Foundations of Mathematical Practice

David Pierce

September 24, 2010

Mathematics Department
Middle East Technical University
Ankara 06531 Turkey
http://metu.edu.tr/~dpierce/
dpierce@metu.edu.tr

Contents

List of Figures

Preface

This book concerns the foundations of mathematics in two ways:

1. this book is about concepts and techniques that all mathematicians use, implicitly or explicitly;
2. this book (or parts of it) is intended for use in a first university-level mathematics course.

More precisely, these notes are originally written for a course called Fundamentals of Mathematics, given at Middle East Technical University in Ankara under the designation Math 111.[1] The notes also offer additional reading for those interested in the topics they discuss. In particular, the notes may be useful for Math 320 (Set Theory) and Math 406 (Introduction to Mathematical Logic and Model Theory) at METU.

What are foundations? A wooden house may by built on a stone foundation. A mason lays down the stones; then a carpenter erects the house on top. The carpenter cannot construct the walls and floors of the house before the stone-mason creates a place to set those floors and walls; but the stone-mason cannot create this foundation without knowing what the carpenter intends to place there.

So it is with the foundations of mathematics. You cannot do mathematics without a place to start; but you cannot create the starting-point without knowing the mathematics that will proceed from it. This is a paradox—a seeming contradiction. It is not a *real* contradiction; but it does suggest that the nascent mathematician (the first-year student) cannot read this book page after page as if it constituted an easy novel. The book might considered as a difficult novel with lots of interrelated events. (However, not every novel has an index or a list of symbols like this one.) Not every section of the book should

[1] The catalogue description of Math 111 is:

> Symbolic logic. Set theory. Cartesian product. Relations. Functions. Injective, surjective and bijective functions. Composition of functions. Equipotent sets. Countability of sets. More about relations: equivalence relations, equivalence classes and partitions. Quotient sets. Order relations: Partial order, Total order, Well ordering. Mathematical induction and recursive definitions of functions.

be studied in sequence during the reader's first encounter. Even if an earlier section *is* required for a later section, still, that earlier section may not be fully comprehensible without some knowledge of the later section.

What can the reader do? Read slowly, but jump ahead; reread what you have already read; *think* the whole time, but do not think too much without really knowing what you are thinking about. Talk to classmates; talk to teachers. Read with a pencil. Summarize passages in your own words. Invent your own symbolism (while remembering that communicating with others requires a common symbolism). Read other books on the same subjects.

Also: do exercises. Create your own exercises. Most sections of the book end with exercises. The student who is in a hurry will find out from a teacher which exercises to work on and will then try to do them immediately, looking back into the sections as necessary for examples. A difficulty in this approach is that most exercises here do not have unique correct *answers;* they have *solutions,* some of which are better than others. Finding the best solutions—even acceptable solutions—will require reading, thinking, and experience. Still, many of the exercises can be approached as puzzles: they do not need deep insight into the nature of things, but aim only to develop facility with some basic ideas.

Most exercises here could not very well be cast as multiple-choice questions. In a multiple-choice question, if you can somehow figure out the correct answer, even without being able to say how you did it, your answer is still 100% correct. Here, correct solutions to problems will carry *within themselves* the reasons why they are correct.

There are no answers at the back of the book. Problems here can have more than one correct solution; *you* should be able to tell whether a particular solution is correct. It is true that you may fail to notice some mistakes; the only way to avoid this is *experience,* not desire or will.

Somebody who does not know a language very well will not avoid mistakes just by trying hard: s/he[2] must *practice.* Likewise with games: even if you memorize all of the moves of chess and think real hard, you will not play a good

[2]The construction s/he can be pronounced as she or he (or as he or she). English has not evolved a generally accepted singular pronoun that refers to humans of either sex: it lacks the o(n) of Turkish. In the fourteenth century, according to the Oxford English Dictionary (OED) [34], the second-person plural pronoun you began to be used respectfully in place of the singular pronoun thou, just as the Turkish siz replaces sen. In the same way, currently, some people use they with a singular sense. Other people are bothered by this usage, and they may insist that he can refer to humans of unknown sex. The original OED does not recognize this usage. However, the OED does claim that she comes from a different base from he, because the feminine form derived from the base of he was too much like the masculine form.

chess-game at first. Depending on how seriously you take mathematics, you can see this book as lessons in a language or a game.

It would be worthwhile for the reader to have a look at Euclid's *Elements*. (Heath's English translation from the Greek is [19]—see the bibliography at the end of the book. This translation is available in print and in various places around the Web.) The present book does not share much *content* with the *Elements;* but Euclid's work does establish a sort of foundation or prototype for the mathematics of his and all succeeding generations, including our own.

Euclid wrote the *Elements*, the original textbook of mathematics, some 2300 years ago.[3] This textbook is still in use in some classrooms today. It consists of 13 books. You are not likely to read all of them; as with the present work, you will jump around, reading what you are interested in, perhaps with the guidance of a teacher. Indeed, perhaps Euclid expected few people to read his work unaided. His work does bring the reader instantly into real mathematics; but it also sets a standard for *spareness* (terseness, economy) of mathematical composition.

The *Elements* contains no commentary, no guidance for the reader. After a few definitions and *axioms*, the work consists solely of *propositions* and their *proofs*. Euclid does not *tell* you, but he *shows* you what proofs of propositions are.

The present book contains more than just propositions and their proofs; but it *does* contain these. Each proof here is labelled as such, and it ends with a little box. (The first example is on p. 25.) The propositions and proofs in the book consist of sentences of ordinary language, with some abbreviative symbolism (as well as the symbolism required by what the proofs are *about*). Such proofs might be called *informal,* because ordinary language is itself informal. Grammatical rules for English or Turkish or any other human language can indeed be formulated, and the conscientious speaker or writer will try to follow them; but it seems impossible to formulate grammatical rules that are obeyed by, and only by, everything that one wants to say.

Informal proofs are to be distinguished from *formal proofs*. Again, the notion of proof itself—*informal* proof—is over two thousand years old; but the notion of a *formal* proof dates only from the 1920s.[4] This book *tells* you, as well as shows you, what formal proofs are. Briefly described, a formal proof is a list of sentences of an *artificial* language; but such a list must satisfy certain requirements. The last sentence on the list is what the formal proof is a proof

[3] Euclid practiced mathematics in Alexandria around 300 BCE, probably having learned mathematics in Athens from the students of Plato [19, vol. I, pp. 1 f.].

[4] Perhaps the invention can be attributed to Hilbert [9, §07, n. 110].

of: it is what the proof *proves*. A machine could check whether a given list of sentences is a formal proof. To establish the truth of an interesting proposition, a formal proof is practically never called for. However, if it is held to the highest standard, an informal proof of some proposition P can be seen as an argument that a formal proof of P could in principle be written.

It will be an exercise in this book to write some formal proofs; but the ultimate goal is the ability to check the validity of *informal* proofs (like Euclid's, or any later mathematician's), *and* the ability to write one's own (informal) proofs.

I assume that you, the reader, have some experience with high-school algebra, and specifically with the algebra of the *integer*s. Then you can prove an identity like

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2) \tag{0.1}$$

(by multiplying out the right member and combining like terms). The algebra of the integers serves as a pattern for *Boolean algebra*, which I shall introduce as the algebra of the numbers 0 and 1 alone. If one considers these numbers to represent *falsity* and *truth,* then Boolean algebra determines an algebra of *propositions*, or a propositional *logic*.

After we have propositional logic, we can say something about *predicate* logic. This logic provides for the analysis of propositions into parts, some of which are *not* propositions. (Some parts of propositions will be *predicates:* hence the name of the logic.) We cannot define everything precisely until we have the notion of a *relation.* Relations are certain *sets;* they are *subsets* of *Cartesian products* of sets. So all of these things will need to be discussed.

A *function* can be defined as a kind of relation. Functions give us a way to say when two sets 'have the same size', or are *equipollent* (or *equipotent*). The set of integers has the same size as the set of *even* integers; both sets are *countably infinite;* but there are strictly *larger*, *uncountable* sets, such as the set of *real numbers*.

The predicate logic given here is more precisely called *first-order* predicate logic. Functions also allow us to give an account of *first-order logic* in general.

The integers have an *ordering*. This is a kind of relation. There is a generalization called a *partial ordering*. We shall prove a *representation theorem*, namely the proposition that every partial ordering behaves like the subset-relation (in a clearly defined way).

Equality is also a relation and is the motivating example of an *equivalence-relation*. The standard sorts of numbers—integers, rational numbers, real numbers, complex numbers—can be formally defined in terms of equivalence-relations, once one has the *natural numbers* 0, 1, 2, 3, ... The idea of this book

is that we do not *really* have these numbers, mathematically, until we can give a logical account of them. This book ends with such an account.

The topics of this book are so interrelated that, in any discussion of them, it is hard to avoid the appearance of circularity. This circularity is a part of the foundational aspect of the book. As I say, I assume that the reader is familiar with the integers; but I also say that we do not officially *have* the integers until the end of the book. Yet my supposedly rigorous account of the integers depends on all of the machinery that the book develops first, with the aid of a familiarity with. . . the integers.

Our path will have been, not circular, but spiral or rather *helical*, as if along a winding staircase. We start from the integers, and then we return to them, but at a higher (or deeper) level than where we started.

Typography

These printed words are assembled by means of the collection of typesetting programs and packages known as $\mathcal{AMS}$-LaTeX. Here, TeX is in Greek letters[5]; the same three letters will appear below, in § 1.0, in the full Greek name of logic. In the Latin alphabet, the letters are written TECH, as in technical. The $\mathcal{AMS}$ is the American Mathematical Society. The original TeX program was expanded into LaTeX and independently into $\mathcal{AMS}$-TeX; then the benefits of both expansions were combined into $\mathcal{AMS}$-LaTeX.

The original TeX program distinguishes between ordinary text and mathematical text. In ordinary text, in this book, words are *italicized* for the usual sorts of reasons: they (or their meanings) are being emphasized, they are titles, they are not in the language of the surrounding text, and so forth. I am also making some further distinctions. Technical terms are in **bold-face** when they are being defined, explicitly or implicitly. Technical terms might simply be *slanted* if their precise definitions will come later or are simply not needed. Words that are being *talked about* or *mentioned* (and not simply being *used*)[6]

[5] See [30, p. 1].

[6] The distinction between the *use* and the *mention* of a word (or symbol) is attributed to Quine in [9, § 08, p. 61]. The sentence 'A woman or a man is a human' uses the word woman. The sentence 'The English word for kadın also has five letters' mentions the word woman without using it. The sentence 'Woman has five letters' uses the word woman to mention the same word. Such a use can be called **autonymous,** following Carnap: again, the attribution is in [9, § 08, p. 61], where it is said that Frege introduced the practice of indicating autonymous use of words by quotation-marks (inverted commas). By this practice, the last quoted sentence would be "'Woman' has five letters."

are in sanserif. However, I may not have always been consistent in making these distinctions.

Footnotes here are intended to contain only material that is not essential to the main point. They may contain historical information that I have happened to discover, although much of the history of what I am discussing is still unknown to me.

Labelled proofs here end with boxes, as noted above; labelled examples end with bullets (the first is on p. 53).

Acknowledgments

The contents of this book have appeared in several editions:

1. Some of the material on logic and numbers was first prepared by me in 2001; at the same time, Andreas Tiefenbach prepared notes on sets and relations. Andreas, Belgin Korkmaz, and I taught Math 111 from those notes.

2. Andreas and I revised our respective notes, with Belgin's advice, the following year.

3. In 2004, in preparing to teach Math 111 that fall along with Ayşe Berkman and Mahmut Kuzucuoğlu, I composed my own complete set of notes, drawing on Andreas's notes in giving my own account of sets and relations.

4. After that semester, I revised the notes, keeping in mind the experience of Ayşe, Mahmut and myself, along with impressions from students. Advice from my friend Steve Thomas was also useful for this revision. The notes were used next year, in the fall semester of 2005/6, when I taught Math 111 with Belgin Korkmaz and Turgut Önder.

5. This new revision is based on that experience. However, there have been many changes, and this book must still be considered as a rough draft, a work in progress.

Many of the topics dealt with in this book are also covered by basic texts like [18] or [41]. I am not trying to write such a book as these are, but I find it useful to look at them. The preface of [41] is particularly reassuring, as it describes the many changes that the authors have made in each new edition of their book.

My own notes on logic draw from various sources, especially [9] and [6]; Ali Nesin's book [35] is an account in Turkish of some of the same material.

Set-theory on the level of my coverage seems generally to be found only in more advanced texts like [49] or [32]. I use these books, but try to give more elementary exercises than they do.

For my notes on natural numbers, [31] is inspirational.

As a student, I appreciated the style of Spivak [47]: not condescending, but treating the reader as a fellow mathematician.

Open Your Own Treasure House

Daiju visited the master Baso in China. Baso asked: "What do you seek?"

"Enlightenment," replied Daiju.

"You have your own treasure house. Why do you search outside?" Baso asked.

Daiju inquired: "Where is my treasure house?"

Baso answered: "What you are asking is your treasure house."

Daiju was enlightened! Ever after he urged his friends: "Open your own treasure house and use those treasures."

Paul Reps and Nyogen Senzaki
'101 Zen Stories'
Zen Flesh, Zen Bones
[40, p. 55]

1. Introduction

1.0. Logic

The name of **logic** comes ultimately from the (ancient) Greek adjective λογική, which is short for ἡ λογικὴ τέχνη. This phrase can be rendered in English as the rational art, or the art of reason. I shall not attempt to define reason. In Latin letters, the Greek phrase is hē logikē technē. But knowing the Greek alphabet is worthwhile, if only because mathematicians use it as a source of symbols. See Figure 1.1 below.

Logic as a field of study can be counted as a part of *philosophy*. One can do logic with ordinary language alone. Aristotle (384–322 BCE [3, pp. vii–ix]) is classically considered the originator of logic, and his texts are in ordinary Greek, albeit with some use of (Greek) letters to stand for parts of sentences. I shall take him as a source for some fundamental ideas: see §§ 1.1 and 1.8, as well as Appendix A.

Symbolic logic consciously develops a special notation for the notions that logic examines. Some two thousand years after Aristotle, George Boole describes the process at the beginning of *The Laws of Thought* [4, **[1]**, p. 1], first published in 1854:

> The design of the following treatise is to investigate the fundamental laws of those operations of the mind by which reasoning is performed; to give expression to them in the symbolic language of a Calculus,[1] and upon this foundation to establish the science of Logic and construct its method; to make the method itself the basis of a general method for the application of the mathematical doctrine of Probabilities; and, finally, to collect from the various elements of truth brought to view in the course of these inquiries some probable intimations concerning the nature and constitution of the human mind.

[1] This is calculus in the sense of a method of calculating; it has little to do with the *infinitesimal* calculus, which is the subject now called just calculus. What this book refers to as propositional logic can also be called *propositional calculus*.

A α	**a**lpha	H η	**ē**ta	N ν	**n**u	T τ	**t**au
B β	**b**eta	Θ ϑ	**th**eta	Ξ ξ	**x**i	Υ υ	**u**psilon
Γ γ	**g**amma	I ι	**i**ota	O ο	**o**micron	Φ φ	**ph**i
Δ δ	**d**elta	K κ	**k**appa	Π π	**p**i	X χ	**ch**i
E ε	**e**psilon	Λ λ	**l**ambda	P ρ	**r**ho	Ψ ψ	**ps**i
Z ζ	**z**eta	M μ	**m**u	Σ ς,ς	**s**igma	Ω ω	**ō**mega

Figure 1.1. The Greek alphabet. Mathematicians use (some of) these letters all the time. In this table, the first letter or two of the (Latin) name for a Greek letter provides a transliteration for that letter. In texts, the rough-breathing mark (῾) over an initial vowel (or ῥ) is transcribed as a preceeding (or following) h; the smooth-breathing mark (᾽) and the three tonal accents (ά, ᾶ, ὰ) can be ignored.

Boole's project is grander than mine. My interest here is almost entirely *mathematical*. The introduction of symbolism to logic allows logical notions to be examined as if they were numbers or geometric figures. In short, symbolism makes **mathematical logic** possible. This, then—*mathematical* logic—is one subject of this book.

Section 1.1 of the book makes a preliminary approach to the notion of a proposition, introducing the terminology of *axioms* and *theorems.* Section 1.2 introduces the basic terminology of *sets* and *natural numbers;* some of this terminology is used in the review of arithmetic in § 1.3. Arithmetic will be familiar to everybody from school; the main purpose here is to develop a point of view, a way of looking at mathematics, which we shall then apply to logic. Also, the notion of *arithmetic term* introduced in § 1.3 will provide an example of a *proof by induction.* Finally, arithmetic is the setting for some ancient mathematical proofs; these are given as examples in § 1.4. Further investigation into these examples is in § 1.5. In §§ 1.6 and 1.7, some operations on the set $\{0, 1\}$ are introduced by means of, and by analogy with, the usual arithmetic operations. What these correspond to in ordinary language is discussed in § 1.8; further logical analysis of language is in § 1.9.

The operations on $\{0, 1\}$ are essential to the study of mathematical logic as such, which begins in Chapter 2.

Exercise

Memorize the Greek alphabet.

1.1. Language and propositions

We are using language right now. We divide up language into **sentences.** Some sentences, but not all, can be described as **true** or **false.** At least, some sentences are true or false when placed in a *situation* or *context.* Let us refer to such sentences as **statements** or **propositions.**[2] For example, the sentence

I went to Van last year

is a statement (or a proposition). Whether it is true or false depends on who says it and when: the speaker and the time would be the *context* in which the sentence is true or false.[3]

We shall mainly be interested in *mathematical* propositions. Such propositions are timeless and personless: their truth or falsity does not change with time or with the person who utters them. Still, in § 3.5, we shall see a way in which, strictly, a mathematical proposition must still be placed in a context in order to become true or false.

The *belief* that a mathematical proposition is true or false may change with time. Certain mathematical propositions have been accepted as true for many years, only to be found false. For example, Proposition I.16 of Euclid's *Elements* can be called false, even in its context, since its proof relies on unstated assumptions that do *not* follow from the stated assumptions; but this falsehood was not recognized[4] until the nineteenth century. However, the philosopher R. G. Collingwood writes in his autobiography [11, pp. 31–33]:

> [Y]ou cannot find out what a man means by simply studying his spoken or written statements, even though he has spoken or written with perfect command of language and perfect truthful intention. In order to find out his meaning you must also know what the question was (a question in his own mind, and presumed by him to be in yours) to which the thing he has said or written was meant as an

[2] We could make a distinction here: we could let a *statement* be a bit of language of a certain grammatical form, letting a *proposition* be the *meaning* of a statement. See [9, p. 26]. I am *not* going to try to make such a distinction.

[3] The context can also include the listener, as when the sentence is You went to Van last year.

[4] See Heath [19, vol. 1, p. 280] for some commentary.

> answer... If the meaning of a proposition is relative to the question it answers, its truth must be relative to the same thing.

If we *translate* Euclid's work into the kind of formal proofs that will be developed in this book, then indeed we shall find errors or gaps in the proofs. Euclid himself was not writing formal proofs; there was no notion of such a thing for over two thousand years. However, Euclid *was* doing mathematics, and correctly, I would say; but this is for you to judge, *after* reading Euclid himself and understanding his purpose—after understanding the questions he was answering.

Euclid's work begins with five propositions that we call *axioms* or *postulates*. (He, apparently [53, p. 442], called them αἰτήματα, that is, requests, demands, or assumptions.) An **axiom** is usually a proposition that satisfies two criteria:

1. it is *self-evident;*
2. it is useful for proving other propositions.

In common usage, the first criterion is probably more important; in mathematical usage, the second.

A **self-evident** proposition is self-evidently *true:* that is, obviously true without any need of appeal to some other authority. A classical use of the compound word self-evident is found in a certain revolutionary manifesto[5] of the eighteenth century. I transcribe from [25, p. 15], with my own formatting:

> We hold these truths to be self-evident,
>
> 1) that all men are created equal,
> 2) that they are endowed by their Creator with certain unalienable rights,
> 3) that among these are life, liberty and the pursuit of happiness.
> 4) That to secure these rights, governments are instituted among men, deriving their just powers from the consent of the governed.
> 5) That whenever any form of government becomes destructive of these ends, it is the right of the people to alter or abolish it, and to institute new government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their safety and happiness.

[5] Namely, the Declaration of Independence of the United States of America, written in 1776 by Thomas Jefferson, who, with other signers of the document, possessed other human beings as slaves. In 1945, Vietnamese revolutionaries led by Ho Chi Minh issued a Declaration of Independence that enunciated some of the truths of the American declaration [59, ch. 18]; this did not prevent a later American invasion.

Two thousand years earlier, before Euclid even, in the collection of books now known as the *Metaphysics* [3], Aristotle writes of axioms, using the Greek source of our word axiom, namely ἀξιώμα. This word has the root meaning of *something worthy,* or an *honor.* Aristotle seems to use axiom almost as a synonym of principle (ἀρχή) or common notion (κοινὴ δόξα). His writing is elliptical, in the style of lecture-notes—which is probably just what his works are [3, pp. xxv & xxxi]; I translate accordingly below, with seemingly missing words supplied in brackets. (Some of the original Greek words in parentheses are the sources of modern technical terms.)

In Book B (that is, Book Beta, also called Book III) of the *Metaphysics*, Aristotle introduces some questions:

> [996 b 26] Yet indeed, concerning the demonstrative (ἀποδεικτικός) principles, whether they belong to one science (ἐπιστήμη) or more (πλειών) is debatable. I call demonstrative the common notions from which everybody proves (δείκνυμι) [propositions], for example, it is necessary to affirm or deny everything,[6] or it is impossible to be and not be at the same time,[7] and however many other such premisses (προτάσις).

Aristotle's examples of common notions are called the Law of the *Excluded Middle* and the Law of *Contradiction;* they are discussed further in Book Γ (IV). That book opens with a statement of the general subject, which we call **metaphysics,** but Aristotle called **first philosophy:**

> [1003 a 20] There is a science (ἐπιστήμη) that looks at (θεωρέω) being as such (τὸ ὂν ᾗ ὄν) and what applies to it (τὰ τούτῳ ὑπάρχοντα) according to itself (καθ' αὑτό).[8]

A Turkish version of this passage, from [1], is

> Varlık olmak bakımından varliğı ve ona özü gereği ait olan ana nitelikleri inceleyen bir bilim vardır.

[6] πᾶν ἀναγκαῖον ἢ φάναι ἢ ἀποφάναι.

[7] ἀδύνατον ἅμα εἶναι καὶ μὴ εἶναι.

[8] The whole Greek sentence, as given in [3], is Ἔστιν ἐπιστήμη τις ᾗ θεωρεῖ τὸ ὂν ᾗ ὄν καὶ τὰ τούτῳ ὑπάρχοντα καθ' αὑτό. The Greek ὄν (stem ὄντ-) is the neuter participle corresponding to the Engish being and the Turkish olan; it appears in modern technical terms like ontology. The feminine stem of the participle is οὔσ-; from this is derived the abstract noun οὐσία, which I translate below as beingness, although a traditional (and misleading) translation is substance.

Later in Book Γ, in ch. 3, Aristotle takes up axioms; but he understands them as something more general than the subject of a particular field like mathematics or physics. First he seems to repeat the question raised in Book B:

> [1005 a 19] It must be said whether [the inquiry] concerning the so-called axioms (ἀξιώματα) of mathematics, and concerning beingness (ἡ οὐσία), belongs to one science (ἐπιστήμη) or another (ἑτέρα).
>
> It is evident (φανερόν) that the inquiry (σκεψίς) concerning these belongs to one [science], namely that of the philosopher (φιλοσόφος).
>
> For, [the axioms] apply to all beings, not just to some particular class (γένος) apart from the others.
>
> Also, all [scientists] use [the axioms]—because they are of being as such—while each class [has] being.
>
> To whatever extent is appropriate for them, to that extent they use [the axioms]—that is, to the extent of the class concerning which they carry out their proofs (ἀποδείξεις).
>
> So, because it is clear (δηλόν) that [the axioms] apply to all things as beings—for this [namely, being] is common to them—the theory (ϑεωρία) concerning them belongs to those who are gaining knowledge (γνωρίζοντοι) concerning being as such.
>
> Therefore, none of those making particular investigations (οἱ κατὰ μέρος ἐπισκοποῦντοι) tries to say something concerning them, whether [they] are true or not—not the geometer (γεωμέτρης), not the arithmetician (ἀριϑμητικός).
>
> But some of the physicists (φυσικοῖ)[9] [were] doing this appropriately (εἰκότως).
>
> For, they thought they alone were doing research (σκοπέω) concerning all nature (ἡ φύσις) and concerning being.
>
> But since there is somebody even higher (ἀνωτέρω) than the physicist—for nature is [just] some one class of being—the inquiry concerning these would belong to the theoretician (ϑεωρητικός) of generality (καϑόλου) and first [or primary] beingness (ἡ πρώτη οὐσία).
>
> Physics (ἡ φυσική) is a kind of wisdom (σοφία), but not the first [or foremost] (πρώτη).

Presently we come to what were called common notions in Book B, then axioms (in Book Γ), and now principles:

[9] Aristotle's 'physicists' are pre-Socratic philosophers such as Thales of Miletus; they are discussed in Book A of the *Metaphysics*.

> [1005 b 8] It is proper for the one who knows best each class [of things] to be able to state the most certain principles (ἀρχαί) of the thing (πράγμα):
>
> So that the one [who knows best] being as such [can state] the most certain [principles] of all [things]. This is the philosopher.
>
> The most certain principle of all is that about which being mistaken is impossible.

This principle is the **Law of Contradiction,** which Aristotle now states more precisely than in Book B:

> [1005 b 19] For the same [*predicate*] to apply and not apply at the same time to the same [*subject*] in the same [respect] is impossible.[10]

The grammatical notions of subject and predicate are discussed briefly in § 1.2 below; there also the Law of Contradiction will be put to use. Meanwhile, a Turkish rendition of Aristotle's formulation of the Law of Contradiction, again from [1], is

> Aynı niteliğin, aynı zamanda, aynı özneye, aynı bakımından hem ait olması, hem de olmaması imkânsızdır.

After a long discussion of the Law of Contradiction and those who question it, Aristotle gives the **Law of the Excluded Middle,** again with slightly different wording from Book B:

> [1011 b 23] Neither does [any]thing admit to being between a contradiction, but it is necessary either to affirm or deny one of one, whatsoever.[11]
>
> Öte yandan çelişik önermeler arasında bir aracının olması da imkânsızdır. Bir özne hakkında tek bir yüklemi—hangi yüklem olursa olsun—, zorunlu olarak ya tasdik etmek veya inkâr etmek gerekir.

In other words, a proposition is true or false; there is no third alternative. A **contradiction** [ἀντιφάσις] for Aristotle is evidently a pair of propositions, one affirming something, the other denying the same thing. The continuation of this passage is in § 1.8 below. If we follow Aristotle, it seems that, as mathematicians,

[10] τὸ γὰρ αὐτὸ ἅμα ὑπάρχειν τε καὶ μὴ ὑπάρχειν ἀδύνατον τῷ αὐτῷ καὶ κατὰ τὸ αὐτό.

[11] Ἀλλὰ μὴν οὐδὲ μεταξὺ ἀντιφάσεως ἐνδέχεται εἶναι οὐθέν, ἀλλ' ἀνάγκη ἢ φάναι ἢ ἀποφάναι ἓν καθ' ἑνὸς ὁτιοῦν.

we need not concern ourselves with the Laws of Contradiction and the Excluded Middle; we can just accept these principles and use them; it is the philosopher's job to identify and enunciate them. But the logician is also a philosopher. In any case, we shall use these principles explicitly in the next section; but we shall also see an apparent violation of one of them. There we shall also begin to state axioms in our mathematical sense.

A **theorem** today is usually considered just as a *noteworthy* proposition with a proof from axioms. The first example is Theorem 1.2.2 in the next section. The word theorem itself comes from the Greek θεώρημα, and it is related to the verb with the meaning of look at. (This verb is found at the beginning of Book Γ of the *Metaphysics* as quoted above on p. 18.) In former times, finer distinctions were considered. A few centuries after Aristotle, Pappus of Alexandria[12] writes:

> Those who favor a more technical terminology in geometrical research use **problem** (πρόβλημα) to mean a [proposition[13]] in which it is proposed to do or construct [something]; and **theorem,** a [proposition] in which the consequences and necessary implications of certain hypotheses are investigated; but among the ancients some described them all as problems, some as theorems.

A **lemma** is a proposition proved mainly for the sake of proving other propositions; the first example will be Lemma 1.4.2. (The Greek λέμμα means that which is peeled off, and is from the verb, λέπω, with the meaning of peel.) A **corollary** to a theorem is a proposition that follows almost immediately from the theorem; the first example will be Corollary 1.4.6. (The word derives from the Latin COROLLARIVM, which is the neuter form of the adjective derived from COROLLA; this means, among other things, a wreath of flowers [34].)

1.2. Classes, sets, and numbers

In Chapter 3, we shall have a lot to say about *sets;* but it will be useful to have the basic notion available from the beginning.

A *set* is many things, made into one. There are many special cases of sets: Two matching earrings make a *pair;* several football-players make a *team;* the

[12] Pappus may have been born during the reign of Theodosius I, 379–395 BCE, or he may have flourished earlier, during the reign of Diocletian, 284–305 BCE. The possibilities are discussed in [54, pp. 564–567], where also are found the text and translation from which the quotation is adapted.

[13] Ivor Thomas [54, p. 567] uses inquiry here; but there is *no* word in the Greek original corresponding to this or proposition.

pigeons descending on bread-crumbs in the park make a *flock.* Words like pair, team and flock are **collective nouns.** In mathematics, the word set is the most general collective noun—except for the word class.[14]

In the previous section, I translated Aristotle's word γένος as class, but that does not mean that our understanding will be the same as Aristotle's. For us, every set is a class, but not every class is a set. Classes and sets are made up of **elements** or **members.** In the context of classes, there is no mathematical difference between the words element and member. (However, in an equation, such as (1.1) below, the expressions on either side of the *sign of equality,* or =, can be called the **members** of the equation.)

A **class** is determined by a **property.** The property **defines** the class. I do not attempt to define property; I shall just say that, for every property, there is a class whose members are precisely the things that have that property. This does not mean that a class is necessarily a thing that can itself be a member of classes. Indeed, if we assume that every class *can* be a member of classes, then we can derive a contradiction. This is what we do in the proof of Theorem 1.2.2 below. The contradiction is the reason why we have to distinguish classes and sets.

A **set** is a class that *is* a member of some classes. If A is a set, and $\mathbf{C}$ is a class, then the sentence

$$A \text{ is a member of } \mathbf{C}$$

is true or false—it is a proposition. Again, all sets are classes; but Theorem 1.2.2 shows that not all classes are sets.

A class can be indicated in writing or print by the presence of **braces** around its members. So, if we have, say, three objects,

$$a, b, c,$$

then we can form the *single* object

$$\{a, b, c\}.$$

This single object is a *class,* namely the class of all things with the property of being one of a, b, and c. In fact, this class will be a *set.* In particular, this set **contains** a, b, and c (and nothing else) as elements.

[14] Levy [32] seems to use collection more generally even than class.

Elements of a class are **in** the class. If **C** is a class, then we have several ways of saying the same thing:

$$\mathbf{C} \text{ contains } d;$$
$$d \text{ is an element of } \mathbf{C};$$
$$d \text{ is a member of } \mathbf{C};$$
$$d \text{ is in } \mathbf{C}.$$

Any of these can be expressed by the symbolism[15]

$$d \in \mathbf{C}.$$

To *deny* that $d \in \mathbf{C}$, we can write

$$d \notin \mathbf{C},$$

which can be read as d is not in $\mathbf{C}$.

One can say that a class **comprises** its elements, and the elements **compose** the class. Unfortunately, the verbs comprise and compose are often confused by native English-speakers. Alternatively, a set **consists of** its elements.

Words like collection, aggregate and family are sometimes used as synonyms for set (or perhaps for class).

I say that a set is *many* things, made into one; but I am using the word many more generally than is usual in ordinary language. A set might have two elements or one element. A set might have *no* element at all: such a set is

$$\varnothing,$$

the **empty set**. I shall also assume that sets can have *infinitely* many elements, and that, in particular, the *natural numbers* compose such a set, namely

$$\{0, 1, 2, 3, 4, \dots\}.$$

In Chapter 4, this assumption will turn out to be a *consequence* of the Axiom of Infinity, 4.0.1.

A class **C** is **included in** a class **D** if every element of **C** is an element of **D**. In this case, we can write

$$\mathbf{C} \subseteq \mathbf{D},$$

[15] The sign $\in$ is apparently derived from the Greek ε. Peano [37] used this letter in 1889 as a symbol with the meaning of is, perhaps because the Greek word for is is ἐστί. For Peano, $d \in \mathbf{C}$ means d is a **C**, that is, d is one of the things denoted by the term **C**.

and we can say also[16] that **D includes C** or that **C** is a **subclass** of **D**. A subclass of **D** that is also a set is a **subset** of **D**. If **C** is *not* a subclass of **D**, we can write

$$\mathbf{C} \not\subseteq \mathbf{D}.$$

The first *axiom* of set-theory is that sets are determined by their elements, so that if two sets have the same elements, then the sets themselves are the same, that is, **equal.** We can express this more symbolically:

Axiom 1.2.1 (Extension)**.** *If A and B are sets such that $A \subseteq B$ and $B \subseteq A$, then*

$$A = B. \tag{1.1}$$

Instead of $A \subseteq B$, some people write

$$A \subset B;$$

but I prefer to use this to mean that A is a **proper** subset of B, that is, $A \subseteq B$, but $A \neq B$.

Again, a class is defined by a property. A property can be symbolized by a **predicate.** A predicate *says something* about a *subject.* (See the Law of Contradiction, in the previous section, as translated from Aristotle.[17]) If P is a predicate, then the corresponding class can be denoted by

$$\{x : Px\}; \tag{1.2}$$

this is read as the class of x such that P [applies to] x; here, the *variable* x takes the place of a grammatical subject of P.

If A is a set, then *being an element of* A is a property; the class defined by this property is

$$\{x \colon x \in A\}.$$

[16] Some people would say here that **D** *contains* **C**; but it is desirable to read $\mathbf{C} \subseteq \mathbf{D}$ differently from $c \in \mathbf{D}$.

[17] The English predicate is from the Latin PRAEDICATVM, a participle of the verb PRAEDICARE. This verb consists of the prefix PRAE- (or PRE-) and the verb DICARE. This verb, with root DIC-, means *say,* and it can be found in various English words, such as indicate and dictionary. The Latin PRAEDICATVM is a translation of the Greek κατηγορεύμενον [50], a participle of κατηγορέω; this verb consists of the prefix κατα- and the verb αγορεύω, which means *speak before an assembly of the people;* such an assembly is an αγορά. See Appendix A. The verb κατηγορέω (or some related word) is the source of the English *category.*

This class is just the set A. Again, by the Extension Axiom, two sets are equal if they have the same members; more generally; two *classes* are equal if they have the same members. In particular, two predicates that are different as symbols may nonetheless define the same class; we may have $\{x\colon Px\} = \{x\colon Qx\}$, even though P and Q are different predicates.

Often, in place of Px in (1.2), we have to write something that features x more than once. For example, there is a property of *not being a member of oneself*. In words, the corresponding predicate is something like

$$\text{\_\_\_\_ is not a member of \_\_\_\_-self,} \tag{1.3}$$

with two spaces left for a subject. The phrase is not a member of is also symbolized by $\notin$; so the given property determines the class

$$\{x : x \notin x\}. \tag{1.4}$$

This is the historically first[18] example of a class that is not a set:

Theorem 1.2.2 (Russell Paradox)**.** *The class* $\{x : x \notin x\}$ *is not a set.*

Proof. Call this class $\mathbf{R}$, and suppose it *is* a set. Then by the Law of the Excluded Middle, either $\mathbf{R} \in \mathbf{R}$ or $\mathbf{R} \notin \mathbf{R}$.

Suppose $\mathbf{R} \in \mathbf{R}$. Then, by the Law of Contradiction, it is not the case that $\mathbf{R} \notin \mathbf{R}$. This means $\mathbf{R}$ fails to have the defining property of members of $\mathbf{R}$, and so $\mathbf{R} \notin \mathbf{R}$. In short, if $\mathbf{R} \in \mathbf{R}$, then $\mathbf{R} \notin \mathbf{R}$. On the other hand, trivially, if $\mathbf{R} \notin \mathbf{R}$, then $\mathbf{R} \notin \mathbf{R}$.

Having considered both possibilities, we conclude $\mathbf{R} \notin \mathbf{R}$. This means $\mathbf{R}$ *does* have the defining property of members of $\mathbf{R}$, so $\mathbf{R} \in \mathbf{R}$. Thus $\mathbf{R}$ is and is not a member of itself. This violates the Law of Contradiction. Therefore the assumption that $\mathbf{R}$ is a set must be mistaken, so $\mathbf{R}$ is not a set (by the Law of the Excluded Middle). □

The proof ends with a box,[19] as noted on p. 8. This particular proof is a **proof by contradiction,** because it assumes the falsity of what is to be proved, and it derives from this a violation of the Law of Contradiction.

[18] Russell gives the example in a letter [44] to Frege in 1902; but Levy [32, p. 6 correction] cites an article attributing an independent discovery of the example to Zermelo.

[19] Other writers use a different symbol, or none at all. An old-fashioned termination of a proof is QED, for the Latin QVOD ERAT DEMONSTRANDVM, with the meaning of which was to be demonstrated.

This particular proof also shows that there is a class to which the predicate in (1.3) neither applies nor fails to apply. So we have an apparent violation of the Law of the Excluded Middle. I would say rather that we have an example of a class that is not a *real thing,* so that it is just meaningless to try to apply predicates to it. *Elements* of classes are the real things.

We do assume that subclasses of sets are sets:[20]

Axiom 1.2.3 (Separation)**.** *Suppose $\mathcal{U}$ is some set, and P is a predicate. The class of elements* of *$\mathcal{U}$ to which P applies is a set.*

The set created by the axiom is denoted by

$$\{x \in \mathcal{U} \colon Px\}.$$

I use the letter $\mathcal{U}$ here because it stands for universe; but the set could be anything. For a mundane example, we could let $\mathcal{U}$ be the set of human beings living now, and let P be the predicate is over two meters tall. Then $\{x \in \mathcal{U} \colon Px\}$ is the set of people now taller than two meters. However, in using sets for mathematics, we have no need to consider classes that contain anything other than sets. This is because, by starting with the empty set, and by putting sets into other sets, we can create the *natural numbers;* from these, we can create all of the other objects of mathematics. The procedure is as follows.

Any two classes **C** and **D** have a **union,** which is the class comprising every element of **C** or **D** (or both); this union is denoted by

$$\mathbf{C} \cup \mathbf{D}.$$

(See § 3.0.)

Axiom 1.2.4 (Adjunction[21])**.** *If A is a set, then for all b, there is a set whose elements are just b and the elements of A.*

The new set guaranteed by the Axiom is denoted by

$$A \cup \{b\}.$$

Theorem 1.2.5 (Pairing)**.** *For every a and b, the classes $\{a\}$ and $\{a, b\}$ are sets.*

[20] The following Axiom of Separation is also called the **Axiom of Comprehension;** but I think this term is better reserved for the original, but false, assumption that every property defines a set.

[21] The terminology is from George Boolos, according to Wikipedia `http://en.wikipedia.org/wiki/General_set_theory` (accessed September 15, 2010).

Proof. By the Adjunction Axiom, the class $\varnothing \cup \{a\}$ is a set; but this set is just $\{a\}$. Then, by the Axiom again, $\{a\} \cup \{b\}$ is a set; but this set is just $\{a, b\}$. □

The set $\{a\}$ is called a **singleton.** Evidently the proof can be continued to show that $\{a, b, c\}$ is a set, $\{a, b, c, d\}$ is a set, and so on; in short, *finite* classes are sets.

From any set A, we can now form the union

$$A \cup \{A\}.$$

This idea can be used to give the following **recursive definition** of the **natural numbers.** First, we declare that the number **zero** is just the empty set:

$$0 = \varnothing.$$

Then we define the natural numbers by two rules:

1. 0 is a natural number.
2. if n is a natural number, then $n \cup \{n\}$ is a natural number.

The latter rule assumes that n is a set; but then $n \cup \{n\}$ is also a set. The latter set can be called the **successor** of n. Hence all natural numbers are sets, and every natural number has a successor, which is a natural number.

To the recursive defition of natural numbers, some writers might add a third condition:

3. Nothing else is a natural number.

However, I understand such a condition to be implicit in every recursive definition as such.

If n is a natural number, let us denote its successor $n \cup \{n\}$ by

$$n'.$$

Then we have

$$n \in n', \qquad\qquad n \subseteq n'. \tag{1.5}$$

The recursive definition of the natural numbers makes **proof by induction** in the following sense possible. Suppose P names a property that some natural numbers may have, and suppose moreover that we can establish the following two conditions.

1. $P0$.
2. For every natural number n, if Pn, then $P(n')$.

Then we have proved by induction that every natural number must have the property (named by) P. In the second condition, Pn is called the **inductive hypothesis.** The method of proof by induction is first used in Lemma 1.2.7 below. In general, an inductive proof consists of two steps:

1) the **base step,** in which $P0$ is proved;
2) the **inductive step,** in which $P(n')$ is proved from the inductive hypothesis Pn.

It is not obvious that there is even a **class** consisting of the natural numbers: what *property* do these numbers share? Well, they share the property that they can be obtained by starting with $\varnothing$ and taking successors; but it is not obvious how to make this property precise. One way that works is the following, as we shall show in § 4.8. We can first define an **ordinal** to be a set α such that

1) α *includes* each of its elements (that is, if $x \in \alpha$, then $x \subseteq \alpha$);
2) if α has two distinct elements, then one of them contains the other;
3) If $A \subseteq \alpha$, and A is not empty, then A has an element b that is contained by all of the other elements of A, though not by b itself.

Then every element of an ordinal is an ordinal. An ordinal is a **limit** if it is not empty and is not of the form $\beta \cup \{\beta\}$ for any set β. Then a natural number is an ordinal that neither *is* a limit nor *contains* limits. Again, this will be worked out in § 4.8; meanwhile, let us accept the informal definition of the natural numbers.

The class of natural numbers is denoted by

$$\omega.$$

This symbol is not the Latin minuscule letter w (the so-called double u); it is the Greek minuscule *omega.* Observe that mega means big, so an omega is a big o—rather, a double o, or oo, which, if written quickly, may come out looking like ω.

As we have just defined them, the natural numbers can be called more precisely the **von-Neumann natural numbers.**[22] The first four von-Neumann natural numbers are

$$\varnothing, \qquad \{\varnothing\}, \qquad \{\varnothing, \{\varnothing\}\}, \qquad \Big\{\varnothing, \{\varnothing\}, \big\{\varnothing, \{\varnothing\}\big\}\Big\},$$

where again $\varnothing = 0$. We have the following standard symbols for some successors:

n	0	1	2	3	4	5	6	7	8
n'	1	2	3	4	5	6	7	8	9

[22] These natural numbers are instances of the von-Neumann *ordinal numbers,* defined by von Neumann in 1923 [57]. However, in his introduction to von Neumann's paper, van Heijenoort cites Bernays as saying that Zermelo had a similar idea for ordinals in 1915; also, in this context, Levy [32, II.3.8, p. 52] cites Zermelo from 1916.

Also, we may write

$$n + 1$$

for n'. If m and n are in ω, and $m \subseteq n$, then we usually write

$$m \leqslant n.$$

The class ω has two more properties, besides admitting proofs by induction; these are given by the next two theorems.

Theorem 1.2.6. 0 *is not the successor of any natural number.*

Proof. We argue by contradiction. Suppose 0 is a successor; say $0 = n'$. But $n \in n'$, as noted in (1.5); so $n \in 0$. This contradicts that 0 is empty. Therefore 0 is not a successor. □

Lemma 1.2.7. *Every von-Neumann natural number includes all of its elements.*

Proof. We use induction. Let P be the predicate

____ includes all of its elements.

Since 0 has no elements, trivially 0 includes all of its elements. Therefore $P0$. This completes the base step of the proof.

For the inductive step, suppose Pn (as an inductive hypothesis). Say $k \in n'$. Since $n' = n \cup \{n\}$, either $k \in n$, or $k \in \{n\}$. If $k \in n$, then $k \subseteq n$ by inductive hypothesis. If $k \in \{n\}$, then $k = n$, so $k \subseteq n$. In either case, $k \subseteq n$. But $n \subseteq n'$. Hence $k \subseteq n'$. (We use the obvious proposition that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$; this proposition will be part of Lemma 3.1.5.) In short, if $k \in n'$, then $k \subseteq n'$. Therefore $P(n')$. This completes the induction. □

Theorem 1.2.8. *Natural numbers with the same successor are the same.*

Proof. Suppose k and n are natural numbers, and $k' = n'$. We must show $k = n$. We have

$$k \cup \{k\} = n \cup \{n\}.$$

In particular, $k \in n \cup \{n\}$ and $n \in k \cup \{k\}$. Suppose if possible $k \neq n$. Then we must have $k \in n$ and $n \in k$, hence $k \subseteq n$ and $n \subseteq k$ by the previous lemma, and therefore $k = n$ by the Axiom of Extension, 1.2.1. This contradicts the assumption that $k \neq n$; therefore the assumption is false, and $k = n$. □

We can call m an **immediate predecessor** of m'. By our recursive definition, every natural number that is not 0 must be m' for some m; that is, every natural number n other than 0 has an immediate predecessor. By the last theorem, this predecessor is *unique:* it is *the* immediate predecessor of n, and it can be denoted by

$$n - 1.$$

The von-Neumann definition of the natural numbers is convenient, because according to this definition, each natural number n is just the set that can be denoted by

$$\{0, \ldots, n - 1\}.$$

If $n = 0$, then this is the empty set.

If we do not happen to care about whether each natural number is a particular set, then we can denote the set of natural numbers by

$$\mathbb{N};$$

this is the usual notation when one is not interested in set-theory. Then $\mathbb{N}$ is just a class that contains an element 0, and whose every element n has a successor, which can be denoted by

$$n^+ \tag{1.6}$$

or $n + 1$, such that:

1) 0 is not the successor of any element of $\mathbb{N}$;
2) elements of $\mathbb{N}$ with the same successor are the same;
3) $\mathbb{N}$ is included in every class that contains 0 and that, for every n in $\mathbb{N}$, contains n^+ if it contains n.

These conditions on $\mathbb{N}$ are the *Peano Axioms;* we shall show in Chapter 4 that all properties of $\mathbb{N}$ follow from them.

Exercises

1. Prove by induction that every element of ω either *is* 0 or *contains* 0.

2. What is wrong with the following proof that every element of ω is equal to each of its elements?

> For all n in ω, if $k \in n$, we show $k = n$. We use induction on n. The claim is trivially true when $n = 0$, since 0 has no elements. Suppose the claim is true when $n = m$. Suppose $k \in m'$. Then either $k \in m$ or $k = m$. If $k \in m$, then by

inductive hypothesis, $k = m$. Therefore, in any case, $k = m$. That is, every element of m' is m. But by inductive hypothesis, m is equal to its immediate predecessor (since this is an element of m). Let the immediate predecessor of m be ℓ. Then $\ell = m$, so $\ell' = m'$. But $\ell' = m$, since ℓ is the immediate predecessor of m. Therefore $m = m'$. If $k \in m'$, we have already shown $k = m$; now we can conclude $k = m'$. This completes the induction.

