered in this book. Sometimes textbooks and courses on Discrete Mathematics also include Abstract Algebra, Classical Probability Theory, Automata Theory, etc. These topics are not included here, mainly for practical reasons.

Logic was born in the works of Aristotle as a philosophical study of reasoning some 25 centuries ago. Over the past 150 years it has gradually developed as a fundamental mathematical discipline, which nowadays has deep and mature mathematical content and also applications spreading far beyond foundational and methodological issues. While the field of Mathematical Logic is often regarded as included in the broad scope of Discrete Mathematics, in this book it is treated essentially on a par with it.

As mathematical fields of their own importance, both Logic and Discrete Mathematics are relatively young and very dynamically developing disciplines, especially since the mid 20th century, when the computer era began. Many of the most exciting current developments

[1] Not to be confused with discreetly done mathematics!

in Logic and Discrete Mathematics are motivated and inspired by applications in Computer Science, Artificial Intelligence and Bioinformatics. We have accordingly included some such selected applications in the book.

About the book

The work on this book started more than a decade ago as a loose collection of lecture notes that we wrote and used to teach courses on Logic and Discrete Mathematics, partly because we could not find available suitable textbooks that would meet our needs and requirements. Eventually we decided to write a book of our own, which would best reflect the content and features we consider most important:

1. Being logicians, we have provided a much more detailed and deeper treatment of Logic than is usual in textbooks on Discrete Mathematics. We believe that such a treatment is necessary for the proper understanding and use of Logic as a mathematical and general reasoning tool, and we consider it a distinguishing feature of the book.
2. We included only what we consider to be the core disciplines within the field of Discrete Mathematics (without claiming that ours is the only good choice) but have treated these disciplines in considerable depth for an undergraduate text. That enabled us to keep the book within reasonable size limits without compromising on the content and exposition of the topics included.
3. We have tried to keep the exposition clear and concise while still including the necessary technical detail and illustrating concepts and techniques with numerous examples.
4. We have included comprehensive sets of exercises, most of them provided with answers or solutions in an accompanying solutions manual.
5. We have also included "boxes" at the end of each section. Some contain mathematics titbits or applications of the content in the section. Others are short biographies of distinguished scientists who have made fundamental contributions to Discrete Mathematics. We hope the reader will find it inspiring to learn a little about their lives and their contributions to the fields covered in the book.

To the instructor

We have aimed this book to be suitable for a variety of courses for students in both Mathematics and Computer Science. Some parts of it are much more relevant to only one of these audiences and we have indicated them by introducing *Mathematics Track* and *Computer Science Track* markers in the text. We regard everything not explicitly on either of these tracks to be suitable for both groups.

In addition, the book can be used for designing courses on different undergraduate or lower graduate levels. Some material that could reasonably be omitted in courses at a lower undergraduate level is indicated with an *Advances Track* marker. These tracks are, of course, only suggestions, which should serve as our recommendations to the instructor.

The single stars shown in the exercises are deemed to be exercises that are more difficult, while the double stars are considered to be exercises that are challenging.

The whole book can be comfortably covered in two semester courses, or various selections can be made for a single semester course. Apart from assuming knowledge of the background material in the preliminary Chapter 1, the chapters are essentially independent and can be taught in any order. The only exception is Chapter 4 on first-order logic, which presupposes knowledge of the material on propositional logic covered in Chapter 3. Also, much of the content of Chapter 2 covers general mathematical background, useful for the rest of the book.