3. From the 'theorem' in the preceeding exercise, prove that all natural numbers are equal to 0.

1.3. Algebra of the integers

Now that we have, from the previous section, a precise definition of the natural numbers, I want to review some things that we know about them from school. We cannot yet define all of these things precisely, or prove them: this will happen in Chapter 4. Meanwhile, we just have a set called $\mathbb{N}$, whose members form the list

$$0, 1, 2, 3, \ldots .$$

As we have seen, every natural number n has a successor, which is usually denoted by $n + 1$. Some mathematicians start the list of natural numbers at 1 instead of 0; but I shall just say that the members of the set $\{1, 2, 3, \ldots\}$ are the **positive** natural numbers.

The number 0 does not have an immediate predecessor that is a natural number; but it does have the immediate predecessor called -1. This is not a natural number, but it is an *integer*. The set of **integers** comprises every natural number, along with a **negative,** denoted by $-n$, for each positive natural number n. Then $-n$ has the successor $-(n-1)$ and the immediate predecessor $-(n+1)$. The integers that are not natural numbers are also called **negative** integers. *Every* integer n has a **negative,** denoted by $-n$, although this number is itself negative only if n is positive.

The set of integers is commonly denoted by[23]

$$\mathbb{Z}.$$

This set is equipped with three *operations,* namely **addition, additive inversion,** and **multiplication.** (Operations are *functions;* functions in general and operations in particular are defined formally in § 3.3.) In particular, if x and y are integers, then so are

1) $x + y$ (the **sum** of x and y, which here are **addends**),
2) $-x$ (**minus-**x, the **additive inverse** or **negative** of x), and
3) $x \cdot y$ (the **product** of the **factors** x and y).

By convention, multiplication is also indicated by **juxtaposition;** that is, the product $x \cdot y$ is also denoted by

$$xy.$$

Something like the symbol for additive inversion is also used for a fourth operation, **subtraction,** which can be defined in terms of the other operations. *Subtracting*[24] y from x produces a **difference,** which is denoted by

$$x - y,$$

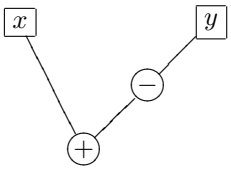
and which is just the sum of x and $-y$. Note that $x - y$ is not generally the same as $y - x$. If we want to assign names, then, in the difference $x - y$, we can call x the **minuend** (from the Latin, with the meaning of that which is to be diminished), and we can call y the **subtrahend** (that which is to be subtracted).

Subtraction is thus a **composition** of two other operations. The process of

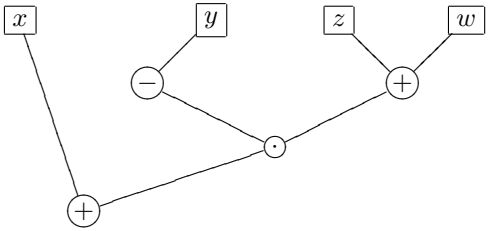
[23] Here the letter zed or zee stands for the German Zahl, number. In English, the integers are also called **whole numbers.** In fact, the English word integer comes from the Latin INTEGER, which means whole. This Latin word developed in France into the French word entier, which entered English and became entire. Thus two English words—integer and entire—represent the same Latin word. People interested in such matters may refer to such pairs of words as *doublets.*

[24] The English verb subtract is sometimes pronounced as if it were substract. The English verb comes from a participle of the Latin verb whose infinitive is SUBTRAHERE. This verb is in turn built up from TRAHERE (meaning draw or carry) and the preposition SUB (meaning from below or away). According to the OED [34], in medieval times, an s was inserted between SUB and TRAHERE, yielding SUBSTRAHERE, from which came substract in English; but this formation is considered incorrect. The English word abstract is from the Latin ABSTRAHERE, but here the s belongs properly to the preposition ABS, although the preposition is more commonly seen as AB or even A.

computing $x - y$ can be indicated by a **tree,**[25] thus:



More complicated compositions and trees are possible. For example, the tree



indicates the sum of x and the product of minus-y and the sum of z and w. Usually this sum is written on one line, as

$$x + -y \cdot (z + w), \tag{1.7}$$

or more simply as

$$x - y(z + w).$$

I shall refer to such a **string** of symbols as an *arithmetic term.*[26] (The Greek word[27] for number is ἀριθμός, which is ARITHMOS in Latin letters. Our general definition[28] of term comes in § 3.5.)

Officially, **(arithmetic) terms** will be certain strings composed of

1) the symbols $+$, $-$ and $\cdot$ (a dot);
2) **variables,** such[29] as x, y and z;

[25] Trees as such are covered in a later course, Math 112.

[26] Here the word arithmetic is an adjective and is pronounced with the stress on the penultimate (next-to-last) syllable.

[27] Strictly, the Greek word ἀριθμός refers to *a number of things*, in particular, more than one;—certainly not zero or 'fewer' than zero. See [28].

[28] In another context, Aristotle's definition of term is in Appendix A.

[29] The convention of using letters from the end of the Latin alphabet for 'unknown quantities' dates back to Descartes; see [13]. Since we don't want any limit on the number of variables we can use, and yet we want to define things precisely, we could declare officially that our variables must come from the list x, x', x'', and so forth.

3) symbols for certain integers, such as 12, 0 and −137—such symbols can be called **numerals**[30] or **(numeral) constants**[31];
4) the parentheses (and).

The formal definition of arithmetic terms is recursive, in the sense of the previous section:

1. Every variable is an arithmetic term.
2. Every numeral is an arithmetic term.
3. If t is an arithmetic term, then so is $-t$.
4. If t_0 and t_1 are arithmetic terms, then so are $(t_0 + t_1)$ and $(t_0 \cdot t_1)$.

Our definition of arithmetic terms is recursive in the following way. Suppose A is *some* set of strings of symbols such that each of the following conditions holds:

1. Every variable is in A.
2. Every numeral is in A.
3. If t is in A, then $-t$ is in A.
4. If t_0 and t_1 are in A, then so are $(t_0 + t_1)$ and $(t_0 \cdot t_1)$.

Then A contains all arithmetic terms. Therefore, proof by induction on arithmetic terms is possible; here is an example:

Proposition 1.3.1. *Every arithmetic term has as many left parentheses as right parentheses.*

Proof. Let A be the set of arithmetic terms that have as many left parentheses as right parentheses. Then A contains all variables and constants (since these have no parentheses). Suppose A contains t. Then t has as many left as right parentheses (just because it is in A), so the same is true of $-t$. This means $-t$ is in A. Similarly, if t_0 and t_1 are in A, then each of them has as many left as right parentheses, so the same is true of $(t_0 + t_1)$ and $(t_0 \cdot t_1)$; this means these terms are also in A. By the recursive definition of arithmetic terms, every term is in A. □

By the formal definition of arithmetic terms, string (1.7) above is not strictly

[30] It is probably simplest to think of a numeral as a single symbol, even though, typographically, it may be a string of digits, possibly preceeded by a minus-sign. For example, the numeral −137 should be thought of as a single symbol like c_{-137} (that's c with the subscript −137). Our decimal convention for writing numerals is just that, a convention; it has no essential relation to our definition of arithmetic terms. See also Footnote 34 below.

[31] Letters from the front of the Latin alphabet are used to denote such constants; again the convention is found in Descartes. Used in this way, the letters can be called **literal constants,** where the word literal is just the adjectival form of letter. But for us, literal constants are not *literally* parts of terms; they just *stand* for parts of terms—namely, numerals.

a term; to satisfy the definition, the term should be written as

$$(x + (-y \cdot (z + w))).$$

By convention, we can leave out the dot between $-y$ and $(z + w)$, and we can remove some of the parentheses. But we can do this only because we have a conventional **order of operations** in terms. By this convention, expressions in brackets are evaluated before all else, and then multiplication is performed before addition (and subtraction), but otherwise operations are performed as they are read from left to right. So, $(x + y)z$ means something different from $x + yz$: the former is an informal version of the term $((x + y) \cdot z)$; the latter, of $(x + (y \cdot z))$.

The formal definition of arithmetic terms should ensure that each term indicates uniquely how to calculate an integer, once integral values are assigned to the variables. In short, arithmetic terms should be **uniquely readable.** As we have defined them, they *are* uniquely readable: this is a theorem with a proof like that of Theorem 2.1.4 below.

An arithmetic term is not exactly the same thing as a *polynomial.* For example, the terms $(x \cdot (y + z))$ and $((x \cdot y) + (x \cdot z))$ are different. However, they always yield the same number if x, y and z are respectively replaced by the same three integers. We therefore write

$$x(y + z) = xy + xz, \tag{1.8}$$

and we shall say that the two members of this equation **represent** the same **polynomial.** Also, Equation (1.8) is called an **(arithmetic) identity.**

An equation of arithmetic terms can be called a **Diophantine equation,** in memory of the ancient Alexandrian mathematician Diophantus, who studied such equations.[32] A Diophantine equation is an example of an *(arithmetic) formula.* For example, the equation

$$y^2 = 4x^3 - ax - b \tag{1.9}$$

[32] Diophantus wrote the *Arithmetica,* in thirteen books, of which six have come down to us [54, pp. 516, n. *a*]. One problem that he considers, for example, is, in our notation, to find rational solutions to the pair

$$8x + 4 = y^2,$$
$$6x + 4 = y^2$$

of equations [54, pp. 526–535].

(where a and b are understood to be integers) is an arithmetic formula. Its **solutions** are those pairs of integers that **satisfy** the equation: those pairs (c, d) of integers such that $d^2 = 4c^3 - ac - b$. Formula (1.9) is not an identity, because not every pair of integers satisfies it. (For example, if (c, d_0) and (c, d_1) satisfy it, then we must have $d_1 = \pm d_0$; there is no other possibility.)[33]

By our definition, a polynomial is an abstraction from the notion of a term. It is an *equivalence-class* of terms, in the sense of § 3.7. You can think of a polynomial as an operation. Then a term is a set of instructions—a recipe for how to perform the operation. The point then is that the same operation can be performed in different ways. This is why different terms can represent the same polynomial; this is why we have nontrivial identities like (1.8).

For example, the term $x + y$ says, 'Start with x, and add y'; the term $y + x$ says, 'To y, add x.' These are different activities, but they yield the same result; so we write $x + y = y + x$.

How can you tell when two terms represent the same polynomial? It is easy to show when they represent different polynomials. For example, x^2 (that is, xx) represents a different polynomial from x, since $(-1)^2 \neq -1$. But how do we know that the two members of Equation (1.8) represent the same polynomial? As an identity, the equation expresses the **distributive** property of multiplication over addition. So how do we know that multiplication *has* this property with respect to addition? We can check it for certain integers, say $x = 5$ and $y = 17$ and $z = -14$:

$$5(17 + -14) = 5 \cdot 3 = 15;$$
$$5 \cdot 17 + 5 \cdot -14 = 85 - 70 = 15.$$

But we cannot check the property for all integers in this way, since there are infinitely many integers.

Strictly speaking, if one wants to use the distributive property with full understanding, then one should give precise definitions of the integers and their operations, and then one should *prove* the distributive property. We shall be able to do this in Chapter 4: see Theorem 4.2.4. However, we did not need to know all of the properties like the distributive property, just to be able to *define* the notion of a polynomial.

[33] Equations like (1.9) are of ongoing interest to number-theorists. It is a twentieth-century result that the equation $y^2 = x^3 + 17$ has two solutions, $(-2, 3)$ and $(2, 5)$, from which all rational solutions can be found by certain rules; and only eight of these solutions are integral [45, Example III.2.4, pp. 59 f.].

As we have discussed them so far, the integers form the *structure*

$$(\mathbb{Z}, -, +, \cdot). \tag{1.10}$$

Structures are defined generally in §§ 3.2 and 3.5. The structure in (1.10) is the set $\mathbb{Z}$ equipped with certain specified operations, namely addition, additive inversion and multiplication. Now, $\mathbb{Z}$ also has the named[34] elements 0 and 1. Moreover, $\mathbb{Z}$ is equipped with the *ordering* denoted by $<$. An ordering is a kind of *relation;* relations are defined generally in § 3.2. So we may think of the integers as composing the structure

$$(\mathbb{Z}, 0, 1, -, +, \cdot, <). \tag{1.11}$$

The ordering on $\mathbb{Z}$ allows us to write some new arithmetic formulas, on of the simplest being

$$x < y,$$

read as x is less than y. There are some 'derivative' relations:

1. $x > y$ is read as x is greater than y, and means $y < x$.
2. $x \leqslant y$ means $x < y$ or $x = y$: that is, $x \leqslant y$ is satisfied by those (a, b) such that $a < b$ or $a = b$.
3. $x \geqslant y$ is read as x is greater than or equal to y, and means $y \leqslant x$.

These are all *(arithmetic) inequalities*; as such, they are new examples of arithmetic formulas. In general, an **inequality** is an expression

$$t_0 * t_1,$$

where t_0 and t_1 are terms, and $*$ is one of the symbols, $<$, $>$, $\leqslant$, and $\geqslant$. In this context, we may also speak of the **inequation**

$$t_0 \neq t_1,$$

which is satisfied in $\mathbb{Z}$ by just those integers that do *not* satisfy the equation $t_0 = t_1$.

The positive integers are just the positive natural numbers; symbolically, these are the integers that satisfy the inequality $0 < x$. The negative integers are those integers that satisfy $x < 0$. The non-negative integers satisfy $0 \leqslant x$ and are the natural numbers, composing the set $\mathbb{N}$ as we said in § 1.2.

[34] In fact, *every* integer can be given a name in decimal notation. Alternatively we can just write every positive integer as the appropriate sum $1 + 1 + \cdots + 1$, write zero as 0, and write every negative integer as $-(1 + \cdots + 1)$.

An integer x is a **factor** or **divisor** of the integer y if $xz = y$ for some integer z. In this case, if $x \neq 0$, then z is unique; we may then say that z is the **quotient** of y by x; this quotient is denoted by

$$\frac{y}{x}$$

or y/x. In general, for any integer y and non-zero integer x, there is a quotient y/x, but this quotient may only be an element of the set of **rational numbers;** it may not be an integer. The set of rational numbers is denoted by

$$\mathbb{Q};$$

but I prefer to work only with integers for now.

If x is a divisor of y, we write

$$x \mid y,$$

and we say that x **divides** y, or y is **divisible** by x. So the symbol $\mid$ denotes a relation, just as $<$ denotes a relation.

A positive integer is called **prime** if its only positive factors are 1 and itself, and these are distinct. So 1 itself is not prime. A positive integer that is not 1 and is not prime is **composite.** The list of prime numbers begins:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Does the list end? That the list does *not* end is Proposition IX.20 of Euclid's *Elements*; a version of Euclid's proof is in the next section.

Exercises

1. Is there a way to define arithmetic terms without using brackets? (See § 2.1 for some ideas.)

2. Which of the following equations are arithmetic identities?
   (a) $xy = yx$,
   (b) $x(yz) = xyz$,
   (c) $(x + y)^2 - 2xy - y^2 = x^2$,
   (d) $2x + 3 = 4$,
   (e) $2x + 3y = 4$,
   (f) $x^2 + y^2 = 2xy$,

(g) $x^4 + y^4 = (x^2 + y^2)^2 - 2x^2y^2$,

(h) $(x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2$,

(i) $x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$.

3. There are terms like $x + (y + z)$; are there formulas like $x < (y < z)$? Explain.

1.4. Some classical theorems

We have a few proofs so far, as of Theorem 1.2.2 and of Proposition 1.3.1. What constitutes a proof in general? It is hard to say. By means of reason alone, a proof should persuade any (sufficiently knowledgeable) reader that a certain proposition is true. This is the ideal. In practice, the standards for what is 'reasonable' in a proof can vary.

I said in the last section that we should be proving the distributive property of the integers in Chapter 4. By some standards—ultimately, the standards of this book—such basic properties of the integers were not proved until about a century ago. On the other hand, by taking for granted these basic properties, mathematicians have known for over two thousand years how to prove important propositions about the integers. Many of these propositions are stated and proved in Euclid's *Elements* [19].

Here I shall offer proofs of three of these propositions, namely:

1) that there are infinitely many prime numbers;
2) that the diagonal and side of a (geometrical) square have no common measure (that is they are not both integral multiples of the same unit);
3) that there is a method for determining the greatest common divisor of two positive integers.

The proofs of these propositions rely on claims that should be plausible, but that we have not yet fully justified. A goal of this entire collection of notes is to provide some of the justification.

Of the three propositions named, the first two might be called theorems, and the last, a problem, in the ancient sense given by Pappus in § 1.1.

Infinity of primes

Without more ado, we can state the following, and prove it by contradiction:

Proposition 1.4.1. *There are infinitely many prime numbers.*[35]

Proof. Suppose there are only finitely many prime numbers. Then there are n primes for some n in $\mathbb{N}$. We can now list the primes thus:

$$p_0, p_1, \ldots, p_{n-1}.$$

The product $p_0 p_1 \cdots p_{n-1}$ must be divisible by each prime p_i on our list, and therefore the sum

$$1 + p_0 p_1 \cdots p_{n-1}$$

is indivisible by each prime p_i (why?). Therefore this sum has a prime factor not on our list of primes. This contradicts our assumption that our list contains all primes. Therefore there are infinitely many primes. □

Are you satisfied with the proof of Proposition 1.4.1? What details does it leave out? We have not proved that every positive integer (besides 1) *has* prime factors. (However, this fact is Euclid's Proposition VII.32; see also Example 4.7.6 below.) Nor have we defined what 'infinitely many' means. (We shall in § 4.0.)

Still, by some standards, we *have* given a proof: a proof by contradiction.[36]

Incommensurability of diagonal and side

The next proposition is also proved by contradiction. We first need a definition and some lemmas.

An integer is **even** if 2 divides it; otherwise, the integer is **odd**; so $2n$ is even, but $2n + 1$ is odd.

Lemma 1.4.2. *The product of two integers is*
1) even*, if one of the integers is even;*
2) odd*, otherwise.*

Proof. Let the two integers be a and b. If a is even, so that $2 \mid a$, then $a = 2c$ for some integer c, so $ab = 2cb$, which means ab is even. If a and b are odd, then they are $2c + 1$ and $2d + 1$ for some integers c and d, so that $ab = (2c + 1)(2d + 1) = 4cd + 2c + 2d + 1 = 2(2cd + c + d) + 1$, which is odd. □

[35] Euclid puts it a bit differently: Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν: 'The prime numbers are more than any given multitude of prime numbers.' If for multitude we understand set, then, for Euclid, there is no such thing as an *infinite* set; in particular, there is no set such as we have called $\mathbb{N}$.

[36] A proof with a similar level of detail is offered to the general reader by Hardy [24, § 12].

The following is a fundamental property[37] of $\mathbb{N}$; we shall use it here and there before proving it in Chapter 4. (It is a consequence of the *Peano Axioms* given at the end of § 1.2, but it cannot be proved by induction alone.)

Lemma 1.4.3 (Infinite Descent)**.** *Every strictly decreasing sequence of positive integers must be finite: that is, if there is a sequence* $(a_0, a_1, a_2, a_3, \dots)$ *of positive integers such that*

$$a_0 > a_1 > a_2 > a_3 > \cdots ,$$

then the sequence must stop—must have a final entry a_n *for some* n *in* $\mathbb{N}$.

Proof. The claim follows because $\mathbb{N}$ is *well-ordered*, which means that every non-empty subset of $\mathbb{N}$ has a least element; we shall discuss this in § 4.7. The set of terms in a strictly decreasing sequence $(a_0, a_1, \dots)$ of positive integers must have a least element, a_n; then there can be no term after this, since it would be less than a_n. □

We can now state and prove the following. Its geometric interpretation is that there is no unit length into which the diagonal and side of a square can be divided. Aristotle[38] alludes to a proof similar to ours.

Proposition 1.4.4. *The Diophantine equation*

$$x^2 = 2y^2 \tag{1.12}$$

has no non-zero integral solution.

Proof. Suppose, if possible, that (a_0, a_1) satisfies the equation, where a_0 and a_1 are non-zero integers. In particular then,

$$a_0{}^2 = 2a_1{}^2. \tag{1.13}$$

Hence $a_0{}^2$ is even, so a_0 is even by Lemma 1.4.2 (since if a_0 were odd, then $a_0{}^2$ would be odd[39]); say $a_0 = 2a_2$. Then $a_0{}^2 = 4a_2{}^2$; this, with (1.13), implies[40] that $2a_1{}^2 = 4a_2{}^2$, hence

$$a_1{}^2 = 2a_2{}^2.$$

[37] Born around 1601, Pierre Fermat developed the method of *infinite descent* to prove such theorems as that no right triangle whose sides are integral has an area that is the *square* of an integer: If there were such a triangle, then there would be a smaller one, and so on. See Weil [58, II.IX, pp. 75 ff.].

[38] In the *Prior Analytics;* the passage is quoted and discussed at [53, pp. 110 f.].

[39] Here, in the notation of § 2.7, we use $\boldsymbol{P} \Rightarrow \boldsymbol{Q}, \neg\boldsymbol{P} \Rightarrow \neg\boldsymbol{Q} \vDash \boldsymbol{Q} \Rightarrow \boldsymbol{P}$.

[40] The properties of equality that allow this conclusion are discussed in detail in [52, Ch. III, pp. 54–67].

Thus (a_1, a_2) is also a solution of (1.12). In short, given the solution (a_0, a_1), we can find a solution (a_1, a_2). Continuing, we can find an integer a_3 such that ${a_2}^2 = 2{a_3}^2$, and so forth. That is, there is an infinite sequence

$$a_0, a_1, a_2, a_3, \ldots$$

of integers a_k such that (a_k, a_{k+1}) is a solution of (1.12) for each natural number k. (Strictly, the existence of such a sequence is only justified by the Recursion Theorem, which is 4.1.1 below.) But we may also assume (why?) that each integer a_k is *positive*. Then

$$a_0 > a_1 > a_2 > a_3 > \cdots,$$

which is absurd: no such sequence can be infinite, by Lemma 1.4.3. Therefore such a_0 and a_1 cannot exist. □

Euclidean algorithm

An alternative proof of the last proposition is given in § 1.5 in terms of the *Euclidean algorithm* for finding the greatest common divisor of two positive integers.

Suppose a and b are positive integers. Then there is a unique natural number k such that

$$ka \leqslant b < (k+1)a. \tag{1.14}$$

We say that k is the **number of times** that a goes into b. Then $b - ka$ is the **remainder** after division of b by a. Let us denote this remainder by

$$\mathrm{rem}(b, a).$$

So we have $b = ka + \mathrm{rem}(b, a)$ for some integer k, and $0 \leqslant \mathrm{rem}(b, a) < a$, and these rules determine $\mathrm{rem}(b, a)$.

For the sake of completeness, we can extend this analysis to arbitrary integers. Every integer a has an **absolute value**, which is denoted by $|a|$ and is given by the following rule:

$$|a| = \begin{cases} a, & \text{if } 0 \leqslant a; \\ -a, & \text{if } a < 0. \end{cases}$$

If $a \neq 0$, and b is any integer, then there is a unique natural number $\mathrm{rem}(b, a)$ satisfying two requirements:

1. $0 \leqslant \mathrm{rem}(b, a) < |a|$;

2. $b = ka + \mathrm{rem}(b, a)$ for some integer k.

Here k is also uniquely determined. If a and b are positive, then $\mathrm{rem}(b, a)$ and k are as before. We can now say that $a \mid b$ just in case $\mathrm{rem}(b, a) = 0$.

The following is similar to Euclid's Proposition VII.2. The proof omits some details; supplying them is left as an exercise.

Proposition 1.4.5. *Any two integers that are not both zero have a greatest common divisor. This divisor is found by alternately replacing each number with its remainder after division by the other, until one of the numbers becomes* 0*; then the other number is the greatest common divisor.*

Proof. Let a and b be integers, not both zero. If $|a| = |b|$, then $|a|$ is the greatest common divisor of a and b. Suppose now $|b| < |a|$. We *recursively* define a sequence of natural numbers in the following way. Let $a_0 = |a|$ and $a_1 = |b|$. Suppose $a_0, \ldots, a_{i+1}$ have been defined. Then let

$$a_{i+2} = \begin{cases} \mathrm{rem}(a_i, a_{i+1}), & \text{if } a_{i+1} \neq 0; \\ 0, & \text{if } a_{i+1} = 0. \end{cases}$$

The sequence is strictly decreasing until it reaches 0; therefore, by Lemma 1.4.3, the sequence *must* reach 0. Let c be its last non-zero entry. Then c is positive and divides each a_i; in particular, it divides a and b. Also, if $d \mid a$ and $d \mid b$, then d divides each a_i; so $d \mid c$. Thus c is the greatest of the common divisors of a and b. □

The greatest common divisor of a and b can be denoted by

$$\gcd(a, b).$$

The technique of Proposition 1.4.5 for calculating this number is the **Euclidean algorithm.**[41] A modern formulation of this algorithm is found in [17]:

$$\gcd(a, b) = \begin{cases} b, & \text{if } \mathrm{rem}(a, b) = 0; \\ \gcd(b, \mathrm{rem}(a, b)), & \text{otherwise;} \end{cases}$$

assuming $0 < b \leqslant a$.

[41] The word algorithm is an 'erroneous refashioning' [34], apparently influenced by ἀριθμός, of the earlier English algorism, which was adapted from al-Kowārasmī, the surname of Abu Ja'far Mohammed Ben Musa, whose work in algebra gave the so-called Arabic numerals to Europe.

There is a set of **real numbers,** denoted by

$$\mathbb{R},$$

which contains all of the integers and rational numbers, and more. The real numbers can be thought of as corresponding to points on a geometrical line, once distinct points corresponding to 0 and 1 are chosen. Richard Dedekind [12, p. 2] claims to have discovered a rigorous formulation of this correspondence only in 1858; in § 4.6 below is a formal definition of the real numbers based ultimately on Dedekind's work. One of the real numbers is a positive number, denoted by[42]

$$\sqrt{2},$$

whose *square,* $(\sqrt{2})^2$, is 2. Real numbers that are not rational are **irrational.** From Proposition 1.4.4 then, we have the following consequence.

Corollary 1.4.6. *The real number* $\sqrt{2}$ *is irrational.*

I proposed in § 1.1 that propositions are sentences that, in context, are either true or false. In Chapter 2, we shall develop a formal way to work with propositions, merely with regard to whether they are true or false. (We have already worked with them *informally* in this way, as in defining $\leqslant$ on p. 37: the proposition $a \leqslant b$ is true if and only if one of the propositions $a < b$ and $a = b$ is true.) Our formal method will be to think of a true proposition as having the value 1, and to think of a false proposition as having the value 0. Then we shall be able to do computations involving these values; we shall have a **propositional calculus.**

This is a reason why we looked at the structure $(\mathbb{Z}, +, -, \cdot)$. In § 1.7, we shall develop a similar structure, based on the set $\{0, 1\}$ instead of $\mathbb{Z}$.

Exercises

1. Using Lemma 1.4.3 (and standard facts about $(\mathbb{Z}, <)$), prove that every integer different from 1 and -1 has prime factors.

2. Suppose x and p are integers, and p is prime. If $p \mid x$, prove that $p \nmid 1 + x$.

[42] This number is also written $\sqrt{2}$. However, the symbol $\sqrt{\ }$ is strictly made up of two parts: a **radical,** $\surd$, and a **vinculum,** $\overline{\ }$. The vinculum serves merely as a grouping-symbol. So writing $\sqrt{2}$ is like writing $\surd(2)$; that is, the vinculum is unnecessary. Note the properly omitted vincula in the facsimile from a 1637 publication at [13, p. 77]. Note also that $\sqrt{(4+5)} = \sqrt{4+5} = 3$, while $\sqrt{4+5} = 7$.

3. Use the Euclidean algorithm to find $\gcd(136, -192)$.
4. Prove that $\sqrt{3}$ is irrational.
5. Prove that $\sqrt{p}$ is irrational, whenever p is prime.
6. Prove that $\sqrt{n}$ is irrational, unless n is a square.
7. Prove that $\sqrt{[3]2}$ is irrational.
8. In the proof of Proposition 1.4.4, why may we assume that $a_k > 0$?
9. Supply the missing details of the proof of Proposition 1.4.5; specifically, for all n in $\mathbb{N}$, prove:
   (a) $a_{n+1} < a_n$ if $a_n \neq 0$;
   (b) $c \mid a_n$;
   (c) if $d \mid a$ and $d \mid b$, then $d \mid a_n$.

1.5. Excursus on anthyphaeresis

We have now proved three important propositions about integers. In this section, an alternative proof of Proposition 1.4.4 is developed; a version of this proof may possibly have been known in ancient times, even before the proof above. Suppose a, b, c and d are integers such that $ad = bc$. Let us then write[43]

$$a : b :: c : d$$

and say that a **is to** b **as** c **is to** d. This expresses the relation called **proportionality** among the four numbers.

Lemma 1.5.1. *If $a : b :: c : d$, and k is an integer, then*

$$a : b :: a - kc : b - kd.$$

Proof. If $a : b :: c : d$, then $ad = bc$, so $ab - kad = ab - kbc$, that is,

$$a(b - kd) = b(a - kc),$$

so $a : b :: a - kc : b - kd$. □

[43] Why not write $a/b = c/d$? Just because I prefer to work only with integers for now.

Lemma 1.5.2. *Suppose a, b, c and d are positive integers such that $a : b :: c : d$. Then b goes into a just as many times as d goes into c.*

Proof. The assumption is that $ad = bc$. Then $nad = nbc$, that is,

$$a(nd) = (nb)c,$$

for all natural numbers n. Hence $a < nb$ if and only if $c < nd$, and $nb \leqslant a$ if and only if $nd \leqslant c$. Consideration of (1.14) yields the claim. □

Proposition 1.5.3. *There are no positive integers a and b such that*

$$b : a :: a : \mathrm{rem}(b, a).$$

Proof. Suppose a_0 and a_1 are positive integers, and let $a_2 = \mathrm{rem}(a_0, a_1)$. Suppose if possible

$$a_0 : a_1 :: a_1 : a_2. \tag{1.15}$$

We shall derive a contradiction. Now, $a_2 < a_1$, so we may assume $a_1 < a_0$ (otherwise (1.15) is false). We may also assume $a_2 \neq 0$. By Lemma 1.5.2, if $a_0 = ka_1 + a_2$, then $a_1 = ka_2 + a_3$, where $a_3 = \mathrm{rem}(a_1, a_2)$; hence, by Lemma 1.5.1,

$$a_0 : a_1 :: a_2 : a_3.$$

Thus, applying the Euclidean algorithm yields a strictly decreasing sequence a_0, a_1, a_2, ..., such that $a_0 : a_1 :: a_n : a_{n+1}$ for all natural numbers n; this is absurd. Therefore Proportion (1.15) fails. □

For another proof of Proposition 1.4.4, suppose $2a^2 = b^2$. Then $a^2 = b^2 - a^2 = (b + a)(b - a)$, so

$$b + a : a :: a : b - a.$$

But also, $a < b < 2a$; so a goes into $a + b$ exactly twice, leaving the remainder $b - a$. This contradicts the last proposition.

This proof of the irrationality of $\sqrt{2}$ can be recast as a *positive* result. Suppose we take two positive real numbers a_0 and a_1; we can apply a version of the Euclidean algorithm to them (as Euclid himself does in his Propositions X.2 and 3). Then a_1 goes into a_0 some number n_0 (possibly zero) of times, leaving a remainder a_2; so $0 \leqslant a_2 < a_1$. If a_2 is not 0, then it goes into a_1 some number n_1 of times, leaving a remainder a_3; so $0 \leqslant a_3 < a_2$. We can continue this process of **alternating subtraction** or **anthyphaeresis,**[44] generating a sequence a_0,

[44] ἀνθυφαίρεσις; see [53, pp. 504–509].

a_1, a_2, ..., possibly finite, of non-negative real numbers, and a corresponding sequence, n_0, n_1, ..., of natural numbers. Call the latter sequence the **anthyphaeretic sequence** of (a_0, a_1). Then we have shown that the anthyphaeretic sequence of $(1 + \sqrt{2}, 1)$ is 2, 2, 2, ..., never ending.

That the Ancients found interest in such sequences can be inferred from certain old texts: see the brief discussion at [53, pp. 508 f.]. In modern notation, we have

$$a_k = n_k \cdot a_{k+1} + a_{k+2},$$

$$\frac{a_k}{a_{k+1}} = n_k + \frac{a_{k+2}}{a_{k+1}} = n_k + \frac{1}{\left(\frac{a_{k+1}}{a_{k+2}}\right)},$$

$$\frac{a_0}{a_1} = n_0 + \cfrac{1}{n_1 + \cfrac{1}{n_2 + \cfrac{1}{n_3 + \cfrac{1}{\ddots}}}}.$$

Thus we can express quotients of real numbers as **continued fractions.** In particular, we have

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}},$$

although we cannot here say exactly what this *means.*

Exercises

1. Give a *geometrical* argument for the incommensurability of the diagonal and side of a square. (One way to start is to let $ABCD$ be a square. Draw a circle with center A and radius AC. Extend AB to meet the circle at E; extend BA to meet the circle at F. Then $FB : BC :: BC : BE$.)

2. The expression for $\sqrt{2}$ as a continued fraction determines a sequence of rational numbers that approaches $\sqrt{2}$ as a limit. Calculate a few terms of this sequence, and find a recursive definition of the sequence.

1.6. Parity

Here I propose one possible approach to the so-called *Boolean connectives*, which will be defined in § 1.7. I also give a warning about how *not* to write a proof.

Every integer has a **parity,** which is 0 if the integer is even, and 1 if it is odd. Let the parity of the integer x be denoted by

$$\mathrm{p}(x).$$

Some basic facts about evenness and oddness can be expressed in terms of this:

Lemma 1.6.1. *The equation* $\mathrm{p}(x+2) = \mathrm{p}(x)$ *is an identity.*

Proof. If a is even, then so is $a+2$, so each member of the equation is 0. If a is odd, then so is $a+2$, so each member of the equation is 1. Hence the equation is satisfied by all integers. □

The taking of parities respects multiplication in the following sense:

Lemma 1.6.2. *The equation* $\mathrm{p}(xy) = \mathrm{p}(x)\,\mathrm{p}(y)$ *is an identity.*

Parity respects addition too, but in a more complicated sense:

Lemma 1.6.3. *The equation* $\mathrm{p}(x+y) = \mathrm{p}(\mathrm{p}(x) + \mathrm{p}(y))$ *is an identity.*

Finally, applying the parity-operation twice is the same as applying it once:[45]

Lemma 1.6.4. *The equation* $\mathrm{p}(\mathrm{p}(x)) = \mathrm{p}(x)$ *is an identity.*

I have introduced parity so as to be able to define two new operations on $\mathbb{Z}$ in the following way. *By definition* of the operations $\odot$ and $\oplus$, the following equations are identities:

$$x \odot y = \mathrm{p}(xy),$$
$$x \oplus y = \mathrm{p}(x+y).$$

These symbols are not standard, and they will not be used beyond the next section. I define two more operations. The following are also identities, by definition:

$$\ominus x = x \oplus 1, \tag{1.16}$$
$$x \sqcup y = (x \odot y) \oplus (x \oplus y). \tag{1.17}$$

For $\sqcup$, an alternative (but equivalent) definition is possible:

[45] Therefore parity can be called **idempotent.**

Theorem 1.6.5. *The equation*

$$x \sqcup y = \ominus(\ominus x \odot \ominus y) \tag{1.18}$$

is an identity.

There are two ways we can proceed.

Proof 1. We reduce everything to the ordinary arithmetic operations. By the definitions and Lemma 1.6.3, we have the following chain of identities:

$$\begin{aligned} x \sqcup y &= (x \odot y) \oplus (x \oplus y) \\ &= \mathrm{p}((x \odot y) + (x \oplus y)) \\ &= \mathrm{p}(\mathrm{p}(xy) + \mathrm{p}(x + y)) \\ &= \mathrm{p}(xy + x + y). \end{aligned}$$

Similarly,

$$\begin{aligned} \ominus(\ominus x \odot \ominus y) &= ((x \oplus 1) \odot (y \oplus 1)) \oplus 1 \\ &= \mathrm{p}(\mathrm{p}(\mathrm{p}(x + 1)\,\mathrm{p}(y + 1)) + 1) \\ &= \mathrm{p}(\mathrm{p}(\mathrm{p}((x + 1)(y + 1))) + 1) && \text{[by Lemma 1.6.2]} \\ &= \mathrm{p}(\mathrm{p}((x + 1)(y + 1)) + 1) && \text{[by Lemma 1.6.4]} \\ &= \mathrm{p}(\mathrm{p}((x + 1)(y + 1)) + \mathrm{p}(1)) && \text{[by definition of parity]} \\ &= \mathrm{p}((x + 1)(y + 1) + 1) && \text{[by Lemma 1.6.3]} \\ &= \mathrm{p}(xy + x + y + 2) && \text{[by arithmetic]} \\ &= \mathrm{p}(xy + x + y) && \text{[by Lemma 1.6.1].} \end{aligned}$$

Our computations show that $x \sqcup y$ and $\ominus(\ominus x \odot \ominus y)$ are equal to the same thing (namely $\mathrm{p}(xy + x + y)$); so they are equal to each other. This completes one possible proof. □

Alternatively, we show that all that matters is the parities of x and y.

Proof 2. By definition of $\oplus$ and by Lemma 1.6.3, we have

$$\mathrm{p}(x) \oplus \mathrm{p}(y) = \mathrm{p}(\mathrm{p}(x) + \mathrm{p}(y)) = \mathrm{p}(x + y) = x \oplus y.$$

By definition of $\odot$ and by Lemmas 1.6.2 and 1.6.4, we have

$$\mathrm{p}(x) \odot \mathrm{p}(y) = \mathrm{p}(\mathrm{p}(x)\,\mathrm{p}(y)) = \mathrm{p}(\mathrm{p}(xy)) = \mathrm{p}(xy) = x \odot y.$$

Therefore, to verify any identity involving only $\odot$ and $\oplus$ (and operations derived from them, like $\ominus$ and $\sqcup$), it suffices to replace each variable with its parity. More precisely, to verify (1.18), it is enough to check the four possibilities when x and y are chosen from the set $\{0, 1\}$. We have the following computations:

x	y	$x \odot y$	$x \oplus y$	$x \sqcup y$	$\ominus x$	$\ominus y$	$\ominus x \odot \ominus y$	$\ominus(\ominus x \odot \ominus y)$
0	0	0	0	0	1	1	1	0
1	0	0	1	1	0	1	0	1
0	1	0	1	1	1	0	0	1
1	1	1	0	1	0	0	0	1

The columns headed by the two members of (1.18) are identical, so this equation is an identity. □

Either of the two proofs just offered should be sufficient to establish the theorem as true. Note well the *format* of the first proof. The aim was to arrive at (1.18). The proof did not *begin* with this equation; it began with one of the *members* of the equation, and it showed that this member was equal to a new term. Then the *other* member of (1.18) was shown to be equal to the same term. To write the proof as follows would *not* be good style:

$$\begin{aligned} x \sqcup y &\stackrel{?}{=} \ominus(\ominus x \odot \ominus y), \\ (x \odot y) \oplus (x \oplus y) &\stackrel{?}{=} ((x \oplus 1) \odot (y \oplus 1)) \oplus 1, \\ \mathrm{p}((x \odot y) + (x \oplus y)) &\stackrel{?}{=} \mathrm{p}(\mathrm{p}(\mathrm{p}(x+1)\,\mathrm{p}(y+1)) + 1), \\ \dots &\stackrel{?}{=} \dots, \\ \mathrm{p}(xy + x + y) &= \mathrm{p}(xy + x + y). \end{aligned} \tag{1.19}$$

Do not write proofs this way! It does not show the connexion between consecutive lines. Equations (1.19) don't tell the reader that, for example, $\ominus(\ominus x \odot \ominus y) = ((x \oplus 1) \odot (y \oplus 1)) \oplus 1$. In fact, the equations tell us *nothing* that can be assumed to be correct.

Think of the following example:

$$\begin{aligned} -1 &\stackrel{?}{=} 1 \\ (-1)^2 &\stackrel{?}{=} (1)^2 \\ 1 &= 1. \end{aligned} \tag{1.20}$$

It certainly does not show that $-1 = 1$.

If you are *searching* for a proof of (1.18), then you might possibly write something like Equations (1.19). Then, after you have found a correct line of argument, you should rewrite your findings before presenting them to somebody else as a proof. The next chapter will make this point again with the notion of *formal proof*: What one writes down when *looking* for a formal proof is generally a lot different from the formal proof itself.

Exercises

1. Prove Lemmas 1.6.2, 1.6.3 and 1.6.4.

2. Explain why the equations (1.20) do not constitute a valid proof of the equation $-1 = 1$.

3. Suppose $\rightsquigarrow$ is a new arithmetic operation defined on the set $\{0, 1\}$ as follows:

x	y	$x \rightsquigarrow y$
0	0	1
1	0	1
0	1	0
1	1	1

   Find an arithmetic term t such that the equation $\mathrm{p}(t) = \mathrm{p}(x) \rightsquigarrow \mathrm{p}(y)$ is an identity.

1.7. Boolean connectives

In memory of George Boole,[46] let us refer to the set $\{0, 1\}$ as $\mathbb{B}$. In the last section, I defined some operations that convert integers into elements of $\mathbb{B}$. Considering the elements of $\mathbb{B}$ as integers, I want to restrict those operations on $\mathbb{Z}$ so as to apply *only* to elements of $\mathbb{B}$. In so doing, I change their names:

on $\mathbb{Z}$:	$\otimes$	$\oplus$	$\ominus$	$\sqcup$
on $\mathbb{B}$:	$\&$	$\not\Leftrightarrow$	$\neg$	$\vee$

I shall not use the four operations $\otimes$, $\oplus$, $\ominus$ and $\sqcup$ anymore. Operations on $\mathbb{B}$ can be called **(Boolean) connectives.** Specific English names can be given as follows:

1) $\&$ is **conjunction;**

[46] See Boole himself [4, III.12, **[47]**, p. 51].

2) $\neg$ is **negation;**
3) $\vee$ is **(inclusive) disjunction;**
4) $\not\Leftrightarrow$ is **exclusive disjunction** or **(material) non-equivalence.**

Since $\mathbb{B}$ is finite, the definitions of connectives can be given in tables like the table in the last section:

P	Q	$P \,\&\, Q$	$P \vee Q$	$P \not\Leftrightarrow Q$
0	0	0	0	0
1	0	0	1	1
0	1	0	1	1
1	1	1	1	0

P	$\neg P$
0	1
1	0

It will be convenient to have two more connectives, namely:

5) **(material) implication** or the **conditional:** $\Rightarrow$;
6) **(material) equivalence** or the **biconditional:** $\Leftrightarrow$.

Again the definitions can be given in a table:

P	Q	$P \Rightarrow Q$	$P \Leftrightarrow Q$
0	0	1	1
1	0	0	0
0	1	1	0
1	1	1	1

Certain identities should be evident: For example, $P \not\Leftrightarrow Q$ seems to mean the same thing as $\neg(P \Leftrightarrow Q)$. Here though, we shall *not* put a sign of equality between the two expressions. Rather, as will be discussed more fully in § 2.2, we shall write

$$P \not\Leftrightarrow Q \sim \neg(P \Leftrightarrow Q), \tag{1.21}$$

using the **swung dash** $\sim$ rather than the sign $=$ of equality. Why? First, by analogy with the definition of arithmetic terms in § 1.3, we define **Boolean terms** recursively as follows. Boolean terms are certain strings containing (some of) the following symbols:

1) $\&$, $\neg$, $\vee$, $\not\Leftrightarrow$, $\Rightarrow$, $\Leftrightarrow$ (or other connectives, should we choose to define them);
2) the **constants** 0 and 1;
3) **variables** from the list P_0, P_1, P_2, ...;
4) the parentheses (and).

Then the Boolean terms are determined by the following rules:

1. Variables and constants are Boolean terms;
2. If $\boldsymbol{F}$ is a Boolean term, then so is $\neg\boldsymbol{F}$;

3. If $\boldsymbol{F}$ and $\boldsymbol{G}$ are Boolean terms, then so is $(\boldsymbol{F} * \boldsymbol{G})$, where $*$ is one of the connectives $\&$, $\vee$, $\not\Leftrightarrow$, $\Rightarrow$, $\Leftrightarrow$.

Note that the constants 0 and 1 can also be considered as Boolean connectives, since they give values (namely, themselves) in $\mathbb{B}$.

We could now define Boolean polynomials, and we could make from them what me might call Boolean polynomial equations; these would be examples of so-called Boolean formulas. We shall *not* use such expressions however, since our main interest will lie in Boolean terms *as such.* To suggest this, we shall refer to Boolean terms mainly as **(propositional) formulas.**

As with arithmetic terms, so with propositional formulas, we can establish a conventional order of operations so as to avoid writing too many parentheses. We can always leave out an outer pair of parentheses. Then:

1) $\neg$ has priority over all other connectives;
2) $\&$ and $\vee$ have priority over $\Rightarrow$, $\Leftrightarrow$, and $\not\Leftrightarrow$;
3) in case of two instances of $\Rightarrow$, the one on the *right* has priority—we shall use this convention, because propositional formulas like $(P_0 \Rightarrow (P_1 \Rightarrow P_2))$ are more common than $((P_0 \Rightarrow P_1) \Rightarrow P_2)$; so it will be convenient to let $P_0 \Rightarrow P_1 \Rightarrow P_2$ stand for the *former;*
4) in case of two instances of $\&$ or of $\vee$ or of $\not\Leftrightarrow$, the one on the right has priority—we could just as well give priority to the one on the left; we just want to allow ourselves to let strings like $P_0 \,\&\, P_1 \,\&\, P_2$ denote Boolean terms.

Also, instead of writing variables P_k, we may use $\boldsymbol{P}$, $\boldsymbol{Q}$ and $\boldsymbol{R}$ instead. Similarly, we may use letters like $\boldsymbol{F}$, $\boldsymbol{G}$ and $\boldsymbol{H}$ to stand for formulas.

The symbols P_0, P_1, and so on are the variables that can appear officially in propositional formulas. The symbols $\boldsymbol{P}$, $\boldsymbol{Q}$ are **syntactical variables;** in the sense of [9, § 08] we use them to *refer* to the variables in formulas. Likewise, $\boldsymbol{F}$ and so on are not literally formulas; we use them as syntactical variables for formulas.

Examples 1.7.1. By the order of operations,

1) the propositional formula denoted by $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \vee \boldsymbol{R}$ is $(\boldsymbol{P} \Rightarrow (\boldsymbol{Q} \vee \boldsymbol{R}))$;
2) $\neg \boldsymbol{P} \,\&\, \boldsymbol{Q}$ is $((\neg \boldsymbol{P}) \,\&\, \boldsymbol{Q})$;
3) $\boldsymbol{P} \,\&\, \boldsymbol{Q} \vee \boldsymbol{R}$ is ambiguous; the writer must say whether $(\boldsymbol{P} \,\&\, \boldsymbol{Q}) \vee \boldsymbol{R}$ or $\boldsymbol{P} \,\&\, (\boldsymbol{Q} \vee \boldsymbol{R})$ is intended;
4) $\boldsymbol{P} \,\&\, \boldsymbol{Q} \,\&\, \boldsymbol{R}$ is $(\boldsymbol{P} \,\&\, (\boldsymbol{Q} \,\&\, \boldsymbol{R}))$;
5) $\boldsymbol{P} \,\&\, \boldsymbol{Q} \,\&\, \boldsymbol{R} \vee \boldsymbol{P}$ is ambiguous;
6) $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \Rightarrow \boldsymbol{R}$ is $\boldsymbol{P} \Rightarrow (\boldsymbol{Q} \Rightarrow \boldsymbol{R})$;
7) $\boldsymbol{P} \not\Leftrightarrow \boldsymbol{Q} \not\Leftrightarrow \boldsymbol{R}$ is $(\boldsymbol{P} \not\Leftrightarrow (\boldsymbol{Q} \not\Leftrightarrow \boldsymbol{R}))$;

8) $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \,\&\, \boldsymbol{R} \Rightarrow \boldsymbol{S}$ is $(\boldsymbol{P} \Rightarrow ((\boldsymbol{Q} \,\&\, \boldsymbol{R}) \Rightarrow \boldsymbol{S}))$.

A propositional formula like $0 \Rightarrow 1$ can be called **closed,** because it has no variables. By definition of the connective $\Rightarrow$, this formula $0 \Rightarrow 1$ has the **value** 1. The formulas $0 \Rightarrow 1$ and 1 are not equal *as formulas*; but the former can be considered as a **name** for the latter (considered as an element of $\mathbb{B}$).

Propositional formulas are so defined that every *closed* formula is the name of a *unique* element of $\mathbb{B}$. We shall prove this in § 2.1; meanwhile, some applications are in the following exercises.

Exercises

1. By the order of operations, which propositional formulas, if any, are denoted by the following?
   (a) $\boldsymbol{P} \,\&\, \neg\boldsymbol{Q} \not\Leftrightarrow \boldsymbol{R} \vee \boldsymbol{P}$;
   (b) $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \not\Leftrightarrow \boldsymbol{R}$;
   (c) $P_0 \Rightarrow P_1 \Rightarrow P_2 \Rightarrow P_3$;
   (d) $P_0 \Rightarrow P_1 \Rightarrow \ldots \Rightarrow P_n$.
2. The following closed formulas are names of which elements of $\mathbb{B}$?
   (a) $1 \Rightarrow 1 \Rightarrow 1$,
   (b) $1 \Rightarrow 0 \Rightarrow 1$,
   (c) $(0 \Rightarrow 1) \Leftrightarrow 1$,
   (d) $\neg(0 \not\Leftrightarrow 1) \Leftrightarrow (0 \Leftrightarrow 1)$,
   (e) $\neg\neg\neg 0$,
   (f) $(1 \vee 0) \,\&\, 0$,
   (g) $1 \vee (0 \,\&\, 0)$.

1.8. Propositional formulas and language

In one sense of the word, a *model* is a representation or description of something that one wants to build or understand. Think of an architect's model, or an orrery (a model of the solar system). In this sense, symbolic logic can be seen as a model of ordinary language. In propositional logic, the Boolean connectives represent words such as and, but, or, if, and not, some of which are traditionally called *conjunctions* (bağlaçlar). Our main interest here is how such words affect the truth of statements, especially statements in mathematics.

Truth

Aristotle defines truth in the *Metaphysics* (IV, vii, 1: 1011 b 26). A literal translation of his words[47] is:

> To declare the being not to be, or the not being to be, is false;—the being to be, and the not being not to be, is true.

Alternatively, 'It is false to say that what is, is not, or what is not, is; it is true to say that what is, is, and what is not, is not.'

I propose (inspired by Alfred Tarski [51]) to refine this definition as follows: Let A be a statement. Then:

> A is true if A, and A is false if not A.

This is a *definition*; implicitly then, A is true *only* if A, and A is false only if not A. The definition is obscure. It becomes slightly less cryptic in an example where we can use the typographical convention established in the Preface:

> Grass is green is true if grass is green;
> Grass is green is false if grass is not green.

Note what happens when we translate this into Turkish:

> Çimen yeşilse, Grass is green doğrudur;
> çimen yeşil değilse, Grass is green yanlıştır.

Compound statements

We can now analyse certain compound statements. Let A and B be statements.

Conjunctions, disjunctions, and negations

The statement A and B is true if and only if A and B; hence A and B is true if and only if A is true and B is true. Compare this with the observation that $\boldsymbol{P}\,\&\,\boldsymbol{Q}$ takes the value 1 if and only if $\boldsymbol{P}$ takes the value 1 and $\boldsymbol{Q}$ takes the value 1. If 1 represents truth, then the connective & represents the conjunction and. The proposition A and B and the propositional formula $\boldsymbol{F}\,\&\,\boldsymbol{G}$ can alike be called

[47] The words are in [3]: τὸ μὲν γὰρ λέγειν τὸ ὂν μὴ εἶναι ἢ τὸ μὴ ὂν εἶναι ψεῦδος, τὸ δὲ τὸ ὂν εἶναι καὶ τὸ μὴ ὂν μὴ εἶναι ἀληθές (Varlığın var olmadığını veya varolmayanın var olduğunu söylemek yanlıştır. Bunu karşılık varlığın var olduğunu, var olmayanın var olmadığını söylemek doğrudur).

conjunctions. Note well, however, that the proposition A and B belongs to *our* ordinary language, while the formula $\boldsymbol{F} \,\&\, \boldsymbol{G}$ belongs to propositional logic.

Similarly, A or B is true if and only if A is true or B is true. Also, $\boldsymbol{P} \vee \boldsymbol{Q}$ takes the value 1 if and only if $\boldsymbol{P}$ takes the value 1, or $\boldsymbol{Q}$ takes the value 1. So the connective $\vee$ represents the conjunction or. The proposition A or B and the propositional formula $\boldsymbol{F} \vee \boldsymbol{G}$ can alike be called **disjunctions.**

More precisely, $\vee$ represents or in its *inclusive* sense. The *exclusive* sense of or is intended in a sentence like You may have tea or coffee after your meal, if this means that you are allowed to have tea, and you are allowed to have coffee, but you are not allowed to have both. The exclusive or is represented by the connective $\Leftrightarrow$.

The sentence Not-A is true if and only if A is false; and $\neg\boldsymbol{P}$ takes the value 1 if and only if $\boldsymbol{P}$ takes the value 0. If now 0 represents falsity, then $\neg$ represents not. Both Not-A and $\neg\boldsymbol{F}$ can be called **negations.** (In fact the negation of an English statement is almost never formed simply by the prefixing of the word not; the not goes inside, perhaps with some other changes.)

Mathematics often involves ignoring certain distinctions. From the propositions A and B, we can form several compound propositions:

$$A \text{ and } B$$
$$A, \text{ but } B$$
$$A;\ B$$

Each of these may have its own rhetorical coloration, but we shall take them all to have the same truth-value. We may use for any of them the abbreviation

$$A \ \&\ B.$$

(Note the slight typographical distinction between & and &.) The sentence A & B here is not a propositional formula; it is just a proposition or sentence of ordinary language.

Implications

We can form some more compounds, all having the same truth-value:

If A, then B
When A, then B
A implies B
B if A
B, provided A
A only if B

These can be called **implications** and **conditional** statements. Each of them has the **antecedent** A and the **consequent** B. We shall understand the compounds to be true if B is true or A is false (or both); otherwise, the compounds are false. We may use the abbreviation

$$A \implies B.$$

The propositional formula $\boldsymbol{P} \Rightarrow \boldsymbol{Q}$ can be analysed similarly, and we can apply the same terminology.

The formulation B if A can be understood as emphasizing that A is a **sufficient condition** for B. The formulation A only if B emphasizes that B is a **necessary condition** for A.

In ordinary language, the sentence If A, then B suggests causation. If you drop that İznik vase, then it will break—you will cause the vase to break by dropping it. In mathematics though, the sentence If A, then B means no more than B is true or A is false. This is why the connective $\Rightarrow$ is called **material implication;**[48] it is to be distinguished from **formal implication,** that is, the implication suggested by a sentence like If A, then B in ordinary language. I suggest the following mnemonic device. In Platonic philosophy, the *form* of something has a higher level of reality than its *matter*.[49] In the sentence about a vase, there is a *formal* connexion between antecedent and consequent: they both refer to the same vase, for example. Such a connexion is missing in a sentence like If water is wet, then Constantine founded Constantinople; but we count the sentence as 'materially' true if we accept the consequent as true. (In this case, it is irrelevant that the antecedent is true.)[50]

There is a saying in English, If wishes were horses, then beggars would ride. We cannot analyse this as a material implication, simply because the antecedent

[48] See the discussions in Church [9, § 05, n. 89, pp. 37f.] and Tarski [52, §§ 8, 9]; but these sources do not discuss the origin of the terminology.

[49] I suspect Descartes alludes to this distinction when he says in the third of the *Meditations on First Philosophy* (p. 41)

> That this idea contains this or that objctive reality rather than some other one results from the fact that the idea gets its objective [that is, material?] reality from a cause in which there is at least as much formal reality as there is objective reality contained in the idea. [14]
>
> Ama bu idea belirli bir nesnel olgusallık kapsadığı için, onu hiç kuşkusuz en azından kendisinin kapsadığı nesnel olgusallık denli biçimsel olgusallık kapsayan bir nedenden türetiyor olmalıdır. [15]

[50] Elsewhere in mathematics, the term *formal* is used to denote what might be called a *lower* level of reality than usual. An expression $a + b$ may be called a *formal sum* if a and b cannot 'really' be added, except to produce the expression $a + b$.

and consequent are not propositions. We can try to recast the sentence as, If wishes are horses, then beggars ride. Then we can argue that the sentence is true, simply because the antecedent is false: wishes are *not* horses. This observation says nothing about the truth of the original saying.

In some mathematical writing, one sees statements like

$$A \implies B \implies C.$$

This should be understood as an abbreviation for

$$(A \implies B) \ \& \ (B \implies C).$$

This conjunction is *not* the same statement as the implication

$$A \implies (B \implies C),$$

even though we understand the formula $\boldsymbol{F} \Rightarrow \boldsymbol{G} \Rightarrow \boldsymbol{H}$ as an abbreviation for the formula $\boldsymbol{F} \Rightarrow (\boldsymbol{G} \Rightarrow \boldsymbol{H})$.

In mathematics, we often have occasion to write sentences like A is true, and therefore B is true, or more simply, A, therefore B. Logically, the truth-value of the sentence is the same as the truth-value of $A \ \& \ B$; so please resist the temptation to write the sentence as $A \implies B$, or as

$$\begin{array}{l} A \\ \implies B. \end{array}$$

Instead of an arrow, just use words, such as therefore, hence, consequently, or as a result.

Equivalences

In ordinary language, we can write indifferently

$$\begin{array}{c} A \text{ if and only if } B \\ A \text{ just in case } B \end{array}$$

These are **equivalences** and **biconditional** statements, and for them we can use the abbreviation

$$A \iff B.$$

The formula $\boldsymbol{P} \Leftrightarrow \boldsymbol{Q}$ has a similar analysis and description. In mathematical writing, one may see statements like

$$A \iff B \iff C;$$

this should be understood an abbreviation for

$$(A \iff B) \ \& \ (B \iff C).$$

Reasoning with compounds

Some fundamental rules of reasoning can be abbreviated thus:

$$A \ \& \ (A \implies B) \implies B; \tag{1.22}$$

$$\text{not-}(A \implies B) \iff A \ \& \ \text{not-}B. \tag{1.23}$$

(We are using a convention like that established in § 1.7: the expression & has priority over $\implies$ and $\iff$.)

The operations of **conversion** and **contraposition** can be performed on implications:

1) the **converse** of $A \implies B$ is $B \implies A$;

2) the **contrapositive** of $A \implies B$ is $\text{not-}B \implies \text{not-}A$.

The contrapositive of an implication is true if and only if the original implication is true:

$$(A \implies B) \iff (\text{not-}B \implies \text{not-}A).$$

This observation is of great value in the proving of mathematical propositions. In particular, it often allows for proofs that are superior in style to proofs by contradiction. The stylistic problem with a proof by contradiction is that it contains false or even meaningless statements. The proof may still be correct, but it is inelegant. For example, in the proof of the Russell Paradox (Theorem 1.2.2), since $\mathbf{R}$ turns out not to be a set, the expressions $\mathbf{R} \in \mathbf{R}$ and $\mathbf{R} \notin \mathbf{R}$ turn out to be meaningless. A proof that avoids this problem is the following.

Alternative proof of the Russell Paradox. Let A be an arbitrary set. Then either $A \in A$, or $A \notin A$. If $A \in A$, then $A \notin \mathbf{R}$, so $A \neq \mathbf{R}$. If $A \notin A$, then $A \in \mathbf{R}$, so again $A \neq \mathbf{R}$. Thus $A \neq \mathbf{R}$. That is, no set is equal to $\mathbf{R}$; so $\mathbf{R}$ is not a set. □

Exercises

1. Find a true implication whose converse is true.

2. Find a true implication whose converse is false.

3. Recast all foregoing proofs-by-contradiction to avoid any contradictions.

1.9. Quantifiers

As the Boolean connectives are used to model the conjunctions of ordinary language, so the symbols called *quantifiers* can be used to model certain so-called *determiners*, especially all and some. Quantifiers are a part of *predicate logic*.

In a section of the 'XVII. Meditation' of his *Devotions upon Emergent Occasions* of 1624, the clergyman and so-called metaphysical poet John Donne uses the determiners no, every, and any, in addition to the indefinite article a(n). The Meditation begins as follows (and here I preserve Donne's original spelling and typography, as found in [16, pp. 44of.]): 'PERCHANCE hee for whom this *Bell* tolls, may be so ill, as that he knowes not it tolls for him;' later, the Meditation continues:

> No man is an *Iland,* intire of it selfe; every man is a peece of the *Continent,* a part of the *maine;* if a *Clod* bee washed away by the *Sea, Europe* is the lesse, as well as if a *Promontorie* were, as well as if a *Mannor* of thy *friends* or of *thine owne* were; any mans *death* diminishes *me,* because I am involved in *Mankinde;* And therefore never send to know for whom the *bell* tolls; It tolls for *thee.*

This text contains the following three clauses (and now I modernize the spelling):

> No man is an island.
> Every man is a piece of the continent.
> Any man's death diminishes me.

The first clause is contradicted some 350 years later by a verse of a popular song by Simon and Garfunkel [46]:

> I am a rock, I am an island.

Donne says that the proposition I am an island is false, no matter who says it: it is false that some man is an island. (I take Donne's man to be a *human being,* male or female.) So we can abbreviate the first two of Donne's clauses above by:

> Not-(some x is an island) & (every x is a piece of the continent),

where the variable x is understood to range over humanity. We can *expand* this to

> Not-(there is some x such that x is an island) & (for every x, x is a piece of the continent).

The reason for this expansion is that the predicate [is] an island might be denoted by P, and [is] a piece of the continent might be denoted by Q. For the phrase there is some x such that, we write

$$\exists x;$$

for the phrase for all x, we write

$$\forall x.$$

Then Donne's two clauses can be written

$$\neg\exists x\ Px\ \&\ \forall x\ Qx.$$

The symbol $\exists$ is the **existential quantifier;** the symbol $\forall$ is the **universal quantifier.**[51] We have just seen that these correspond respectively to the determiners some and every, and $\neg\exists$ corresponds to no. We shall discuss, by and by, what $\neg\forall$ corresponds to.

Let $\mathcal{U}$ be some universal set as in § 1.2, let P be a predicate, and let A be the resulting set $\{x \in \mathcal{U}\colon Px\}$. We can form several equations and inequations whose members are $\varnothing$, A and $\mathcal{U}$; with quantifiers, we can describe them.

1. $\forall x\ Px$ means $A = \mathcal{U}$.
2. $\exists x\ Px$ means $A \neq \varnothing$.
3. $\neg\exists x\ Px$ means $A = \varnothing$.
4. $\neg\forall x\ Px$ means $A \neq \mathcal{U}$.

The set denoted by

$$\{x \in \mathcal{U}\colon \neg Px\}$$

consists of those elements of $\mathcal{U}$ that are *not* in A: it is the set

$$A^{\mathrm{c}}, \tag{1.24}$$

called the **complement** of A (in $\mathcal{U}$). Then we can form more equations, inequations and propositions on the pattern of those above:

1. $\forall x\ \neg Px$ means $A^{\mathrm{c}} = \mathcal{U}$.
2. $\exists x\ \neg Px$ means $A^{\mathrm{c}} \neq \varnothing$.
3. $\neg\exists x\ \neg Px$ means $A^{\mathrm{c}} = \varnothing$.

[51] With Chiswell and Hodges [8], one may prefer to say that the compound symbols $\exists x$ and $\forall x$ are the quantifiers.

4. $\neg\forall x\ \neg Px$ means $A^{\mathrm{c}} \neq \mathcal{U}$.

But we have, for example,

$$A^{\mathrm{c}} = \mathcal{U} \iff A = \varnothing;$$
$$A^{\mathrm{c}} \neq \varnothing \iff A \neq \mathcal{U}.$$

Correspondingly, we also have

$$\neg\exists x\ Px \iff \forall x\ \neg Px; \tag{1.25}$$
$$\neg\forall x\ Px \iff \exists x\ \neg Px. \tag{1.26}$$

These equivalences are valuable tools for understanding propositions written with quantifiers.

Example 1.9.1. In calculus, a function f on $\mathbb{R}$ is said to be *continuous* at a real number a if, for every positive real number ε, there is a positive real number δ such that, for every real number x, if $|x - a| < \delta$, then $|f(x) - f(a)| < \varepsilon$. In our new symbolism, we can write the definition as

$$\forall\varepsilon\ (\varepsilon > 0 \implies \exists\delta\ (\delta > 0\ \&\ \forall x\ (|x - a| < \delta \implies |f(x) - f(a)| < \varepsilon))). \tag{1.27}$$

Some people abbreviate this proposition to

$$\forall\varepsilon > 0\ \exists\delta > 0\ \forall x\ (|x - a| < \delta \implies |f(x) - f(a)| < \varepsilon).$$

By (1.25) and (1.26) above, as well as (1.23) in § 1.8, along with the proposition that, in $\mathbb{R}$, $x < y$ fails if and only if $x \geqslant y$,—by all of this, the negation of (1.27) is

$$\exists\varepsilon\ (\varepsilon > 0\ \&\ \forall\delta\ (\delta > 0 \implies \exists x\ (|x - a| < \delta\ \&\ |f(x) - f(a)| \geqslant \varepsilon))),$$

which some people write as

$$\exists\varepsilon > 0\ \forall\delta > 0\ \exists x\ (|x - a| < \delta\ \&\ |f(x) - f(a)| \geqslant \varepsilon).$$

For a specific example, let f be the function given by

$$f(x) = \begin{cases} \sin\dfrac{1}{x}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0; \end{cases}$$

and $a = 0$. We can show that f is not continuous at a as follows. The function $x \mapsto \sin x$ is periodic, with period 2π: that is,

$$\forall x\ \sin(x + 2\pi) = \sin x.$$

Also, $\sin(\pi/2) = 1$. Let $\varepsilon = 1/2$. Say $\delta > 0$. There is some integer n greater than $1/2\pi\delta$. Then $2n\pi + \pi/2 > 2n\pi > 1/\delta$. Let $x = 1/(2n\pi + \pi/2)$. Then $|x - a| = x < \delta$, but $|f(x) - f(a)| = |f(x)| = \sin(2n\pi + \pi/2) = 1 \geqslant \varepsilon$. This proves that f is not continuous at 0.

In (1.27), note that the expression

$$|x - a| < \delta \implies |f(x) - f(a)| < \varepsilon \tag{1.28}$$

can be understood as a predicate with *three* subjects—let's call them **arguments:** x, δ, and ε. If we wanted to abbreviate (1.28), we might write it as $Sx\delta\varepsilon$. Then S is a **ternary** predicate. Ternary predicates are common in mathematics, at least implicitly; for example, the equations

$$x + y = z, \qquad\qquad xy = z$$

can be understood as featuring ternary predicates. The signs $=$ and $<$ are **binary** predicates. **Singulary** predicates—predicates that take a single argument—are uncommon in mathematics, though they are needed in general treatments such as ours.

Quantifier elimination and introduction

Let us return to the general setting where $\mathcal{U}$ is some set, P is a singulary predicate, and $A = \{x \in \mathcal{U} \colon Px\}$. In proofs, there are several moves we might make that involve introducing or eliminating quantifiers from known propositions.

$\forall$-**elimination:** If we know $\forall x\ Px$, and b is some element of $\mathcal{U}$, then $b \in A$, so we can conclude

$$Pb.$$

$\exists$-**introduction:** If c is an element of $\mathcal{U}$ such that Pc, then $c \in A$, so $a \neq \varnothing$, and therefore

$$\exists x\ Px.$$

$\forall$-**introduction:** If b is an *arbitrary* element of $\mathcal{U}$, and we can show Pb, then it must be the case that

$$\forall x\ Px.$$

Of course it is essential that b be **arbitrary.** This means, in the proof of Pb, nothing about b can be used, except its membership in $\mathcal{U}$.

$\exists$-**elimination:** Suppose $\exists x\ Px$. If, by assuming Pb for some unknown element of $\mathcal{U}$, we are able to prove a proposition σ that says nothing about b, then we can conclude that σ is true.

These rules are illustrated in the next subsection.

Prenex forms

In compound propositions involving quantifiers, it may be desirable to move all of the quantifiers to the front, in order to better understand the complexity of the proposition, or simply to avoid confusion. The result is said to be in **prenex** form. For example, (1.27) can be rewritten in prenex form as

$$\forall\varepsilon\ \exists\delta\ \forall x\ (\varepsilon > 0 \implies (\delta > 0\ \&\ (|x - a| < \delta \implies |f(x) - f(a)| < \varepsilon))).$$

This is a consequence of the following lemmas, where σ is a statement and P is a singulary predicate.

Lemma 1.9.2. $(\sigma \implies \exists x\ Px) \iff \exists x\ (\sigma \implies Px)$.

Proof. **(⇒)** Suppose $\sigma \implies \exists x\ Px$. We consider two cases.
Suppose first σ is true. Then so is $\exists x\ Px$, and hence for some a in $\mathcal{U}$ we have Pa and therefore $\sigma \implies Pa$. By ∃-introduction, we can conclude $\exists x\ (\sigma \implies Px)$.
On the other hand, if σ is false, then for all a in $\mathcal{U}$, we have $\sigma \implies Pa$. Since in particular there is *some* a in $\mathcal{U}$, again by ∃-introduction we can conclude $\exists x\ (\sigma \implies Px)$.
(⇐) Suppose $\exists x\ (\sigma \implies Px)$. By ∃-elimination, $\sigma \implies Pa$ for some a in $\mathcal{U}$. If σ is false, then $\sigma \implies \exists x\ Px$ is true. If σ is true, then so is Pa, and therefore $\exists x\ Px$ is true; hence also $\sigma \implies \exists x\ Px$ is true. □

Lemma 1.9.3. $(\sigma\ \&\ \forall x\ Px) \iff \forall x\ (\sigma\ \&\ Px)$.

Proof. **(⇒)** Say $\sigma\ \&\ \forall x\ Px$. Let a be arbitrary. then Pa (by ∀-elimination), so $\sigma\ \&\ Pa$, hence $\forall x\ (\sigma\ \&\ Px)$ by ∀-introduction (since a was arbitrary).
(⇐) Say $\forall x\ (\sigma\ \&\ Px)$. Let a be arbitrary. Then $\sigma\ \&\ Pa$ (by ∀-elimination), so $\forall x\ Px$ by ∀-introduction (since a was arbitrary) and hence $\sigma\ \&\ \forall x\ Px$. □

Lemma 1.9.4. $(\sigma \implies \forall x\ Px) \iff \forall x\ (\sigma \implies Px)$.

Now, writing $Sx\delta\varepsilon$ for (1.28), we can rewrite (1.27) as

$$\forall\varepsilon\ (\varepsilon > 0 \implies \exists\delta\ (\delta > 0\ \&\ \forall x\ Sx\delta\varepsilon)),$$
$$\forall\varepsilon\ \exists\delta\ (\varepsilon > 0 \implies (\delta > 0\ \&\ \forall x\ Sx\delta\varepsilon)),$$
$$\forall\varepsilon\ \exists\delta\ (\varepsilon > 0 \implies \forall x\ (\delta > 0\ \&\ Sx\delta\varepsilon)),$$
$$\forall\varepsilon\ \exists\delta\ \forall x\ (\varepsilon > 0 \implies (\delta > 0\ \&\ Sx\delta\varepsilon)).$$

The various rules must be applied with sensitivity to variables:

Lemma 1.9.5. $(\forall x\ Px \implies \forall x\ Qx) \iff \forall y\ \exists x\ (Px \implies Qy)$.

Proof. The following are equivalent.

$$\begin{aligned}
&\forall x\ Px \implies \forall x\ Qx, && \\
&\forall x\ (\forall x\ Px \implies Qx), && \\
&\forall x\ Px \implies Qa && \text{for arbitrary } a, \\
&\neg Qa \implies \exists x\ \neg Px && \text{for arbitrary } a, \\
&\exists x\ (\neg Qa \implies \neg Px) && \text{for arbitrary } a, \\
&\exists x\ (Px \implies Qa) && \text{for arbitrary } a, \\
&\forall y\ \exists x\ (Px \implies Qy). &&
\end{aligned}$$

□

Models

The assertion that the Diophantine equation $x^2 - y^2 = (x + y)(x - y)$ is an identity is the proposition

$$\forall x\ \forall y\ x^2 - y^2 = (x + y)(x - y),$$

where x and y are understood to range over $\mathbb{Z}$. To express this last qualification, we can write

$$\mathbb{Z} \vDash \forall x\ \forall y\ x^2 - y^2 = (x + y)(x - y)$$

(a notation to be developed in § 3.5). The expression $\mathbb{Z} \vDash \sigma$ can be read as one of

$$\begin{gathered}
\sigma \text{ is true in } \mathbb{Z}, \\
\mathbb{Z} \text{ satisfies } \sigma, \\
\mathbb{Z} \text{ is a model of } \sigma;
\end{gathered}$$

here $\mathbb{Z}$ is the *context* in which σ is true (see § 1.1). The symbol $\vDash$ can be called the **semantic turnstile:** *semantic,* because it concerns the *meaning* of propositions (rather than the form), and *turnstile,* because that is roughly what it looks like: a gate with a horizontal bar that you can turn away if you are allowed to pass (as for example when leaving the METU library). The *syntactic turnstile* $\vdash$ will be introduced in § 2.8.

The notation $\mathbb{Z} \nvDash \sigma$ means σ is false in $\mathbb{Z}$, that is, $\mathbb{Z} \vDash \neg\sigma$.

Example 1.9.6. The sentence $\forall x\ (x \neq 0 \implies \exists y\ xy = 1)$ is false in $\mathbb{Z}$, but true in $\mathbb{Q}$, that is,

$$\mathbb{Z} \nvDash \forall x\ (x \neq 0 \implies \exists y\ xy = 1), \qquad \mathbb{Q} \vDash \forall x\ (x \neq 0 \implies \exists y\ xy = 1).$$

Hence also $\mathbb{Z} \vDash \exists x\ (x \neq 0\ \&\ \forall y\ xy \neq 1)$; for example, $\mathbb{Z} \vDash (2 \neq 0\ \&\ \forall y\ 2y \neq 1)$.

Ordinary language

Look again at the equations

$$A = \mathcal{U}, \quad A \neq \varnothing, \quad A = \varnothing, \quad A \neq \mathcal{U}.$$

These can be verbalized respectively as

1) everything is in A,
2) something is in A,
3) nothing is in A,
4) not everything is in A.

The first three of these clauses are obtained from the clause thing is in A by adding, respectively, a universal, an existential, and a negative determiner. The last clause needs the addition of not every; alternatively, the clause could be written as something is not in A. Apparently, in English, there is not a one-word expression with the meaning of not every and some... not.

Some people might write the last clause on the list as Everything is not in A, or All things are not in A. For example, there is a saying:

All that glitters is not gold.

It is pretty clear that what is meant is that *some* things that glitter are not gold: some shiny attractive things are not worth much. But the saying looks as if it could be written as All that glitters fails to be gold. This does not have the intended meaning, since gold itself does glitter. To avoid possible misunderstanding, it seems better to write

Not all that glitters is gold,

with not moved to the beginning.

Turkish avoids the ambiguities possible from a misplaced not. In the Antalya *otogar,* I once bought a bag of bananas with the brand name Asal. The bag displayed the slogan

Her muz Asal muz değildir.

This should be translated as Not every banana is a Prime banana. According to our understanding, the sentence Every banana is not a Prime banana would be rendered in Turkish as

Hiçbir muz Asal muz değildir.

The words a(n) and any are ambiguous. If you say A dog has three legs, you probably mean the a existentially: there is a dog that has three legs. But if you say A dog has four legs, probably you are describing dogs in general: every dog has four legs. The sentence Anybody can come could be a general invitation to everybody, or it could express a worry over the possibility that somebody will come.

Still, the word any seems useful in ordinary life. Again, Donne writes:

Any man's death diminishes me.

Could he write, instead, Every man's death diminishes me? In a mathematical context, the every is preferable; but every man's death suggests the image of all people dying at once; any man's death takes the deaths one by one.

Exercises

1. Prove Lemma 1.9.4.
2. Find (with proof) prenex forms for the following:
   a) $\sigma \ \& \ \exists x \, Px$,
   b) $\forall x \, Px \implies \sigma$,
   c) $\exists x \, Px \implies \sigma$,
   d) $\exists x \, Px \implies \forall x \, Qx$,
   e) $\forall x \, Px \implies \exists x \, Qx$.
3. Rewrite $\forall x \, \exists y \, Rxy$ in a form that does not use $\exists$.
4. Write the negation of $\exists x \, (Px \implies \forall y \, Rxy)$ in prenex form.
5. Write the following sentences σ in symbolic form, with quantifiers, and in each case, determine whether $\mathfrak{M} \vDash \sigma$, where $\mathfrak{M}$ is $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$:
   a) every number has a square root;
   b) every positive number has a square root;
   c) for all coefficients b and c, the equation $x^2 + bx + c = 0$ has two distinct solutions, provided $b^2 \neq 4c$;
   d) there is no least number;
   e) between any two distinct numbers, there is another number.

2. Propositional logic

2.0. Truth-tables

Propositional formulas were defined in § 1.7. It was suggested there that every *closed* propositional formula $\boldsymbol{F}$ has a **value.** Let us denote this value by

$$\widehat{\boldsymbol{F}};$$

it is an element of $\mathbb{B}$ and can be found in the following way. First note that $\boldsymbol{F}$ meets one of the following conditions:

1) $\boldsymbol{F}$ is a constant from $\mathbb{B}$ (that is, 0 or 1), or
2) $\boldsymbol{F}$ is $\neg\boldsymbol{G}$ for some closed formula $\boldsymbol{G}$, or
3) $\boldsymbol{F}$ is $(\boldsymbol{G} * \boldsymbol{H})$ for some closed formulas $\boldsymbol{G}$ and $\boldsymbol{H}$, where $*$ is one of the connectives $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, and $\not\Leftrightarrow$.

Then we can find $\widehat{\boldsymbol{F}}$ by the following **recursive** procedure:

1. If $\boldsymbol{F}$ is in $\mathbb{B}$, then $\widehat{\boldsymbol{F}}$ is $\boldsymbol{F}$ itself.
2. If $\boldsymbol{F}$ is $\neg\boldsymbol{G}$, then $\widehat{\boldsymbol{F}}$ is the value of $\neg\widehat{\boldsymbol{G}}$ as determined by the table in § 1.7.
3. If $\boldsymbol{F}$ is $(\boldsymbol{G} * \boldsymbol{H})$, then $\widehat{\boldsymbol{F}}$ is the value of $\widehat{\boldsymbol{G}} * \widehat{\boldsymbol{H}}$ as determined by the tables in § 1.7.

In the terminology introduced at the end of § 1.7, $\boldsymbol{F}$ is a **name** for $\widehat{\boldsymbol{F}}$. It is proved in the next section below that $\widehat{\boldsymbol{F}}$ is *uniquely* determined by the procedure just given for finding it; we can then indeed call $\widehat{\boldsymbol{F}}$ the **value,** or more precisely the **truth-value,** of $\boldsymbol{F}$.

If a formula is not closed, then it does not have a value in $\mathbb{B}$. However, any formula can be made into a closed formula by *substitution* of values for its variables.

For each propositional formula $\boldsymbol{F}$, there is some n in $\mathbb{N}$ such that, for each k in $\mathbb{N}$, if the variable P_k appears in $\boldsymbol{F}$, then $k < n$. Then we can write $\boldsymbol{F}$ as

$$\boldsymbol{F}(P_0, \ldots, P_{n-1}),$$

and we may refer to $\boldsymbol{F}$ as an n**-ary** formula. A 3-ary formula is also called **ternary;** a 2-ary formula, **binary;** a 1-ary formula, **singulary.**[1] A 0-ary or **nullary** formula has *no* variables: it is **closed** in the sense of § 1.7. An n-ary formula is also $(n+1)$-ary, $(n+2)$-ary, and so on.

Examples 2.0.1.

1. Suppose $\boldsymbol{F}$ is $P_0 \& P_1 \Rightarrow P_0 \vee P_1$ (that is, $((P_0 \& P_1) \Rightarrow (P_0 \vee P_1))$, according to the convention established in § 1.7). Then $\boldsymbol{F}$ is binary and can be described as

$$\boldsymbol{F}(P_0, P_1).$$

It can also be considered as the ternary formula $\boldsymbol{F}(P_0, P_1, P_2)$, but *not* as the singulary $\boldsymbol{F}(P_0)$.

2. By the convention established here, the formula $P_4 \vee P_{21}$ is 22-ary and 175-ary; it is not 21-ary, much less binary.

If $\boldsymbol{F}$ is an $(n+1)$-ary formula, then it can be converted to an n-ary formula in two different ways by **substitution.** Indeed, if e is one of the two elements of $\mathbb{B}$, then each occurrence of the variable P_n in $\boldsymbol{F}$ can be replaced with e; all the remaining variables of $\boldsymbol{F}$ belong to $\{P_0, \ldots, P_{n-1}\}$, so $\boldsymbol{F}$ has become n-ary. In turn, other elements of $\mathbb{B}$ can be substituted for other variables in $\boldsymbol{F}$, so that, in the end, a closed formula results.

In general, if $\boldsymbol{F}$ is an n-ary formula, and $(e_0, \ldots, e_{n-1})$ is a list of n elements of $\mathbb{B}$, then there is a closed formula

$$\boldsymbol{F}(e_0, \ldots, e_{n-1}),$$

which is the result of subtituting e_k for P_k in $\boldsymbol{F}$ for each k that is less than n. The list $(e_0, \ldots, e_{n-1})$ can be called an n**-tuple** from $\mathbb{B}$ and can be abbreviated by

$$\vec{e}.$$

[1] The word unary is often used instead of singulary. Following Quine, Church [9, § 02, p. 12, n. 29] suggests singulary as a more etymologically correct word than unary. Indeed, whereas the first five Latin cardinal numbers are UN-, DU-, TRI-, QUATTUOR, QUINQUE, the first five Latin *distributive* numbers—corresponding to the Turkish birer, ikişer, üçer, dörder, beşer [36]—are SINGUL-, BIN-, TERN-, QUATERN-, QUIN-. It is the latter sequence that gives us binary and ternary—also quaternary and quinary, if these are desired. So singulary appears to be a better word than unary. In fact, singulary does not appear in the original *Oxford English Dictionary* [34]. The word unary *does* appear in this dictionary, but it is considered obsolete: only one use of the word, from 1576, was discovered in English literature. There, unary meant *unit*, although the word unit was not actually invented until 1570, when it was introduced by [John] Dee to correspond to the Greek μονάδ-.

(The definition of n-tuple will be refined in § 3.2.) Here the tuple $\vec{e}$ is an n-ary **truth-assignment** (or a truth-assignment for the n-ary formula $\boldsymbol{F}$). The truth-value of $\boldsymbol{F}(\vec{e})$ can be denoted by[2]

$$\widehat{\boldsymbol{F}}(\vec{e}).$$

Example 2.0.2. Again suppose $\boldsymbol{F}$ is $P_0 \,\&\, P_1 \Rightarrow P_0 \vee P_1$; consider this as $\boldsymbol{F}(P_0, P_1)$. If $\vec{e} = (0, 1)$, then $\boldsymbol{F}(\vec{e})$ is $0 \,\&\, 1 \Rightarrow 0 \vee 1$; the value of this is the value of $0 \Rightarrow 1$, which is 1. That is, $\widehat{\boldsymbol{F}}(0, 1) = 1$.

A **truth-table** is a list of the values attained by a propositional formula under its possible truth-assignments. If a formula is n-ary, then its truth-table has $n+1$ columns: a column for each variable, and one column for the formula itself; also, aside from the headings of the columns, the table must have 2^n rows.

Example 2.0.3. Truth-tables defining certain connectives were given in § 1.7.

If $k < 2^n$, then

$$k = e_0^k + 2e_1^k + 4e_2^k + \cdots + 2^{n-1}e_{n-1}^k = \sum_{j<n} 2^j e_j^k$$

for some e_j^k in $\mathbb{B}$; that is, k is $e_{n-1}^k e_{n-2}^k \cdots e_1^k e_0^k$ in binary notation. Then the truth-table for an arbitrary n-ary formula $\boldsymbol{F}(P_0, \ldots, P_{n-1})$ has the form of

P_0	P_1	P_2	$\cdots$	P_{n-1}	$\boldsymbol{F}$
0	0	0	$\cdots$	0	$\widehat{\boldsymbol{F}}(0, 0, 0, \ldots, 0)$
1	0	0	$\cdots$	0	$\widehat{\boldsymbol{F}}(1, 0, 0, \ldots, 0)$
0	1	0	$\cdots$	0	$\widehat{\boldsymbol{F}}(0, 1, 0, \ldots, 0)$
1	1	0	$\cdots$	0	$\widehat{\boldsymbol{F}}(1, 1, 0, \ldots, 0)$
0	0	1	$\cdots$	0	$\widehat{\boldsymbol{F}}(0, 0, 1, \ldots, 0)$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
e_0^k	e_1^k	e_2^k	$\cdots$	e_{n-1}^k	$\widehat{\boldsymbol{F}}(e_0^k, e_1^k, e_2^k, \ldots, e_{n-1}^k)$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$

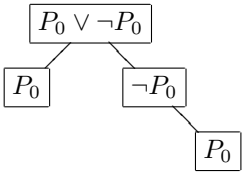
To be able to *compute* the truth-table of a formula, we need to know the truth-tables of the *proper sub-formulas* of the given formula. The **sub-formulas** of a formula are determined by the following conditions:

[2]The notation is from [6, Definition 2.1.8, p. 41].

1. $\boldsymbol{F}$ is a sub-formula of itself.
2. $\boldsymbol{F}$ is a sub-formula of $\neg\boldsymbol{F}$.
3. $\boldsymbol{F}$ and $\boldsymbol{G}$ are sub-formulas of $(\boldsymbol{F} * \boldsymbol{G})$ (where $*$ is $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ or $\nLeftrightarrow$; remember that, by the convention established in § 1.7, $\boldsymbol{F}$ and $\boldsymbol{G}$ here are not just strings, but *formulas*).
4. Every sub-formula of a sub-formula of $\boldsymbol{F}$ is a sub-formula of $\boldsymbol{F}$.

A sub-formula of $\boldsymbol{F}$ is a **proper sub-formula** if it is not $\boldsymbol{F}$ itself.

The sub-formulas of a given formula can be arranged in a tree. For example, the sub-formulas of $P_0 \vee \neg P_0$ are the nodes of the following tree:



The sub-formulas of $P_0 \vee \neg P_0$ are thus P_0, $P_0 \vee \neg P_0$ itself, $\neg P_0$, and P_0 again. I write P_0 twice because it appears twice as a sub-formula of $P_0 \vee \neg P_0$. However, we can give the truth-table for $P_0 \vee \neg P_0$ (along with an extra column for our computations) thus:

P_0	$\neg P_0$	$P_0 \vee \neg P_0$
0	1	1
1	0	1

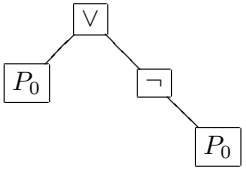
.

Alternatively, we can include a column for each sub-formula (even if it is the same as another sub-formula):

P_0	$P_0 \vee \neg P_0$	$\neg P_0$	P_0
0	1	1	0
1	1	0	1

.

Why would we do this? The sub-formulas of any formula are in one-to-one correspondence with the variables and the connectives in the formula (that is, there is a bijection between them, in the sense of § 3.3). Indeed, compare the previous tree with the following:



We have the following correspondence between sub-formulas and symbols:

$$\begin{array}{rcl} P_0 & \rightsquigarrow & P_0 \\ P_0 \vee \neg P_0 & \rightsquigarrow & \vee \\ \neg P_0 & \rightsquigarrow & \neg \\ P_0 & \rightsquigarrow & P_0 \end{array}$$

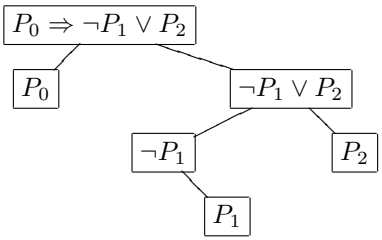
Using this correspondence, we can rewrite the last truth-table thus:

P_0	$\vee$	$\neg$	P_0
0	1	1	0
1	1	0	1

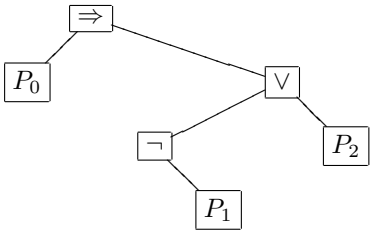
I propose to call this the **full truth-table** of $P_0 \vee \neg P_0$; from it we can extract the **proper truth-table** of $P_0 \vee \neg P_0$ by taking only one column headed by P_0, along and the column headed by $\vee$ (which corresponds to the whole formula):

P_0	$P_0 \vee \neg P_0$
0	1
1	1

For another example, let $\boldsymbol{F}$ be the formula $P_0 \Rightarrow \neg P_1 \vee P_2$. The sub-formulas of $\boldsymbol{F}$ compose the tree



The corresponding tree of variables and connectives is:



From this we can get the full truth-table as described below. This table itself is:

P_0	$\Rightarrow$	$\neg$	P_1	$\vee$	P_2
0	1	1	0	1	0
1	1	1	0	1	0
0	1	0	1	0	0
1	0	0	1	0	0
0	1	1	0	1	1
1	1	1	0	1	1
0	1	0	1	1	1
1	1	0	1	1	1

.

We can construct this in stages, working our way through the trees drawn above, starting with the variables:

P_0	$\Rightarrow$	$\neg$	P_1	$\vee$	P_2
0			0		0
1			0		0
0			1		0
1			1		0
0			0		1
1			0		1
0			1		1
1			1		1

,

P_0	$\Rightarrow$	$\neg$	P_1	$\vee$	P_2
0		1	0		0
1		1	0		0
0		0	1		0
1		0	1		0
0		1	0		1
1		1	0		1
0		0	1		1
1		0	1		1

,

then

P_0	$\Rightarrow$	$\neg$	P_1	$\vee$	P_2
0		1	0	1	0
1		1	0	1	0
0		0	1	0	0
1		0	1	0	0
0		1	0	1	1
1		1	0	1	1
0		0	1	1	1
1		0	1	1	1

and finally the complete table given earlier. The column giving the values of $\boldsymbol{F}$ itself is the last to be filled in: in this case, the second column, under $\Rightarrow$. The

proper truth-table for $\boldsymbol{F}$ is then

P_0	P_1	P_2	$\boldsymbol{F}$
0	0	0	1
1	0	0	1
0	1	0	1
1	1	0	0
0	0	1	1
1	0	1	1
0	1	1	1
1	1	1	1

.

Exercises

1. Write full truth-tables and proper truth-tables for the formulas:
   (a) $P_0 \Rightarrow P_1 \Rightarrow P_0$;
   (b) $P_0 \,\&\, P_1 \,\&\, P_2$;
   (c) $P_0 \not\Leftrightarrow P_1 \not\Leftrightarrow P_2$;
   (d) $(P_0 \Rightarrow P_1 \vee P_2) \Rightarrow \neg P_0 \vee P_1$;
   (e) $(P_0 \Rightarrow P_1 \vee \neg P_2) \,\&\, (P_1 \Rightarrow P_0 \,\&\, P_2) \Rightarrow P_0 \Rightarrow P_2$;
   (f) $\neg(\neg P_2 \Rightarrow P_0 \Rightarrow \neg(P_2 \Rightarrow P_1))$.
   How many columns has each table?
2. What does the truth-table for a nullary (closed) formula look like?
3. For each n in $\mathbb{N}$, describe the n-ary formulas whose full truth-tables have fewer columns than their proper truth-tables.

2.1. Unique readability

We have to justify our definition of $\widehat{\boldsymbol{F}}$ for closed formulas $\boldsymbol{F}$: that is, we have to confirm that only one value of $\widehat{\boldsymbol{F}}$ can be computed for each $\boldsymbol{F}$.

We have called a propositional formula n-ary if its variables are among the first n variables on the list $(P_0, P_1, P_2, \dots)$. The notion of **arity** applies to connectives themselves:

1. $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ and $\not\Leftrightarrow$ are **binary**, because they are used to join *two* formulas.
2. $\neg$ is **singulary**.

3. The constants 0 and 1 are **nullary.**

Although, by our convention, an n-ary formula is also $(n+1)$-ary, a connective has a unique arity: since $\neg$ is singulary, it is not binary.

The formulas joined by a connective in a formula are the **arguments** of the connective. In the formula

$$\boldsymbol{P} \Rightarrow \neg \boldsymbol{Q} \,\&\, 1$$

(which stands for $(\boldsymbol{P} \Rightarrow (\neg \boldsymbol{Q} \,\&\, 1))$), the arguments of $\Rightarrow$ are $\boldsymbol{P}$ and $\neg \boldsymbol{Q} \,\&\, 1$ (in that order); the arguments of $\&$ are $\neg \boldsymbol{Q}$ and 1; the argument of $\neg$ is $\boldsymbol{Q}$; and 1 has no argument.

By definition, each propositional formula $\boldsymbol{F}$ meets one of the following conditions:

1) $\boldsymbol{F}$ is a variable;
2) $\boldsymbol{F}$ is a nullary connective;
3) $\boldsymbol{F}$ is $\neg \boldsymbol{G}$ for some $\boldsymbol{G}$;
4) $\boldsymbol{F}$ is $(\boldsymbol{G} * \boldsymbol{H})$ for some $\boldsymbol{G}$ and $\boldsymbol{H}$ and some binary connective $*$.

It is obvious that $\boldsymbol{F}$ can meet *only* one of these conditions. It is *not* obvious that a formula $(\boldsymbol{G} * \boldsymbol{H})$ cannot also be written $(\boldsymbol{G}' *' \boldsymbol{H}')$, where $\boldsymbol{G}'$ is a *different* formula from $\boldsymbol{G}$.