Acknowledgements

A number of people have contributed, one way or another, to our work on this book over the years. With the risk of inadvertently omitting some names, for which we apologize in advance, we would like to thank Gerhard Benadé, Thomas Bolander, Izak Broere, Ruaan Kellerman, Heidi Maartens, Chantel Marais and Claudette Robinson for helpful feedback, comments, technical or editorial corrections and some solutions to exercises. Besides them, thanks are due to many students at the University of Johannesburg, the University of the Witwatersrand and the Technical University of Denmark, who pointed out some errors in earlier versions of the manuscript. We thank Justin Southey for the use of the GraphScribe application authored by him, which greatly speeded up the drawing of some combinatorial graphs, and also for his suggestions on the applications of Graph Theory. Valentin is also grateful to Nina Ninova for her general support during the work on this book as well as help with collecting photos and references for many of the historical boxes. Willem would like to thank Dion Govender for his patience and support during the final months of intense work on the book. Last but not least, we wish to thank Richard Davies, Audrey Koh, Kathryn Sharples, Mark Styles and Jo Taylor from Wiley as well as Krupa Muthu from Laserwords for their kind support and technical advice during the work on this book.

About the Companion Website

This book is accompanied by a companion website:

www.wiley.com/go/conradie/logic

The website includes:

- Lecture Slides
- Quizzes

1

Preliminaries

Here we briefly review some minimal background knowledge that we will assume in the rest of the book. Besides a small amount of that nebulous quality called "mathematical maturity", we only expect some basic concepts from set theory and mathematical indiction. The reader who is familiar with these concepts can safely skip on to the next chapter.

Some notation

We denote the set of natural numbers $\{0, 1, 2, \ldots\}$ by $\mathbb{N}$. There is some inconsistency in the mathematical literature as to whether 0 belongs to the natural numbers or not: some authors choose to include it, other do not. For our purposes it is convenient to include 0 as a natural number. Other number sets which will be of importance to us include the sets of integers $\mathbb{Z}$, positive integers $\mathbb{Z}^+$, rational numbers $\mathbb{Q}$, positive rational numbers $\mathbb{Q}^+$, real numbers $\mathbb{R}$, and positive real numbers $\mathbb{R}^+$.

The product $1 \times 2 \times 3 \times \cdots \times n$ of the first n positive integers turns up in many mathematical situations. It is therefore convenient to have a more compact notation for it. We accordingly define $0! = 1$ and $n! = 1 \times 2 \times 3 \times \cdots \times n$, for $n \geq 1$. We read $n!$ as 'n factorial'. The definition of $0!$ as 1 is not supposed to carry any intuitive meaning: it is simply a useful convention.

Logic and Discrete Mathematics: A Concise Introduction, First Edition. Willem Conradie and Valentin Goranko.

Companion Website: www.wiley.com/go/conradie/logic

1.1. Sets

Sets and elements. By a **set** we intuitively mean a collection of objects of any nature (numbers, people, concepts, sets themselves, etc.) that is considered as a single entity. The objects in that collection are called **elements** of the set. If an object x is an element of a set A, we denote that fact by

$$x \in A;$$

otherwise we write

$$x \notin A.$$

We also say that *x is a member of the set A* or that *x belongs to A*. If a set has finitely many elements (here we rely on your intuition of what *finite* is), we can describe it precisely by listing all of them, for example:

$$A = \{3, 4, 5\}.$$

We often rely on our common intuition and use ellipses, as in

$$A = \{1, 2, \dots, n\}.$$

We sometimes go further and use the same for *infinite* sets; for example, the set of natural numbers can be specified as

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

Further we will discuss a more universal method of describing sets.

Equality and containment of sets. Two sets are declared **equal** if and only if they have the same elements. In other words, the sets A and B are equal, denoted as usual by $A = B$, if every element of A is an element of B and every element of B is an element of A. For example, the sets $\{a, b, c\}$ and $\{b, c, a\}$ are equal, and so are the sets $\{1, 9, 9, 7\}$, $\{1, 9, 7\}$ and $\{7, 1, 9, 1, 7, 1\}$.

A set A is a **subset** of a set B, denoted $A \subseteq B$, if every element of A is an element of B. If $A \subseteq B$, we also say that A **is included in** B, or that B **contains** A. For example, $\{3, 5\} \subseteq \{5, 4, 3\}$. Note that every set is a subset of itself.

The following facts are very useful. They are direct consequences of the definitions of equality and containment of sets.