Let $\boldsymbol{G}$ be $(\boldsymbol{P} \,\&\, \boldsymbol{Q})$, and let $\boldsymbol{H}$ be $\boldsymbol{R}$. Then $(\boldsymbol{G} \vee \boldsymbol{H})$ is $((\boldsymbol{P} \,\&\, \boldsymbol{Q}) \vee \boldsymbol{R})$, which can be written as $(\boldsymbol{U} \,\&\, \boldsymbol{V})$, where $\boldsymbol{U}$ is $(\boldsymbol{P}$, and $\boldsymbol{V}$ is $\boldsymbol{Q}) \vee \boldsymbol{R}$. But $\boldsymbol{U}$ is not a formula (why not?); neither is $\boldsymbol{V}$.

How do we know that, if $\boldsymbol{G}$ and $\boldsymbol{H}$ are more complicated, $(\boldsymbol{G} * H)$ *still* cannot be analyzed as a different application of a binary connective? How do we know that $(\boldsymbol{G} * \boldsymbol{H})$ is **uniquely readable?** Our definition of $\widehat{\boldsymbol{F}}(\vec{e})$ requires unique readability. To *prove* unique readability; we can use the notion of an *initial segment* of a formula.

Every formula is a string of symbols, written left to right. If we cut the string, then it is divided into two segments: an **initial** and a **final** segment. I allow the cut to come at an end: that is, I allow one of the two segments to be empty, so that the other segment is the whole string:

Example 2.1.1. The initial segments of $(\boldsymbol{P} \vee \neg \boldsymbol{P})$ are $(\boldsymbol{P} \vee \neg \boldsymbol{P})$ itself, $(\boldsymbol{P} \vee \neg \boldsymbol{P}$, $(\boldsymbol{P} \vee \neg$, $(\boldsymbol{P} \vee$, $(\boldsymbol{P}$, (, and the empty string.

An initial segment of $\boldsymbol{F}$ that is not $\boldsymbol{F}$ itself is a **proper initial segment** of $\boldsymbol{F}$.

Lemma 2.1.2.

1. *Every propositional formula has* just as many *left parentheses as right parentheses.*

2. *If* $\boldsymbol{F}$ *is a variable, a constant, or a negation, then every initial segment of* $\boldsymbol{F}$ *has* at least as many *left parentheses as right parentheses.*
3. *If* $\boldsymbol{F}$ *is a propositional formula that is not a variable, a constant, or a negation, then every non-empty proper initial segment of* $\boldsymbol{F}$ *has* more *left parentheses than right parentheses.*

Proof. To prove the first claim, follow the pattern of Proposition 1.2.

To prove the second and third claims, let A be the set of formulas $\boldsymbol{F}$ that do satisfy those claims. Then, trivially, A contains all variables and constants. If A contains $\boldsymbol{F}$, then $\boldsymbol{F}$ has at least as many left as right parentheses, hence so does $\neg\boldsymbol{F}$, which is a negation, so $\neg\boldsymbol{F}$ is in A. Finally, suppose A contains $\boldsymbol{F}$ and $\boldsymbol{G}$, and $*$ is a binary connective. Every non-empty proper initial segment of $(\boldsymbol{F} * \boldsymbol{G})$ is either $(\boldsymbol{F} * \boldsymbol{U}$ for some initial segment $\boldsymbol{U}$ of $\boldsymbol{G}$, or $(\boldsymbol{V}$ for some initial segment $\boldsymbol{V}$ of $\boldsymbol{F}$. But then $\boldsymbol{U}$ and $\boldsymbol{V}$ must have *at least* as many left as right parentheses, since $\boldsymbol{F}$ and $\boldsymbol{G}$ are in A; so $(\boldsymbol{F} * \boldsymbol{U}$ and $(\boldsymbol{V}$ have *more* left than right parentheses. Therefore $(\boldsymbol{F} * \boldsymbol{G})$ is in A. By the recursive definition of propositional formulas, A contains all propositional formulas. □

Lemma 2.1.3. *No proper initial segment of a propositional formula is a propositional formula.*

Proof. Let A comprise all formulas $\boldsymbol{F}$ such that no proper initial segment of $\boldsymbol{F}$ is a formula. Then A contains all variables and constants. Suppose A contains $\boldsymbol{F}$, and $\boldsymbol{U}$ is an initial segment of $\neg\boldsymbol{F}$ that is a formula. Then $\boldsymbol{U}$ is $\neg\boldsymbol{V}$ for some initial segment $\boldsymbol{V}$ of $\boldsymbol{F}$ that is also a formula; so $\boldsymbol{V}$ is $\boldsymbol{F}$; hence $\boldsymbol{U}$ is $\neg\boldsymbol{F}$. Therefore $\neg\boldsymbol{F}$ is in A.

Finally, suppose $\boldsymbol{F}$ and $\boldsymbol{G}$ are in A, and $*$ is a binary connective. Every proper initial segment of $(\boldsymbol{F}*\boldsymbol{G})$ is either empty or has more left than right parentheses, by Lemma 2.1.2, so it is not a formula. Thus $(\boldsymbol{F} * \boldsymbol{G})$ is in A. By definition of propositional formulas, A contains all of them. □

An alternative proof of this lemma is by the method of **infinite descent:** that is, it relies on something like Lemma 1.4.3. Suppose some proper initial segment of a formula is also a formula. Then the original formula is either $\neg\boldsymbol{F}$ or $(\boldsymbol{F} * \boldsymbol{G})$. If it is $\neg\boldsymbol{F}$, then its proper initial segment is $\neg\boldsymbol{F}'$, where $\boldsymbol{F}'$ is a formula that is a proper initial segment of $\boldsymbol{F}$. If the original formula is $(\boldsymbol{F} * \boldsymbol{G})$, then its proper initial segment must have the form $(\boldsymbol{F}' *' \boldsymbol{G}')$, and then there are two possibilities:

1) one of $\boldsymbol{F}$ and $\boldsymbol{F}'$ is a proper initial segment of the other, or
2) $\boldsymbol{F}$ and $\boldsymbol{F}'$ are the same formula, and $\boldsymbol{G}'$ is a proper initial segment of $\boldsymbol{G}$.

Thus, for every formula with a proper initial segment that is a formula, there is a *shorter* formula with the same property. In this way, we get an infinite sequence of formulas, each one strictly shorter then the preceding, which is absurd.

Theorem 2.1.4 (Unique Readability)**.** *If* $(\boldsymbol{F} * \boldsymbol{G})$ *and* $(\boldsymbol{F}' *' \boldsymbol{G}')$ *are the same propositional formula, then* $\boldsymbol{F}$ *and* $\boldsymbol{F}'$ *are the same (hence* $*$ *is* $*'$*, and* $\boldsymbol{G}$ *is* $\boldsymbol{G}'$*).*

Proof. If $(\boldsymbol{F} * \boldsymbol{G})$ and $(\boldsymbol{F}' *' \boldsymbol{G}')$ are the same formula, then one of $\boldsymbol{F}$ and $\boldsymbol{F}'$ is an initial segment of the other, so they are the same by Lemma 2.1.3. □

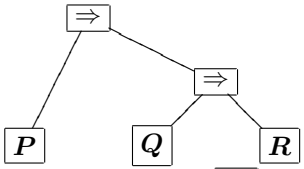
Now we know that $\widehat{\boldsymbol{F}}(\vec{e})$ is well defined, so truth-tables are uniquely determined.

It may seem as if parentheses are required to ensure unique readability. We do have a convention that allows us to dispense with some parentheses: we can write $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \Rightarrow \boldsymbol{R}$ for $(\boldsymbol{P} \Rightarrow (\boldsymbol{Q} \Rightarrow \boldsymbol{R}))$. But we cannot dispense with the parentheses in $(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \Rightarrow \boldsymbol{R}$, unless we come up with a completely new system of notation.

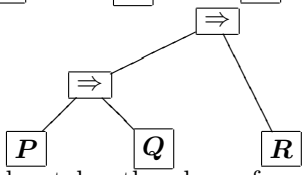
Polish notation

When we move into a second dimension and write formulas as trees, then

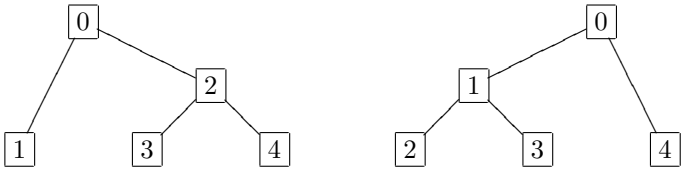
1) $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \Rightarrow \boldsymbol{R}$ becomes



2) $(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \Rightarrow \boldsymbol{R}$ becomes



The arrangement of the branches takes the place of parentheses. Now convert the trees back into strings, but write the symbols in the following orders, respectively:



The resulting strings are

$$\Rightarrow \boldsymbol{P} \Rightarrow \boldsymbol{Q}\boldsymbol{R}; \qquad \Rightarrow \Rightarrow \boldsymbol{P}\boldsymbol{Q}\boldsymbol{R}.$$

These are formulas written in *Łukasiewicz* or *Polish notation*.[3]

A **signature** is a set of connectives. Our definition of propositional formulas in § 1.7 is a definition of the formulas of the signature $\{0, 1, \neg, \&, \vee, \Rightarrow, \Leftrightarrow, \nLeftrightarrow\}$ in **infix notation.** Infix notation makes sense only when the connectives in use are 0-, 1- or 2-ary. Of a signature $\mathcal{L}$ containing connectives of possibly higher arities, the formulas in **Polish notation** can be defined as follows:

1. All variables are formulas of $\mathcal{L}$ in Polish notation;
2. if $n \in \mathbb{N}$, and $*$ is an n-ary connective in $\mathcal{L}$, and if $\boldsymbol{F}_0$, $\boldsymbol{F}_1$, …, $\boldsymbol{F}_{n-1}$ are formulas of $\mathcal{L}$ in Polish notation, then

$$* \, \boldsymbol{F}_0 \boldsymbol{F}_1 \cdots \boldsymbol{F}_{n-1}$$

is a formula of $\mathcal{L}$ in Polish notation.

(The latter condition includes the case $n = 0$; in this case, the list $(\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1})$ is empty, so the nullary connective by itself is a formula.) Thus, in Polish notation, every connective is followed by the list of its arguments. In **reverse Polish notation** (or **RPN**), the connective comes *after* its arguments. The corresponding RPN for arithmetic can be convenient for electronic calculators, and it bears some resemblance to Turkish word-order. Compare:

	One	plus	two	is	three.
infix notation:	1	+	2	=	3
	Bir	iki	daha	üç	-tür.
RPN:	1	2	+	3	=

Exercises

1. Prove part 1 of Lemma 2.1.2.

2. For each symbol in the formula $(\boldsymbol{P} \Rightarrow \boldsymbol{Q} \vee \neg \boldsymbol{R}) \& (1 \Rightarrow \boldsymbol{P} \& \boldsymbol{R}) \Rightarrow (0 \Rightarrow \boldsymbol{R})$, give the list of arguments, if it exists. Write the formula in Polish notation.

3. Prove that formulas in Polish notation have unique readability. (You can use infinite descent; but can you *avoid* using this technique?)

[3] Church [9, p. 38, n. 91] calls it Łukasiewicz notation, after its inventor—who was Polish; the common term today seems to be Polish notation.

4. Letting $\triangledown$ be the *ternary* operation on $\mathbb{B}$ that converts a triple (x, y, z) to $\mathrm{p}((x+1)(y+1)(z+1))$ (where p is as in § 1.6), construct a truth-table for $\triangledown \boldsymbol{PQR}$.

2.2. Logical equivalence

Recall the distinction, stated in § 1.3, between terms and polynomials. Suppose $\boldsymbol{F}$ and $\boldsymbol{G}$ are two n-ary Boolean terms, that is, propositional formulas. They represent the same Boolean polynomial if

$$\widehat{\boldsymbol{F}}(\vec{e}) = \widehat{\boldsymbol{G}}(\vec{e})$$

for all truth-assignments $\vec{e}$. In this case, as suggested in § 1.7, we shall write

$$\boldsymbol{F} \sim \boldsymbol{G};$$

and we shall say that $\boldsymbol{F}$ and $\boldsymbol{G}$ are **logically equivalent** (or just **equivalent**). Here we have a clear test for equivalence: *Two formulas are equivalent if and only if they have the same proper truth-table;* more precisely, the formulas must have the same truth-table when the formulas are treated as being n-ary for the same n. Let us call this test for equivalence the **truth-table method.**

Example 2.2.1. Are the formulas P_0 and $(P_1 \vee \neg P_1) \Rightarrow P_0$ equivalent? Their full truth-tables are

P_0
0
1

$(P_1$	$\vee$	$\neg$	$P_1)$	$\Rightarrow$	P_0
0	1	1	0	0	0
0	1	1	0	1	1
1	1	0	1	0	0
1	1	0	1	1	1

.

As a binary formula, each formula has the same proper truth-table

P_0	P_1	$\boldsymbol{F}$
0	0	0
1	0	1
0	1	0
1	1	1

;

so the formulas are equivalent.

The truth-table method is a method of *proving* that two formulas are equivalent. The method is highly specific: For example, it cannot obviously[4] be used to prove the arithmetic identities mentioned in § 1.3, or to prove trigonometric identities like

$$\tan^2 x + 1 = \sec^2 x.$$

To prove *this* identity, we can write a chain of recognizable identities:

$$\tan^2 x + 1 = \frac{\sin^2 x}{\cos^2 x} + 1 = \frac{\sin^2 x}{\cos^2 x} + \frac{\cos^2 x}{\cos^2 x} = \frac{\sin^2 x + \cos^2 x}{\cos^2 x} = \frac{1}{\cos^2 x} = \sec^2 x.$$

This proof is an example of the *method of simplification*. This method can also be used for propositional formulas. In this context, we shall develop the theoretical background of simplification in the next section; the method itself is developed in § 2.6, but will rely on the lemma below. A proof by simplification, suitably expressed, will be an example of a *formal proof*.

Lemma 2.2.2.

1. ***Definitions:***

$$\begin{aligned} &\boldsymbol{P} \Rightarrow \boldsymbol{Q} \sim \neg \boldsymbol{P} \vee \boldsymbol{Q}, \\ &\boldsymbol{P} \Leftrightarrow \boldsymbol{Q} \sim (\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \Rightarrow \boldsymbol{P}), \\ &\boldsymbol{P} \not\Leftrightarrow \boldsymbol{Q} \sim \neg(\boldsymbol{P} \Leftrightarrow \boldsymbol{Q}). \end{aligned}$$

2. ***Double negation:***

$$\neg\neg \boldsymbol{P} \sim \boldsymbol{P}.$$

3. ***De Morgan's Laws:***

$$\neg(\boldsymbol{P} \vee \boldsymbol{Q}) \sim \neg \boldsymbol{P} \,\&\, \neg \boldsymbol{Q}, \qquad \neg(\boldsymbol{P} \,\&\, \boldsymbol{Q}) \sim \neg \boldsymbol{P} \vee \neg \boldsymbol{Q}.$$

4. ***Commutativity:***

$$\boldsymbol{P} \,\&\, \boldsymbol{Q} \sim \boldsymbol{Q} \,\&\, \boldsymbol{P}, \qquad \boldsymbol{P} \vee \boldsymbol{Q} \sim \boldsymbol{Q} \vee \boldsymbol{P}.$$

[4] A one-variable nonzero polynomial of degree n has at most n zeros; so if $f(x)$ and $g(x)$ are polynomials of degree n at most, and

$$0 = f(x_0) - g(x_0) = f(x_1) - g(x_1) = \cdots = f(x_n) - g(x_n),$$

where all of the x_k are distinct, then $\forall x\ f(x) = g(x)$. This method does not work for polynomials in more than one variable.

5. ***Associativity:***

$$(\boldsymbol{P} \,\&\, \boldsymbol{Q}) \,\&\, \boldsymbol{R} \sim \boldsymbol{P} \,\&\, (\boldsymbol{Q} \,\&\, \boldsymbol{R}), \qquad (\boldsymbol{P} \vee \boldsymbol{Q}) \vee \boldsymbol{R} \sim \boldsymbol{P} \vee (\boldsymbol{Q} \vee \boldsymbol{R}).$$

6. ***Distributivity:***

$$\boldsymbol{P} \,\&\, (\boldsymbol{Q} \vee \boldsymbol{R}) \sim (\boldsymbol{P} \,\&\, \boldsymbol{Q}) \vee (\boldsymbol{P} \,\&\, \boldsymbol{R}), \qquad \boldsymbol{P} \vee (\boldsymbol{Q} \,\&\, \boldsymbol{R}) \sim (\boldsymbol{P} \vee \boldsymbol{Q}) \,\&\, (\boldsymbol{P} \vee \boldsymbol{R}).$$

7. ***Redundancies:***

$$\begin{array}{llll} \boldsymbol{P} \,\&\, \boldsymbol{P} \sim \boldsymbol{P}, & \boldsymbol{P} \,\&\, \neg\boldsymbol{P} \sim 0, & \boldsymbol{P} \,\&\, 1 \sim \boldsymbol{P}, & \boldsymbol{P} \,\&\, 0 \sim 0, \\ \boldsymbol{P} \vee \boldsymbol{P} \sim \boldsymbol{P}, & \boldsymbol{P} \vee \neg\boldsymbol{P} \sim 1, & \boldsymbol{P} \vee 0 \sim \boldsymbol{P}, & \boldsymbol{P} \vee 1 \sim 1. \end{array}$$

8. ***New variables:***

$$\boldsymbol{P} \sim (\boldsymbol{P} \,\&\, \boldsymbol{Q}) \vee (\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}), \qquad \boldsymbol{P} \sim (\boldsymbol{P} \vee \boldsymbol{Q}) \,\&\, (\boldsymbol{P} \vee \neg\boldsymbol{Q}).$$

The proof of the lemma is an exercise. (The label Definitions in part 1 of the lemma is not a literal account of how the connectives were defined in § 1.7.)

The problem of checking for equivalence can be formulated in other ways. If $\boldsymbol{F} \sim 1$, then we write

$$\vDash \boldsymbol{F}, \tag{2.1}$$

and we say that $\boldsymbol{F}$ is a **tautology.**[5] (The semantic turnstile $\vDash$ was introduced in § 1.9. To be consistent with the notation in that earlier section, we might write (2.1) as $\mathbb{B} \vDash \boldsymbol{F}$; but the variables in propositional formulas will always range over $\mathbb{B}$.) If $\boldsymbol{F} \sim 0$, we call $\boldsymbol{F}$ a **contradiction.** We say $\boldsymbol{F}$ is **satisfiable** if it is not a contradiction. If both $\boldsymbol{F}$ and $\neg\boldsymbol{F}$ are satisfiable, then $\boldsymbol{F}$ is a **contingency.** Hence, in the truth-table for $\boldsymbol{F}$, if the column for $\boldsymbol{F}$ itself contains:

1) only 1s, then $\boldsymbol{F}$ is a tautology;
2) only 0s, then $\boldsymbol{F}$ is a contradiction;
3) at least one 1, then $\boldsymbol{F}$ is satisfiable;
4) at least one 1, and at least one 0, then $\boldsymbol{F}$ is a contingency.

Also, the following statements mean the same thing:

1) $\boldsymbol{F} \sim \boldsymbol{G}$;
2) $\vDash \boldsymbol{F} \Leftrightarrow \boldsymbol{G}$;
3) $\neg(\boldsymbol{F} \Leftrightarrow \boldsymbol{G})$ is not satisfiable.

Thus, in effect, a test for equivalence is a test for tautology, which is a test for satisfiability.

[5] From the Greek το αὐτο, meaning the same. Originally a tautology was a redundant expression, such as cease and desist.

Exercises

1. Test for the equivalence of the following pairs of formulas by the truth-table method:
   a) $\boldsymbol{P}$ and $\boldsymbol{Q} \Rightarrow \boldsymbol{P}$;
   b) $\boldsymbol{P}$ and $\boldsymbol{Q} \Rightarrow (\boldsymbol{P} \,\&\, \boldsymbol{Q})$;
   c) $\boldsymbol{P} \Rightarrow (\boldsymbol{Q} \Rightarrow \boldsymbol{R})$ and $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \Rightarrow (\boldsymbol{P} \Rightarrow \boldsymbol{R})$.
2. Give examples of tautologies, contradictions, and contingencies.
3. Prove Lemma 2.2.2.
4. Establish the following equivalences:
   (a) $\neg \boldsymbol{P} \sim 1 \nLeftrightarrow \boldsymbol{P}$;
   (b) $\boldsymbol{P} \vee \boldsymbol{Q} \sim \boldsymbol{P} \nLeftrightarrow \boldsymbol{Q} \nLeftrightarrow \boldsymbol{P} \,\&\, \boldsymbol{Q}$;
   (c) $\boldsymbol{P} \nLeftrightarrow \boldsymbol{Q} \sim \boldsymbol{Q} \nLeftrightarrow \boldsymbol{P}$;
   (d) $(\boldsymbol{P} \nLeftrightarrow \boldsymbol{Q}) \nLeftrightarrow \boldsymbol{R} \sim \boldsymbol{P} \nLeftrightarrow \boldsymbol{Q} \nLeftrightarrow \boldsymbol{R}$;
   (e) $\boldsymbol{P} \,\&\, (\boldsymbol{Q} \nLeftrightarrow \boldsymbol{R}) \sim \boldsymbol{P} \,\&\, \boldsymbol{Q} \nLeftrightarrow \boldsymbol{P} \,\&\, \boldsymbol{R}$;
   (f) $\boldsymbol{P} \nLeftrightarrow \boldsymbol{P} \sim 0$.
5. Is there a formula $\boldsymbol{F}$ such that

$$\vDash (\boldsymbol{F} \Rightarrow (\boldsymbol{P} \Leftrightarrow \boldsymbol{Q})) \,\&\, (\boldsymbol{P} \vee (\boldsymbol{Q} \vee \boldsymbol{F}))?$$

   (One way to solve this problem is to write out a truth table for $(\boldsymbol{R} \Rightarrow (\boldsymbol{P} \Leftrightarrow \boldsymbol{Q})) \,\&\, (\boldsymbol{P} \vee (\boldsymbol{Q} \vee \boldsymbol{R}))$, then try to write a truth-table for $\boldsymbol{F}$. An alternative is to use the next two sections to write the original formula in an equivalent form $(\boldsymbol{G} \Rightarrow \boldsymbol{F}) \,\&\, (\boldsymbol{F} \Rightarrow \boldsymbol{H})$, then check whether $\vDash \boldsymbol{G} \Rightarrow \boldsymbol{H}$.)

2.3. Substitution and replacement

If $\boldsymbol{F}$ is a formula for which $(e_0, \ldots, e_{n-1})$ is a truth-assignment, then the constant formula $\boldsymbol{F}(e_0, \ldots, e_{n-1})$ is obtained by **substitution.** In this substitution, it is not essential that each e_i be in the set $\mathbb{B}$, that is, $\{0, 1\}$; if $(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$ is a list of n formulas, then from $\boldsymbol{F}$ we can obtain the formula

$$\boldsymbol{F}(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$$

by *substitution* of $\boldsymbol{G}_j$ for each instance of P_j in $\boldsymbol{F}$, for each j less than n. Note that, if we are using the usual infix notation (see § 2.1), but have removed parentheses as allowed by our conventions, then the substitutions must be done with parentheses as necessary to ensure that each substituted formula becomes a *sub-formula* of the new formula.

Example 2.3.1. Suppose $\boldsymbol{F}$ is $P_0 \,\&\, (P_1 \Rightarrow P_0)$, and $\boldsymbol{G}_0$ is $P_0 \Rightarrow P_1$, and $\boldsymbol{G}_1$ is $P_1 \Rightarrow (P_0 \vee P_2)$. Then $\boldsymbol{F}(\boldsymbol{G}_0, \boldsymbol{G}_1)$ is

$$(P_0 \Rightarrow P_1) \,\&\, ((P_1 \Rightarrow (P_0 \vee P_2)) \Rightarrow P_0 \Rightarrow P_1).$$

rather than $P_0 \Rightarrow P_1 \,\&\, (P_1 \Rightarrow (P_0 \vee P_2) \Rightarrow P_0 \Rightarrow P_1)$.

Substitution is **associative** in that, if we substitute some formulas $\boldsymbol{G}_i$ into $\boldsymbol{F}$, and then substitute some formulas $\boldsymbol{H}_j$ into the result, we get the same formula as if we substitute the $\boldsymbol{H}_j$ first into the $\boldsymbol{G}_i$, and then the results into $\boldsymbol{F}$. Likewise, if you put a book in a box, then put the box on a table, you get the same result as if you first put the box on the table before putting the book in the box. The formal statement is the following:

Lemma 2.3.2 (Associativity)**.** *Suppose $\boldsymbol{F}$ is an n-ary formula, and*

$$(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$$

is a list of n formulas, each one of them being ℓ-ary. Let $\boldsymbol{H}$ be the formula $\boldsymbol{F}(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$. Then $\boldsymbol{H}$ is ℓ-ary. Suppose $(\boldsymbol{K}_0, \ldots, \boldsymbol{K}_{\ell-1})$ is a list of ℓ formulas. Then the formula

$$\boldsymbol{H}(\boldsymbol{K}_0, \ldots, \boldsymbol{K}_{\ell-1})$$

is the formula

$$\boldsymbol{F}(\boldsymbol{G}_0(\boldsymbol{K}_0, \ldots, \boldsymbol{K}_{\ell-1}), \ldots, \boldsymbol{G}_{n-1}(\boldsymbol{K}_0, \ldots, \boldsymbol{K}_{\ell-1})).$$

Finally, suppose $\vec{e}$ is a truth-assignment for the $\boldsymbol{G}_j$. Then $\vec{e}$ is a truth-assignment for $\boldsymbol{H}$. If also

$$\widehat{\boldsymbol{G}}_j(\vec{e}) = f_j$$

for each j in $\{0, \ldots, n-1\}$, then $(f_0, \ldots, f_{n-1})$ is a truth-assignment $\vec{f}$ for $\boldsymbol{F}$, and

$$\widehat{\boldsymbol{H}}(\vec{e}) = \widehat{\boldsymbol{F}}(\vec{f}).$$

Proof. I claim that the proposition is obvious,[6] in the sense that no written proof will make the truth of the proposition clearer than it already is to the reader who has understood the proposition. □

Is a truth-assignment for $\boldsymbol{F}(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$ also a truth-assignment for the $\boldsymbol{G}_j$? It is, if all of the variables $P_0, \ldots, P_{n-1}$ actually *appear* in $\boldsymbol{F}$; otherwise it may not be:

Example 2.3.3. Suppose $\boldsymbol{F}$ is just P_0, *considered* as a binary formula. Let $\boldsymbol{G}_i$ be P_i when $i \in \{0, 1\}$. Then $\boldsymbol{F}(\boldsymbol{G}_0, \boldsymbol{G}_1)$ is P_0. Now, (0) is a truth-assignment for the formula P_0; but (0) is not long enough to be a truth-assignment for $\boldsymbol{G}_1$.

Theorem 2.3.4 (Substitution)**.** *If*

$$\boldsymbol{F}(P_0, \ldots, P_{n-1}) \sim \boldsymbol{G}(P_0, \ldots, P_{n-1}),$$

and $(\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{n-1})$ *is a list of* n *formulas, then*

$$\boldsymbol{F}(\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{n-1}) \sim \boldsymbol{G}(\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{n-1}).$$

Proof. Since $\boldsymbol{F} \sim \boldsymbol{G}$, we have

$$\widehat{\boldsymbol{F}}(\vec{e}) = \widehat{\boldsymbol{G}}(\vec{e}) \tag{2.2}$$

for all truth-assignments $\vec{e}$ for $\boldsymbol{F}$ and $\boldsymbol{G}$. Let $\boldsymbol{F}'$ be $\boldsymbol{F}(\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{n-1})$, and let $\boldsymbol{G}'$ be $\boldsymbol{G}(\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{n-1})$. Suppose $\vec{f}$ is a truth-assignment for the $\boldsymbol{H}_j$, and let $\widehat{\boldsymbol{H}}_j(\vec{f}\,) = e_j$. Then

$$\begin{aligned}
\widehat{\boldsymbol{F}'}(\vec{f}\,) &= \widehat{\boldsymbol{F}}(\vec{e}) && \text{[by Lemma 2.3.2]} \\
&= \widehat{\boldsymbol{G}}(\vec{e}) && \text{[by (2.2)]} \\
&= \widehat{\boldsymbol{G}'}(\vec{f}\,) && \text{[by Lemma 2.3.2].}
\end{aligned}$$

Therefore $\boldsymbol{F}' \sim \boldsymbol{G}'$. This completes the proof.[7] □

Corollary 2.3.5. *A tautology remains a tautology when arbitrary formulas are substituted for the variables.*

Example 2.3.6. Since $\boldsymbol{P} \vee \neg\boldsymbol{P}$ is a tautology, so is $(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \vee \neg(\boldsymbol{P} \Rightarrow \boldsymbol{Q})$.

[6] However, Church [9, § 15, p. 97] proves a version of this lemma by induction.

[7] This is also Burris's proof [6, § 2.3, pp. 46f.], although Burris's use of the fact given in Lemma 2.3.2 is not entirely explicit.

In ordinary language, the words substitution and replacement are nearly synonyms, although there is a distinction. From the expression *abc*, we get *adc* in a way that can be described in two ways:

1. by replacing *b with d*, or
2. by substituting *d for b*.

When doing logic, we shall make another important distinction. If $\boldsymbol{F}$ is a sub-formula of $\boldsymbol{G}$, then we may **replace** $\boldsymbol{F}$ with another formula $\boldsymbol{F'}$. Here, to replace $\boldsymbol{F}$ is to replace a particular *occurrence* of $\boldsymbol{F}$ (since possibly $\boldsymbol{F}$ appears more than once as a sub-formula of $\boldsymbol{G}$).

Example 2.3.7. In $\boldsymbol{P} \vee \neg \boldsymbol{P}$, replacing the second occurrence of $\boldsymbol{P}$ with $\boldsymbol{Q}$ yields $\boldsymbol{P} \vee \neg \boldsymbol{Q}$.

Theorem 2.3.8 (Replacement)**.** *Suppose* $\boldsymbol{F}$ *is a sub-formula of* $\boldsymbol{G}$*, and*

$$\boldsymbol{F} \sim \boldsymbol{F'}.$$

Let $\boldsymbol{G'}$ *be the result of replacing* $\boldsymbol{F}$ *with* $\boldsymbol{F'}$ *in* $\boldsymbol{G}$*. Then*

$$\boldsymbol{G} \sim \boldsymbol{G'}.$$

Proof. Say $\boldsymbol{G}$ is n-ary. Let $\boldsymbol{H}(P_0, \ldots, P_n)$ be the result of replacing $\boldsymbol{F}$ with P_n in $\boldsymbol{G}$. Then $\boldsymbol{G}$ itself is the formula

$$\boldsymbol{H}(P_0, \ldots, P_{n-1}, \boldsymbol{F}),$$

and $\boldsymbol{G'}$ is $\boldsymbol{H}(P_0, \ldots, P_{n-1}, \boldsymbol{F'})$. The remainder of the proof[8] is an exercise involving Lemma 2.3.2. □

Corollary 2.3.9. *A tautology remains a tautology when a sub-formula is replaced with an equivalent sub-formula.*

Example 2.3.10. Since $\vDash (\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \vee \neg(\boldsymbol{P} \Rightarrow \boldsymbol{Q})$ by Example 2.3.6, and

$$\neg(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \sim \boldsymbol{P} \,\&\, \neg \boldsymbol{Q},$$

we have $\vDash (\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \vee (\boldsymbol{P} \,\&\, \neg \boldsymbol{Q})$.

[8] Burris [6, § 2.4, pp. 48ff.] gives an elaborate proof using induction; but I think the work is unnecessary, once one has Lemma 2.3.2. Church's proof [9, § 15, p. 101] leaves details to the reader, but also involves induction. Moreover, Church's proof refers to the principle of unique readability, which Burris seems not to discuss.

The Substitution and Replacement Theorems work together in the following way. From known equivalences, Substitution lets us derive many more. By Replacement, we can use these equivalences to write given formulas in different (but equivalent) form.

That, in short, is the method of simplification, to be developed in § 2.6. Our first example of the procedure will be in § 2.5. Meanwhile, in § 2.4, we shall describe some formulas such that *every* formula is equivalent to one of them. These equivalences can be established by the procedure just described, using the stock of equivalences presented in Lemma 2.2.2.

Exercises

1. If $\boldsymbol{F}(\boldsymbol{P})$ is $\boldsymbol{P} \Rightarrow \boldsymbol{P} \Rightarrow \boldsymbol{P}$, what is $\boldsymbol{F}(\boldsymbol{F}(\boldsymbol{P}))$, written with the fewest possible parentheses?

2. Prove Corollary 2.3.5.

3. Complete the proof of the Replacement Theorem (2.3.8).

4. Prove Corollary 2.3.9.

2.4. Normal forms

We noted in § 1.3 that different arithmetic *terms* may represent the same *polynomial.* Among those terms, there may be a preferred term, which might be called a *normal form* of the polynomial.

Example 2.4.1. The normal form of $(5+x^2-2x)(1+x)-(x-1+2x^2)(x^3+6)$ might be

$$11 - x - 13x^2 + 2x^3 - x^4 - 2x^5,$$

since the latter term is usually easier to work with.

If we have the truth-table of a formula, then we can read off an equivalent formula in so-called *disjunctive normal form.* The general procedure is described immediately, then illustrated by Example 2.4.2.

Suppose we have the truth-table for a formula $\boldsymbol{F}(P_0, \ldots, P_{n-1})$. Say there are m rows in which the entry for $\boldsymbol{F}$ itself is 1. Then $m \leqslant 2^n$. If we ignore the other

rows (namely, those rows in which the entry for $\boldsymbol{F}$ is 0), then what remains has the form

P_0	P_1	$\dots$	P_{n-1}	$\boldsymbol{F}$
e_0^0	e_1^0	$\dots$	e_{n-1}^0	1
e_0^1	e_1^1	$\dots$	e_{n-1}^1	1
$\vdots$	$\vdots$		$\vdots$	$\vdots$
e_0^{m-1}	e_1^{m-1}	$\dots$	e_{n-1}^{m-1}	1

where each e_j^i is in $\mathbb{B}$. If $i < m$ and $j < n$, then let us define P_j^i to be the formula

$$\begin{cases} \neg P_j, & \text{if } e_j^i = 0; \\ P_j, & \text{if } e_j^i = 1. \end{cases}$$

If $i < m$, let $\boldsymbol{G}^i$ be the conjunction

$$P_0^i \,\&\, \cdots \,\&\, P_{n-1}^i.$$

The formulas $\boldsymbol{G}^i$ can be called the **normal disjunctive constituents** of $\boldsymbol{F}$. Their disjunction,

$$\boldsymbol{G}^0 \vee \boldsymbol{G}^1 \vee \cdots \vee \boldsymbol{G}^{m-1},$$

is called a **disjunctive normal form** for $\boldsymbol{F}$. (The other disjunctive normal forms for $\boldsymbol{F}$ are obtained by re-ordering the constituents $\boldsymbol{G}^i$.) It is Theorem 2.4.4 below that every formula is equivalent to its disjunctive normal forms.

Note here that we speak of conjunctions and disjunctions of arbitrarily many formulas. The disjunction of the formulas $\boldsymbol{H}_0, \dots, \boldsymbol{H}_{r-1}$ is

$$\boldsymbol{H}_0 \vee \boldsymbol{H}_1 \vee \cdots \vee \boldsymbol{H}_{r-1},$$

which can also be written as

$$\bigvee_{i<r} \boldsymbol{H}_i. \tag{2.3}$$

If $r = 1$, then this formula is just $\boldsymbol{H}_0$. If $r = 0$, then, by convention,[9] the formula in (2.3) is understood to be 0. In particular, the disjunctive normal form of a contradiction is 0. The conjunction

$$\bigwedge_{i<r} \boldsymbol{H}_i$$

[9] The convention is reasonable: Instead of (2.3), we could write $\bigvee\{\boldsymbol{H}_0, \dots, \boldsymbol{H}_{r-1}\}$; informally, this says that *at least one* of the formulas $\boldsymbol{H}_i$ is true. If $r = 0$, then there are no formulas $\boldsymbol{H}_i$, and in particular there is no such *true* formula, so $\bigvee\{\boldsymbol{H}_0, \dots, \boldsymbol{H}_{r-1}\}$ is false.

is defined analogously, and is 1 if $r = 0$.

Example 2.4.2. Here is the full truth-table of a particular disjunction:

$\neg$	$(P_0$	$\Rightarrow$	$P_1)$	$\vee$	$(P_2$	$\&$	$\neg$	$P_0)$
0	0	1	0	0	0	0	1	0
1	1	0	0	1	0	0	0	1
0	0	1	1	0	0	0	1	0
0	1	1	1	0	0	0	0	1
0	0	1	0	1	1	1	1	0
1	1	0	0	1	1	0	0	1
0	0	1	1	1	1	1	1	0
0	1	1	1	0	1	0	0	1

.

Extract the rows in which the column headed $\vee$ features 1, and take only one each of the columns for P_0, P_1 and P_2:

P_0	P_1	P_2
1	0	0
0	0	1
1	0	1
0	1	1

.

The disjunctive normal form for $\neg(P_0 \Rightarrow P_1) \vee (P_2 \,\&\, \neg P_0)$ is therefore

$$(P_0 \,\&\, \neg P_1 \,\&\, \neg P_2) \vee (\neg P_0 \,\&\, \neg P_1 \,\&\, P_2) \vee (P_0 \,\&\, \neg P_1 \,\&\, P_2) \vee (\neg P_0 \,\&\, P_1 \,\&\, P_2).$$

An n-ary formula is in disjunctive normal form if the formula is precisely

$$\bigvee_{i<m} \bigwedge_{j<n} P_j^i,$$

where each sub-formula P_j^i is either P_j or $\neg P_j$, but all of the constituents $\bigwedge_{j<n} P_j^i$ are distinct. Note especially that each constituent must contain the same variables.

Example 2.4.3. The formula $\neg(P_0 \Rightarrow P_1) \vee (P_2 \,\&\, \neg P_0)$ is equivalent to

$$(P_0 \,\&\, \neg P_1) \vee (\neg P_0 \,\&\, \neg P_1 \,\&\, P_2) \vee (\neg P_0 \,\&\, P_1 \,\&\, P_2),$$

but this is *not* a disjunctive normal form, since one of the constituents does not contain P_2.

Theorem 2.4.4. *Every formula is equivalent to its disjunctive normal forms.*

Proof. Let us use the notation of the definition above, in which $\boldsymbol{F}$ has the DNF $\bigvee_{i<m} \boldsymbol{G}^i$. Write $\boldsymbol{H}$ for the latter formula. Then we have to show $\boldsymbol{F} \sim \boldsymbol{H}$. For the truth-assignment $(e^i_0, \ldots, e^i_{n-1})$, let us write $\vec{e}^{\,i}$. For arbitrary truth-assignments $\vec{f}$ for the $\boldsymbol{G}^i$, we have

$$\widehat{\boldsymbol{G}^i}(\vec{f}\,) = \begin{cases} 1, & \text{if } \vec{f} = \vec{e}^{\,i}; \\ 0, & \text{if } \vec{f} \neq \vec{e}^{\,i}. \end{cases}$$

Then

$$\widehat{\boldsymbol{H}}(\vec{f}\,) = \begin{cases} 1, & \text{if } \vec{f} \in \{\vec{e}^{\,0}, \ldots, \vec{e}^{\,m-1}\}; \\ 0, & \text{if } \vec{f} \notin \{\vec{e}^{\,0}, \ldots, \vec{e}^{\,m-1}\}. \end{cases}$$

Hence $\boldsymbol{H}$ and $\boldsymbol{F}$ have the same truth-table. □

There is also a **conjunctive normal form** or **CNF;** it looks like the disjunctive form, except that the & and the ∨ have switched roles. You read it off from the truth-table again, but you look for 0 (not 1) in the column for the formula, and P^j_i resolves to P_i if there is 0 in the corresponding column and row.

In particular, if a disjunctive form for an n-ary formula has m constituents, then a conjunctive form for the same formula will have $2^n - m$ constituents. Whether it is easier to work with the disjunctive or the conjunctive normal form depends on how big m is.

Example 2.4.5. To obtain the conjunctive normal form of the formula in Example 2.4.2, from its truth-table we extract

P_0	P_1	P_2
0	0	0
0	1	0
1	1	0
1	1	1

,

from which we read off

$$(P_0 \vee P_1 \vee P_2)\,\&\,(P_0 \vee \neg P_1 \vee P_2)\,\&\,(\neg P_0 \vee \neg P_1 \vee P_2)\,\&\,(\neg P_0 \vee \neg P_1 \vee \neg P_2).$$

Theorem 2.4.6. *Every formula is equivalent to its conjunctive normal form.*

If $\boldsymbol{F}$ is a tautology in the variables $P_0, \ldots, P_{n-1}$, then its disjunctive normal form will be the disjunction of the 2^n possible constituents

$$P_0^j \,\&\, \ldots \,\&\, P_{n-1}^j.$$

Suppose in general that we have a method of finding disjunctive normal forms that does not rely on truth-tables. (In § 2.6 we shall describe such a method.) Applying this method to a formula in n variables, if we arrive at a disjunction of 2^n distinct constituents, then the original formula must have been a tautology.

Exercises

1. Find a CNF for $P_0 \Rightarrow P_1 \Rightarrow \cdots \Rightarrow P_n$.

2. Find two formulas $\boldsymbol{F}$ with the truth-table

P_0	P_1	P_2	$\boldsymbol{F}$
0	0	0	1
1	0	0	1
0	1	0	0
1	1	0	0
0	0	1	0
1	0	1	1
0	1	1	0
1	1	1	0

3. Find a DNF for $P_0 \not\Leftrightarrow P_1 \not\Leftrightarrow \cdots \not\Leftrightarrow P_n$.

4. What is the DNF for a tautology in no variables?

5. Find the disjunctive and conjunctive normal forms for:
   (a) $P_0 \Rightarrow P_1 \Rightarrow P_2$;
   (b) $(\neg P_0 \Rightarrow P_1) \,\&\, (\neg P_1 \Rightarrow P_0) \Rightarrow (\neg P_0 \vee \neg P_1)$;
   (c) $P_0 \not\Leftrightarrow P_1 \Leftrightarrow P_2$.

6. Prove Theorem 2.4.6.

7. Show that for any formula $\boldsymbol{F}(P_0, P_1, P_2, P_3)$, either the disjunctive or the conjunctive normal form has no more than 8 constituents.

8. Here is an alternative approach to disjunctive normal forms. Supposing $I \subseteq \{0, \dots, n-1\}$ and $j < n$, let

$$e_j^I = \begin{cases} 1, & \text{if } j \in I, \\ 0, & \text{if } j \notin I. \end{cases}$$

Then let $\vec{e}^{\,I} = (e_0^I, \dots, e_{n-1}^I)$. If $\boldsymbol{F}$ is an n-ary formula, show

$$\boldsymbol{F} \sim \bigvee_{\widehat{\boldsymbol{F}}(\vec{e}^{\,I})=1} \left(\bigwedge_{j \in I} P_i \,\&\, \bigwedge_{\substack{k \notin I \\ k<n}} \neg P_k \right).$$

9. This exercise develops a new kind of normal form.

   A. Supposing $\boldsymbol{F}$ has the DNF $\boldsymbol{G}^0 \vee \dots \vee \boldsymbol{G}^{m-1}$, show

$$\boldsymbol{F} \sim \boldsymbol{G}^0 \nLeftrightarrow \dots \nLeftrightarrow \boldsymbol{G}^{m-1}.$$

   B. For a formula $\boldsymbol{G}^0 \nLeftrightarrow \dots \nLeftrightarrow \boldsymbol{G}^{m-1}$, use also the notation $\sum_{i<m} \boldsymbol{G}^i$. If $I \subseteq \{0, \dots, n-1\}$, show

$$\bigwedge_{j \in I} P_j \,\&\, \bigwedge_{\substack{k \notin I \\ k<n}} \neg P_k \sim \sum_{J \subseteq \{0,\dots,n-1\}} \bigwedge_{k \in J} P_k.$$

   C. Show that every satisfiable n-ary formula is equivalent to a formula

$$\boldsymbol{F}_0 \nLeftrightarrow \boldsymbol{F}_1 \nLeftrightarrow \dots \nLeftrightarrow \boldsymbol{F}_{m-1},$$

   where all of the $\boldsymbol{F}_i$ are distinct, and, for each i in $\{0, 1, \dots, m-1\}$, there is a subset I of $\{0, 1, \dots, n-1\}$ such that $\boldsymbol{F}_i$ is the conjunction $\bigwedge_{j \in I} P_j$.

2.5. Adequacy

In § 2.1, a set of connectives is called a signature. I said in § 1.8 that propositional logic was the study of propositional formulas. I want now to say more precisely that **a propositional logic** is (the study of) the *set* of propositional formulas *of a particular signature*. Then we have been studying the propositional logic of the signature

$$\{\&, \vee, \neg, \Rightarrow, \Leftrightarrow, \nLeftrightarrow, 0, 1\}.$$

However, we have just seen that every formula with a truth-table is equivalent to a formula with the smaller signature $\{\&, \vee, \neg\}$. (If the formula is a contingency, then just take a conjunctive or disjunctive normal form. For a contradiction, take $P_0 \,\&\, \neg P_0$; for a tautology, $P_0 \vee \neg P_0$.)

Another way to say this is that every Boolean polynomial is represented by a formula in $\{\&, \vee, \neg\}$. A technical term for this feature of a signature is **adequacy.** A signature $\mathcal{L}$ is **adequate** if every formula in *every* signature is equivalent to a formula in $\mathcal{L}$. The following is obvious.

Lemma 2.5.1. *If $\mathcal{L}$ is an adequate signature, and $\mathcal{L}'$ is a signature that includes $\mathcal{L}$, then $\mathcal{L}'$ is adequate.*

In short, if a signature is adequate, then so is any *larger* signature.

There are proper subsets of $\{\&, \vee, \neg\}$ that are adequate. The following was proved by Emil Post in 1921.[10]

Theorem 2.5.2. *The signature $\{\vee, \neg\}$ is adequate.*

Proof. Since $\{\&, \neg, \vee\}$ is adequate, it is enough to show that any formula in *this* signature is equivalent to a formula in $\{\&, \neg\}$. Suppose $\boldsymbol{F}$ is in $\{\&, \neg, \vee\}$. Every instance of $\&$ in $\boldsymbol{F}$ determines (as in § 2.1) a sub-formula of $\boldsymbol{F}$ that is a conjunction. Say this conjunction is $\boldsymbol{G} \,\&\, \boldsymbol{H}$, where $\boldsymbol{G}$ and $\boldsymbol{H}$ are sub-formulas of $\boldsymbol{F}$. We have an equivalence

$$\boldsymbol{P} \,\&\, \boldsymbol{Q} \sim \neg(\neg \boldsymbol{P} \vee \neg \boldsymbol{Q})$$

(as can be checked by truth-tables); therefore, by the Substitution Theorem (2.3.4), we have

$$\boldsymbol{G} \,\&\, \boldsymbol{H} \sim \neg(\neg \boldsymbol{G} \vee \neg \boldsymbol{H}).$$

By the Replacement Theorem (2.3.8), in $\boldsymbol{F}$ we can replace $\boldsymbol{G} \,\&\, \boldsymbol{H}$ with $\neg(\neg \boldsymbol{G} \vee \neg \boldsymbol{H})$. In this way, we can remove all instances of $\&$ from $\boldsymbol{F}$, obtaining a formula in $\{\vee, \neg\}$ that is equivalent to $\boldsymbol{F}$. □

Similarly, we have:

Theorem 2.5.3. *The signature $\{\&, \neg\}$ is adequate.*

Corollary 2.5.4. *The signature $\{\&, \nLeftrightarrow, 1\}$ is adequate.*

[10] Post's method is different from ours; see his article [39, pp. 167 f.].

Proof. The signature $\{\&, \neg\}$ is adequate, but the connective $\neg$ can be expressed in terms of $\nLeftrightarrow$ and 1, since

$$\neg \boldsymbol{P} \sim 1 \nLeftrightarrow \boldsymbol{P}$$

by § 2.2, Exercise (4a); so $\{\&, \nLeftrightarrow, 1\}$ is adequate. □

The proofs of the last three numbered propositions are examples of a general method for proving adequacy of a signature $\mathcal{L}$: Take a signature $\mathcal{L}'$ that is known to be adequate, and show that every connective in $\mathcal{L}'$ can be expressed with the connectives of $\mathcal{L}$. Note well the two ingredients of the argument:

1. $\mathcal{L}'$ is known to be adequate.
2. The elements of $\mathcal{L}'$ can be expressed in terms of $\mathcal{L}$.

Although students sometimes do it anyway, it would be useless to observe in this context that the elements of $\mathcal{L}$ can be expressed in terms of $\mathcal{L}'$. Remember that this observation is immediate if $\mathcal{L} \subseteq \mathcal{L}'$; then surely the adequacy of $\mathcal{L}'$ says nothing about the adequacy of $\mathcal{L}$.

For another example, let $\curlywedge$ be the **Schröder connective;**[11] this is defined so that

$$\boldsymbol{P} \curlywedge \boldsymbol{Q} \sim \neg \boldsymbol{P} \,\&\, \neg \boldsymbol{Q}.$$

So $\curlywedge$ is defined in terms of $\&$ and $\neg$. This fact by itself tells us *nothing* about the adequacy of $\{\curlywedge\}$; it has no relevance to the proof of the following:

Theorem 2.5.5. *The signature* $\{\curlywedge\}$ *is adequate.*

Proof. It is enough to write $\neg \boldsymbol{P}$ and $\boldsymbol{P} \& \boldsymbol{Q}$ using only $\curlywedge$. We have $\neg \boldsymbol{P} \sim \boldsymbol{P} \curlywedge \boldsymbol{P}$, and also

$$\begin{aligned} \boldsymbol{P} \,\&\, \boldsymbol{Q} &\sim (\neg \boldsymbol{P}) \curlywedge (\neg \boldsymbol{Q}) \\ &\sim (\boldsymbol{P} \curlywedge \boldsymbol{P}) \curlywedge (\boldsymbol{Q} \curlywedge \boldsymbol{Q}). \end{aligned}$$

Hence all formulas in the adequate signature $\{\&, \neg\}$ can be written in terms of $\curlywedge$. Thus $\{\curlywedge\}$ is adequate. □

Adequate n-ary connectives where $n > 2$ can also be found (this is an exercise).

How might we show that a certain signature is *not* adequate? Note that the signature $\{\&, \neg\}$ is adequate, even though it contains no nullary connectives: the two constant Boolean polynomials are represented in $\{\&, \neg\}$ by $\boldsymbol{P} \,\&\, \neg \boldsymbol{P}$ and $\neg(\boldsymbol{P} \,\&\, \neg \boldsymbol{P})$ respectively.

[11] According to Burris [6, § 2.5.2, p. 53], Schröder showed in 1880 that the 'standard connectives'—say, the ones we have been using so far—can be expressed using this connective. Post's later result—our Theorem 2.5.2—then establishes the adequacy of $\{\curlywedge\}$.

Theorem 2.5.6. *The signature* $\{\&, \not\Leftrightarrow\}$ *is* not *adequate.*

Proof. We shall show that no formula in $\{\&, \not\Leftrightarrow\}$ represents 1. Now, if

$$\boldsymbol{F}(P_0, P_1, P_2, \ldots, P_n) \sim 1,$$

then $\boldsymbol{F}(P_0, P_0, P_0, \ldots, P_0) \sim 1$ by the Substitution Theorem. Hence it is enough to show that no *singulary* formula in $\{\&, \not\Leftrightarrow\}$ represents 1. In $\{\&, \not\Leftrightarrow\}$, we can represent 0 by $\boldsymbol{P} \not\Leftrightarrow \boldsymbol{P}$. We also have

$$\begin{aligned} 0 \,\&\, 0 &\sim 0, & 0 \not\Leftrightarrow 0 &\sim 0, \\ 0 \,\&\, \boldsymbol{P} &\sim 0, & 0 \not\Leftrightarrow \boldsymbol{P} &\sim \boldsymbol{P}, \\ \boldsymbol{P} \,\&\, 0 &\sim 0, & \boldsymbol{P} \not\Leftrightarrow 0 &\sim \boldsymbol{P}, \\ \boldsymbol{P} \,\&\, \boldsymbol{P} &\sim \boldsymbol{P}, & \boldsymbol{P} \not\Leftrightarrow \boldsymbol{P} &\sim 0. \end{aligned}$$

By the Replacement Theorem, we can create no singulary formula in $\{\&, \not\Leftrightarrow\}$ that is *not* equivalent to 0 or a variable. □

Exercises

1. Prove Theorem 2.5.3.
2. Prove that $\{\neg, \Rightarrow\}$ is adequate.
3. Prove that $\neg$ by itself is *not* adequate.
4. Prove the adequacy of the **Sheffer stroke,** namely the connective $|$ such that $\boldsymbol{P} \mid \boldsymbol{Q} \sim \neg\,(\boldsymbol{P} \,\&\, \boldsymbol{Q})$.
5. Find an adequate ternary (3-ary) connective. (See § 2.1, Exercise 4.)

2.6. Simplification

In proving Theorem 2.5.2, we used a known equivalence, and the Theorems of Substitution and Replacement, to 'simplify' a formula in the sense of eliminating instances of disjunction. In the same way, we can simplify any formula to disjunctive normal form. The procedure relies on Lemma 2.2.2. Using this lemma, given any formula, we can:

1) eliminate instances of $\Rightarrow$, $\Leftrightarrow$, and $\not\Leftrightarrow$;
2) eliminate multiple negations, and make sure that the only arguments of $\neg$ are variables;

3) eliminate conjunctions of disjunctions;
4) eliminate redundancies; now the formula is a disjunction of conjunctions of variables and negated variables, so we can finally:
5) add variables as necessary to obtain a disjunctive normal form.

Example 2.6.1. Suppose $\boldsymbol{F}$ is the formula $\neg(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \vee \boldsymbol{Q}$. The reduction of $\boldsymbol{F}$ to disjunctive normal form can proceed as follows:

$$\begin{aligned}
\boldsymbol{F} &\sim \neg(\neg\boldsymbol{P} \vee \boldsymbol{Q}) \vee \boldsymbol{Q} && \text{[def'n of } \Rightarrow\text{]}\\
&\sim (\neg\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \vee \boldsymbol{Q} && \text{[De Morgan]}\\
&\sim (\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \vee \boldsymbol{Q} && \text{[double negation]}\\
&\sim (\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \vee (\boldsymbol{Q} \,\&\, \boldsymbol{P}) \vee (\boldsymbol{Q} \,\&\, \neg\boldsymbol{P}) && \text{[new variable]}\\
&\sim (\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \vee (\boldsymbol{P} \,\&\, \boldsymbol{Q}) \vee (\neg\boldsymbol{P} \,\&\, \boldsymbol{Q}) && \text{[commutativity]}
\end{aligned}$$

There may be more than one way to proceed:

Example 2.6.2. Let $\boldsymbol{F}$ be $\neg(\neg\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P})$. Then

$$\begin{aligned}
\boldsymbol{F} &\sim \neg(\neg\neg\boldsymbol{P} \vee \boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P}) && \text{[def'n of } \Rightarrow\text{]}\\
&\sim \neg(\boldsymbol{P} \vee \boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P}) && \text{[double neg.]}\\
&\sim (\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P}) && \text{[De Morgan]}\\
&\sim ((\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \,\&\, \boldsymbol{Q}) \vee ((\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \,\&\, \neg\boldsymbol{P}) && \text{[dist.]}\\
&\sim (\neg\boldsymbol{P} \,\&\, (\neg\boldsymbol{Q} \,\&\, \boldsymbol{Q})) \vee (\neg\boldsymbol{P} \,\&\, (\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q})) && \text{[assoc.; comm.]}\\
&\sim (\neg\boldsymbol{P} \,\&\, 0) \vee ((\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{P}) \,\&\, \neg\boldsymbol{Q}) && \text{[red.; assoc.]}\\
&\sim 0 \vee (\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) && \text{[red.]}\\
&\sim \neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q} && \text{[red.]}
\end{aligned}$$

Alternatively,

$$\begin{aligned}
\boldsymbol{F} &\sim \neg(\boldsymbol{P} \vee \boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P}) && \text{[def'n of } \Rightarrow\text{; double neg.]}\\
&\sim (\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P}) && \text{[De Morgan]}\\
&\sim \neg\boldsymbol{P} \,\&\, (\neg\boldsymbol{Q} \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{P})) && \text{[assoc.]}\\
&\sim \neg\boldsymbol{P} \,\&\, ((\neg\boldsymbol{Q} \,\&\, \boldsymbol{Q}) \vee (\neg\boldsymbol{Q} \,\&\, \neg\boldsymbol{P})) && \text{[dist.]}\\
&\sim \neg\boldsymbol{P} \,\&\, (0 \vee (\neg\boldsymbol{Q} \,\&\, \neg\boldsymbol{P})) && \text{[red.]}\\
&\sim \neg\boldsymbol{P} \,\&\, (\neg\boldsymbol{Q} \,\&\, \neg\boldsymbol{P}) && \text{[red.]}\\
&\sim (\neg\boldsymbol{P} \,\&\, \neg\boldsymbol{P}) \,\&\, \neg\boldsymbol{Q} && \text{[comm; assoc]}\\
&\sim \neg\boldsymbol{P} \,\&\, \neg\boldsymbol{Q} && \text{[red.]}
\end{aligned}$$

Lemma 2.6.3 (Absorption Laws)**.**

$$\boldsymbol{P} \,\&\, (\boldsymbol{P} \vee \boldsymbol{Q}) \sim \boldsymbol{P}, \qquad \boldsymbol{P} \vee (\boldsymbol{P} \,\&\, \boldsymbol{Q}) \sim \boldsymbol{P}.$$

If two formulas $\boldsymbol{F}$ and $\boldsymbol{G}$ are equivalent, then we can use simplification to show this as follows.

1. Simplify $\boldsymbol{F}$ to a disjunctive normal form $\boldsymbol{F}'$.
2. Simplify $\boldsymbol{G}$ to a disjunctive normal form $\boldsymbol{G}'$.
3. Note that $\boldsymbol{F}' \sim \boldsymbol{G}'$. (They should be the same formula, except possibly in the order of the constituents.)

However, it may be easier to simplify directly from one formula to the other, or to use *conjunctive* normal forms.

Example 2.6.4. The formulas $P_0 \Rightarrow P_1 \Rightarrow P_2$ and $P_1 \Rightarrow P_0 \Rightarrow P_2$ are equivalent, because

$$\begin{aligned} P_0 \Rightarrow P_1 \Rightarrow P_2 &\sim \neg P_0 \vee (P_1 \Rightarrow P_2) && [\text{def'n of } \Rightarrow] \\ &\sim \neg P_0 \vee \neg P_1 \vee P_2 && [\text{def'n of } \Rightarrow] \\ &\sim \neg P_1 \vee \neg P_0 \vee P_2 && [\text{comm.}] \\ &\sim \neg P_1 \vee (P_0 \Rightarrow P_2) && [\text{def'n of } \Rightarrow] \\ &\sim P_1 \Rightarrow P_0 \Rightarrow P_2. && [\text{def'n of } \Rightarrow] \end{aligned}$$

(Associativity was used silently.) The reduction of each formula to disjunctive normal form would be tedious, since that normal form is

$$\begin{aligned} &(\neg P_0 \,\&\, \neg P_1 \,\&\, \neg P_2) \vee (P_0 \,\&\, \neg P_1 \,\&\, \neg P_2) \vee (\neg P_0 \,\&\, P_1 \,\&\, \neg P_2) \vee \\ &\vee (\neg P_0 \,\&\, \neg P_1 \,\&\, P_2) \vee (P_0 \,\&\, \neg P_1 \,\&\, P_2) \vee (\neg P_0 \,\&\, P_1 \,\&\, P_2) \vee (P_0 \,\&\, P_1 \,\&\, P_2); \end{aligned}$$

but the conjunctive normal form is just the formula $\neg P_0 \vee \neg P_1 \vee P_2$, found in the original simplification.

Exercises

1. Given a formula in normal form, how would you write down its truth-table?
2. Prove the Absorption Laws (2.6.3) using simplification.
3. Use simplification to prove the following equivalences:
   a) $\neg(\boldsymbol{P} \,\&\, \boldsymbol{Q}) \vee \boldsymbol{R} \sim \boldsymbol{P} \,\&\, \boldsymbol{Q} \Rightarrow \boldsymbol{R}$;

b) $(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \,\&\, (\boldsymbol{R} \Rightarrow \boldsymbol{Q}) \,\&\, \neg\boldsymbol{Q} \Rightarrow \neg(\boldsymbol{P} \vee \boldsymbol{R}) \sim 1$;

c) $\boldsymbol{P} \Rightarrow (\boldsymbol{Q} \Rightarrow \boldsymbol{R}) \sim \boldsymbol{P} \Rightarrow \boldsymbol{Q} \Rightarrow (\boldsymbol{P} \Rightarrow \boldsymbol{R})$;

d) $(\boldsymbol{P} \vee \boldsymbol{R}) \,\&\, (\boldsymbol{Q} \vee \neg\boldsymbol{R}) \sim (\boldsymbol{P} \,\&\, \neg\boldsymbol{R}) \vee (\boldsymbol{Q} \,\&\, \boldsymbol{R})$;

e) $(\boldsymbol{P}_0 \vee \boldsymbol{P}_1) \,\&\, (\boldsymbol{Q}_0 \vee \boldsymbol{Q}_1) \sim \bigvee_{i<2} \bigvee_{j<2} (\boldsymbol{P}_i \,\&\, \boldsymbol{Q}_j)$.

4. For $(\neg P_0 \Rightarrow P_1) \,\&\, (\neg P_1 \Rightarrow P_0) \Rightarrow (\neg P_0 \vee \neg P_1)$, find the disjunctive normal form using simplification.

5. Use simplification to verify the equivalences listed in § 2.2, Exercise 4.

6. Use simplification to establish $\boldsymbol{P} \Leftrightarrow \boldsymbol{Q} \sim \boldsymbol{P} \not\Leftrightarrow \neg\boldsymbol{Q}$.

2.7. Logical entailment

Simplification is a way to prove that two formulas are logically equivalent. There are other relations between formulas that we may want to prove. If $\boldsymbol{F}$ is an n-ary formula such that $\widehat{\boldsymbol{F}}(\vec{e})$ for all truth-assignments $\vec{e}$, then as in § 2.2 we write

$$\vDash \boldsymbol{F}.$$

Suppose $(\boldsymbol{F}_0, \ldots, \boldsymbol{F}_m)$ is a list of $m+1$ formulas, each of them n-ary, such that, for all n-ary truth-assignments $\vec{e}$, if $\widehat{\boldsymbol{F}}_i(\vec{e}) = 1$ for each i in $\{0, \ldots, m-1\}$, then $\widehat{\boldsymbol{F}}_m(\vec{e}) = 1$. Then we say that $\boldsymbol{F}_m$ is a **logical consequence** of $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$, or $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$ **logically entails** $\boldsymbol{F}_m$, and we write

$$\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m;$$

if the set $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$ is denoted by Σ, then we can also write

$$\Sigma \vDash \boldsymbol{F}_m.$$

Logical entailment can in principle be established by truth-tables. However, this method is practical only when the numbers of variables and formulas are low.

Examples 2.7.1. 1. $\boldsymbol{P} \vDash \boldsymbol{P} \vee \boldsymbol{Q}$ because the table

$\boldsymbol{P}$	$\vee$	$\boldsymbol{Q}$
0	0	0
1	1	0
0	1	1
1	1	1

shows $\boldsymbol{P} \vee \boldsymbol{Q}$ is true whenever $\boldsymbol{P}$ is true. (It is irrelevant that $\boldsymbol{P} \vee \boldsymbol{Q}$ can be true when $\boldsymbol{P}$ is false.)

2. Similarly $\boldsymbol{P}, \boldsymbol{Q} \vDash \boldsymbol{P} \,\&\, \boldsymbol{Q}$.

3. $\boldsymbol{P} \vee \boldsymbol{Q},\ \boldsymbol{Q} \Rightarrow \boldsymbol{R} \vDash \boldsymbol{P} \vee \boldsymbol{R}$ by consideration of the starred rows in the table:

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{R}$	$\boldsymbol{P} \vee \boldsymbol{Q}$	$\boldsymbol{Q} \Rightarrow \boldsymbol{R}$	$\boldsymbol{P} \vee \boldsymbol{R}$	
0	0	0	0	1	0	
1	0	0	1	1	1	*
0	1	0	1	0	0	
1	1	0	1	0	1	
0	0	1	0	1	1	
1	0	1	1	1	1	*
0	1	1	1	1	1	*
1	1	1	1	1	1	*

There are alternative methods for establishing logical entailment. The following should be compared with Lemma 2.5.1.

Lemma 2.7.2. *If $\Sigma \vDash \boldsymbol{F}$, and $\Sigma \subseteq \Sigma'$, then $\Sigma' \vDash \boldsymbol{F}$.*

Proof. If $\Sigma \vDash \boldsymbol{F}$, and $\Sigma \subseteq \Sigma'$, and $\vec{e}$ is a truth-assignment under which every formula in Σ' is true, then every formula in Σ is true under $\vec{e}$, so $\widehat{\boldsymbol{F}}(\vec{e}) = 1$. This means $\Sigma' \vDash \boldsymbol{F}$. □

Corresponding to Theorem 2.3.4, we have

Theorem 2.7.3 (Substitution)**.** *If $(\boldsymbol{F}_0, \ldots, \boldsymbol{F}_m)$ is a list of n-ary formulas such that*

$$\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m,$$

and $(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$ is a list of n formulas, then

$$\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{m-1} \vDash \boldsymbol{H}_m,$$

where $\boldsymbol{H}_i$ is $\boldsymbol{F}_i(\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{n-1})$ for each i in $\{0, \ldots, m\}$.

Proof. Say $\vec{e}$ is a truth-assignment for the $\boldsymbol{G}_j$ such that $\widehat{\boldsymbol{H}}_i(\vec{e}) = 1$ when $i < m$. Let $f_j = \widehat{\boldsymbol{G}}_i(\vec{e})$ when $j < n$. Then $\widehat{\boldsymbol{F}}_i(\vec{f}) = 1$ when $i < m$, by the associativity of substitution (Lemma 2.3.2). Hence also $\widehat{\boldsymbol{H}}_m(\vec{e}) = \widehat{\boldsymbol{F}}_m(\vec{f}) = 1$ (since $\boldsymbol{F}_m$ is a logical consequence of $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$). Therefore $\boldsymbol{H}_0, \ldots, \boldsymbol{H}_{m-1} \vDash \boldsymbol{H}_m$. □

The following is immediate from the definitions.

Theorem 2.7.4. *If* $\boldsymbol{F} \sim \boldsymbol{G}$*, then* $\boldsymbol{F} \vDash \boldsymbol{G}$*.*

Theorem 2.7.5 (Transitivity)**.** *If* Σ *and* Π *are finite sets of formulas, and* $\Sigma \vDash \boldsymbol{F}$ *for every* $\boldsymbol{F}$ *in* Π*, and* $\Pi \vDash \boldsymbol{G}$*, then* $\Sigma \vDash \boldsymbol{G}$*.*

Proof. Under the given assumptions, suppose also that every formula in Σ is true under $\vec{e}$. Then every formula in Π is true under $\vec{e}$, so $\widehat{\boldsymbol{G}}(\vec{e}) = 1$. Thus $\Sigma \vDash \boldsymbol{G}$. □

Example 2.7.6. Since $\boldsymbol{P} \vee \boldsymbol{Q},\ \boldsymbol{Q} \Rightarrow \boldsymbol{R} \vDash \boldsymbol{P} \vee \boldsymbol{R}$ as in the last example, and $\boldsymbol{Q} \Rightarrow \boldsymbol{R} \sim \neg\boldsymbol{Q} \vee \boldsymbol{R}$, we have

$$\boldsymbol{P} \vee \boldsymbol{Q},\ \neg\boldsymbol{Q} \vee \boldsymbol{R} \vDash \boldsymbol{P} \vee \boldsymbol{R}$$

by the last two theorems, hence $\boldsymbol{F} \vee \boldsymbol{G}, \neg\boldsymbol{G} \vee \boldsymbol{H} \vDash \boldsymbol{F} \vee \boldsymbol{H}$ by substitution.

A number of rules for establishing logical entailments correspond to some standard forms of argument in mathematical proofs.

Lemma 2.7.7.

1. ***Contradiction:*** *If* $\Sigma \cup \{\neg\boldsymbol{F}\} \vDash \boldsymbol{G}$ *and* $\Sigma \cup \{\neg\boldsymbol{F}\} \vDash \neg\boldsymbol{G}$*, then*
$$\Sigma \vDash \boldsymbol{F}.$$
2. ***Contraposition:*** *If* $\Sigma \cup \{\neg\boldsymbol{F}\} \vDash \neg\boldsymbol{G}$*, then*
$$\Sigma \cup \{\boldsymbol{G}\} \vDash \boldsymbol{F}.$$
3. ***Deduction:*** *If* $\Sigma \cup \{\boldsymbol{F}\} \vDash \boldsymbol{G}$*, then*
$$\Sigma \vDash \boldsymbol{F} \Rightarrow \boldsymbol{G}.$$

Lemma 2.7.8.

1. ***Detachment:***[12]
$$\boldsymbol{F},\ \boldsymbol{F} \Rightarrow \boldsymbol{G} \vDash \boldsymbol{G}, \qquad \boldsymbol{F} \Rightarrow \boldsymbol{G},\ \neg\boldsymbol{G} \vDash \neg\boldsymbol{F}.$$
2. ***Simplification:***
$$\boldsymbol{P} \,\&\, \boldsymbol{Q} \vDash \boldsymbol{Q}.$$

[12] These rules also have the Latin names ***Modus Ponens*** (method of affirming) and ***Modus Tollens*** (method of denying).

3. ***Cases:***

$$\boldsymbol{P} \Rightarrow \boldsymbol{Q}_0 \vee \cdots \vee \boldsymbol{Q}_n,\ \boldsymbol{Q}_0 \Rightarrow \boldsymbol{R},\ \ldots,\ \boldsymbol{Q}_m \Rightarrow \boldsymbol{R} \vDash \boldsymbol{P} \Rightarrow \boldsymbol{R}.$$

4. ***Addition:***

$$\boldsymbol{P} \vDash \boldsymbol{P} \vee \boldsymbol{Q}, \qquad \boldsymbol{P} \vDash \boldsymbol{Q} \vee \boldsymbol{P}.$$

5. ***Hypothetical Syllogism:***[13]

$$\boldsymbol{P} \Rightarrow \boldsymbol{Q},\ \boldsymbol{Q} \Rightarrow \boldsymbol{R} \vDash \boldsymbol{P} \Rightarrow \boldsymbol{R}. \tag{2.4}$$

6. ***Disjunctive Syllogism:***

$$\boldsymbol{P} \vee \boldsymbol{Q},\ \neg\boldsymbol{P} \vDash \boldsymbol{Q}, \qquad \boldsymbol{P} \vee \boldsymbol{Q},\ \neg\boldsymbol{Q} \vDash \boldsymbol{P}.$$

7. ***Constructive Dilemma:***

$$\boldsymbol{P}_0 \Rightarrow \boldsymbol{Q}_0,\ \boldsymbol{P}_1 \Rightarrow \boldsymbol{Q}_1,\ \boldsymbol{P}_0 \vee \boldsymbol{P}_1 \vDash \boldsymbol{Q}_0 \vee \boldsymbol{Q}_1.$$

Proof. To prove Detachment, is enough to show $P_0,\ P_0 \Rightarrow P_1 \vDash P_1$, by the preceding Substitution Theorem. The truth-table

P_0	P_0	$\Rightarrow$	P_1	P_1
0	0	1	0	0
1	1	0	0	0
0	0	1	1	1
1	1	1	1	1

shows that $(1, 1)$ is the only truth-assignment where both P_0 and $P_0 \Rightarrow P_1$ are true. Under this assignment, P_1 is true. □

Exercises

1. Show that $\boldsymbol{F}_0,\ \ldots,\ \boldsymbol{F}_{m-1} \vDash \boldsymbol{G}$ if and only if $\bigwedge_{k<m} \boldsymbol{F}_k \vDash \boldsymbol{G}$.
2. Show that $\boldsymbol{P} \Rightarrow \boldsymbol{Q},\ \boldsymbol{R} \Rightarrow \boldsymbol{Q},\ \neg\boldsymbol{Q} \vDash \neg(\boldsymbol{P} \vee \boldsymbol{R})$.
3. Prove Lemma 2.7.7.
4. Prove Lemma 2.7.8.
5. Prove the following:
   (a) $\boldsymbol{P} \Leftrightarrow \boldsymbol{Q},\ \boldsymbol{Q} \Leftrightarrow \boldsymbol{R} \vDash \boldsymbol{P} \Leftrightarrow \boldsymbol{R}$;
   (b) $\boldsymbol{P} \not\Leftrightarrow \boldsymbol{Q},\ \boldsymbol{Q} \not\Leftrightarrow \boldsymbol{R} \vDash \boldsymbol{P} \Leftrightarrow \boldsymbol{R}$.

[13] A **syllogism** is a classical form of argument; Aristotle's definition is quoted in Appendix A.

2.8. Formal proofs

For a given propositional logic, a **proof-system** consists of:

1) certain distinguished formulas, called **axioms;**
2) **rules of inference**, which are clearly described ways of obtaining new formulas from finitely many given formulas.

One can think of an axiom $\boldsymbol{F}$ as the rule of inference that allows $\boldsymbol{F}$ to be obtained from *no* given formulas.

Suppose $\mathcal{N}$ is a proof-system, and Σ is a set $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$ of formulas. In $\mathcal{N}$, a **deduction** or **formal proof** of a formula $\boldsymbol{F}_m$ from Σ is a finite sequence

$$\boldsymbol{G}_0, \ldots, \boldsymbol{G}_\ell,$$

where $\boldsymbol{G}_\ell$ is $\boldsymbol{F}_m$ and, for each k in $\{0, \ldots, \ell\}$, the formula $\boldsymbol{G}_k$ is:

1) an axiom of $\mathcal{N}$, or
2) one of the formulas $\boldsymbol{F}_i$, where $i < m$, or
3) a formula obtainable from (some of) the formulas in $\{\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{k-1}\}$ by one of the rules of inference of $\mathcal{N}$.

If there is such a deduction, then we may write one of

$$\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vdash_{\mathcal{N}} \boldsymbol{F}_m, \qquad\qquad \Sigma \vdash_{\mathcal{N}} \boldsymbol{F}_m,$$

and we say that $\boldsymbol{F}_m$ is **derivable** or **formally provable** in $\mathcal{N}$ from Σ, or that Σ **formally entails** $\boldsymbol{F}_m$ in $\mathcal{N}$. In this case, Σ is a set of **hypotheses** from which $\boldsymbol{F}_m$ can be derived. In case $m = 0$, we write

$$\vdash_{\mathcal{N}} \boldsymbol{F}_0$$

and say that $\boldsymbol{F}_0$ is a **validity** of $\mathcal{N}$ or a **theorem** of $\mathcal{N}$. Here $\vdash$ is the **syntactic turnstile.** We may drop the subscript $\mathcal{N}$ on $\vdash$ if the identity of $\mathcal{N}$ is clear.

Many proof-systems are possible. Some are more useful than others. As a minimum requirement, we should like a proof-system $\mathcal{N}$ to be

1) **sound:**
$$\Sigma \vdash_{\mathcal{N}} \boldsymbol{G} \implies \Sigma \vDash \boldsymbol{G};$$
2) **complete:**
$$\Sigma \vDash \boldsymbol{G} \implies \Sigma \vdash_{\mathcal{N}} \boldsymbol{G}.$$

The remainder of this section establishes two such systems.

The system of detachment

Let $\mathcal{D}$ be the proof-system in which

1) the axioms are just the tautologies;
2) the rules of inference are two:
   a) if the formula $\boldsymbol{F}$ is given, and $\boldsymbol{F} \sim \boldsymbol{G}$, then $\boldsymbol{G}$ may be obtained;
   b) **Detachment:**[14] if the formulas $\boldsymbol{F}$ and $\boldsymbol{F} \Rightarrow \boldsymbol{G}$ are given, then the formula $\boldsymbol{G}$ may be obtained.

Example 2.8.1. $\boldsymbol{F} \,\&\, \boldsymbol{G} \vdash_{\mathcal{D}} \boldsymbol{G}$, because the following is a deduction in $\mathcal{D}$ of $\boldsymbol{G}$ from $\boldsymbol{F} \,\&\, \boldsymbol{G}$:

(0)	$\boldsymbol{F} \,\&\, \boldsymbol{G}$	[hyp.]
(1)	1	[taut.]
(2)	$\neg \boldsymbol{F} \vee 1$	[red.]
(3)	$\neg \boldsymbol{F} \vee \neg \boldsymbol{G} \vee \boldsymbol{G}$	[red.]
(4)	$\neg(\boldsymbol{F} \,\&\, \boldsymbol{G}) \vee \boldsymbol{G}$	[De Morgan]
(5)	$(\boldsymbol{F} \,\&\, \boldsymbol{G}) \Rightarrow \boldsymbol{G}$	[def'n of $\Rightarrow$]
(6)	$\boldsymbol{G}$	[Detachment, lines 0 & 5]

Strictly, the deduction itself is just the list

$$\boldsymbol{F} \,\&\, \boldsymbol{G},\ 1,\ \neg \boldsymbol{F} \vee 1,\ \neg \boldsymbol{F} \vee \neg \boldsymbol{G} \vee \boldsymbol{G},\ \neg(\boldsymbol{F} \,\&\, \boldsymbol{G}) \vee \boldsymbol{G},\ (\boldsymbol{F} \,\&\, \boldsymbol{G}) \Rightarrow \boldsymbol{G},\ \boldsymbol{G}$$

of formulas. In fact, there is a shorter deduction of $\boldsymbol{F}$ from $\boldsymbol{F} \,\&\, \boldsymbol{G}$, namely

$$\boldsymbol{F} \,\&\, \boldsymbol{G},\ \boldsymbol{F} \,\&\, \boldsymbol{G} \Rightarrow \boldsymbol{G},\ \boldsymbol{G}.$$

However, *recognizing* this as a deduction requires, in part, recognizing that $\boldsymbol{F} \,\&\, \boldsymbol{G} \Rightarrow \boldsymbol{G}$ is a tautology.

Theorem 2.8.2. *The proof-system $\mathcal{D}$ is sound and complete.*

Proof. We shall prove the following circle of implications:

$$\begin{array}{ccc} (\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m) & \Longrightarrow & (\vDash \boldsymbol{F}_0 \Rightarrow \boldsymbol{F}_1 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m) \\ \Uparrow & & \Downarrow \\ (\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vdash_{\mathcal{D}} \boldsymbol{F}_m) & \Longleftarrow & (\vdash_{\mathcal{D}} \boldsymbol{F}_0 \Rightarrow \boldsymbol{F}_1 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m) \end{array}$$

[14] Or ***Modus Ponens.***

Suppose $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m$. Then for every truth-assignment $\vec{e}$ for the $\boldsymbol{F}_i$, either $\widehat{\boldsymbol{F}}_m(\vec{e}) = 1$, or $\widehat{\boldsymbol{F}}_i(\vec{e}) = 0$ for some i in $\{0, \ldots, m-1\}$. If $\widehat{\boldsymbol{F}}_i(\vec{e}) = 0$ and $i < m$, then $\boldsymbol{F}_i \Rightarrow \boldsymbol{F}_{i+1} \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$ is true at $\vec{e}$, and hence so is $\boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$. For the same reason, if $\widehat{\boldsymbol{F}}_m(\vec{e}) = 1$, then $\boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$ is true at $\vec{e}$. Hence $\vDash \boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$.

Suppose $\vDash \boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$. Then, since it is a tautology, the formula $\boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$ is its own proof of itself. Hence $\vdash_{\mathcal{D}} \boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$.

Suppose $\vdash_{\mathcal{D}} \boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$. Let $\boldsymbol{G}_0, \ldots, \boldsymbol{G}_\ell$ be a deduction of $\boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$. Then we have the following deduction of $\boldsymbol{F}_m$ from $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$.

(0)	$\boldsymbol{G}_0$	
$\ldots$	$\ldots$	
$(\ell - 1)$	$\boldsymbol{G}_{\ell-1}$	
(ℓ)	$\boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$	
$(\ell + 1)$	$\boldsymbol{F}_0$	[hyp.]
$(\ell + 2)$	$\boldsymbol{F}_1 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$	[Detachment]
$(\ell + 3)$	$\boldsymbol{F}_1$	[hyp.]
$(\ell + 4)$	$\boldsymbol{F}_2 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$	[Detachment]
$\ldots$	$\ldots$	
$(\ell + 2m - 2)$	$\boldsymbol{F}_{m-1} \Rightarrow \boldsymbol{F}_m$	[Detachment]
$(\ell + 2m - 1)$	$\boldsymbol{F}_{m-1}$	[hyp.]
$(\ell + 2m)$	$\boldsymbol{F}_m$	[Detachment]

Thus $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vdash_{\mathcal{D}} \boldsymbol{F}_m$.

Suppose finally $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vdash_{\mathcal{D}} \boldsymbol{F}_m$. We use the method of infinite descent. Let $\boldsymbol{G}_0, \ldots, \boldsymbol{G}_{\ell-1}, \boldsymbol{F}_m$ be a deduction of $\boldsymbol{F}_m$ from $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$. Let $\vec{e}$ be a truth-assignment such that $\widehat{\boldsymbol{F}}_i(\vec{e}) = 1$ whenever $i < m$. Suppose if possible that $\widehat{\boldsymbol{F}}_m(\vec{e}) = 0$. Then $\boldsymbol{F}_m$ is not in $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$, nor is $\boldsymbol{F}_m$ a tautology. Hence, by the definition of a deduction, either $\boldsymbol{F}_m \sim \boldsymbol{G}_i$ for some i in $\{0, \ldots, \ell - 1\}$, or there are i and j in $\{0, \ldots, \ell - 1\}$ such that $\boldsymbol{G}_j$ is $\boldsymbol{G}_i \Rightarrow \boldsymbol{F}_m$. In the first case, $\boldsymbol{G}_i$ is false at $\vec{e}$; in the second case, either $\boldsymbol{G}_i$ or $\boldsymbol{G}_j$ is false at $\vec{e}$. In either case, $\widehat{\boldsymbol{G}}_k(\vec{e}) = 0$ for some k in $\{0, \ldots, \ell - 1\}$. But $\boldsymbol{G}_0, \ldots, \boldsymbol{G}_k$ is still a deduction from $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1}\}$, strictly shorter then the original one, but with the same property (namely that its last formula is false at $\vec{e}$). We cannot take shorter deductions indefinitely. Hence $\widehat{\boldsymbol{F}}_m(\vec{e}) = 1$. Therefore $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m$. □

The system $\mathcal{D}$ can be simplified, at the cost of requiring longer deductions:

Corollary 2.8.3. *That proof-system is sound and complete which has only* 1 *as an axiom, and which has, as rules of inference,*

(1) Deduction,
(2) From $\boldsymbol{F}$*, obtain* $\boldsymbol{G}$*, if* $\boldsymbol{F} \sim \boldsymbol{G}$ *or* $\boldsymbol{G} \sim \boldsymbol{F}$ *directly by Lemma 2.2.2 and Substitution (2.3.4).*

Łukasiewicz's proof system

Here is developed the proof-system $\mathcal{L}$ (named for its inventor Łukasiewicz). It is of interest for the simplicity of its definition. It involves only formulas in the signature $\{\Rightarrow, \neg\}$. (We know from § 2.5, Exercise 2 that this signature is adequate.) The only rule of inference of $\mathcal{L}$ is Detachment (as in the definition of $\mathcal{D}$ above). The axioms of $\mathcal{L}$ are of three kinds:[15]

1) **Affirmation of the Consequent:**

$$\vdash_{\mathcal{L}} \boldsymbol{F} \Rightarrow \boldsymbol{G} \Rightarrow \boldsymbol{F};$$

2) **Self-Distributivity of Implication:**

$$\vdash_{\mathcal{L}} (\boldsymbol{F} \Rightarrow \boldsymbol{G} \Rightarrow \boldsymbol{H}) \Rightarrow (\boldsymbol{F} \Rightarrow \boldsymbol{G}) \Rightarrow \boldsymbol{F} \Rightarrow \boldsymbol{H};$$

3) **Contraposition:**

$$\vdash_{\mathcal{L}} (\neg \boldsymbol{F} \Rightarrow \neg \boldsymbol{G}) \Rightarrow \boldsymbol{G} \Rightarrow \boldsymbol{F}.$$

Theorem 2.8.4. *System* $\mathcal{L}$ *is sound.*

To prove completeness, we shall need the following.

Lemma 2.8.5. $\vdash_{\mathcal{L}} \boldsymbol{F} \Rightarrow \boldsymbol{F}$.

Proof. The formal proof is

$$\begin{aligned}
&\boldsymbol{F} \Rightarrow \boldsymbol{F} \Rightarrow \boldsymbol{F},\\
&\boldsymbol{F} \Rightarrow (\boldsymbol{F} \Rightarrow \boldsymbol{F}) \Rightarrow \boldsymbol{F},\\
&(\boldsymbol{F} \Rightarrow (\boldsymbol{F} \Rightarrow \boldsymbol{F}) \Rightarrow \boldsymbol{F}) \Rightarrow (\boldsymbol{F} \Rightarrow \boldsymbol{F} \Rightarrow \boldsymbol{F}) \Rightarrow \boldsymbol{F} \Rightarrow \boldsymbol{F},\\
&(\boldsymbol{F} \Rightarrow \boldsymbol{F} \Rightarrow \boldsymbol{F}) \Rightarrow \boldsymbol{F} \Rightarrow \boldsymbol{F},\\
&\boldsymbol{F} \Rightarrow \boldsymbol{F},
\end{aligned}$$

where the first three entries are axioms (1), (1), and (2) respectively, and the last two follow by Detachment. □

[15] Frege had an earlier proof-system in this signature that used three additional kinds of axioms.

Lemma 2.8.6. *If* $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1} \vdash_{\mathcal{L}} \boldsymbol{G} \Rightarrow \boldsymbol{H}$*, then* $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1}, \boldsymbol{G} \vdash_{\mathcal{L}} \boldsymbol{H}$.

The converse of Lemma 2.8.6 is the following; the proof is by cases (and the method of infinite descent).

Theorem 2.8.7 (Deduction)**.** *If* $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1}, \boldsymbol{G} \vdash_{\mathcal{L}} \boldsymbol{H}$*, then*

$$\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1} \vdash_{\mathcal{L}} \boldsymbol{G} \Rightarrow \boldsymbol{H}.$$

Proof. There are three possibilities for $\boldsymbol{H}$:

If $\boldsymbol{H}$ is an axiom of $\mathcal{L}$, or is one of the formulas $\boldsymbol{F}_i$, then $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1} \vdash_{\mathcal{L}} \boldsymbol{H}$; but also $\vdash_{\mathcal{L}} \boldsymbol{H} \Rightarrow \boldsymbol{G} \Rightarrow \boldsymbol{H}$; hence $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1} \vdash_{\mathcal{L}} \boldsymbol{G} \Rightarrow \boldsymbol{H}$ by Detachment.

If $\boldsymbol{H}$ is $\boldsymbol{G}$, then $\vdash_{\mathcal{L}} \boldsymbol{G} \Rightarrow \boldsymbol{H}$ by Lemma 2.8.5.

Finally, suppose $\boldsymbol{K}_0, \ldots, \boldsymbol{K}_m$ is the formal proof in $\mathcal{L}$ of $\boldsymbol{H}$ from $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1}$ and $\boldsymbol{G}$, and suppose the last step in the proof is by Detachment. (If it is not, then we have already treated this possibility.) Then $\boldsymbol{K}_i$ is $\boldsymbol{F}$, and $\boldsymbol{K}_j$ is $\boldsymbol{F} \Rightarrow \boldsymbol{H}$, for some formula $\boldsymbol{F}$, and for some i and j that are less than m. If $\boldsymbol{G} \Rightarrow \boldsymbol{K}_i$ and $\boldsymbol{G} \Rightarrow \boldsymbol{K}_j$ can be deduced in $\mathcal{L}$ from $\{\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{n-1}\}$, then, by Detachment and the Self-Distributivity Axiom, so can $\boldsymbol{G} \Rightarrow \boldsymbol{H}$. Also, both $\boldsymbol{K}_i$ and $\boldsymbol{K}_j$ have shorter deductions than $\boldsymbol{H}$ in $\mathcal{L}$. Hence, if $\boldsymbol{G} \Rightarrow \boldsymbol{H}$ cannot be deduced, then neither can $\boldsymbol{G} \Rightarrow \boldsymbol{K}$ for some $\boldsymbol{K}$ with a shorter deduction than $\boldsymbol{H}$, which would be absurd. □

Lemma 2.8.8. *The following are validities of* $\mathcal{L}$*:*

1) $\neg\boldsymbol{G} \Rightarrow \boldsymbol{G} \Rightarrow \boldsymbol{F}$*;*

2) $\neg\neg\boldsymbol{F} \Rightarrow \boldsymbol{F}$*;*

3) $\boldsymbol{F} \Rightarrow \neg\neg\boldsymbol{F}$*;*

4) $(\boldsymbol{F} \Rightarrow \boldsymbol{G}) \Rightarrow \neg\boldsymbol{G} \Rightarrow \neg\boldsymbol{F}$*;*

5) $\boldsymbol{F} \Rightarrow \neg\boldsymbol{G} \Rightarrow \neg(\boldsymbol{F} \Rightarrow \boldsymbol{G})$.

6) $(\boldsymbol{F} \Rightarrow \boldsymbol{G}) \Rightarrow (\neg\boldsymbol{F} \Rightarrow \boldsymbol{G}) \Rightarrow \boldsymbol{G}$.

Proof. 1. The following is a formal proof in $\mathcal{L}$ from $\neg\boldsymbol{G}$:

$$\neg\boldsymbol{G},\ \neg\boldsymbol{G} \Rightarrow (\neg\boldsymbol{F} \Rightarrow \neg\boldsymbol{G}),\ \neg\boldsymbol{F} \Rightarrow \neg\boldsymbol{G},\ \neg\boldsymbol{F} \Rightarrow \neg\boldsymbol{G} \Rightarrow (\boldsymbol{G} \Rightarrow \boldsymbol{F}),\ \boldsymbol{G} \Rightarrow \boldsymbol{F}.$$

So $\neg\boldsymbol{G} \vdash_{\mathcal{L}} \boldsymbol{G} \Rightarrow \boldsymbol{F}$. By the Deduction Theorem, the claim follows.

2. By part (1) (and Lemma 2.8.6) we have $\neg\neg\boldsymbol{F} \vdash_{\mathcal{L}} \neg\boldsymbol{F} \Rightarrow \neg\neg\neg\boldsymbol{F}$. Use contraposition to get $\neg\neg\boldsymbol{F} \vdash_{\mathcal{L}} \boldsymbol{F}$, then use the Deduction Theorem to get the claim. □

We know how to evaluate a formula at a given truth-assignment. The following shows that we can prove in $\mathcal{L}$ the correctness of our computation.

Theorem 2.8.9. *Let $\boldsymbol{F}$ be an n-ary formula in the signature $\{\Rightarrow, \neg\}$. Let $\vec{e}$ be a truth-assignment for $\boldsymbol{F}$. Define*

$$P_i' = \begin{cases} P_i, & \text{if } e_i = 1; \\ \neg P_i, & \text{if } e_i = 0; \end{cases} \quad \text{and} \quad \boldsymbol{F}' = \begin{cases} \boldsymbol{F}, & \text{if } \widehat{\boldsymbol{F}}(\vec{e}) = 1; \\ \neg\boldsymbol{F}, & \text{if } \widehat{\boldsymbol{F}}(\vec{e}) = 0. \end{cases}$$

Then $P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} \boldsymbol{F}'$.

Proof. If $\boldsymbol{F}$ is P_i, then P_i' is $\boldsymbol{F}'$, so $P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} \boldsymbol{F}'$.

Now we can suppose $\boldsymbol{F}$ is not just a variable, and use infinite descent. So, assume $\boldsymbol{F}'$ is *not* deducible in $\mathcal{L}$ from $P_0', \ldots, P_{n-1}'$. There are two cases:

Say $\boldsymbol{F}$ is $\neg\boldsymbol{G}$ for some formula $\boldsymbol{G}$. Then

$$\boldsymbol{F}' = \begin{cases} \boldsymbol{G}', & \text{if } \widehat{\boldsymbol{F}}(\vec{e}) = 1; \\ \neg\neg\boldsymbol{G}', & \text{if } \widehat{\boldsymbol{F}}(\vec{e}) = 0. \end{cases}$$

Hence $\boldsymbol{G}'$ is also not deducible; but $\boldsymbol{G}$ is shorter then $\boldsymbol{F}$.

Say $\boldsymbol{F}$ is $\boldsymbol{G} \Rightarrow \boldsymbol{H}$ for some formulas $\boldsymbol{G}$ and $\boldsymbol{H}$. Then

$$P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} \boldsymbol{G}' \qquad\qquad P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} \boldsymbol{H}'.$$

There are three sub-cases to consider, according as

1) $\boldsymbol{G}'$ is $\neg\boldsymbol{G}$, or
2) $\boldsymbol{H}'$ is $\boldsymbol{H}$, or
3) $\boldsymbol{G}'$ is $\boldsymbol{G}$ and $\boldsymbol{H}'$ is $\neg\boldsymbol{H}$.

□

Corollary 2.8.10. *The proof-system $\mathcal{L}$ is complete.*

Proof. Suppose $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m$, the formulas being n-ary. Let $\boldsymbol{G}$ be the tautology $\boldsymbol{F}_0 \Rightarrow \ldots \Rightarrow \boldsymbol{F}_m$. Then for all n-ary truth-assignments $\vec{e}$, we have

$$P_0' \ldots, P_{n-1}' \vdash_{\mathcal{L}} \boldsymbol{G}.$$

If $n = 0$, we are done. If $n > 0$, then by the Deduction Theorem we have

$$P_0' \ldots, P_{n-2}' \vdash_{\mathcal{L}} P_{n-1} \Rightarrow \boldsymbol{G}, \qquad P_0' \ldots, P_{n-2}' \vdash_{\mathcal{L}} \neg P_{n-1} \Rightarrow \boldsymbol{G},$$

so $P_0' \ldots, P_{n-2}' \vdash_{\mathcal{L}} \boldsymbol{G}$ by Lemma 2.8.8 (6). Continuing, we find $\vdash_{\mathcal{L}} \boldsymbol{G}$, so $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vdash_{\mathcal{L}} \boldsymbol{F}_m$. □

Exercises

1. Prove Corollary 2.8.3.
2. Prove Theorem 2.8.4.
3. Prove Lemma 2.8.6.
4. Prove parts (3), (4), (5) and (6) of Lemma 2.8.8.
5. Supply the missing details in the proof of Theorem 2.8.9.