- Two sets A and B are equal if, and only if, $A \subseteq B$ and $B \subseteq A$.
- A set A is not a subset of a set B, denoted $A \nsubseteq B$, if, and only if, there is an element of A that is not an element of B.
- A set A is not equal to a set B if A is not a subset of B *or* if B is not a subset of A.

A set A is a **proper subset** of a set B, denoted $A \subset B$ or $A \subsetneqq B$, if $A \subseteq B$ and $A \neq B$. In other words, A is a proper subset of B if A is a subset of B and B is *not* a subset of A, i.e. if at least one element of B is not in A. In particular, no set is a proper subset of itself. If A is not a proper subset of B, we denote that by $A \not\subset B$.

The empty set. Amongst all sets there is one that is particularly special. That is the **empty set**, i.e. the set that has no elements. By definition of equality of sets, there is only one empty set. One might think that the empty set is a useless abstraction. On the contrary, it is a very important set, and probably the most commonly used one in mathematics (like the number 0 is the most commonly used number). That is why it has a special notation: $\varnothing$.

Sets and properties. Set-builder notation. We cannot always list the elements of a set, even if it is finite, so we need a more universal method for specifying sets. The commonly used method is to *describe the property that determines membership of the set*, e.g.:

"A is the set of all objects x such that $\ldots x\ldots$."

where "$\ldots x\ldots$" is a certain property (predicate) involving x. We use the following convenient notation, called the **set-builder notation** for the set described above:

$$A = \{x \mid \ldots x \ldots\}.$$

Here are some examples:

- $\{x \mid x \textit{ is a negative real number}\}$ defines the set of negative real numbers;
- $\{x \mid x \textit{ is a student in the MATH3029 class}\}$ defines the set of students in the MATH3029 class.
- $\{x \mid x \in \mathbb{Z} \textit{ and } 3 \geq x > -2\}$ defines the set $\{-1, 0, 1, 2, 3\}$.
- $\{x \mid x = \frac{m}{n}, \textit{ where } m \in \mathbb{Z} n \in \mathbb{Z} \textit{ and } n \neq 0\}$ defines the set of rational numbers.

Sometimes, we use the set-builder notation more liberally and, for instance, describe the set of rational numbers as $\left\{\frac{m}{n} \middle| m \text{ and } n \text{ are integers and } n \neq 0\right\}$ or the set of positive real numbers as $\{x \in \mathbb{R} \mid x > 0\}$.

Operations on sets. We describe below the basic operations on sets.

Intersection. The intersection of two sets A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

consisting of all elements that are both in A and in B. If $A \cap B = \varnothing$, then A and B are called **disjoint**.

Union. The union of two sets A and B is the set

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

consisting of all elements that are in at least one of A and B.

Difference. The difference of the sets A and B is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

consisting of all elements that are in A but not in B. An alternative notation for $A - B$ is $A \backslash B$.

For example, if $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$ then $A \cap B = \{3, 4\}$, $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$, $A - B = \{1, 2\}$ and $B - A = \{5, 6, 7\}$.

Universal sets and complements of sets. Often, all sets that we consider are subsets of one set, called the **domain of discourse**. We also call that set the **universe** or the **universal set**. For example, in arithmetic, the universe is usually the set of natural numbers or the set of integers, while in algebra and calculus, the universe is the set of real numbers; talking about humans, the universe is the set of all humans, etc.

Definition 1.1.1 *Let a universal set* $\mathbf{U}$ *be fixed and* $A \subseteq \mathbf{U}$*. The* complement of A *(with respect to* $\mathbf{U}$*) is the set*

$$A' = \mathbf{U} - A.$$

The complement of a set A *is sometimes also denoted by* $\overline{A}$*.*

Thus, the complement of A consists of those objects from the universal set that do not belong to A. For example, if the universal set is $\mathbb{R}$, then the complement of the interval $(0, 2]$ is $(-\infty, 0] \cup (2, \infty)$; the complement of $\mathbb{Q}$ is the set of irrational numbers.