2.9. Compactness

So far, we have dealt with only finitely many formulas at once. But suppose $\mathcal{A}$ is a possibly infinite set of formulas. If $\mathcal{N}$ is a proof-system, then the expression

$$\mathcal{A} \vdash_{\mathcal{N}} \boldsymbol{F}$$

has the same meaning as before. So does the expression

$$\mathcal{A} \vDash \boldsymbol{F}, \tag{2.5}$$

except that there may be no n such that each formula in $\mathcal{A} \cup \{\boldsymbol{F}\}$ is n-ary.

A **truth-assignment,** simply, is a function from $\mathbb{N}$ to $\mathbb{B}$. Then $\mathcal{A}$ is **satisfied** by a truth-assignment $k \mapsto e_k$ if $\widehat{\boldsymbol{G}}(e_0, \ldots, e_{n-1}) = 1$ for every n-ary formula $\boldsymbol{G}$ in $\mathcal{A}$, for every n in $\mathbb{N}$; and $\boldsymbol{F}$ is **true** in this assignment if $\widehat{\boldsymbol{F}}(e_0, \ldots, e_{n-1}) = 1$ (assuming $\boldsymbol{F}$ is n-ary). Then (2.5) holds, by definition, if $\boldsymbol{F}$ is true in every truth-assignment that satisfies $\mathcal{A}$. Hence the following are equivalent:

1) $\mathcal{A}$ does not logically entail $\boldsymbol{F}$;
2) $\mathcal{A} \cup \{\neg \boldsymbol{F}\}$ is **satisfiable** (that is, satisfied by some truth-assignment; note that this definition is compatible with the one in §2.2).

Theorem 2.9.1 (Compactness)**.** *If every finite subset of a set of formulas is satisfiable, then the whole set is satisfiable.*

Proof. Suppose $\mathcal{A}$ is an infinite set of formulas such that every finite subset of $\mathcal{A}$ is satisfiable. For any n in $\mathbb{N}$, let $\mathcal{A}_n$ consist of the n-ary formulas in $\mathcal{A}$. Then $\mathcal{A}_n$ is finite, so it is satisfiable by assumption. In particular, $\mathcal{A}_n$ is satisfied by a certain truth-assignment

$$(e_0^n, e_1^n, \ldots, e_{n-1}^n).$$

For each n, let such an assignment be chosen. So for each pair (i, n) of natural numbers, if $i < n$, then we have chosen an a certain element e_i^n of $\mathbb{B}$.

In the following way, we can recursively define an infinite truth-assignment $(e_0, e_1, e_2, \dots)$ satisfying $\mathcal{A}$. Suppose $(e_0, \dots, e_{k-1})$ has been chosen so that there are *infinitely many* values of n such that $k \leqslant n$ and

$$(e_0^n, \dots, e_{k-1}^n) = (e_0, \dots, e_{k-1}).$$

(This is a trivial assumption if $k = 0$.) Then choose e_k so that

$$(e_0^n, \dots, e_k^n) = (e_0, \dots, e_k)$$

for infinitely many values of n. (Why does this e_k exist?)

We now have that $(e_0, \dots, e_{n-1})$ satisfies $\mathcal{A}_n$ for each n in $\mathbb{N}$. Therefore the whole assignment $(e_0, e_1, \dots)$ satisfies $\mathcal{A}$. □

Corollary 2.9.2. *If $\mathcal{N}$ is a sound, complete proof-system, then*

$$\mathcal{A} \vDash \boldsymbol{F} \iff \mathcal{A} \vdash_{\mathcal{N}} \boldsymbol{F}$$

for all formulas $\boldsymbol{F}$ and sets $\mathcal{A}$ of formulas.

Proof. If $\mathcal{A} \vdash_{\mathcal{N}} \boldsymbol{F}$, then $\boldsymbol{G}_0, \dots, \boldsymbol{G}_{m-1} \vdash_{\mathcal{N}} \boldsymbol{F}$ for some formulas $\boldsymbol{G}_i$ in $\mathcal{A}$, since proofs are finite. Hence $\boldsymbol{G}_0, \dots, \boldsymbol{G}_{m-1} \vDash \boldsymbol{F}$, so $\mathcal{A} \vDash \boldsymbol{F}$.

If $\boldsymbol{F}$ is not derivable in $\mathcal{N}$ from $\mathcal{A}$, then it is not derivable from any finite subset of $\mathcal{A}$. This means $\boldsymbol{F}$ is not a consequence of any finite subset of $\mathcal{A}$, which means that every finite subset of

$$\mathcal{A} \cup \{\neg \boldsymbol{F}\}$$

is satisfiable. Hence the whole set is satisfiable by the Compactness Theorem, so $\boldsymbol{F}$ is not a consequence of $\mathcal{A}$. □

Exercise

Identify the parts of the proof of Theorem 2.9.1 that do not seem fully justified, and justify them if you can.

3. Sets and Relations

3.0. Boolean operations on sets

As observed in § 1.8, propositional logic is a model of the use of conjunctions in ordinary language. A basic *application* of propositional logic is to *sets.* In fact, the sets that will be discussed here need only be classes; I call them sets, because this is the usual terminology.

As in §§ 1.2 and 1.9, suppose $\mathcal{U}$ is some large set—a **universal set**, which will include all of the other sets that we shall work with. Again, by the Axiom of Separation, 1.2.3, if P is a predicate and $\mathcal{U}$ is a set, then we can form a set

$$\{x \in \mathcal{U} \colon Px\}. \tag{3.1}$$

We have not yet said much about what P might be. Now we do.

If $A \subseteq \mathcal{U}$ and $c \in \mathcal{U}$, then we can form the proposition

$$c \in A,$$

which is either true or false. We can analyze this proposition into two parts:

c	$\in A$
subject	predicate

With the predicate $\in A$ and an **individual variable**, x, we can make the *formula*

$$x \in A.$$

This is not a *propositional* formula, since $\in$ is not a symbol of propositional logic. Let us call the formula a **set-theoretic formula** or an **$\in$-formula.** In particular, it is an $\in$-formula with A as a **parameter.** We may replace this parameter with other sets, but for now, our only individual variable will be x. We shall allow more variables in § 3.2.

Meanwhile, we can create new $\in$-formulas in x from formulas $x \in A$, just as we create new propositional formulas from the propositional variables P_k. So 0

and 1, along with $x \in A$, are $\in$-formulas in x, and if $\varphi(x)$ and $\psi(x)$ are arbitrary $\in$-formulas in x, then so are $\neg\varphi(x)$ and $(\varphi(x) * \psi(x))$, where $*$ is one of $\&$, $\vee$, $\not\Leftrightarrow$, $\Rightarrow$, and $\Leftrightarrow$. Then each $\in$-formula in x can be written as

$$\boldsymbol{F}(x \in A_0, \ldots, x \in A_{n-1})$$

for some n in $\mathbb{N}$, where $\boldsymbol{F}$ is an n-ary propositional formula, and each parameter A_k is a set. We shall always choose these parameters from among the subsets of $\mathcal{U}$.

Suppose $\varphi(x)$ is an $\in$-formula, and $c \in \mathcal{U}$. Then we can obtain the **$\in$-sentence** $\varphi(c)$, which is the result of replacing each x in $\varphi(x)$ with c. This sentence is true or false. Indeed, the sentence $c \in A$ is true if and only if c is in A; and $\neg\varphi(c)$ is true if and only if $\varphi(c)$ is false; and $(\varphi(c) \,\&\, \psi(d))$ is true if and only if both $\varphi(c)$ and $\psi(c)$ are true; and so forth. Alternatively, if $\varphi(x)$ is $\boldsymbol{F}(x \in A_0, \ldots, x \in A_{n-1})$, then $\varphi(c)$ is true if and only if

$$\widehat{\boldsymbol{F}}(\vec{e}) = 1,$$

where $\vec{e}$ is defined by

$$e_k = \begin{cases} 1, & \text{if } c \in A_k, \\ 0, & \text{if } c \notin A_k. \end{cases} \tag{3.2}$$

Now each $\in$-formula $\varphi(x)$ can be understood as a predicate applied to x. By the Axiom of Separation (1.2.3) then, the formula **defines** a subset of $\mathcal{U}$, namely

$$\{x \in \mathcal{U} \colon \varphi(x)\},$$

comprising those c in $\mathcal{U}$ such that $\varphi(c)$ is true.

In particular, the set $\{x \in \mathcal{U} \colon x \in A\}$ is just A itself. We usually write the negation $\neg\, x \in A$ as

$$x \notin A.$$

Then by § 1.9, this formula defines the **complement** of A in $\mathcal{U}$:

$$\{x \in \mathcal{U} \colon x \notin A\} = A^{\mathrm{c}}.$$

Suppose also $B \subseteq \mathcal{U}$. Using both of the formulas $x \in A$ and $x \in B$, we obtain the following standard combinations:

$$\{x \in \mathcal{U} \colon x \in A \,\&\, x \in B\} = A \cap B,$$

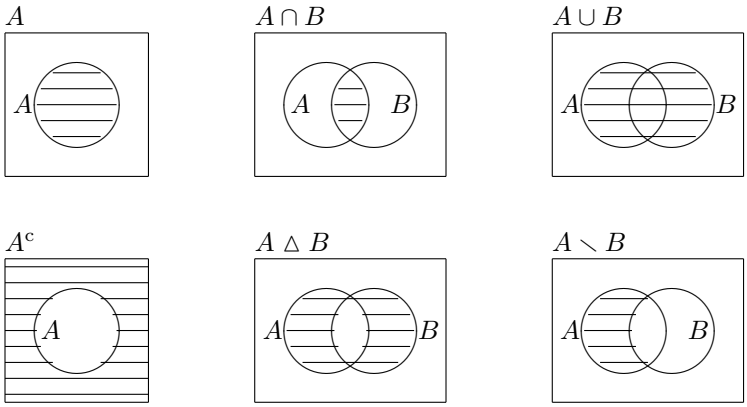


Figure 3.1. Venn diagrams of combinations of sets

the **intersection** of A and B, which contains everything that is in *both* A and B;

$$\{x \in \mathcal{U} \colon x \in A \vee x \in B\} = A \cup B,$$

the **union** of A and B, which contains everything that is in (at least) *one* of A and B (the union was defined first in § 1.2);

$$\{x \in \mathcal{U} \colon x \in A \nLeftrightarrow x \in B\} = A \mathbin{\triangle} B,$$

the **symmetric difference** of A and B, which contains everything that is in *exactly one* of A and B;

$$\{x \in \mathcal{U} \colon x \in A \mathbin{\&} x \notin B\} = A \mathbin{\diagdown} B,$$

the **difference** of A and B, which contains everything that is in A, but *not* in B.

Pictures of these combinations are in Figure 3.1. The symbols $^{\mathrm{c}}$, $\cap$, $\cup$, $\triangle$, and $\diagdown$, along with $\varnothing$, stand for **Boolean operations**. If $\varphi(x)$ is $\boldsymbol{F}(x \in A_0, \dots, x \in A_{n-1})$, then $\{x \in \mathcal{U} \colon \varphi(x)\}$ is a **Boolean combination** of the sets A_k. A set is a Boolean combination of itself; beyond this, there are two trivial Boolean combinations:

$$\{x \in \mathcal{U} \colon 0\} = \varnothing, \qquad \{x \in \mathcal{U} \colon 1\} = \mathcal{U}.$$

We now have a sort of correspondence between propositional logic and set-theory:

$$\begin{array}{ccc} \& & \rightsquigarrow & \cap \\ \vee & \rightsquigarrow & \cup \\ \nLeftrightarrow & \rightsquigarrow & \triangle \\ \neg & \rightsquigarrow & {}^{c} \\ 0 & \rightsquigarrow & \varnothing \\ 1 & \rightsquigarrow & \mathcal{U} \end{array}$$

The set $\mathcal{U}$ depends on the situation.

We can determine membership in Boolean combinations of sets by means of truth-tables:

Example 3.0.1. From the truth-table

$\boldsymbol{P}$	$\Rightarrow$	$\boldsymbol{Q}$
0	1	0
1	0	0
0	1	1
1	1	1

,

by considering the lines where the formula $\boldsymbol{P} \Rightarrow \boldsymbol{Q}$ takes the value 1, we can conclude that the set $\{x \in \mathcal{U} \colon x \in A \Rightarrow x \in B\}$ consists of those c in $\mathcal{U}$ such that one of the following holds:

1) $c \notin A \ \& \ c \notin B$, or
2) $c \notin A \ \& \ c \in B$, or
3) $c \in A \ \& \ c \in B$.

Alternatively, from the line of the truth-table where $\boldsymbol{P} \Rightarrow \boldsymbol{Q}$ takes the value 0, we conclude that the set $\{x \in \mathcal{U} \colon x \in A \Rightarrow x \in B\}$ consists of those c such that either $c \notin A$ or $c \in B$.

The foregoing example should recall the notions of disjunctive and conjunctive normal forms in § 2.4.

The Axiom of Extension, 1.2.1, is that sets are determined by their members. That is, two subsets A and B of $\mathcal{U}$ are equal if

$$c \in A \iff c \in B \tag{3·3}$$

for all c in $\mathcal{U}$. Strictly, we need this to conclude $A = \{x \in \mathcal{U} : x \in A\}$. The *converse* of the Extension Axiom is obviously true: If two sets are equal, then in particular, they have the same members.

Theorem 3.0.2. *Two subsets A and B of $\mathcal{U}$ are equal if and only if*

$$\{x \in \mathcal{U} \colon x \in A \Leftrightarrow x \in B\} = \mathcal{U}. \tag{3.4}$$

Proof. If (3.4) holds, then, for all c in $\mathcal{U}$, the sentence $c \in A$ is true if and only if the sentence $c \in B$ is true—that is, (3.3) holds, so $A = B$ by the Axiom of Extension. Conversely, if $A = B$, then the two members of (3.4) have the same elements, so the equation is true by the Axiom. □

Another consequence of the Axiom of Extension is that equivalent propositional formulas give rise to equal sets in the following sense.

Theorem 3.0.3. *Suppose $\boldsymbol{F}_0$ and $\boldsymbol{F}_1$ are n-ary propositional formulas such that*

$$\boldsymbol{F}_0 \sim \boldsymbol{F}_1.$$

When $e \in \mathbb{B}$, let $\varphi_e(x)$ be the $\in$-formula $\boldsymbol{F}_e(x \in A_0, \ \ldots, \ x \in A_{n-1})$. Then

$$\{x \in \mathcal{U} \colon \varphi_0(x)\} = \{x \in \mathcal{U} \colon \varphi_1(x)\}. \tag{3.5}$$

Proof. If $c \in \mathcal{U}$, let the n-ary truth-assignment $\vec{e}$ be as defined by (3.2) above. Then

$$c \in \{x \in \mathcal{U} \colon \varphi_0(x)\} \iff \widehat{\boldsymbol{F}}_0(\vec{e}) = 1 \iff \widehat{\boldsymbol{F}}_1(\vec{e}) = 1 \iff c \in \{x \in \mathcal{U} \colon \varphi_1(x)\},$$

so (3.5) holds. □

Hence for example we have

$$A^{\mathrm{c}} = \mathcal{U} \smallsetminus A.$$

Equation (3.5) is an **identity,** more precisely a **set-theoretic identity,** because it holds for all choices of $A_0, \ \ldots, \ A_{n-1}$.

Example (3.0.1 continued)**.** Because $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \sim \neg \boldsymbol{P} \vee \boldsymbol{Q}$, we have

$$\{x \in \mathcal{U} \colon x \in A \Rightarrow x \in B\} = \{x \in \mathcal{U} \colon x \notin A \vee x \in B\}.$$

Again, we have $\{x \in \mathcal{U} \colon x \in A \,\&\, x \in B\} = A \cap B$ by definition; therefore, it seems obvious that

$$\{x \in \mathcal{U} \colon \varphi(x) \,\&\, \psi(x)\} = \{x \in \mathcal{U} \colon \varphi(x)\} \cap \{x \in \mathcal{U} \colon \psi(x)\} \tag{3.6}$$

for all $\in$-formulas $\varphi(x)$ and $\psi(x)$. However, (3.6) is not immediate, since the formulas $x \in A$ and $x \in B$ are only special cases of $\in$-formulas. We can prove (3.6) by letting $\{x \in \mathcal{U} \colon \varphi(x)\} = A$ and $\{x \in \mathcal{U} \colon \psi(x)\} = B$. Then

$$\begin{aligned} c \in \{x \in \mathcal{U} \colon \varphi(x) \,\&\, \psi(x)\} &\iff \varphi(c) \,\&\, \psi(c) \text{ is true} \\ &\iff \varphi(c) \text{ is true and } \psi(c) \text{ is true} \\ &\iff c \in A \text{ is true and } c \in B \text{ is true} \\ &\iff c \in A \,\&\, c \in B \text{ is true} \\ &\iff c \in \{x \in \mathcal{U} \colon x \in A \,\&\, x \in B\} \\ &\iff c \in A \cap B \\ &\iff c \in \{x \in \mathcal{U} \colon \varphi(x)\} \cap \{x \in \mathcal{U} \colon \psi(x)\}, \end{aligned}$$

so (3.6) follows.

We can also obtain (3.6) from

$$\{x \in \mathcal{U} \colon x \in A \,\&\, x \in B\} = \{x \in \mathcal{U} \colon x \in A\} \cap \{x \in \mathcal{U} \colon x \in B\}$$

by *replacing* the formula $x \in A$ with $\varphi(x)$, and $x \in B$ with $\psi(x)$. That such an action preserves equality is a consequence of the following, which should be compared with Theorem 2.3.8.

Theorem 3.0.4 (Replacement)**.** *Suppose $\boldsymbol{F}$ is a sub-formula of the n-ary formula $\boldsymbol{G}$, so that $\boldsymbol{G}$ itself is $\boldsymbol{H}(P_0, \ldots, P_{n-1}, \boldsymbol{F})$ for some formula $\boldsymbol{H}$. Let*

$$B = \{x \in \mathcal{U} \colon \boldsymbol{F}(x \in A_0,\ \ldots,\ x \in A_{n-1})\}.$$

Then the set $\{x \in \mathcal{U} \colon \boldsymbol{G}(x \in A_0,\ \ldots,\ x \in A_{n-1})\}$ is equal to

$$\{x \in \mathcal{U} \colon \boldsymbol{H}(x \in A_0,\ \ldots,\ x \in A_{n-1},\ x \in B)\}.$$

Theorem 3.0.5. *For all $\in$-formulas $\varphi(x)$ and $\psi(x)$,*

$$\begin{aligned} \{x \in \mathcal{U} \colon \varphi(x) \,\&\, \psi(x)\} &= \{x \in \mathcal{U} \colon \varphi(x)\} \cap \{x \in \mathcal{U} \colon \psi(x)\}, \\ \{x \in \mathcal{U} \colon \varphi(x) \vee \psi(x)\} &= \{x \in \mathcal{U} \colon \varphi(x)\} \cup \{x \in \mathcal{U} \colon \psi(x)\}, \\ \{x \in \mathcal{U} \colon \varphi(x) \nLeftrightarrow \psi(x)\} &= \{x \in \mathcal{U} \colon \varphi(x)\} \vartriangle \{x \in \mathcal{U} \colon \psi(x)\}, \\ \{x \in \mathcal{U} \colon \neg\varphi(x)\} &= \{x \in \mathcal{U} \colon \varphi(x)\}^{\mathrm{c}}. \end{aligned} \tag{3.7}$$

Proof. We have already proved (3.7); but to obtain it from Theorem 3.0.4, we can argue as follows. Let $A = \{x \in \mathcal{U} \colon \varphi(x)\}$ and $B = \{x \in \mathcal{U} \colon \psi(x)\}$, and let

$\boldsymbol{H}$ be the binary formula $P_0 \,\&\, P_1$. Then

$$\begin{aligned}
&\{x \in \mathcal{U}\colon \varphi(x) \,\&\, \psi(x)\} \\
&= \{x \in \mathcal{U}\colon \boldsymbol{H}(\varphi(x), \psi(x))\} && \text{[by def'n of } \boldsymbol{H}\text{]} \\
&= \{x \in \mathcal{U}\colon \boldsymbol{H}(x \in A,\ x \in B)\} && \text{[by Replacement]} \\
&= \{x \in \mathcal{U}\colon x \in A \,\&\, x \in B\} && \text{[by def'n of } \boldsymbol{H}\text{]} \\
&= A \cap B && \text{[by def'n of } \cap\text{]} \\
&= \{x \in \mathcal{U}\colon \varphi(x)\} \cap \{x \in \mathcal{U}\colon \psi(x)\} && \text{[by def'n of } A \text{ and } B\text{]}.
\end{aligned}$$

The other identities are established likewise. □

Example (3.0.1 continued again)**.** We now have

$$\begin{aligned}
\{x \in \mathcal{U}\colon x \in A \Rightarrow x \in B\} &= \{x \in \mathcal{U}\colon x \notin A \vee x \in B\} \\
&= \{x \in \mathcal{U}\colon x \notin A\} \cup \{x \in \mathcal{U}\colon x \in B\} \\
&= A^{\mathrm{c}} \cup B,
\end{aligned}$$

and similarly, $\{x \in \mathcal{U}\colon x \in A \Rightarrow x \in B\} = (A^{\mathrm{c}} \cap B^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B) \cup (A \cap B)$. Hence the equation

$$A^{\mathrm{c}} \cup B = (A^{\mathrm{c}} \cap B^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B) \cup (A \cap B)$$

is an identity.

Example 3.0.6. From the truth-table

$\boldsymbol{P}$	&	($\boldsymbol{Q}$	$\vee$	$\boldsymbol{R}$)
0	0	0	0	0
1	0	0	0	0
0	0	1	1	0
1	1	1	1	0
0	0	0	1	1
1	1	0	1	1
0	0	1	1	1
1	1	1	1	1

we can infer that the set $\{x \in \mathcal{U}\colon x \in A \,\&\, (x \in B \vee x \in C)\}$ is precisely

$$(A \cap B \cap C^{\mathrm{c}}) \cup (A \cap B^{\mathrm{c}} \cap C) \cup (A \cap B \cap C);$$

alternatively, the set is $A \cap \{x \in \mathcal{U}\colon x \in B \vee x \in C\}$, which is $A \cap (B \cup C)$.

As a consequence of Lemmas 2.2.2 and 2.6.3, we have:

Lemma 3.0.7. *The following are set-theoretic identities.*

1. ***Definition:***

$$\begin{aligned} A \triangle B &= (A \cup B) \smallsetminus (A \cap B) && (3.8)\\ &= (A \smallsetminus B) \cup (B \smallsetminus A), && (3.9)\\ A \smallsetminus B &= A \cap B^{\mathrm{c}}; && (3.10) \end{aligned}$$

2. ***Double complementation:***

$$A^{\mathrm{cc}} = A; \tag{3.11}$$

3. ***De Morgan's Laws:***

$$\begin{aligned} (A \cup B)^{\mathrm{c}} &= A^{\mathrm{c}} \cap B^{\mathrm{c}},\\ (A \cap B)^{\mathrm{c}} &= A^{\mathrm{c}} \cup B^{\mathrm{c}}; \end{aligned} \tag{3.12}$$

4. ***Commutativity:***

$$A \cap B = B \cap A, \qquad A \cup B = B \cup A; \tag{3.13}$$

5. ***Associativity:***

$$(A \cap B) \cap C = A \cap (B \cap C), \qquad (A \cup B) \cup C = A \cup (B \cup C), \tag{3.14}$$

6. *Mutual* ***Distributivity*** *of* $\cap$ *and* $\cup$*:*

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C),\\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C); \end{aligned} \tag{3.15}$$

7. ***Redundancy:***

$$\varnothing^{\mathrm{c}} = \mathcal{U}, \qquad \mathcal{U}^{\mathrm{c}} = \varnothing; \tag{3.16}$$

$$A \cap A = A, \quad A \cap A^{\mathrm{c}} = \varnothing, \quad A \cap \mathcal{U} = A, \quad A \cap \varnothing = \varnothing, \tag{3.17}$$

$$A \cup A = A, \quad A \cup A^{\mathrm{c}} = \mathcal{U}, \quad A \cup \varnothing = A, \quad A \cup \mathcal{U} = \mathcal{U}, \tag{3.18}$$

8. ***New set:***

$$A = (A \cap B) \cup (A \cap B^{\mathrm{c}}); \tag{3.19}$$

9. ***Absorption:***

$$\begin{aligned} A \cap (A \cup B) &= A, \\ A \cup (A \cap B) &= A. \end{aligned} \tag{3.20}$$

We can now prove other set-theoretic identities by a process of simplification parallel to the one we use for logical equivalences:

Theorem 3.0.8. *The equations*

$$A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C), \tag{3.21}$$
$$A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C) \tag{3.22}$$

are identities of sets.

Proof. For (3.21), we have the chain of identities

$$\begin{aligned} A \smallsetminus (B \cap C) &= A \cap (B \cap C)^{\mathrm{c}} && \text{[def'n of } \smallsetminus\text{]} \\ &= A \cap (B^{\mathrm{c}} \cup C^{\mathrm{c}}) && \text{[De Morgan]} \\ &= (A \cap B^{\mathrm{c}}) \cup (A \cap C^{\mathrm{c}}) && \text{[distributivity]} \\ &= (A \smallsetminus B) \cup (A \smallsetminus C) && \text{[def'n of } \smallsetminus\text{].} \end{aligned}$$

Equation (3.22) is an exercise. □

An alternative method for proving set-theoretic identities uses the original statement of the Axiom of Extension on § 1.2. To prove (3.10) for example, it is enough to prove $A \smallsetminus B \subseteq A \cap B^{\mathrm{c}}$ and $A \cap B^{\mathrm{c}} \subseteq A \smallsetminus B$. To prove the former, suppose $c \in A \smallsetminus B$. Then $c \in A$, but $c \notin B$. Hence also $c \in B^{\mathrm{c}}$. Hence $c \in A \cap B^{\mathrm{c}}$. Therefore $A \smallsetminus B \subseteq A \cap B^{\mathrm{c}}$. The other inclusion can be proved similarly.

Exercises

1. Prove the converse of Theorem 3.0.3 in the following sense: Show that, if $\boldsymbol{F}$ and $\boldsymbol{G}$ are not equivalent, then there is a set $\mathcal{U}$ with subsets A_k such that $\{x \in \mathcal{U} \colon \boldsymbol{F}(x \in A_0,\ \ldots,\ x \in A_{n-1})\} \neq \{x \in \mathcal{U} \colon \boldsymbol{G}(x \in A_0,\ \ldots,\ x \in A_{n-1})\}$. (*Suggestion:* Let $\mathcal{U}$ be a set of truth-assignments, and let A_k comprise those $\vec{e}$ such that $e_k = 1$.)

2. Prove Theorem 3.0.4.

3. Complete the proof of Theorem 3.0.5.
4. Complete the proof of Lemma 3.0.7.
5. Complete the proof of Theorem 3.0.8.
6. Prove that $(A \smallsetminus B) \cup (B \smallsetminus A) = A \triangle B$.
7. Prove that $(A \cap B) \cup (A \cup B)^{\mathrm{c}} = \{x : x \in A \Leftrightarrow x \in B\}$.
8. Prove the following set-theoretic identities:
   (a) $(A \smallsetminus B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B$
   (b) $B^{\mathrm{c}} \smallsetminus A^{\mathrm{c}} = A \smallsetminus B$
   (c) $A \smallsetminus (B \smallsetminus C)^{\mathrm{c}} = (A \cap B) \smallsetminus C$

3.1. Inclusions and implications

We consider inclusion in place of equality. Corresponding to Theorem 3.0.2, we have

Theorem 3.1.1. *For two subsets A and B of $\mathcal{U}$, we have $A \subseteq B$ if and only if*

$$\{x \in \mathcal{U} \colon x \in A \Rightarrow x \in B\} = \mathcal{U}.$$

Corresponding to Theorem 3.0.3, we have:

Theorem 3.1.2. *Suppose $\boldsymbol{F}_0$ and $\boldsymbol{F}_1$ are n-ary propositional formulas such that*

$$\boldsymbol{F}_0 \vDash \boldsymbol{F}_1.$$

When $e \in \mathbb{B}$, let $\varphi_e(x)$ be the $\in$-formula $\boldsymbol{F}_e(x \in A_0, \ldots, x \in A_{n-1})$. Then

$$\{x \in \mathcal{U} \colon \varphi_0(x)\} \subseteq \{x \in \mathcal{U} \colon \varphi_1(x)\}.$$

Some of the rules of inference in Lemma 2.7.8 now translate into **tautological** inclusions (inclusions that are true for all sets):

Lemma 3.1.3. *The following inclusions are tautological:*

$$A \cap B \subseteq B; \tag{3.23}$$
$$A \subseteq A \cup B; \tag{3.24}$$
$$(A \cup B) \cap A^{\mathrm{c}} \subseteq B. \tag{3.25}$$

Proof. The first two inclusions are translations (justified by Theorem 3.1.2) of the logical consequences $\boldsymbol{P} \,\&\, \boldsymbol{Q} \vDash \boldsymbol{Q}$ and $\boldsymbol{P} \vDash \boldsymbol{P} \vee \boldsymbol{Q}$; the last inclusion is a translation of the rule of Disjunctive Syllogism, in view of § 2.7, Exercise 1. □

There is no common symbol for the Boolean operation corresponding to the connective $\Rightarrow$; so Rules of inference like Hypothetical Syllogism and Constructive Dilemma, which involve $\Rightarrow$, do not translate into inclusions like those in the lemma. However, Theorem 3.1.1 shows a connexion between $\Rightarrow$ itself and inclusion. Moreover, logical entailment corresponds to implication in the following sense.

Theorem 3.1.4. *Suppose $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_m$ are n-ary propositional formulas such that*

$$\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{F}_m.$$

When $e \leqslant m$, let $\varphi_e(x)$ be the $\in$-formula $\boldsymbol{F}_e(x \in A_0, \ \ldots, \ x \in A_{n-1})$. Then

$$\{x \in \mathcal{U} \colon \varphi_0(x)\} = \mathcal{U} \ \&\ \ldots \ \&\ \{x \in \mathcal{U} \colon \varphi_{m-1}(x)\} = \mathcal{U} \implies \{x \in \mathcal{U} \colon \varphi_m(x)\} = \mathcal{U}.$$

Now Hypothetical Syllogism and Constructive Dilemma can be expressed set-theoretically as implications: **tautological implications.**

Lemma 3.1.5. *The following implications are tautological:*

$$A \subseteq B \ \&\ B \subseteq C \implies A \subseteq C; \tag{3.26}$$

$$A \subseteq B \ \&\ C \subseteq D \implies A \cup C \subseteq B \cup D \ \&\ A \cap C \subseteq B \cap D. \tag{3.27}$$

Proof. Here (3.26) is a direct translation of (2.4) by means of the theorems above. Alternatively, suppose $A \subseteq B$ and $B \subseteq C$ and $d \in A$. Then $d \in B$, so $d \in C$. Thus $A \subseteq C$.

For (3.27), suppose $A \subseteq B$ and $C \subseteq D$. Say $d \in A \cup C$. Then $d \in A$ or $d \in C$. If $d \in A$, then $d \in B$, so $d \in B \cup D$. The same conclusion follows similarly if $d \in C$. Therefore $A \cup C \subseteq B \cup D$. The remaining inclusion is an exercise. □

By (3.26), we can reasonably abbreviate the proposition $A \subseteq B \ \&\ B \subseteq C$ by

$$A \subseteq B \subseteq C.$$

By (3.17) and (3.18) above, (3.27) has the special cases:

$$A \subseteq B \ \&\ A \subseteq C \implies A \subseteq B \cap C, \tag{3.28}$$

$$A \subseteq B \ \&\ C \subseteq B \implies A \cup C \subseteq B. \tag{3.29}$$

Their converses are a part of the following:

Lemma 3.1.6. *The following are true for all sets.*

1. $A \subseteq B \cap C \implies A \subseteq B$.
2. $A \cup B \subseteq C \implies A \subseteq C$.
3. $A \cap B = \varnothing \ \& \ A \subseteq B \implies A = \varnothing$.
4. $A^{\mathrm{c}} \subseteq A \iff A^{\mathrm{c}} = \varnothing \iff A = \mathcal{U}$.
5. $A \smallsetminus B = \varnothing \iff A \subseteq B$.

Proof. Suppose $A \subseteq B \cap C$. Since $B \cap C \subseteq B$ by Lemma 3.1.3, we get $A \subseteq B$ by Lemma 3.1.5. The remaining implications are exercises. □

We are now equipped to prove some non-obvious claims:

Example 3.1.7. Suppose $A^{\mathrm{c}} \cup (B \vartriangle C) \subseteq A \cap B^{\mathrm{c}} \cap C$. Then

$$A \cap (B \cup C) = (A \cup B) \cap C. \tag{3.30}$$

Indeed, to see this, note first

$$\begin{aligned} A^{\mathrm{c}} &\subseteq A^{\mathrm{c}} \cup (B \vartriangle C) && \text{[by Lemma 3.1.3]} \\ &\subseteq A \cap B^{\mathrm{c}} \cap C && \text{[by assumption]} \\ &\subseteq A. && \text{[by Lemma 3.1.3]} \end{aligned}$$

Then $A^{\mathrm{c}} \subseteq A$ by Lemma 3.1.5, and therefore

$$A = \mathcal{U}$$

by Lemma 3.1.6. By the same lemmas, and Lemma 3.0.7, our assumption now gives us

$$(B \smallsetminus C) \cup (C \smallsetminus B) = B \vartriangle C \subseteq B^{\mathrm{c}} \cap C = B \smallsetminus C;$$

therefore $C \smallsetminus B \subseteq B \smallsetminus C$, that is,

$$C \cap B^{\mathrm{c}} \subseteq B \cap C^{\mathrm{c}}.$$

Say $a \in C \cap B^{\mathrm{c}}$. Then $a \in B^{\mathrm{c}}$. But also, $a \in B \cap C^{\mathrm{c}}$, so $a \in B$. Thus $a \in B^{\mathrm{c}} \cap B = \varnothing$, which is absurd. So $C \cap B^{\mathrm{c}}$ must be empty, which means

$$B \subseteq C.$$

Finally then,

$$A \cap (B \cup C) = B \cup C = C = (A \cup B) \cap C$$

since $A = \mathcal{U} = A \cup B$.

Where did this example come from? And, where did the proof come from? First, note that variations of the proof are possible: For example, part of the proof is showing

$$C \cap B^{\mathrm{c}} \subseteq B \cap C^{\mathrm{c}} \implies C \cap B^{\mathrm{c}} = \varnothing.$$

But if $C \cap B^{\mathrm{c}} \subseteq B \cap C^{\mathrm{c}}$, then

$$C \cap B^{\mathrm{c}} \subseteq (B \cap C^{\mathrm{c}}) \cap (C \cap B^{\mathrm{c}}) = B \cap (C^{\mathrm{c}} \cap C) \cap B^{\mathrm{c}} = \varnothing.$$

Thus there is no need to look at individual elements of $C \cap B^{\mathrm{c}}$, as in the proof above.

Whatever minor adjustments we make, the proof in Example 3.1.7 does not seem to follow a general pattern. Each step is justified, and the conclusion is as desired; so the proof is correct. But this observation does not tell us how to *find* the proof.

There *is* an alternative proof that follows a general pattern; this proof also suggests how the proposition being proved was discovered. The key is the set-theoretic analogue of the disjunctive normal forms of § 2.4:

Example (3.1.7 continued)**.** We can analyze the given Boolean combinations of A, B, and C as follows. First note that

$$\begin{aligned} A^{\mathrm{c}} &= (A^{\mathrm{c}} \cap B^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B) \\ &= (A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C) \cup (A^{\mathrm{c}} \cap B \cap C^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B \cap C), \end{aligned}$$

while

$$\begin{aligned} B \mathbin{\triangle} C &= (B \cap C^{\mathrm{c}}) \cup (B^{\mathrm{c}} \cap C) \\ &= (A^{\mathrm{c}} \cap B \cap C^{\mathrm{c}}) \cup (A \cap B \cap C^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C) \cup (A \cap B^{\mathrm{c}} \cap C). \end{aligned}$$

Therefore

$$\begin{aligned} A^{\mathrm{c}} \cup (B \mathbin{\triangle} C) = (A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C) \cup (A^{\mathrm{c}} \cap B \cap C^{\mathrm{c}}) \cup \\ \cup (A^{\mathrm{c}} \cap B \cap C) \cup (A \cap B \cap C^{\mathrm{c}}) \cup (A \cap B^{\mathrm{c}} \cap C). \end{aligned}$$

The six constituents of this union are disjoint, and the whole set $A^{\mathrm{c}} \cup (B \mathbin{\triangle} C)$ is assumed to be a subset of its last constituent, $A \cap B^{\mathrm{c}} \cap C$; therefore the first five constituents are empty. We aim to prove Equation (3.30). Analyzing the

two members of this equation, we have

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ &= (A \cap B \cap C^{\mathrm{c}}) \cup (A \cap B \cap C) \cup (A \cap B^{\mathrm{c}} \cap C), \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \\ &= (A \cap B^{\mathrm{c}} \cap C) \cup (A \cap B \cap C) \cup (A^{\mathrm{c}} \cap B \cap C). \end{aligned}$$

Under the assumption, two constituents in each case are empty, and each member of Equation (3.30) is $A \cap B \cap C$.

Thus the alternative proof takes more writing, although it follows a general procedure that involves writing every set in question as a union of intersections of the sets A, B, and C and their complements.

Exercises

1. Prove Theorem 3.1.1.
2. Prove Theorem 3.1.2.
3. Prove Theorem 3.1.4.
4. Complete the proof of Lemma 3.1.5.
5. Complete the proof of Lemma 3.1.6.
6. Prove the following tautological inclusions:
   a) $A \cap (A \setminus B)^{\mathrm{c}} \subseteq B$
   b) $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$
   c) $(A \setminus B)^{\mathrm{c}} \cap (B \setminus C)^{\mathrm{c}} \subseteq (A \setminus C)^{\mathrm{c}}$
   d) $A \setminus C \subseteq (A \setminus (B \setminus C)^{\mathrm{c}}) \cup (A \setminus B)$
   e) $A \subseteq A \setminus (B \cap B^{\mathrm{c}})$
   f) $(A^{\mathrm{c}} \setminus A)^{\mathrm{c}} \subseteq A$
   g) $A^{\mathrm{c}} \subseteq A^{\mathrm{c}} \setminus A$
   h) $(A \cup B) \setminus C \subseteq (A \setminus C) \cup (B \setminus C)$
   i) $B^{\mathrm{c}} \subseteq (A \setminus B) \cup (A^{\mathrm{c}} \setminus B)$
   j) $A \setminus B \subseteq B^{\mathrm{c}}$

k) $B \setminus A \subseteq B$

7. Prove the following implications:
   a) $\mathcal{U} \subseteq B \implies \mathcal{U} = B$
   b) $A \subseteq B \ \&\ A \subseteq (B \setminus C)^{\mathrm{c}} \implies A \subseteq C$
   c) $A^{\mathrm{c}} \subseteq B \cap B^{\mathrm{c}} \implies A = \mathcal{U}$
   d) $A \subseteq B \ \&\ A \subseteq B^{\mathrm{c}} \implies A = \varnothing$
   e) $A^{\mathrm{c}} = \mathcal{U} \implies A \subseteq B$
   f) $A \subseteq B \implies A \cap C \subseteq B \cap C$

8. Prove the following equivalences:
   a) $A \subseteq B \iff A^{\mathrm{c}} \cup B = \mathcal{U}$
   b) $A \not\subseteq B \iff A \cap B^{\mathrm{c}} \neq \varnothing$
   c) $A \subseteq B \iff B^{\mathrm{c}} \subseteq A^{\mathrm{c}}$
   d) $A \subseteq (B \setminus C)^{\mathrm{c}} \iff A \cap B \subseteq C$

9. Simplify the following to the form $A^{\mathrm{c}} \cup (B \triangle C)$:

$$(A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B^{\mathrm{c}} \cap C) \cup (A^{\mathrm{c}} \cap B \cap C^{\mathrm{c}}) \cup \\ \cup (A^{\mathrm{c}} \cap B \cap C) \cup (A \cap B \cap C^{\mathrm{c}}) \cup (A \cap B^{\mathrm{c}} \cap C).$$

10. Compose an example like 3.1.7.

3.2. Cartesian products, and relations

Suppose $\varphi(x)$ is an $\in$-formula as in § 3.0. Again, this formula **defines,** in $\mathcal{U}$, the set $\{x \in \mathcal{U} \colon \varphi(x)\}$. This set can be called the **interpretation** of $\varphi(x)$ in $\mathcal{U}$. The interpretation of $\varphi(x)$ may change if $\mathcal{U}$ changes. For example, the interpretation of $x \notin A$ in $\mathcal{U}$ is $\mathcal{U} \setminus A$, which depends on $\mathcal{U}$. However, as long as $\mathcal{U}$ includes A, the interpretation of $x \in A$ in $\mathcal{U}$ does not change: it is just A.

We now allow variables besides x, and we ask, for example, whether the **binary** $\in$-formula

$$x \in A \,\&\, y \in B$$

defines a set. It *does* define a set, which is denoted by

$$A \times B$$

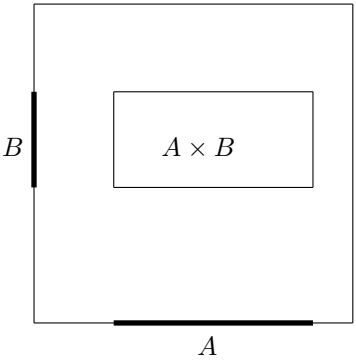


Figure 3.2. Cartesian product

and called the **Cartesian product** of A and B. This set $A \times B$ can be depicted as in Figure 3.2. If $a \in A$ and $b \in B$, then there will be an element of $A \times B$, denoted by

$$(a, b)$$

and called an **ordered pair**. Such objects will have the property that

$$(a, b) = (a', b') \iff a = a' \ \& \ b = b'; \tag{3.31}$$

consequently,

$$(a, b) \in A \times B \iff a \in A \ \& \ b \in B.$$

But what *is* an ordered pair?

So far (in this chapter), all of our sets have been Boolean combinations of given sets. But recall that the Adjunction Axiom (1.2.4) and its consequence, the Pairing Theorem (1.2.5), give alternative ways of producing new sets. If $a \neq b$, then the $\{a, b\}$ is an **(unordered) pair.**

Lemma 3.2.1. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \iff a = c \ \& \ b = d.$

Now we can define ordered pairs so as to have the desired Property (3.31): by definition,

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Note well that we make this definition solely so that ordered pairs will have Property (3.31). It is true but unimportant[1] that $\{a\} \in (a, b)$—except that, in

[1] Some discussion of this point is in [23, § 6].

the usual treatment of set-theory, one still needs the precise definition of (a, b) to justify *axiomatically* the existence of the set $A \times B$. I shall discuss this point later. Meanwhile, we can write

$$A \times B = \{(x, y) \in \mathcal{U} \times \mathcal{U} \colon x \in A \,\&\, y \in B\}.$$

Suppose now F is a $2n$-ary propositional formula. Then we have the binary $\in$-formula

$$F(x \in A_0,\ \ldots,\ x \in A_{n-1},\ y \in A_0,\ \ldots,\ y \in A_{n-1}). \tag{3·32}$$

Call this $\varphi(x, y)$. Its interpretation in $\mathcal{U}$ is a subset of $\mathcal{U} \times \mathcal{U}$, namely

$$\{(x, y) \in \mathcal{U} \times \mathcal{U} \colon \varphi(x, y)\}, \tag{3·33}$$

which consists precisely of those (c, d) in $\mathcal{U} \times \mathcal{U}$ such that

$$\widehat{F}(\vec{e}, \vec{f}) = 1,$$

where $\vec{e}$ and $\vec{f}$ are the n-ary truth assignments such that

$$e_k = 1 \iff c \in A_k,$$
$$f_k = 1 \iff d \in A_k$$

for each k in $\{0, \ldots, n-1\}$. As special cases, we have

$$\{(x, y) \in \mathcal{U} \times \mathcal{U} \colon x \in A\} = A \times \mathcal{U};$$
$$\{(x, y) \in \mathcal{U} \times \mathcal{U} \colon y \in B\} = \mathcal{U} \times B.$$

These sets are *also* the interpretations in $\mathcal{U} \times \mathcal{U}$ of $(x, y) \in A \times \mathcal{U}$ and $(x, y) \in \mathcal{U} \times B$ respectively. Hence, for example, the formulas $x \in A$ and $(x, y) \in A \times \mathcal{U}$ are interchangeable or, as we may say, **equivalent** as binary formulas. In (3·33), we can now replace $\varphi(x, y)$ with the formula

$$F((x, y) \in A_0 \times \mathcal{U},\ \ldots,\ (x, y) \in A_{n-1} \times \mathcal{U},\ (x, y) \in \mathcal{U} \times A_0,\ \ldots,\ (x, y) \in \mathcal{U} \times A_{n-1}), \tag{3·34}$$

without changing the set.

Since we have a new operation on sets, we may wonder how it interacts with the ones that we already have. Let use first establish the notational convention that $\times$ has priority over $\cap$, $\cup$, $\triangle$, and $\setminus$, but not over $^{\mathrm{c}}$, so that, for example,

$$A \times B \cap C = (A \times B) \cap C;$$
$$A \times B^{\mathrm{c}} = A \times (B^{\mathrm{c}}).$$

Then we have:

Theorem 3.2.2. *The following are set-theoretic identities:*

$$A \times (B \cap C) = A \times B \cap A \times C, \qquad (A \cap B) \times C = A \times C \cap B \times C,$$
$$A \times (B \cup C) = A \times B \cup A \times C, \qquad (A \cup B) \times C = A \times C \cup B \times C,$$
$$\mathcal{U} \times A^{\mathrm{c}} = (\mathcal{U} \times A)^{\mathrm{c}}, \qquad A^{\mathrm{c}} \times \mathcal{U} = (A \times \mathcal{U})^{\mathrm{c}}.$$

Proof. We prove the first identity in two ways; the rest are exercises.

Suppose $(a, b) \in A \times (B \cap C)$. Then $a \in A$, and $b \in B \cap C$. Hence also $b \in B$ and $b \in C$. Therefore $(a, b) \in A \times B$ and $(a, b) \in A \times C$. Consequently $(a, b) \in (A \times B) \cap (A \times C)$. Thus $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$. The reverse inclusion is an exercise.

Alternatively, by (a slight variant of) Theorem 3.0.3, we have

$$\begin{aligned} A \times (B \cap C) &= \{(x, y) \in \mathcal{U} \times \mathcal{U} \colon x \in A \,\&\, y \in B \cap C\} \\ &= \{(x, y) \in \mathcal{U} \times \mathcal{U} \colon x \in A \,\&\, y \in B \,\&\, y \in C\} \\ &= \{(x, y) \in \mathcal{U} \times \mathcal{U} \colon (x \in A \,\&\, y \in B) \,\&\, (x \in A \,\&\, y \in C)\} \\ &= \{(x, y) \in \mathcal{U} \times \mathcal{U} \colon (x, y) \in A \times B \,\&\, (x, y) \in A \times C\}, \end{aligned}$$

which is $(A \times B) \cap (A \times C)$ by definition of intersection. To save writing, we might just note that $A \times (B \cap C)$ is the interpretation of the following equivalent formulas:

$$x \in A \,\&\, y \in B \cap C, \qquad x \in A \,\&\, y \in B \,\&\, y \in C,$$
$$(x \in A \,\&\, y \in B) \,\&\, (x \in A \,\&\, y \in C), \qquad (x, y) \in A \times B \,\&\, (x, y) \in A \times C$$

—while the last formula defines $(A \times B) \cap (A \times C)$. □

The identity for $A \times B^{\mathrm{c}}$ is not so neat: see Exercise 3. Part of the last theorem can be generalized:

Theorem 3.2.3. *The equation*

$$A \times B \cap C \times D = (A \cap C) \times (B \cap D)$$

is an identity.

Proof. $A \times B \cap C \times D$ is the interpretation of

$$x \in A \,\&\, y \in B \,\&\, x \in C \,\&\, y \in D,$$

which is equivalent to

$$x \in A \,\&\, x \in C \,\&\, y \in B \,\&\, y \in D,$$

which is the interpretation of $(A \cap C) \times (B \cap D)$. □

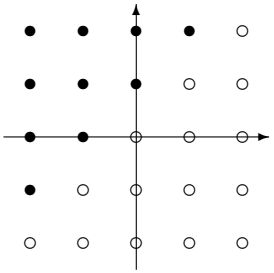


Figure 3.3. The less-than relation on $\mathbb{Z}$

For $A \times B \cup C \times D$ and $(A \times B)^{\mathrm{c}}$, see Exercise 5.

We have observed that (3.32) and (3.34) are equivalent. This suggests a further generalization: If $(R_0, \ldots, R_{n-1})$ is a list of n subsets of $\mathcal{U} \times \mathcal{U}$, and $\boldsymbol{G}$ is an n-ary propositional formula, then we have a binary $\in$-formula

$$\boldsymbol{G}((x, y) \in R_0,\ \ldots,\ (x, y) \in R_{n-1}).$$

A subset of $\mathcal{U} \times \mathcal{U}$ is a **binary relation** on $\mathcal{U}$. If $R \subseteq \mathcal{U} \times \mathcal{U}$, and $(a, b) \in R$, then we may also write

$$a\ R\ b.$$

Then $R = \{(x, y) \in \mathcal{U} \times \mathcal{U} \colon x\ R\ y\}$.

Example 3.2.4. The less-than relation on $\mathbb{Z}$ (named in § 1.3) is the set

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x < y\},$$

which can be depicted as in Figure 3.2.

There are two generalizations:

1. If $R \subseteq A \times B$, then R is a relation **from** A **to** B; then A can be called the **domain** of R, and B can be called the **co-domain** of R.
2. There are n-ary relations on $\mathcal{U}$ for every n in $\mathbb{N}$.

The first of these will be taken up in the next section. On the latter point, note that we can form an n-ary $\in$-formula

$$x_0 \in A_0 \,\&\, \ldots \,\&\, x_{n-1} \in A_{n-1};$$

its interpretation in $\mathcal{U}$ can be denoted by

$$A_0 \times \cdots \times A_{n-1}.$$

This is a subset of $\underbrace{\mathcal{U} \times \cdots \times \mathcal{U}}_{n}$, which we can also denote by

$$\mathcal{U}^n.$$

The elements of $\mathcal{U}^n$ are just the **(ordered) n-tuples,** written as one of

$$(c_0, \ldots, c_{n-1}), \qquad \vec{c}$$

where each c_k is in $\mathcal{U}$. Such an n-tuple is just what we have called a **list** of n elements of $\mathcal{U}$. In particular, an n-ary truth-assignment is an element of $\mathbb{B}^n$.

Instead of $A \times A$, we can write A^2. We can let A^1 be A itself. We can define A^3 to be $A^2 \times A$; define A^4 to be $A^3 \times A$; and so on. By our precise definition then,

$$(a_0, \ldots, a_n) = ((a_0, \ldots, a_{n-1}), a_n) = \{\{(a_0, \ldots, a_{n-1})\}, \{(a_0, \ldots, a_{n-1}), a_n\}\},$$

but this is not important; we could also use the definition

$$(a_0, \ldots, a_{n-1}) = \{\{a_0\}, \{a_0, a_1\}, \ldots, \{a_0, a_1, \ldots, a_{n-1}\}\}$$

for example. (See also § 3.6.) In any case, we should understand

$$(a_0, \ldots, a_{n-1}) = \begin{cases} a_0, & \text{if } n = 1; \\ \varnothing, & \text{if } n = 0; \end{cases}$$

that is, (a) is just a, and $(\,)$ is $\varnothing$. Then $A^1 = A$ as we said; also, $A^0 = \{\varnothing\}$, which is 1 in the von-Neumann definition of the natural numbers in § 1.2. Finally, if $\vec{a}$ is the n-tuple $(a_0, \ldots, a_{n-1})$, and $\vec{b}$ is the m-tuple $(b_0, \ldots, b_{m-1})$, then we treat the ordered pair $(\vec{a}\,, \vec{b}\,)$ as the ordered $(n+m)$-tuple $(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1})$. Then we have

$$A^m \times A^n = A^{m+n}$$

for all m and n in ω. (We do not have a meaning for A^n if n is a negative integer.)

An **n-ary relation** on $\mathcal{U}$ is a subset of $\mathcal{U}^n$. In particular, a singulary relation on $\mathcal{U}$ is just a subset of $\mathcal{U}$. A nullary relation on $\mathcal{U}$ is a subset of $\mathcal{U}^0$; which is $\{\varnothing\}$; so a nullary relation is either $\varnothing$ or $\{\varnothing\}$. In the von-Neumann definition, these sets are 0 and 1 respectively; so a nullary relation is just a truth-value.

An **n-ary predicate** is a name for an n-ary relation. An n-ary relation is then a possible **interpretation** of an n-ary predicate.

Exercises

1. Prove Lemma 3.2.1.
2. Complete the proof of Theorem 3.2.2.
3. Prove the identity $A \times B^{\mathrm{c}} = A \times \mathcal{U} \setminus \mathcal{U} \times B$.
4. Prove the identities:
   a) $(A \triangle B) \times C = A \times C \triangle B \times C$;
   b) $(A \setminus B) \times C = A \times C \setminus B \times C$.
5. Prove the identities:
   a) $A \times B \cup C \times D = ((A \cup C) \times (B \cup D) \setminus A^{\mathrm{c}} \times D^{\mathrm{c}}) \setminus C^{\mathrm{c}} \times B^{\mathrm{c}}$;
   b) $(A \times B)^{\mathrm{c}} = A^{\mathrm{c}} \times \mathcal{U} \cup \mathcal{U} \times B^{\mathrm{c}}$.

3.3. Functions

A relation R from a set A to a set B is a **function** from A to B if it has two properties:

1. For every a in A there is some b in B such that $(a, b) \in R$.
2. If R contains both (a, b) and (a, c), then $b = c$.

One might abbreviate these properties as follows:

1. $(\forall x \in A)\ (\exists y \in B)\ x\ R\ y$.
2. $(\forall x \in A)\ (\forall y \in B)\ (\forall z \in B)\ (x\ R\ y\ \ \&\ \ x\ R\ z\ \implies\ y = z)$.

Alternatively, R is a function if it has the property:

- For every a in A, there is a *unique* b in B such that $a\ R\ b$.

Unique existence—existence of exactly one—is sometimes abbreviated by the quantifier

$$\exists!.$$

Then the last property can be abbreviated:

- $(\forall x \in A)\ (\exists!\ y \in B)\ a\ R\ b$.

Often a function is denoted by a letter like f; then, instead of writing $(a, b) \in f$, or $a\ f\ b$, one writes

$$f(a) = b.$$

Suppose f is a function from A to B. This can be indicated by one of

$$f\colon A \longrightarrow B, \qquad\qquad A \xrightarrow{f} B.$$

In accordance with the definitions in the previous section, A is then the **domain** of f, and B is the **co-domain** of f. Also, f is a function **on** A, and f is a function **from** A **to** B. Functions are sometimes called **maps;** in the present case, f can be said to **map** A into B.

Considered as a string of symbols, $f(x)$ is a **term.** Then the function f might be given by the notation

$$x \longmapsto f(x),$$

and we might say that f **takes** or **sends** x to $f(x)$. As we shall see presently, the term $f(x)$ might be replaced with another term that does not contain a specific name for f itself.

Note that, considered as a set, a function uniquely determines its domain, but not its co-domain. If $f\colon A \to B$, then

$$A = \{x\colon \exists y\ f(x) = y\}, \qquad \{y\colon \exists x\ f(x) = y\} \subseteq B.$$

An n**-ary operation** on a set A is a function from A^n to A. Then there is at least one singulary operation on A, namely the **identity** on A: this is the function

$$x \longmapsto x$$

on A, which can be denoted by

$$\mathsf{id}_A.$$

More generally, if $k < n$, then there is an n-ary operation

$$(x_0, \ldots, x_{n-1}) \longmapsto x_k$$

on A. (This operation is id_A if $n = 1$ and $k = 0$.) But there are all sorts of operations besides these:

Examples 3.3.1.

1. In §1.2, the successor of a number n in $\mathbb{N}$ is denoted by n^+ or $n + 1$. This means there is a function $x \mapsto x^+$ from $\mathbb{N}$ to itself; this is a singulary operation on $\mathbb{N}$.

2. The operations $+$ and $\cdot$ named in § 1.3 are binary operations on $\mathbb{Z}$ and can be denoted by $(x, y) \mapsto x + y$ and $(x, y) \mapsto xy$ respectively.

3. Hence any arithmetic term t in an n-tuple $(x_0, \ldots, x_n)$ of variables determines the n-ary operation $\vec{x} \mapsto t$ on $\mathbb{Z}$.

4. The fundamental theorem of calculus is that if f is a *continuous* function on $\mathbb{R}$, and $a \in \mathbb{R}$, then the function $x \mapsto \int_a^x f$ is a *primitive* for f (that is, a function whose derivative is f).

Several refinements of the notion of a function are useful. Suppose again that $f\colon A \to B$. Then f is:

1) **surjective** or **onto,** if every element of B is $f(a)$ for *at least* one a in A;
2) **injective** or **one-to-one,** if every element of B is $f(a)$ for *at most* one a in A;
3) **bijective,** if it is one-to-one and onto (injective and surjective).

A surjective function is a **surjection;** an injective function is an **injection;** a bijective function is a **bijection.** An injection is also called an **embedding;** a bijection is also called a **one-to-one correspondence.** More symbolically, f is:

1) surjective, if $(\forall y \in B)\ (\exists x \in A)\ f(x) = y$;
2) injective, if $(\forall x \in A)\ (\forall y \in A)\ (f(x) = f(y) \implies x = y)$.

Examples 3.3.2.

1. id_A is a bijection.
2. The squaring function $x \mapsto x^2$ is injective on $\mathbb{N}$, but not on $\mathbb{Z}$; as a function from $\mathbb{C}$ to $\mathbb{C}$, it is surjective, but not as a function from $\mathbb{R}$ to $\mathbb{R}$.
3. The tangent-function $x \mapsto \tan x$ from $\mathbb{R}$ to $\mathbb{R}$ is surjective, but not injective.
4. The cubing function $x \mapsto x^3$ from $\mathbb{R}$ to $\mathbb{R}$ is bijective.

Again suppose $f\colon A \to B$. The **range** of f is the set

$$\{y \in B\colon (\exists x \in A)\ f(x) = y\};$$

this is a subset of the co-domain of f, and can be denoted by

$$\{f(x)\colon x \in A\},$$

or more simply by $f(A)$. However, since the latter notation suggests—usually wrongly—that A is actually an *element* of the domain of f, I prefer to use the notation

$$f[A].$$

A function is surjective if and only if its range is equal to its co-domain.

Examples 3.3.3.

1. The co-domain of $x \mapsto \sin x$ is usually considered to be $\mathbb{R}$, although the range of the function is the interval $[-1, 1]$.
2. The function $x \mapsto 1 + x^2$, as a function on $\mathbb{R}$, has range $[1, \infty)$.

Suppose also $g\colon B \to C$. The **composition** of f and g is

$$\{(x, z) \in A \times C\colon g(f(x)) = z\};$$

This can be denoted by

$$g \circ f,$$

which can be read as g composed with f. Showing that $g \circ f$ is a function is Exercise 1 below; it is Exercise 2 to show that the composition of injective functions is injective, and the composition of surjective functions is surjective.

Many of the foregoing ideas are connected by the following:

Theorem 3.3.4. *Suppose $A \neq \varnothing$ and $f\colon A \to B$.*

1. *The function f is injective if and only if $g \circ f = \mathsf{id}_A$ for some function g from B to A.*
2. *The function f is surjective if and only if $f \circ g = \mathsf{id}_B$ for some function g from B to A.*
3. *The function f is bijective if and only if $g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$ for some function g from B to A.*

Proof. 1. Suppose f is injective. Then for every b in $f[A]$, there is exactly one a in A such that $f(a) = b$. This means that the set $\{(f(x), x)\colon x \in A\}$ (which is the range of the function $x \mapsto (f(x), x)$ from A to $B \times A$) is a function from $f[A]$ to A. Since $A \neq \varnothing$, there is some c in A; then $y \mapsto c$ is a function from $B \setminus f[A]$ to A. The union of these two functions, as sets, is a function g from B to A, and $g(f(a)) = a$ for all a in A, so $g \circ f = \mathsf{id}_A$.
Suppose conversely that $g \circ f = \mathsf{id}_A$. If $f(a) = f(a')$, then $g(f(a)) = g(f(a'))$, that is, $\mathsf{id}_A(a) = \mathsf{id}_A(a')$, which means $a = a'$. Thus f is injective.

2. Suppose f is surjective. Then for every b in B, there is *at least* one a in A such that $f(a) = b$. Now we have to do something sneaky: We pick *one* such a, and define $g(b) = a$. We do this for all b in B, and this gives us g as desired. (That such picking can be done once for all is perhaps not obvious, but it is a consequence of the set-theoretic *Axiom of Choice*.)
The converse, and the remaining part, are left as an exercise. □

Theorem 3.3.5. *Suppose $f\colon A \to B$ and is bijective. Then there is* exactly one *function g from B to A such that $g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$.*

Proof. By the last theorem, there is at least one such function. Suppose g_0 and g_1 are such functions, and $b \in B$. Then $b = f(a)$ for some a in A, since f is surjective. Hence

$$g_0(b) = g_0(f(a)) = g_0 \circ f(a) = \mathsf{id}_A(a) = g_1 \circ f(a) = g_1(f(a)) = g_1(b).$$

Thus $g_0 = g_1$. □

The unique function g in the theorem is the **inverse** of f and can be denoted by

$$f^{-1}.$$

A bijection can also be called an **invertible** function.

In general, if $f\colon A \to B$ and $C \subseteq A$, then $f \cap (C \times B)$ is a function from C to B; this can be denoted by

$$f \restriction C;$$

it is the **restriction** of f to C, and its range is $f[C]$. This range is also called the **image** of C under f.

Exercises

1. Show that the composition of two functions is a function.

2. Show that the composition if injective functions is injective; of surjective, surjective.

3. Complete the proof of Theorem 3.3.4.

4. Suppose f and g are functions from A to B. For each of the relations

$$f \cup g, \qquad\qquad f \cap g,$$

   - prove whether it is always a function; and
   - prove whether it is always *not* a function.

5. Let $f\colon A \to B$ and $g\colon B \to C$.

   a) Supposing g and f are invertible, write $(g \circ f)^{-1}$ as a composition of inverses (rather than an inverse of compositions).

   b) If $g \circ f$ is injective, does it follow that f is injective?—that g is injective?

   c) Same question, with surjective for injective.

   d) Same question, with bijective for surjective.

3.4. More functions

Induced functions

If $f\colon A \to B$ and $C \subseteq A$, then we have defined $f[C]$ as a subset of B. This suggests that we have a function $X \mapsto f[X]$; but what are its domain and co-domain?

I noted at the beginning of the chapter that the sets we would discuss need only be classes. This is no longer the case. In particular, if $\mathbf{C}$ is a class, we define the *power class* of $\mathbf{C}$ to be the class of all sub*sets* of $\mathbf{C}$; there is not necessarily a class of sub*classes* of $\mathbf{C}$. The power class of a set A is denoted by

$$\mathcal{P}(A).$$

If $f\colon A \to B$, then the function $X \mapsto f[X]$ has domain $\mathcal{P}(A)$ and co-domain $\mathcal{P}(B)$.

The power class of a set is called its **power set** because of the following.

Axiom 3.4.1 (Power Set)**.** *The power class of a set is a set.*

We shall not actually use this axiom until § 3.6.

Examples 3.4.2.

1. $\mathcal{P}(\varnothing) = \{\varnothing\}$, that is, $\mathcal{P}(0) = 1$ in the definition of von Neumann;
2. $\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$, that is, $\mathcal{P}(1) = 2$.
3. $\varnothing \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$ for all sets A.

Lemma 3.4.3. *Suppose $f\colon A \to B$. Then*

$$X \subseteq Y \implies f[X] \subseteq f[Y]$$

for all subsets X and Y of A.

Proof. Suppose $x \in f[X]$. Then $x = f(u)$ for some u in X. But $X \subseteq Y$, so $u \in Y$, and hence $f(u) \in f[Y]$, that is, $x \in f[Y]$. □

Theorem 3.4.4. *Suppose $f\colon A \to B$. Then*

$$f[X \cup Y] = f[X] \cup f[Y], \tag{3.35}$$
$$f[X \cap Y] \subseteq f[X] \cap f[Y] \tag{3.36}$$

for all subsets X and Y of A.

Proof. We have that $f[X]$ and $f[Y]$ are subsets of $f[X \cup Y]$ by the last lemma. Hence

$$f[X] \cup f[Y] \subseteq f[X \cup Y]$$

by (3.29). For the reverse inclusion, suppose $x \in f[X \cup Y]$. Then $x = f(u)$ for some u in $X \cup Y$. Either $u \in X$ or $u \in Y$, hence, either $x \in f[X]$ or $x \in f[Y]$. In either case, $x \in f[X] \cup f[Y]$. This proves (3.35).

For (3.36), note that if $f[X \cap Y]$ is a subset of both $f[X]$ and $f[Y]$, by the last lemma; we are now done, by (3.28). □

The inclusion (3.36) can be strict. To see this, one need only consider a non-injective function on a set of size 2:

Example 3.4.5. If f is $\{(0,0),(1,0)\}$ and $X = \{0\}$ and $Y = \{1\}$, then $X \cap Y = \varnothing$, but $f[X] \cap f[Y] = \{0\}$.

Theorem 3.4.6. *Suppose $f\colon A \to B$.*

1. *The following are equivalent:*
   a) *f is injective.*
   b) *$f[X \cap Y] = f[X] \cap f[Y]$ for all subsets X and Y of A.*
2. *If f is injective, then*

$$f[X^{\mathrm{c}}] \subseteq (f[X])^{\mathrm{c}},$$
$$f[X \smallsetminus Y] \subseteq f[X] \smallsetminus f[Y]$$

   for all subsets X and Y of A.
3. *The following are equivalent:*
   a) *f is bijective.*
   b) *$f[X^{\mathrm{c}}] = (f[X])^{\mathrm{c}}$ for all subsets X of A.*

If $f\colon A \to B$, and $C \subseteq B$, then A has the subset

$$\{x \in A\colon f(x) \in C\},$$

which can be denoted by

$$f^{-1}[C];$$

this is the **pre-image** of C under f. Thus we have a function

$$Y \longmapsto f^{-1}[Y]$$

with domain $\mathcal{P}(B)$ and co-domain $\mathcal{P}(A)$. Note well that this function exists, whether f is invertible or not. The function $Y \mapsto f^{-1}[Y]$ behaves more nicely than $X \mapsto f[X]$ with respect to the Boolean operations:

Theorem 3.4.7. *Suppose $f\colon A \to B$. Then*

$$f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y], \tag{3.37}$$
$$f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y], \tag{3.38}$$
$$f^{-1}[X^{\mathrm{c}}] = (f^{-1}[X])^{\mathrm{c}}, \tag{3.39}$$
$$f^{-1}[X \smallsetminus Y] = f^{-1}[X] \smallsetminus f^{-1}[Y] \tag{3.40}$$

for all subsets X and Y of B.

Proof. Exercise. Note that, by adequacy of the signature $\{\&, \neg\}$, the other equations follow from (3.38) and (3.39). □

Operations on relations

It is possible to give a neat account of functions by first defining the composition of *relations*. Suppose $R \subseteq A \times B$ and $S \subseteq B \times C$. Then the **composition** of R and S is the set

$$\{(x, z) \in A \times C : (\exists y \in B)\ (x\ R\ y\ \ \&\ \ y\ S\ z)\},$$

which can be denoted by

$$S \circ R.$$

Note well the order in which R and S are written, which seems unnatural, but agrees with the notation for the composition of functions. At the expense of introducing a new symbol, I propose to write[2]

$$R/S$$

for $S \circ R$.

The relation R from A to B has a **converse,** namely, the relation

$$\{(y, x) \in B \times A : x\ R\ y\}$$

[2] Tarski [52, § 28, p. 92] and Suppes [49, § 3.1, Definition 7, p. 63] are among those who use this notation.

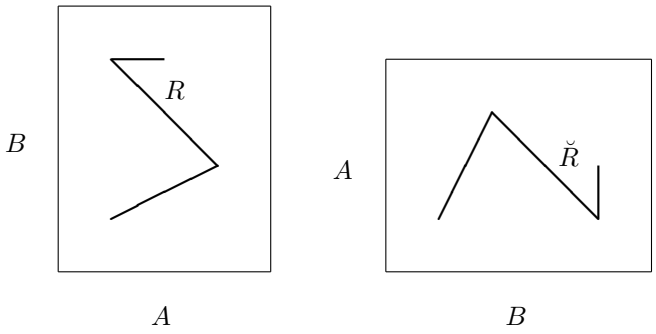


Figure 3.4. Converse of a relation

from B to A; it can be denoted by

$$\breve{R}.$$

(See Figure 3.4.) This is sometimes denoted by R^{-1}, but such notation can be misleading.

Finally, the binary relation of **equality** on A is just the set

$$\{(x, y) \in A \times A : x = y\}.$$

We can also call this the **diagonal** on A, and give it the symbol

$$\Delta_A.$$

(The delta stands for diagonal; see Figure 3.5.)

We can now make the following definitions: R is

1) **full,** if $\Delta_A \subseteq R/\breve{R}$;
2) **functional,** if $\breve{R}/R \subseteq \Delta_B$.

Theorem 3.4.8. *Let $R \subseteq A \times B$. Then R is a function from A to B if and only if R is full and functional (as a relation from A to B).*

Proof. Exercise. □

We have alternative characterizations for notions in § 3.3:

Theorem 3.4.9. *Suppose $f\colon A \to B$.*

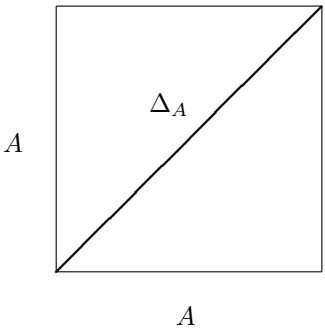


Figure 3.5. Diagonal on a set

1. *f is surjective if and only if $\Delta_B \subseteq \breve{f}/f$.*
2. *f is injective if and only if $f/\breve{f} \subseteq \Delta_A$.*
3. *f is bijective if and only if $\breve{f}/f = \Delta_B$ and $f/\breve{f} = \Delta_A$.*

Exercises

1. Prove Theorem 3.4.6.
2. Prove Theorem 3.4.7.
3. Prove Theorem 3.4.8.
4. Prove Theorem 3.4.9.

3.5. First-order logic

First-order logic provides a formal way to talk about particular operations and relations. It allows for a precise definition of the *context,* mentioned in § 1.1, in which a mathematical proposition is true or false. First-order logic is a large subject; this section will be only a cursory treatment. However, we have already mentioned the ingredients of first-order logic, in an informal way at least. A *signature* for a *first-order logic* consists of *constants,*[3] *function-symbols,* and

[3]Constants are also called *constant-symbols.*

predicates.[4] A *structure* in a signature $\mathcal{L}$ is a non-empty set A along with a function that takes:

1) each constant of $\mathcal{L}$ to an element of A;
2) each function-symbol of $\mathcal{L}$ to an operation on A;
3) each predicate of $\mathcal{L}$ to a relation on A.

Thus the elements of $\mathcal{L}$ *symbolize* elements of A and operations and relations on A. More elements and operations are symbolized by *terms*, which are strings made of constants, function-symbols, and *variables*. More relations are symbolized by *formulas*. The simplest formulas are the *atomic*[5] formulas, which consist of terms joined by the sign of equality or by a predicate. Atomic formulas can be preceded by quantifiers (with variables) or combined by means of Boolean connectives; formulas in general are obtained in this way. New constants symbolizing particular elements of A can be used as *parameters* in terms and formulas.

Example 3.5.1. The set $\mathbb{Z}$ of integers can be understood as a structure in the signature $\{0, 1, -, +, \cdot, <\}$ (see § 1.3 (1.11)); a term in this signature (with parameters from $\mathbb{Z}$ as desired) is an *arithmetic term* as defined in § 1.3. Diophantine equations and arithmetic inequalities are the atomic formulas in this signature.

The terminology of first-order logic is a means to give a precise but general account of some ideas that one encounters in high-school mathematics.

Structures

By formal definition, a **structure**is an ordered pair $(A, \mathcal{I})$—which can also be referred to as $\mathfrak{A}$—where:

1) A is a non-empty set, which is called the **universe** of the structure;
2) $\mathcal{I}$ is a function, written also as

$$s \longmapsto s^{\mathfrak{A}},$$

   whose domain $\mathcal{L}$ is called the **signature** of the structure;
3) $s^{\mathfrak{A}}$ is either an element of A or an n-ary operation or relation on A for some positive integer n, for each s in $\mathcal{L}$.

[4] Predicates are also called *relation-symbols*.

[5] From the Greek ἄτομος uncuttable, not compound, from τόμος a slice.

Here $\mathfrak{A}$ may be called a structure **of** $\mathcal{L}$, or an **$\mathcal{L}$-structure.** If $\mathcal{L} = \{s_0, s_1, \dots\}$, then $\mathfrak{A}$ can be written as

$$(A, s_0{}^{\mathfrak{A}}, s_1{}^{\mathfrak{A}}, \dots),$$

or just as $(A, s_0, s_1, \dots)$ unless ambiguity would result (that is, unless another structure of interest has the same universe and signature as $\mathfrak{A}$). Moreover, if the intended signature is clear, then $\mathfrak{A}$ may be written simply as A; that is, the universe may stand for the structure. The function $\mathcal{I}$ is almost never referred to, except in general accounts like this one.

Examples 3.5.2. The following are structures:

1) $(\mathbb{N}, {}^+, 0)$, or more briefly $\mathbb{N}$ (see § 1.2);
2) the power-set structure on a non-empty set Ω, namely

$$(\mathcal{P}(\Omega), \varnothing, \Omega, \cap, \cup, {}^{\mathrm{c}}, \subseteq);$$

3) the **truth-structure**[6]

$$(\mathbb{B}, 0, 1, \&, \vee, \neg, \vDash),$$

where $\vDash$ is the binary relation $\{(0,0), (0,1), (1,1)\}$ on $\mathbb{B}$.

The last two examples are the same if the elements of $\mathbb{B}$ are von-Neumann natural numbers and Ω is the von-Neumann natural number 1. Propositional logic studies the truth-structure. The area of mathematics and logic called **model-theory** studies *all* structures.

When $\mathcal{I}$ is as above in the structure $(A, \mathcal{I})$, and s is an element of $\mathcal{L}$, then:

1) $s^{\mathfrak{A}}$ is called the **interpretation** in $\mathfrak{A}$ of s;
2) s is called a **symbol** for $s^{\mathfrak{A}}$.

So s is one of the following, according to its interpretation:

1) a **constant;**
2) an **n-ary function-symbol** for some positive n in ω;
3) an **n-ary predicate** (or **relation-symbol**) for some positive n in ω.

Since nullary operations on A can be considered as elements of A, a constant can be considered as a nullary function-symbol.

Here are some observations about the definition of structure:

1. I am following the old convention[7] of denoting the universe of a structure by a Roman letter, and the structure itself by the corresponding Fraktur or Gothic letter. One might not bother to make a typographical distinction between a

[6] This is not a standard term.

[7] Used for example by Chang and Keisler [7]. Recent writers (as Marker [33] and Rothmaler [42]) use 'calligraphic' letters, not Fraktur:

structure and its universe. Indeed, as suggested in the examples, the distinction is not easy to make with standard structures like $\mathbb{B}$ or $\mathbb{Z}$ (which are commonly denoted by letters in a so-called blackboard-bold font).

2. Similarly, it is not always easy or convenient to distinguish in writing between a symbol and its interpretation.

3. In a structure $(A, \mathcal{I})$, the **interpretation-function** $\mathcal{I}$ could be considered to carry, within itself, the universe A. In any case, A and $\mathcal{I}$ work together to provide interpretations of the symbols in $\mathcal{L}$ *as* elements of, or operations or relations on, a certain set, namely A itself. That's all a structure is: something that provides a mathematical interpretation for certain symbols. What makes model-theory interesting is that the same symbols can have different interpretions. Here begins the distinction between **syntax** (formal symbolism) and **semantics** (mathematical meaning).[8]

Terms and formulas

The **terms** of a first-order signature $\mathcal{L}$ are conveniently written in Polish notation (see § 2.1). First, we introduce a list

$$x_0, x_1, x_2, \ldots$$

of **variables** (that is, **individual variables**: variables standing for *individual* elements of a universe). Then, by definition,

1) all variables are terms of $\mathcal{L}$;
2) all constants of $\mathcal{L}$ are terms of $\mathcal{L}$;
3) if f is an n-ary function-symbol in $\mathcal{L}$, and $(t_0, \ldots, t_{n-1})$ is a list of n terms of $\mathcal{L}$, then

$$f t_0 \cdots t_{n-1}$$

is a term of $\mathcal{L}$; if f is binary, then $f t_0 t_1$ may also be written as

$$(t_0\ f\ t_1).$$

For a structure with universe:	A	B	C	...	M	N	...
I write:	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$	...	$\mathfrak{M}$	$\mathfrak{N}$	...
others may write:	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	...	$\mathcal{M}$	$\mathcal{N}$	...

Another option, used by Hodges [27], is to use an ordinary letter like A for a structure, and then $\mathrm{dom}(A)$ for its universe. (Here dom stands for *domain*.)

[8] The distinction was alluded to in § 1.9. In propositional logic, formal entailment ($\vdash$) can be understood as a syntactic notion, while logical entailment ($\models$) is semantic.

Finally, singulary function-symbols are sometimes written as superscripts on their arguments, as in n^+ in § 1.2 (1.6) and A^c in § 1.9 (1.24).

The **atomic formulas** are defined similarly:

1. If t_0 and t_1 are terms of $\mathcal{L}$, then the equation
$$t_0 = t_1$$
is an atomic formula of $\mathcal{L}$;
2. If R is an n-ary predicate of $\mathcal{L}$, and $(t_0, \ldots, t_{n-1})$ is a list of n terms of $\mathcal{L}$, then the string
$$Rt_0 \cdots t_{n-1}$$
is a term of $\mathcal{L}$; if R is binary, then Rt_0t_1 may also be written as
$$t_0 \; R \; t_1.$$

Finally, **formulas** in general can be defined:

1. Atomic formulas of $\mathcal{L}$ are formulas of $\mathcal{L}$.
2. If φ is a formula of $\mathcal{L}$, then so is $\neg\varphi$.
3. If φ and ψ are formulas of $\mathcal{L}$, then $(\varphi \,\&\, \psi)$ is a formula of $\mathcal{L}$.
4. If φ is a formula of $\mathcal{L}$, and x is an individual variable, then $\exists x \; \varphi$ is a formula of $\mathcal{L}$.

These are the **first-order formulas** in the signature $\mathcal{L}$; they constitute the **first-order logic** in that signature. We can use other connectives in addition to, or instead of, $\&$ and $\Rightarrow$. One will generally want to use an adequate signature for propositional logic, like $\{\neg, \&\}$ (Theorem 2.5.3) or $\{\neg, \Rightarrow\}$ (by § 2.5, Exercise 2). Once the criterion of adequacy is met, then using fewer symbols makes the ensuing definitions and proofs easier to write down.

We can also use the quantifier $\forall$; but formulas using $\forall$ can be rewritten with $\exists$ alone by means of (1.25) and (1.26) in § 1.9.

It is standard to write a formula $\neg(t_0 = t_1)$ as $t_0 \neq t_1$.

In the definition of formula, if the last condition is removed, then what is defined is the **quantifier-free formulas** of $\mathcal{L}$.

Interpretations of terms

A term t can be called n**-ary** if the set of its variables is a subset of $\{x_k : k < n\}$; then t is interpreted in an $\mathcal{L}$-structure $\mathfrak{A}$ as an n-ary operation $t^{\mathfrak{A}}$ on A. The possibility that $n = 0$ is allowed; in that case, t is **nullary** or **constant,** and its interpretation in $\mathfrak{A}$ is just an element of A. The precise definition is what one should expect:

1. If $k < n$, then the variable x_k is an n-ary term; as such, it is interpreted in $\mathfrak{A}$ as the n-ary operation $\vec{x} \mapsto x_k$ on A. (Here necessarily $n > 0$.)
2. Every constant c is an n-ary term, interpreted in $\mathfrak{A}$ as the constant n-ary operation $\vec{x} \mapsto c^{\mathfrak{A}}$ on A. (If $n = 0$, then this operation can be understood as the element $c^{\mathfrak{A}}$ of A.)
3. If $(t_0, \dots, t_{k-1})$ is a list of n-ary terms, and f is a k-ary function-symbol, then the term $ft_0 \cdots f_{k-1}$ is n-ary and, as such, is interpreted in $\mathfrak{A}$ as the n-ary operation
$$\vec{x} \longmapsto f^{\mathfrak{A}}({t_0}^{\mathfrak{A}}(\vec{x}), \dots, {t_{k-1}}^{\mathfrak{A}}(\vec{x}))$$
on A. (If $n = 0$, the interpretation is just the element $f^{\mathfrak{A}}({t_0}^{\mathfrak{A}}, \dots, {t_{k-1}}^{\mathfrak{A}})$ of A.)

Example 3.5.3. In $\mathbb{Z}$, the ternary terms $(x_0 \cdot (x_1 + x_2))$ and $((x_0 \cdot x_1) + (x_0 \cdot x_2))$ have the same interpretation, namely the ternary operation
$$(x, y, z) \mapsto x(y + z)$$
on $\mathbb{Z}$. We could also write this operation more precisely as $(x, y, z) \mapsto x \cdot^{\mathbb{Z}} (y +^{\mathbb{Z}} z)$. (See § 1.3 (1.8).)

Interpretations of formulas

Interpretations of formulas take longer to define precisely, but the idea is that $\neg$, $\&$, and $\exists$ symbolize complementation, intersection, and *projection* respectively. An *atomic* formula φ can be called n**-ary** if the set of its variables is a subset of $\{x_i : i < n\}$. Then φ is interpreted in a structure $\mathfrak{A}$ as an n-ary relation $\varphi^{\mathfrak{A}}$ on A. This relation $\varphi^{\mathfrak{A}}$ is the **solution set** in $\mathfrak{A}$ of the formula φ. In particular:

$$(t_0 = t_1)^{\mathfrak{A}} = \{\vec{x} \in A^n : {t_0}^{\mathfrak{A}}(\vec{x}) = {t_1}^{\mathfrak{A}}(\vec{x})\}, \tag{3.41}$$
$$(Rt_0 \cdots t_{k-1})^{\mathfrak{A}} = \{\vec{x} \in A^n : ({t_0}^{\mathfrak{A}}(\vec{x}), \dots, {t_{k-1}}^{\mathfrak{A}}(\vec{x})) \in R^{\mathfrak{A}}\}. \tag{3.42}$$

Example 3.5.4. The interpretation of the equation
$$((x_0 \cdot x_0) + (x_1 \cdot x_1)) = 25$$
(usually written as ${x_0}^2 + {x_1}^2 = 25$) in $\mathbb{R}$ is a circle of radius 5 and center $(0, 0)$; see Fig. 3.6. The interpretation in $\mathbb{Z}$ consists of the integer points on this circle, namely $(\pm 5, 0)$, $(\pm 4, 3)$, $(\pm 4, -3)$, $(\pm 3, 4)$, $(\pm 3, -4)$, and $(0, \pm 5)$. The interpretation of ${x_0}^2 + {x_1}^2 < 25$ in $\mathbb{R}$ is the interior of the disk bounded by the circle.

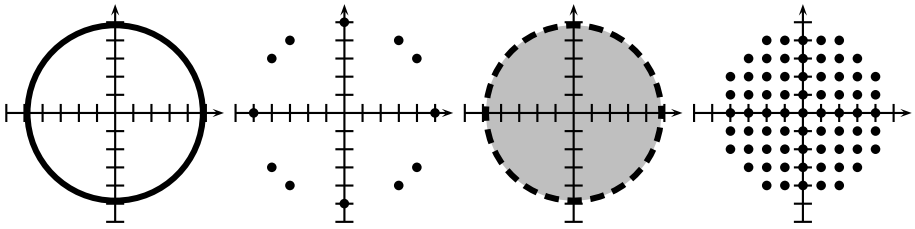


Figure 3.6. Interpretations of ${x_0}^2 + {x_1}^2 = 25$ and ${x_0}^2 + {x_1}^2 < 25$.

In the sense described in § 3.2, a nullary relation is a truth-value, 0 or 1. If $n = 0$, then (3.41) and (3.42) can be written as:

$$(t_0 = t_1)^{\mathfrak{A}} = \begin{cases} 1, & \text{if } {t_0}^{\mathfrak{A}} = {t_1}^{\mathfrak{A}}, \\ 0, & \text{if } {t_0}^{\mathfrak{A}} \neq {t_1}^{\mathfrak{A}}; \end{cases} \tag{3.43}$$

$$(Rt_0 \cdots t_{k-1})^{\mathfrak{A}} = \begin{cases} 1, & \text{if } ({t_0}^{\mathfrak{A}}, \ldots, {t_{k-1}}^{\mathfrak{A}}) \in R^{\mathfrak{A}}, \\ 0, & \text{if } ({t_0}^{\mathfrak{A}}, \ldots, {t_{k-1}}^{\mathfrak{A}}) \notin R^{\mathfrak{A}}. \end{cases} \tag{3.44}$$

Quantifiers complicate matters, such as defining when a formula is n-ary. Assume that we *have* defined this, and that φ and ψ are arbitrary n-ary formulas, whose interpretations $\varphi^{\mathfrak{A}}$ and $\psi^{\mathfrak{A}}$ are n-ary relations on A. Then the interpretations of $\neg\varphi$ and $(\varphi \,\&\, \psi)$ are given by

$$(\neg\varphi)^{\mathfrak{A}} = A^n \smallsetminus \varphi^{\mathfrak{A}} = (\varphi^{\mathfrak{A}})^{\mathrm{c}};$$
$$(\varphi \,\&\, \psi)^{\mathfrak{A}} = \varphi^{\mathfrak{A}} \cap \psi^{\mathfrak{A}}.$$

Now we have defined the interpretations of all *quantifier-free* formulas.

Suppose φ is an $(n+1)$-ary formula. Then $(\exists x_n\, \varphi)^{\mathfrak{A}}$ is an n-ary relation on A, namely the set of all $(a_0, \ldots, a_{n-1})$ in A^{n-1} such that $(a_0, \ldots, a_{n-1}, b) \in \varphi^{\mathfrak{A}}$ for *some* b in A. This means

$$(\exists x_n\, \varphi)^{\mathfrak{A}} = \pi_n^{n+1}[\varphi^{\mathfrak{A}}], \tag{3.45}$$

where π_n^{n+1} is the function

$$(x_0, \ldots, x_{n-1}, x_n) \longmapsto (x_0, \ldots, x_{n-1}) \tag{3.46}$$

from A^{n+1} to A^n; such a function can be called a **projection.** (See Figure 3.7 and § 3.7.) Note then that the formula $\exists x_n\, \varphi$ is considered as n-ary, not $(n+1)$-

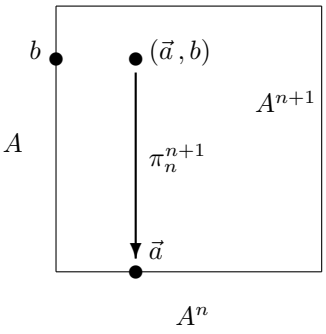


Figure 3.7. Projection

ary, even though it contains the variable x_n. The point is that this variable is not *free* in the formula; it is only *bound*.

Example (3.5.4 continued)**.** The formula $\exists x_1\ {x_0}^2 + {x_1}^2 = 25$ is singulary. Its interpretation in $\mathbb{R}$ is the interval $[-5, 5]$; in $\mathbb{Z}$, the set $\{-5, -4, -3, 0, 3, 4, 5\}$.

The set $\mathrm{fv}(\varphi)$ of **free variables**in a formula φ is defined recursively.

1. $\mathrm{fv}(\varphi)$ is the set of variables appearing in φ, if φ is atomic.
2. $\mathrm{fv}(\neg\varphi) = \mathrm{fv}(\varphi)$.
3. $\mathrm{fv}(\varphi \,\&\, \psi) = \mathrm{fv}(\varphi) \cup \mathrm{fv}(\psi)$.
4. $\mathrm{fv}(\exists x\ \varphi) = \mathrm{fv}(\varphi) \smallsetminus \{x\}$.

Thus quantifiers **bind** variables, making them not free.

Example 3.5.5. Suppose R and S are binary predicates. Then the free variables of

$$\exists x\ (x\ R\ y \,\&\, x\ S\ z)$$

are y and z, but the free variables of

$$\exists x\ x\ R\ y \,\&\, x\ S\ z$$

are x, y, and z.

The second formula in the example is complicated by having bound *occurrences* of x, even though x is a free variable of the formula. In practice one avoids this situation by using instead a formula like $\exists u\ u\ R\ y \,\&\, x\ S\ z$. For lack of a better term, let us refer to such a formula as **good.** There is a recursive definition of good formulas:

1. Atomic formulas of $\mathcal{L}$ are good formulas of $\mathcal{L}$.
2. If φ is a good formula of $\mathcal{L}$, then so is $\neg\varphi$.
3. If φ and ψ are good formulas of $\mathcal{L}$, and every variable that occurs in both formulas is a *free* variable of both formulas, then $(\varphi \& \psi)$ is a good formula of $\mathcal{L}$.
4. If φ is a good formula of $\mathcal{L}$, and x is a free variable of φ, then $\exists x\ \varphi$ is a good formula of $\mathcal{L}$.

Example 3.5.6. If φ and ψ are formulas, then so are $\exists x\ \varphi \& \exists x\ \psi$ and $\exists x\ \exists x\ \varphi$; but these are not *good* formulas.

Lemma 3.5.7. *Suppose x is a free variable of a good formula φ, and c is a constant.*

1. *In φ, the variable x never occurs right after $\exists$.*
2. *The result of replacing each occurrence of x in φ with c is a good formula.*

We never need work with any formulas other than good formulas. Also, restricting our attention to good formulas makes some general definitions easier. An arbitrary formula is **n-ary** if its *free* variables are among $x_0, \ldots, x_{n-1}$. If φ is such a formula, we may write it as

$$\varphi(x_0, \ldots, x_{n-1}).$$

Suppose in particular φ is a *good* formula. If $t_0, \ldots, t_{n-1}$ are terms, we denote by

$$\varphi(t_0, \ldots, t_{n-1})$$

the formula that results from substituting t_k for each occurrence of x_k in φ, *provided* x_k is actually a free variable of φ. If φ is not necessarily good, then $\varphi(t_0, \ldots, t_{n-1})$ is the result of substituting t_k for each free *occurrence* of x_k; but then one must define the free occurrences of variables. We avoid having to do this by restricting our attention to good formulas.

Example 3.5.8. If φ is ternary, and ψ is $\exists x_1\ \varphi$, then ψ is also ternary, but $\psi(c_0, c_1, c_2)$ is $\exists x_1\ \varphi(c_0, x_1, c_2)$.

The notation for substitution can be modified in an obvious way. If φ has at most one variable, x (which could be x_{1066}, for all we know), then we can write φ as $\varphi(x)$; then $\varphi(t)$ is the result of substituting t for x in φ, as long as x really is a free variable of φ; otherwise $\varphi(t)$ is just φ.

A nullary formula is a **sentence.** In a given signature $\mathcal{L}$, a sentence σ is either **true** or **false** in a structure $\mathfrak{A}$; if true, we write

$$\mathfrak{A} \vDash \sigma; \tag{3·47}$$

otherwise, $\mathfrak{A} \nvDash \sigma$. The definition is recursive:

1. If σ is atomic, then
$$\mathfrak{A} \vDash \sigma \iff \sigma^{\mathfrak{A}} = 1.$$
2. If σ is $\neg\tau$, then
$$\mathfrak{A} \vDash \sigma \iff \mathfrak{A} \nvDash \tau.$$
3. If σ is $\tau \,\&\, \rho$, then
$$\mathfrak{A} \vDash \sigma \iff \mathfrak{A} \vDash \tau \;\&\; \mathfrak{A} \vDash \rho.$$
If σ is $\exists x\, \varphi$, then $\mathfrak{A} \vDash \sigma$ if and only if
$$\mathfrak{A}' \vDash \varphi(c_b)$$
for *some* element b of A, where c_b is a new constant, and $\mathfrak{A}'$ is the same as $\mathfrak{A}$, except that it interprets c_b as b.

Another way to write the last condition is as follows. Given the structure $\mathfrak{A}$ of $\mathcal{L}$, we let $\mathcal{L}(A)$ be $\mathcal{L}$, together with a new constant c_b for each element b of A. Then we define $\mathfrak{A}_A$ as a structure of $\mathcal{L}(A)$ in the obvious way: it interprets symbols of $\mathcal{L}$ as $\mathfrak{A}$ does, and it interprets each new constant c_b as b. If φ is a quantifier-free formula of $\mathcal{L}(A)$, then we can denote by $\varphi^{\mathfrak{A}}$ the interpretation of φ in $\mathfrak{A}_A$. If σ is a sentence of $\mathcal{L}(A)$, then we write $\mathfrak{A} \vDash \sigma$ if σ is true in $\mathfrak{A}_A$. Usually we denote the constant c_b by b. If σ is $\exists x\, \varphi$, then we have simply that $\mathfrak{A} \vDash \sigma$ if and only if

$$\mathfrak{A} \vDash \varphi(b)$$

for some element b of A.

The following is an easy consequence of the definitions.

Lemma 3.5.9. *In some signature, if $\mathfrak{A}$ is a structure, and φ is a quantifier-free n-ary formula, then $\varphi^{\mathfrak{A}}$ is the set of all $\vec{b}$ in A^n such that*

$$\mathfrak{A} \vDash \varphi(\vec{b}).$$

Now we can use the lemma as a *definition* of $\varphi^{\mathfrak{A}}$ for arbitrary formulas φ. Then the following is also easy.