Powersets. The *power set of a set* A is the set of all subsets of A:

$$\mathscr{P}(A) = \{X \mid X \subseteq A\}.$$

Here are some examples:

- $\mathscr{P}(\emptyset) = \{\emptyset\}$;
- $\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$, in particular, $\mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$;
- $\mathscr{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$;
- $\mathscr{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Cartesian products of sets. In order to introduce the next operation we need the notion of **ordered pair**. Let a, b be any objects. Intuitively, the ordered pair of a and b, denoted (a, b) (do not confuse this with an open interval of real numbers!), is something like a set consisting of a as a *first element* (or first *component*) and b as a *second element* (or second *component*). Thus, if $a \neq b$, then the ordered pair (a, b) is *different* from the ordered pair (b, a) and each of these is different from the set $\{a, b\}$ because the elements of a set are not ordered. In particular, the ordered pair (a, a) is different from the set $\{a, a\} = \{a\}$. Here is a formal definition of an ordered pair as a set that satisfies the intuition:

Definition 1.1.2 *Given the objects* a *and* b*, the* **ordered pair** (a, b) *is the set* $\{\{a\}, \{a, b\}\}$*.*

Here is the fundamental property of ordered pairs:

Proposition 1.1.3 *The ordered pairs* (a_1, a_2) *and* (b_1, b_2) *are equal if and only if* $a_1 = b_1$ *and* $a_2 = b_2$*.*

Proof: Exercise.

Definition 1.1.4 *The* **Cartesian product** *of the sets* A *and* B *is the set*

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\},$$

consisting of all ordered pairs where the first component comes from A *and the second component comes from* B*. In particular, we denote* $A \times A$ *by* A^2 *and call it the* **Cartesian square** *of* A*.*

For example, if $A = \{a, b\}$, $B = \{1, 2, 3\}$, then

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\},$$

while

$$B \times A = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Note that if A or B is empty, then $A \times B$ is empty too. Moreover, if A has n elements and B has m elements, then $A \times B$ has mn elements (why?). This is one of the reasons for the term "product".

The Cartesian coordinate system in the plane is a representation of the plane as the Cartesian[1] square $\mathbb{R}^2$ of the real line $\mathbb{R}$, where we associate a unique ordered pair of real numbers (its **coordinates**) with every point in the plane.

The notion of an ordered pair can be generalized to **ordered n-tuple**, for any $n \in \mathbb{N}^+$. An n-tuple is an object of the type $(a_1, a_2, \ldots, a_n)$ where the order of the components $a_1, a_2, \ldots, a_n$ matters. We will not give a formal set theoretic definition in the style of Definition 1.2.1, but leave this as an exercise (Exercise 11).

Accordingly, the Cartesian product can be extended to n sets:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n\}.$$

As before, we will use the notation A^n for $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$.

Relations. Relations, also called **predicates**, are ubiquitous in mathematics. Relations between numbers like "being equal", "being less than" and "being divisible by" come to mind at once. As these examples indicate, many of the relations we commonly encounter are *binary*, i.e., relations relating *two* objects at a time. It will be convenient for us to identify a binary relation with the set of all ordered pairs of elements that stand in that relation. We thus have the following definition:

Definition 1.1.5 *A* **binary relation** *on a set A is any subset of* A^2.

For example the relation $<$ on the set $\mathbb{N}$ of natural numbers is a binary relation, which we identify with the set

$$\{(a, b) \mid a, b \in \mathbb{N} \text{ and } a \text{ is less than } b\}.$$

The relation of "being the mother of" is a binary relation on the set of humans, which we identify with the following set of ordered pairs:

$$\{(x, y) \mid x \text{ and } y \text{ are humans and } x \text{ is the mother of } y\}.$$

Definition 1.1.6 *An* **n-ary relation** *on a set A is any subset of* A^n.

[1] The term "Cartesian" comes from the name of the French mathematician René Descartes (1596–1650), who was the first to introduce coordinate systems and to apply algebraic methods in geometry.