Lemma 3.5.10. *In some signature, if $\mathfrak{A}$ is a structure, and φ is a quantifier-free $(n+1)$-ary formula, then*

$$(\exists x_n\, \varphi)^{\mathfrak{A}} = \pi_n^{n+1}[\varphi^{\mathfrak{A}}].$$

Entailment

Suppose σ is a sentence of some signature $\mathcal{L}$, and $\mathfrak{A}$ is a structure of $\mathcal{L}$. If σ is true in $\mathfrak{A}$, then we may say that $\mathfrak{A}$ is a **model** of σ. More generally, if Γ is a set of sentences of $\mathcal{L}$, and each sentence in Γ is true in $\mathfrak{A}$, then $\mathfrak{A}$ is a **model** of Γ; in this case, we may write

$$\mathfrak{A} \vDash \Gamma. \tag{3.48}$$

If σ is true in *every* model of Γ, then σ is a **logical consequence** of Γ, or Γ **logically entails** σ, and we write

$$\Gamma \vDash \sigma. \tag{3.49}$$

In case $\Gamma = \{\sigma_0, \ldots, \sigma_{n-1}\}$, we may write also

$$\sigma_0, \ldots, \sigma_{n-1} \vDash \sigma.$$

If $n = 0$ here, that is, Γ is empty, then we write

$$\vDash \sigma;$$

this means σ is true in every structure of $\mathcal{L}$, or in other words σ is a **validity.**

Note well that the semantic turnstile $\vDash$ has completely different meanings in (3.48) and (3.49). To avoid confusion, one might prefer to write (3.48) as

$$\vDash_{\mathfrak{A}} \Gamma.$$

Let us now permit $\Rightarrow$ in formulas, and define interpretations so that

$$(\varphi \Rightarrow \psi)^{\mathfrak{A}} = (\neg(\varphi \,\&\, \neg\psi))^{\mathfrak{A}}.$$

Let us also permit $\forall$ in formulas, so that

$$(\forall x\ \varphi)^{\mathfrak{A}} = (\neg\exists x\ \neg\varphi)^{\mathfrak{A}}.$$

A **generalization** of a formula φ is a *sentence* of the form $\forall u_0 \cdots \forall u_{n-1}\ \varphi$. A **tautology** is a sentence $\boldsymbol{F}(\sigma_0, \ldots, \sigma_{n-1})$, where $\boldsymbol{F}$ is a tautology of propositional logic.

Let $\mathcal{L}$ be a signature with infinitely many constants. We can now define a proof-system for $\mathcal{L}$, in the sense of § 2.8, as follows. The only rule of inference is Detachment. The axioms are defined recursively:

1. Every tautology is an axiom.

2. For all constants c and d and all singulary formulas φ of $\mathcal{L}$, the following are axioms:

$$c = c, \qquad c = d \Rightarrow \varphi(c) \Rightarrow \varphi(d).$$

3. For all singulary formulas φ and ψ of $\mathcal{L}$ with free variable x, and all sentences σ of $\mathcal{L}$, the following are axioms:

$$\forall x\ (\varphi(x) \Rightarrow \psi(x)) \Rightarrow \forall x\ \varphi(x) \Rightarrow \forall x\ \psi(x),$$
$$\forall x\ (\sigma \Rightarrow \psi(x)) \Rightarrow \sigma \Rightarrow \forall x\ \psi(x).$$

4. For all singulary formulas φ of $\mathcal{L}$ with free variable x, the following is an axiom:

$$\exists x\ \varphi(x) \Rightarrow \neg\forall x\ \neg\varphi(x).$$

5. If $\varphi(x)$ is a formula of $\mathcal{L}$ in which a constant c of $\mathcal{L}$ does not appear, and $\varphi(c)$ is an axiom, then the following is an axiom:

$$\forall x\ \varphi(x).$$

As in § 2.8, if Γ is a set of sentences, and σ is a sentence, we write

$$\Gamma \vdash \sigma \tag{3.50}$$

if there is a formal proof of σ from Γ in the proof-system just defined. In this case, we may say that σ is **deducible** from Γ.

The set of sentences deducible from a set Γ is recursively defined:

1. It contains the axioms.
2. It contains the sentences in Γ.
3. If it contains σ and $\sigma \Rightarrow \tau$, then it contains τ.

This allows the use of **induction** to prove statements about those sentences.

Note that, by assuming that $\mathcal{L}$ contains infinitely many constants, we ensures that, if Γ does not formally entail σ in $\mathcal{L}$, then neither does it do so in a larger signature.

Theorem 3.5.11 (Soundness)**.** *If* $\Gamma \vdash \sigma$*, then* $\Gamma \vDash \sigma$*.*

Proof. We use induction. The claim is trivially true when $\sigma \in \Gamma$. The claim is true when σ is an axiom, since in that case $\vDash \sigma$ (exercise). Finally, suppose the claim is true when σ is ρ and when σ is $\rho \Rightarrow \tau$. If these sentences are deducible from Γ, then by inductive hypothesis $\Gamma \vDash \rho$ and $\Gamma \vDash \rho \Rightarrow \tau$; therefore $\Gamma \vDash \tau$. □

The expression in (3.50) can be called a **sequent.** We usually do not write down formal proofs; we show that they exist by considering sequents.

Theorem 3.5.12 (Detachment)**.** *If* $\Gamma \vdash \rho$*, and* $\Gamma \vdash \rho \Rightarrow \sigma$*, then* $\Gamma \vdash \sigma$*.*

Proof. If $\alpha_0, \ldots, \alpha_m$ is a formal proof of ρ from Γ, and $\beta_0, \ldots, \beta_n$ is a formal proof of $\rho \Rightarrow \sigma$ from Γ, then

$$\alpha_0, \ldots, \alpha_m, \beta_0, \ldots, \beta_n, \sigma$$

is a formal proof of σ from Γ. □

Theorem 3.5.13 (Deduction)**.** *If* $\Gamma \cup \{\sigma\} \vdash \tau$*, then*

$$\Gamma \vdash \sigma \Rightarrow \tau.$$

Proof. We use induction on τ. There are three cases to consider.

1. If τ is an axiom or an element of Γ, then

$$\begin{array}{ll} \Gamma \vdash \tau, & \\ \quad \vdash \tau \Rightarrow \sigma \Rightarrow \tau, & \text{[tautology]} \\ \Gamma \vdash \sigma \Rightarrow \tau. & \text{[Detachment]} \end{array}$$

2. If τ is σ, then $\sigma \Rightarrow \tau$ is a tautology, so again the claim follows.

3. The last possibility is that ρ and $\rho \Rightarrow \theta$ are deducible from $\Gamma \cup \{\sigma\}$, and the claim holds for each of these two sentences. Then

$$\begin{array}{ll} \Gamma \vdash \sigma \Rightarrow \rho, & \text{[inductive hyp.]} \\ \Gamma \vdash \sigma \Rightarrow \rho \Rightarrow \theta, & \text{[inductive hyp.]} \\ \quad \vdash (\sigma \Rightarrow \rho) \Rightarrow (\sigma \Rightarrow \rho \Rightarrow \theta) \Rightarrow \sigma \Rightarrow \theta, & \text{[tautology]} \\ \Gamma \vdash \sigma \Rightarrow \theta. & \text{[Detachment (twice)]} \end{array}$$ □

Theorem 3.5.14 (Generalization)**.** *If* $\Gamma \vdash \varphi(c)$*, where* x *is free in* $\varphi(x)$*, and* c *does not occur in* $\varphi(x)$ *or in any sentence of* Γ*, then*

$$\Gamma \vdash \forall x\, \varphi(x).$$

Proof. The claim is true when $\varphi(c)$ is an axiom. The claim is vacuously true when $\varphi(c)$ is in Γ, since then c does occur in a sentence of Γ. The remaining possibility is that $\Gamma \vdash \sigma$ and $\Gamma \vdash \sigma \Rightarrow \varphi(c)$. If c does not occur in σ, then we may assume $\Gamma \vdash \forall x\, (\sigma \Rightarrow \varphi(x))$. By Deduction from the appropriate axiom, $\Gamma \vdash \forall x\, \varphi(x)$. The argument is nearly the same if c does occur in σ. □

Theorem 3.5.15 (Tautology)**.** *If in propositional logic,* $\boldsymbol{F}_0, \ldots, \boldsymbol{F}_{m-1} \vDash \boldsymbol{G}$*, and in first-order logic,* $\Gamma \vdash \boldsymbol{F}_k(\sigma_0, \ldots, \sigma_{n-1})$ *when* $k < n$*, then*

$$\Gamma \vdash \boldsymbol{G}(\sigma_0, \ldots, \sigma_{n-1}).$$

Proof. Use the tautology

$$\boldsymbol{F}_0(\sigma_0, \ldots, \sigma_{n-1}) \Rightarrow \ldots \Rightarrow \boldsymbol{F}_{m-1}(\sigma_0, \ldots, \sigma_{n-1}) \Rightarrow \boldsymbol{G}(\sigma_0, \ldots, \sigma_{n-1}). \qquad \square$$

Theorem 3.5.16 (Equality)**.** $\vdash c = d \Rightarrow d = c$*.*

Proof. It is an axiom that $c = d \Rightarrow d = d \Rightarrow d = c$. $\square$

A sentence $\sigma \,\&\, \neg\sigma$ is a **contradiction.** A set Γ of sentences is **consistent** if it does not formally entail a contradiction.

Lemma 3.5.17. *If every finite subset of a set of sentences is consistent, then the whole set is consistent.*

Proof. Suppose Γ is not consistent. Then there is a formal proof from Γ of some contradiction. Such a formal proof can use only finitely many sentences from Γ. Those sentences compose an inconsistent finite subset of Γ. $\square$

Lemma 3.5.18. *If* Γ *is consistent, then one of* $\Gamma \cup \{\sigma\}$ *and* $\Gamma \cup \{\neg\sigma\}$ *is consistent.*

Lemma 3.5.19. *If* $\Gamma \cup \{\sigma_0, \ldots, \sigma_{n-1}\}$ *is inconsistent, then*

$$\Gamma \vdash \bigvee_{k<n} \neg\sigma_k.$$

All of the foregoing will be used to prove the completeness of our proof-system in § 3.9.

Theories

The **theory** of a structure $\mathfrak{A}$ in a signature $\mathcal{L}$ is the set of sentences of $\mathcal{L}$ that are true in $\mathfrak{A}$. A set of sentences is a **theory** if it contains all of its logical consequences. You should check that the theory *of* a structure is indeed a theory in the sense just defined.

If some theory T is the set of logical consequences of a set Σ of sentences, then Σ **axiomatizes** T, or Σ is a set of **axioms** for T. It is a consequence of Gödel's

Incompleteness Theorem[9] that the theory of $\mathbb{N}$ in the signature $\{^+, +, \cdot, 0, 1\}$ cannot be *recursively* axiomatized: there is no computer program that can generate a complete set of axioms for the theory. By Mojżesz Presburger's earlier work,[10] the theory of $\mathbb{N}$ in the signature $\{+, 0, 1\}$ *is* recursively axiomatizable [33, § 3.1, pp. 81–84]: the axioms are

1) $\forall x\ x + 1 \neq 0$;
2) $\forall x\ \forall y\ (x + 1 = y + 1 \Rightarrow x = y)$;
3) $\forall x\ x + 0 = x$;
4) $\forall x\ x + (y + 1) = (x + y) + 1$;
5) $\varphi(0) \,\&\, \forall x\ (\varphi(x) \Rightarrow \varphi(x+1)) \Rightarrow \forall x\ \varphi(x)$, for all formulas $\varphi(x)$ of $\{+, 0, 1\}$.

The last line is an **axiom-scheme:** it describes a *set* of axioms (in fact, an infinite set).

In general, a theory T in a signature $\mathcal{L}$ is **complete** if

$$T \vDash \sigma \iff T \nvDash \neg\sigma$$

for all sentences σ of $\mathcal{L}$. In particular then, the theory *of* a particular structure is always complete. Two complementary problems of model-theory are:

1. To show that a particular set of sentences axiomatizes a complete theory.
2. To find a set of sentences that axiomatizes the (complete) theory of a particular structure.

Presburger's result shows that the former can sometimes be done; Gödel's result shows that the latter cannot always be done.

If T is a theory in a signature $\mathcal{L}$, then two n-ary formulas $\varphi(\vec{x}\,)$ and $\psi(\vec{x}\,)$ of $\mathcal{L}$ are **T-equivalent** if

$$T \vDash \forall x_0\ \cdots \forall x_{n-1}\ (\varphi(x_0, \ldots, x_{n-1}) \Leftrightarrow \psi(x_0, \ldots, x_{n-1})).$$

One way to learn about a theory and its models is to try to *eliminate quantifiers*. A theory T in a signature $\mathcal{L}$ **admits elimination of quantifiers** if for every formula of $\mathcal{L}$, there is a formula that is T-equivalent to it, but that contains no quantifiers. Presburger proved elimination of quantifiers for the theory axiomatized above, but in a larger signature.

Higher-order logics

First-order logic uses individual variables, but no other kinds of variables. In particular, there are no variables for relations. Relations are symbolized by

[9] Published in 1931; available in English in [56].

[10] In Warsaw, in 1928, in his master's thesis, at the suggestion of Alfred Tarski. Then Presburger went into the insurance industry. He died under the Nazis. [20, pp. 73–74]

predicates in first-order logic, and predicates stand for different relations in different structures; but in a particular first-order logic, predicates are constant in the sense that they cannot be preceded by quantifiers.

In **second-order logic,** variables standing for relations are allowed. The third of the properties of $\mathbb{N}$ listed at the end of § 1.2 is second order in this sense, since it refers to *every* subset of $\mathbb{N}$.

Likewise, $\mathbb{R}$ is characterized (among the structures called *ordered fields*) by the second-order property of *completeness,* namely that every set of real numbers with an upper bound has a least upper bound. See § 4.6.

Like propositional logic (see Theorem 2.9.1), first-order logic has a *compactness theorem,*[11] Corollary 3.9.6 below, namely that if every finite subset of a set of sentences has a model, then the whole set has a model. Second-order logic does not have such a theorem. This is a reason why model-theorists work mostly with first-order logic.

Exercises

1. Prove Lemma 3.5.7.

2. Show that good formulas and their free variables can be defined simultaneously as follows:
   a) An atomic formula of $\mathcal{L}$ is a good formula of $\mathcal{L}$, and each of its variables is free.
   b) If φ is a good formula of $\mathcal{L}$, then so is $\neg\varphi$, and this has the same free variables as φ.
   c) If φ and ψ are good formulas of $\mathcal{L}$, and every variable that occurs in both formulas is a *free* variable of both formulas, then $(\varphi \,\&\, \psi)$ is a good formula of $\mathcal{L}$, and its free variables are the variables that are free variables of φ or ψ.
   d) If φ is a good formula of $\mathcal{L}$, and x is a free variable of φ, then $\exists x\, \varphi$ is a good formula of $\mathcal{L}$, and its free variables are those of φ, except x.

3. Prove Lemma 3.5.9.

4. Letting P and Q be singulary predicates, determine, from the definition of $\vDash$, whether the following hold.

[11] Proved by Kurt Gödel for *countable* signatures in his doctoral dissertation in Vienna in 1929; proved generally by Mal'tsev in the Soviet Union, and independently by Leon Henkin [26] in 1948 in *his* doctoral dissertation at Princeton. [27, p. 318]

a) $(\exists x\ Px \Rightarrow \exists x\ Qx) \vDash \forall x\ (Px \Rightarrow Qx)$;
b) $(\forall x\ Px \Rightarrow \exists x\ Qx) \vDash \exists x\ (Px \Rightarrow Qx)$;
c) $\exists x\ (Px \Rightarrow Qx) \vDash (\forall x\ Px \Rightarrow \exists x\ Qx)$;
d) $\{\exists x\ Px,\ \exists x\ Qx\} \vDash \exists x\ (Px\ \&\ Qx)$;
e) $\exists x\ Px \Rightarrow \exists y\ Qy \vDash \forall x\ \exists y\ (Px \Rightarrow Qy)$.

5. Let $\mathcal{L} = \{R\}$, where R is a binary predicate, and let $\mathfrak{A}$ be the $\mathcal{L}$-structure $(\mathbb{Z}, \leqslant)$. Determine $\varphi^{\mathfrak{A}}$ if φ is:

   a) $\forall x_1\ (Rx_1x_0 \Rightarrow Rx_0x_1)$;
   b) $\forall x_2\ (Rx_2x_0 \vee Rx_1x_2)$.

6. Let $\mathcal{L}$ be $\{S, P\}$, where S and P are binary function-symbols. Then $(\mathbb{R}, +, \cdot)$ is an $\mathcal{L}$-structure. Show that the following sets and relations are definable in this structure:

   a) $\{0\}$;
   b) $\{1\}$;
   c) $\{a \in \mathbb{R} : 0 < a\}$;
   d) $\{(a, b) \in \mathbb{R}^2 : a < b\}$.

7. Show that the following sets are definable in $(\omega, +, \cdot, \leqslant, 0, 1)$:

   a) the set of even numbers;
   b) the set of prime numbers.

8. Let R be the binary relation

$$\{(x, x+1) : x \in \mathbb{Z}\}$$

   on $\mathbb{Z}$. Show that R is 0-definable in the structure $(\mathbb{Z}, <)$; that is, find a binary formula φ in the signature $\{<\}$ such that $\varphi^{(\mathbb{Z},<)} = R$.

9. Prove that the axioms of our proof-system are valid (the missing detail in the proof of Theorem 3.5.11).

10. Prove Lemmas 3.5.18 and 3.5.19.

3.6. Equipollence

In ordinary life, if two sets have the same size, one way to tell this is to count the sets. This procedure has two potential inconveniences:

1. The procedure gives us more information than necessary: it tells us not only *that* the sets have the same size, but also *what* that size is.
2. In the usual sense of counting, the procedure does not work for infinite sets, since we can never count to the end of them.

An alternative procedure is to arrange the sets in *pairs,* each pair containing an element of each set. Strictly, some of those pairs might be singletons, if the two sets have elements in common. So really, if the sets are A and B, we should make *ordered* pairs (c, d), where $c \in A$ and $d \in B$; each element of A should be the left entry of exactly one such pair, and each element of B should be the right entry of exactly one such pair. This just means there should be a *bijection* from A to B, if the two sets are to have the same size.

We introduce a new terminology for the notion of having the same size,—a terminology that avoids introducing the notion of size itself. Two sets are **equipotent** or **equipollent**[12] if there is a bijection from one to the other. If A and B are equipollent, we can write

$$A \approx B.$$

Evidently,

$$A \approx A,$$
$$A \approx B \iff B \approx A,$$
$$A \approx B \ \&\ B \approx C \implies A \approx C.$$

We have in particular

$$\mathbb{N} \approx \{a_0, a_1, a_2, \dots\},$$

provided $a_i \neq a_j$ when $i \neq j$, since then the function $n \mapsto a_n$ is indeed a bijection from the one set to the other.

Examples 3.6.1.

1. $\mathbb{N} \approx \{1, 2, 3, \dots\}$.
2. $N \approx \{k, k+1, k+2, \dots\}$.
3. $\mathbb{N} \approx \{0, 2, 4, 6, \dots\}$; the bijection is $x \mapsto 2x$.
4. $\mathbb{N} \approx \mathbb{Z}$, because of the bijection f given by

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ k, & \text{if } x = 2k-1, \\ -k, & \text{if } x = 2k. \end{cases}$$

[12]The Latin participles POTENT- and POLLENT- both mean *able.*

That is, $\mathbb{N} \approx \mathbb{Z}$, because the elements of $\mathbb{Z}$ can be listed as

$$0, 1, -1, 2, -2, 3, \ldots$$

5. $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$, because the elements of the latter set can be listed as

$$(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), (1,2), \ldots$$

This list is made up of blocks of the form of

$$(0,n), (1,n-1), (2,n-2), \ldots, (n,0);$$

these are just the diagonals of the matrix

$$\begin{array}{llllll} (0,0) & (0,1) & (0,2) & (0,3) & \ldots \\ (1,0) & (1,1) & (1,2) & \ldots\ldots\ldots & \\ (2,0) & (2,1) & \ldots\ldots\ldots\ldots\ldots & & \\ (3,0) & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & \end{array}$$

6. Suppose f is a bijection from $\mathbb{N}$ to $\mathbb{Z}$, and g is a bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$. We can write $g(x)$ as $(g_0(x), g_1(x))$. Then the function

$$x \mapsto (f(g_0(x)), f(g_1(x)))$$

is a bijection from $\mathbb{N}$ onto $\mathbb{Z} \times \mathbb{Z}$. Thus $\mathbb{N} \approx \mathbb{Z} \times \mathbb{Z}$.

7. $\mathbb{N} \approx \{x \in \mathbb{Q} \colon x > 0\}$, because of the list:

$$1, \frac{1}{2}, 2, \frac{1}{3}, 3, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, 4, \frac{1}{5}, 5, \frac{1}{6}, \frac{2}{5}, \frac{3}{4}, \frac{4}{3}, \frac{5}{2}, 6, \frac{1}{7}, \ldots,$$

This list is made up of blocks of the form of

$$\frac{1}{n}, \frac{2}{n-1}, \frac{3}{n-2}, \ldots, \frac{n}{1},$$

but with entries deleted if they are equal to entries that have already appeared.

8. $\mathbb{N} \approx \mathbb{Q}$.

Thus there are sets A and B such that

$$A \subset B \ \ \& \ \ A \approx B.$$

But no such set B can be *finite*. Indeed, to be precise, let us say that a set C is **finite** if, for some n in $\mathbb{N}$,

$$C \approx \{0, \ldots, n-1\},$$

that is, for some n in ω,

$$C \approx n.$$

Theorem 3.6.2. *No element n of ω has a proper subset A such that $A \approx n$.*

Proof. We use induction. The claim is trivially true when $n = 0$, since this has no proper subsets at all. Suppose the claim holds when $n = m$. Now let $n = m + 1$, and suppose $A \subseteq n$, and f is a bijection from n to A. There are two cases to consider.

1. If $f(m) = m$, then $f \smallsetminus \{(n, n)\}$ is a bijection from m to $A \smallsetminus \{m\}$, and the latter set is a subset of m. In this case, by inductive hypothesis, $A \smallsetminus \{m\} = m$, so $A = n$.
2. If $f(m) = k$, where $k < m$, define the function g on m by

$$g(x) = \begin{cases} f(x), & \text{if } f(x) \neq m, \\ k, & \text{if } f(x) = m. \end{cases}$$

   Then g is a bijection from m onto $A \smallsetminus \{m\}$, so again $A \smallsetminus \{m\} = m$, and hence $A = n$.

This completes the induction. □

A set is **infinite** if it is not finite. The contrapositive of the theorem then gives us that, if a set is equipollent with a proper subset of itself, then the set is infinite.[13] In particular, $\mathbb{N}$ and all sets equipollent with it are infinite; to be more precise, such sets are called **countably infinite.** So $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are all countably infinite. A set is called **countable** if it is a subset of a countably infinite set.

Theorem 3.6.3. *Suppose A and B are countable sets.*

1. *$A \cup B$ is countable.*
2. *A^n is countable for all n in $\mathbb{N}$.*

[13] In 1882, Richard Dedekind [12, p. 63] suggested *defining* infinite sets as those that are equipollent with proper subsets of themselves. Agreement of this definition with ours will require the Axiom of Choice, 4.9.3.

Proof. 1. If $A = \{a_0, a_1, \dots\}$ and $B = \{b_0, b_1, \dots\}$, then we can list $A \cup B$ as

$$a_0, b_0, a_1, b_1, a_2, \dots,$$

with any repeats deleted.

2. $A^0 = \{\varnothing\}$, so it is countable. Also, $A^{n+1} \approx A^n \times A$, so if A^n is countable, then so is A^{n+1} by the method of Example 3.6.1 (5). By induction, A^n is countable for all n in $\mathbb{N}$. □

Theorem 3.6.4. *If $\mathcal{L}$ is a countable first-order signature, then the set of formulas of $\mathcal{L}$ is countable.*

Proof. Since $\mathcal{L}$ is countable, the set of all symbols used in formulas of $\mathcal{L}$ is countable. A bijection $k \mapsto s_k$ from $\mathbb{N}$ to this set establishes an **alphabetical ordering** of the set: the symbol s_i comes before s_j in this ordering if and only if $i < j$. Hence we can arrange all of the formulas of length n in alphabetical order; in particular, we can list these formulas as φ_0^n, φ_1^n, φ_2^n, ... Now we can embed the set of *all* formulas of $\mathcal{L}$ in $\mathbb{N} \times \mathbb{N}$; so the set of formulas is countable. □

Instead of $\neg(A \approx B)$, we may write $A \not\approx B$. If there is an *injection* from A to B, we write

$$A \preccurlyeq B.$$

If there is an injection, but no bijection, we write

$$A \prec B; \tag{3.51}$$

in this case, B is **strictly larger** than A. For example, if $A \neq \varnothing$, then $\varnothing \prec A$.

By Theorem 3.6.7 below, (3.51) can hold even when both A and B are infinite. Meanwhile, the following gives some justification for the name power set.

Theorem 3.6.5. *If $n \in \mathbb{N}$, and a set A has n elements, then $\mathcal{P}(A) \approx \mathbb{B}^n$.*

Proof. It is enough to show $\mathcal{P}(n) \approx \mathbb{B}^n$ if $n \in \omega$. Let f be the function from $\mathcal{P}(n)$ to $\mathbb{B}^n$ given by

$$f(B) = (e_0, \dots, e_{n-1}),$$

where

$$e_i = \begin{cases} 1, & \text{if } i \in B; \\ 0, & \text{if } i \notin B. \end{cases}$$

Let g be the function from $\mathbb{B}^n$ to $\mathcal{P}(n)$ given by

$$g((e_0, \dots, e_{n-1})) = \{i \colon e_i = 1\}.$$

Then $g \circ f = \mathsf{id}_{\mathcal{P}(n)}$ and $f \circ g = \mathsf{id}_{\mathbb{B}^n}$. So f is a bijection by Theorem 3.3.4. □

The last theorem can be modified to make sense for infinite sets. In § 3.2, a couple of formal definitions of n-tuples are mentioned. By yet another definition, an n-tuple of elements of a set A is just a function[14] from $\{0, \dots, n-1\}$ (the von-Neumann natural number n) into A. To indicate explicitly the set of such functions, I propose to use the notation

$$^{n}A.$$

Then $^{n}A \approx A^n$. The latter set could be *defined* as the former. I shall use the notation A^n when the precise definition of its elements is not important: when all that matters is that

$$\vec{a} = \vec{b} \iff \bigwedge_{k<n} a_k = b_k$$

for all elements $\vec{a}$ and $\vec{b}$ of A^n. (Compare the use of $\mathbb{N}$ instead of ω for the set of natural numbers, as described in § 1.2, when the composition of an individual natural number is not important.) We can generalize the new notation, writing

$$^{A}B$$

for the set of functions from A to B.

Theorem 3.6.6. *For all sets A,*

$$\mathcal{P}(A) \approx {}^{A}\mathbb{B}.$$

Proof. The function

$$f \longmapsto \{x \in A : f(x) = 1\}$$

is a bijection from $^{A}\mathbb{B}$ to $\mathcal{P}(A)$; for, it has the inverse $C \mapsto \chi_C$, where

$$\chi_C(x) = \begin{cases} 1, & \text{if } x \in C, \\ 0, & \text{if } x \notin C, \end{cases}$$

for all subsets C of A. □

Here χ_C is the **characteristic function** of C on A. Here the letter chi may cause confusion because of its resemblance to X; but χ is the initial of the Greek χαρακτήρ.

[14] Many writers will give this function the domain $\{1, 2, \dots, n\}$ instead of $\{0, 1, \dots, n-1\}$.

The inequality

$$n < 2^n \tag{3.52}$$

holds for all natural numbers n (see § 4.5, Exercise 3); so the power set of a finite set is always strictly larger than the original set. The same is true for *all* sets:

Theorem 3.6.7 (Cantor)**.** *$A \prec \mathcal{P}(A)$ for all sets A.*

Proof. We have an injection $x \mapsto \{x\}$ from A to $\mathcal{P}(A)$, so $A \preccurlyeq \mathcal{P}(A)$. Suppose f is an arbitrary injection from A into $\mathcal{P}(A)$. Let B be the subset $\{x \in A\colon x \notin f(x)\}$ of A. Then B is not in the range of f. For, suppose $x \in A$. If $x \in B$, then $x \notin f(x)$, so $B \neq f(x)$. If $x \notin B$, then $x \in f(x)$, so again $B \neq f(x)$. So there is no bijection between A and $\mathcal{P}(A)$. □

Note the resemblance between this proof and that of the Russell Paradox given on p. 59. A set that is not countable is **uncountable.** We have now that $\mathcal{P}(\mathbb{N})$ is uncountable.

Suppose $A \preccurlyeq B$ and $B \preccurlyeq A$; do we then have $A \approx B$? In fact we do, by Theorem 4.9.9, but the proof is not easy.

Exercises

Suppose A is an infinite set.

1. Can you write down a bijection from A to $A \times A$?
2. Suppose f is a bijection from A to A^2. Can you write down a bijection from A to
   a) A^3?
   b) A^4?
   c) A^n?

3.7. Equivalence-relations

Let R be a binary relation. The **field** of R is the set

$$\{x\colon \exists y\ x\ R\ y\} \cup \{y\colon \exists x\ x\ R\ y\}.$$

Let this set be A. Then (A, R) is a structure in the sense of the last section. We say that R is:

1) **reflexive,** if

$$(A, R) \vDash \forall x\ x\ R\ x;$$

2) **symmetric,** if

$$(A, R) \vDash \forall x\ \forall y\ (x\ R\ y \Rightarrow y\ R\ x);$$

3) **transitive,** if

$$(A, R) \vDash \forall x\ \forall y\ \forall z\ (x\ R\ y\ \&\ y\ R\ z \Rightarrow x\ R\ z).$$

Note that, in these definitions, we need restrict the variables to the field of the relation *only* in the definition of reflexivity. The relation R is reflexive if $b\ R\ b$ for all b *in the field of* R. By contrast, R is symmetric if $c\ R\ b$ whenever $b\ R\ c$,—there is no need to restrict b and c to the field of R, since this is already done by the condition $b\ R\ c$. A similar observation holds for transitivity.

An alternative formulation of the definitions can be given in terms of the notions of § 3.4. The relation R is:

1) reflexive if and only if $\Delta_A \subseteq R$;
2) symmetric if and only if $R = \breve{R}$;
3) transitive if and only if $R/R \subseteq R$.

A reflexive, symmetric, transitive relation is called an **equivalence-relation**.

Examples 3.7.1.

1. Δ_A is an equivalence-relation whose field is A.
2. Equipollence is an equivalence-relation whose field is the class of all sets.
3. Truth-equivalence (§ 2.2) is an equivalence-relation whose field is the set of propositional formulas. (Likewise, if T is a first-order theory of $\mathcal{L}$, then T-equivalence (§ 3.5) is an equivalence-relation whose field is the set of first-order formulas of $\mathcal{L}$.)
4. If n is an integer, then **congruence *modulo*** n is an equivalence-relation with field $\mathbb{Z}$. This relation consists of pairs (a, b) such that

$$a \equiv b \pmod{n},$$

that is, $n \mid a - b$.

5. On $\mathbb{N}^2$, we can define an equivalence-relation $\sim$ by

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

(See § 4.3 for elaboration.)

6. Similarly, on $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, we can define an equivalence-relation $\approx$ by

$$(a, b) \approx (c, d) \iff ad = bc.$$

(Again, see § 4.3.)

7. If $k < n$, and A is a set, then there is an equivalence-relation $\sim_k^n$ on A^n given by

$$\vec{a} \sim_k^n \vec{b} \iff \bigwedge_{\substack{j<n \\ j\neq k}} a_j = b_j,$$

that is, $\vec{a} \sim_k^n \vec{b} \iff \pi_k^n(\vec{a}) = \pi_k^n(\vec{b})$, where π_k^n is as in § 3.5.

Theorem 3.7.2. *If $f\colon A \Rightarrow B$, then $f/\breve{f}$ is an equivalence-relation with field A.*

Suppose $\sim$ is an equivalence-relation on A. If $b \in A$, we can define

$$b/\sim = \{x \in A : b \sim x\};$$

this is the **$\sim$-class** of b, or the **equivalence-class** of b (with respect to $\sim$; the notation here must not be confused with the notation for composition of relations). If the equivalence-relation is clear, one might write $[b]$ instead of $b/\sim$, as in the following:

Lemma 3.7.3. *If an equivalence-relation on A is given, then*

$$[b] = [c] \iff [b] \cap [c] \neq \varnothing$$

for all b and c in A.

The **quotient** of A by the equivalence-relation $\sim$ is the set $\{[b] : b \in A\}$, which can be denoted by

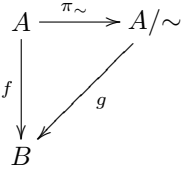
$$A/\sim;$$

this can be read as A *modulo* $\sim$. Then there is a **quotient-map** or **projection** from A to $A/\sim$, namely the function

$$x \longmapsto [x].$$

This function might be denoted by $\pi_\sim$. Suppose also $f\colon A \to B$. One may ask whether there is a function g from $A/\sim$ to B such that $f = g \circ \pi_\sim$. That is,

does g exist so that the following diagram **commutes?**



Yet another way to formulate the question is, does f have $\pi_\sim$ as a **factor?** Necessary and sufficient conditions for a positive answer are given by the following.

Theorem 3.7.4. *Suppose E is an equivalence-relation on A, and $f\colon A \to B$. The following conditions are equivalent:*

1. *$E \subseteq f/\breve{f}$;*
2. *$x\ E\ y \implies f(x) = f(y)$ for all x and y in A;*
3. *there is a function g from A/E to B such that $g([x]) = f(x)$ for all x in A.*

Proof. Exercise; see Examples 3.7.5 below. □

The function g in the theorem can be written

$$[x] \longmapsto f(x).$$

Such an expression does not *automatically* define a function. If it does, we say the function is **well-defined.**

Examples 3.7.5. The following parallel Examples 3.7.1.

1. If $\boldsymbol{F}$ is an n-ary propositional formula in a signature $\mathcal{L}$, then there is a function $\vec{e} \mapsto \widehat{\boldsymbol{F}}(\vec{e})$ or $\widehat{\boldsymbol{F}}$ from $\mathbb{B}^n$ to $\mathbb{B}$. Hence there is a function $\boldsymbol{F} \mapsto \widehat{\boldsymbol{F}}$ from the set $\mathrm{Fm}^n(\mathcal{L})$ of n-ary propositional formulas of $\mathcal{L}$ to the set ${}^{\mathbb{B}^n}\mathbb{B}$. By definition of truth-equivalence, $\boldsymbol{F} \sim \boldsymbol{G}$ if and only if $\widehat{\boldsymbol{F}} = \widehat{\boldsymbol{G}}$. Hence there is a well-defined injection $\boldsymbol{F}/\!\sim \mapsto \widehat{\boldsymbol{F}}$ from $\mathrm{Fm}^n(\mathcal{L})/\!\sim$ to ${}^{\mathbb{B}^n}\mathbb{B}$; if $\mathcal{L}$ is adequate, then this function is also surjective (at least if n is large enough).

2. If $n > 0$, then the distinct elements of the quotient of $\mathbb{Z}$ by congruence *modulo* n are $[0]$, $[1]$, $[2]$, …, $[n-1]$.

3. The function $[a, b] \mapsto a - b$ is a well-defined bijection from $\mathbb{N}^2/\!\sim$ to $\mathbb{Z}$. (In § 4.3, the structure $\mathbb{Z}$ will be *defined* in terms of $\mathbb{N}$ so that there is such a bijection.)

4. The function $[a, b] \mapsto a/b$ is a well-defined bijection from $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})/\!\approx$ to $\mathbb{Q}$. (In § 4.3, the structure $\mathbb{Q}$ will be *defined* in terms of $\mathbb{Z}$ so that there is such a bijection.)

5. The equipollence-class of a set A can be called the **cardinality** of A and denoted by

$$|A|.$$

Equipollent sets are sets having the same equipollence-class; such sets can also be said to have the same cardinality. An alternative definition of cardinality is given in § 4.9, whereby the cardinality of A is a particular *set* in the equipollence-class of A.

6. The function $[\vec{x}\,] \mapsto \pi^n_k(\vec{x}\,)$ is a well-defined bijection from $A^n/{\sim^n_k}$ to A^{n-1}.

A **partition** of A is a subset P of $\mathcal{P}(A)$ such that:
1) if B and C are in P, and $B \cap C \neq \varnothing$, then $B = C$;
2) every element of A is an element of some element of P.

Theorem 3.7.6. *If $\sim$ is an equivalence-relation on A, then $A/\!\sim$ is a partition of A. Conversely, if P is a partition of A, then the relation*

$$\{(x, y) \in A^2 : (\exists X \in P)\ \{x, y\} \subseteq X\}$$

is an equivalence-relation on A.

Exercises

1. Prove Theorem 3.7.2.
2. Prove Lemma 3.7.3.
3. Prove Theorem 3.7.4.
4. Prove Theorem 3.7.6.
5. Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
   a) Define an equivalence-relation E on A so that $|A/E| = 5$.
   b) Can you define an equivalence-relation F on A so that $|A/F| = 7$?
6. Define an equivalence-relation $\sim$ on $\mathbb{Z}$ so that there is a bijection from $\mathbb{Z}/\!\sim$ to $\mathbb{N}$.
7. For every property in the set {reflexive, symmetric, transitive}, find a set A and a relation R on A that has just the other two properties.
8. Suppose R is a reflexive and symmetric relation on A, but $R \not\subseteq R/R$. Can you find an equivalence-relation S on A such that $R \subseteq S$, but $S \neq R \times R$?

3.8. Orderings

Let R be a binary relation with field A. The following possible properties complement those given in § 3.7. The relation R is:

1) **irreflexive,** if

$$(A, R) \vDash \forall x\, \neg(x\ R\ x);$$

2) **anti-symmetric,** if

$$(A, R) \vDash \forall x\, \forall y\, (x\ R\ y\ \&\ y\ R\ x \Rightarrow x = y).$$

Again we have alternative characterizations. The relation R is:

1) irreflexive if and only if $R \cap \Delta_A = \varnothing$;

2) anti-symmetric if and only if $R \cap \breve{R} \subseteq \Delta_A$.

A reflexive, anti-symmetric, transitive relation is called a **partial ordering** of its domain. If R is a partial ordering, and A is its domain, then the structure (A, R) is a **partially ordered set** or a **partial order.** More generally, we may say that a pair (A, R) is a partial order when really it is $(A, R \cap A \times A)$ that is the partial order (see the examples below).

A **strict partial ordering** is an irreflexive, anti-symmetric, transitive relation. If R is a strict partial ordering, and the set A *includes* the domain of R, then the pair (A, R) is a **strict partial order.** Note then that a strict partial order is technically *not* a partial order (see Exercise 1). In any case, in the terminology used here, an *order* is a kind of *structure* (see Figure 3.8); an *ordering* is the *relation* that is part of an order. However, this terminological distinction is not of great importance.

Examples 3.8.1.

1. $(\mathcal{P}(A), \subseteq)$ is a partial order; so is $(B, \subseteq)$, if $B \subseteq \mathcal{P}(A)$.
2. $(\mathcal{P}(A), \subset)$ is a strict partial order.
3. (See the first of Examples 3.7.5.) We can understand logical entailment $\vDash$ as a binary relation on $\mathrm{Fm}^n(\mathcal{L})/\!\sim$. Then $(\mathrm{Fm}^n(\mathcal{L})/\!\sim, \vDash)$ is a partial order. The case $n = 2$ can be depicted as in Figure 3.9. (Such a drawing of a partial order is called a *Hasse diagram.*)
4. $(\mathbb{Z}, \mid)$ is a partial order.
5. (A, Δ_A) is a partial order.
6. $(A, \varnothing)$ is a strict partial order.
7. The relation $\preccurlyeq$ on sets is not a partial ordering; but we shall see in § 4.9 that it 'induces' a partial ordering of *cardinalities.*

Lemma 3.8.2.

Figure 3.8. The remains of the temple at Priene: an example of the Ionic order of architecture. Think of the columns as an order in our sense.

1. *If* (A, R) *is a partial ordering, then* $(A, R \smallsetminus \Delta_A)$ *is a strict partial ordering.*
2. *If* (A, S) *is a strict partial ordering, then* $(A, S \cup \Delta_A)$ *is a partial ordering.*

In the lemma, one might say that $R \smallsetminus \Delta_A$ is **associated** with R, and $S \cup \Delta_A$ with S.

A partial order (A, R) is a **linear order** or a **total order** if

$$(A, R) \vDash \forall x \, \forall y \, (x \; R \; y \vee y \; R \; x),$$

that is,

$$R \cup \breve{R} = A^2.$$

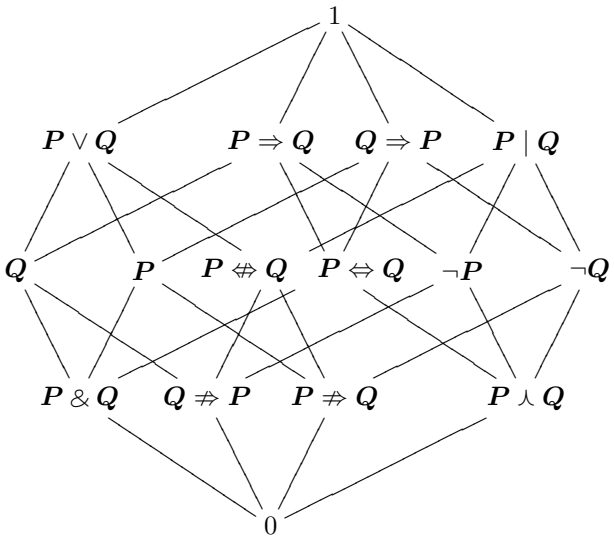


Figure 3.9. In this depiction of the set of (truth-equivalence-classes of) propositional formulas in the variables $\boldsymbol{P}$ and $\boldsymbol{Q}$, $\boldsymbol{F} \vDash \boldsymbol{G}$ if and only if $\boldsymbol{G}$ can be reached from $\boldsymbol{F}$ by travelling upwards along the drawn lines. The new connective $\not\Rightarrow$ here has the obvious meaning.

If $\leqslant$ is a linear ordering, then the associated strict linear ordering can be denoted by $<$, and *vice versa*.

Example 3.8.3. $(\mathbb{Z}, \leqslant)$ is a linear order; $(\mathbb{Z}, <)$ is a strict linear order.

Suppose (A, R) and (B, S) are partial orders, and $f\colon A \to B$. Then f is **order-preserving** if

$$a \mathrel{R} b \implies f(a) \mathrel{S} f(b)$$

for all x and y in A. An order-preserving function is an example of a more general notion:

Suppose $\mathfrak{A}$ and $\mathfrak{B}$ are two structures in a signature $\mathcal{L}$. A function f from A to B is called a **homomorphism** from $\mathfrak{A}$ to $\mathfrak{B}$ if

$$\mathfrak{A} \vDash \varphi(a_0, \ldots, a_{n-1}) \implies \mathfrak{B} \vDash \varphi(f(a_0), \ldots, f(a_{n-1})) \tag{3.53}$$

for all atomic formulas $\varphi(x_0, \ldots, x_{n-1})$ of $\mathcal{L}$ and all a_i in A, for all n in $\mathbb{N}$. If (3.53) holds for all atomic and *negated* atomic formulas $\varphi(x_0, \ldots, x_{n-1})$ of $\mathcal{L}$ and all a_i in A, for all n in $\mathbb{N}$, then f is an **embedding** of $\mathfrak{A}$ to $\mathfrak{B}$. Finally, f is an **isomorphism** if f is invertible and f^{-1} is a homomorphism from $\mathfrak{B}$ to $\mathfrak{A}$.

A homomorphism is thus a function that *preserves structure;* it **preserves** the symbols in a signature (hence it preserves the atomic formulas that use them). An embedding also preserves their complements; in particular, it preserves inequality, so it is an injection. The existence of an isomorphism shows that two structures are the *same* as structures. If an isomorphism exists between $\mathfrak{A}$ and $\mathfrak{B}$, then $\mathfrak{A}$ and $\mathfrak{B}$ are called **isomorphic,** and we write

$$\mathfrak{A} \cong \mathfrak{B}.$$

Isomorphism is an equivalence-relation. Isomorphic structures have the same *theories* (the proof is tedious, but not surprising).

Examples 3.8.4.

1. An order-preserving function is a homomorphism of partial orders. An isomorphism of partial orders is an invertible order-preserving function whose inverse is also order-preserving.

2. The identity is a homomorphism from $(\mathbb{N}, |)$ to $(\mathbb{N}, \leqslant)$, but not an embedding.

3. Any function from a non-empty set to another is a homomorphism of sets. Equipollence is isomorphism of sets.

4. By Theorem 3.4.7, if $f\colon A \to B$, then $X \mapsto f^{-1}[X]$ is a homomorphism from $(\mathcal{P}(B), \cap, \cup, {}^{\mathrm{c}})$ to $(\mathcal{P}(A), \cap, \cup, {}^{\mathrm{c}})$.

5. More examples of homomorphisms and isomorphisms are in §§ 4.1, 4.3 and 4.6.

The following is a **representation theorem:** it shows that every partial order *can be represented by* (is isomorphic to) a structure of the form given in the first of the Examples 3.8.1. Note how the proof of the theorem uses every property in the definition of partial orders.

Theorem 3.8.5. *For every partial order (A, R), there is a subset B of $\mathcal{P}(\Omega)$ such that $(A, R) \cong (B, \subseteq)$.*

Proof. Let f be the function from A to $\mathcal{P}(A)$ given by

$$f(a) = \{y \in A : y \mathrel{R} a\}.$$

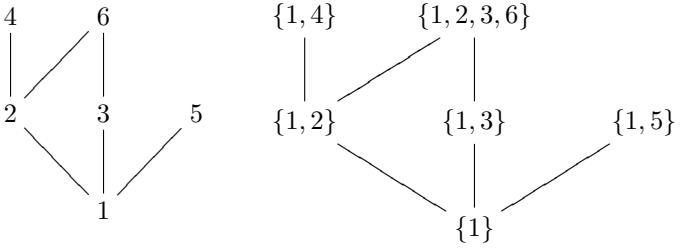


Figure 3.10. Two isomorphic partial orders

Then f is injective: Indeed, suppose c and d are elements of A. If $c\ R\ d$ and $d\ R\ c$, then $c = d$ since R is anti-symmetric. Suppose $c \neq d$. Then we may assume $\neg(c\ R\ d)$. Then $c \notin f(d)$. But $c \in f(c)$ since R is reflexive. Therefore $f(c) \neq f(d)$. Let $B = f[A]$; then f gives a bijection between A and B.

Also, f is order-preserving: Suppose $c\ R\ d$. If $e \in f(c)$, then $e\ R\ c$, so $e\ R\ d$ since R is transitive; hence $e \in f(d)$. Thus $f(c) \subseteq f(d)$. This shows that f is order-preserving.

But $X \mapsto f^{-1}[X]$ is also order-preserving (as a function on B, this set being equipped with the relation $\subseteq$): If $f(c) \subseteq f(d)$, then $c \in f(d)$ since $c \in f(c)$; so $c\ R\ d$. Therefore f is an isomorphism from (A, R) to $(B, \subseteq)$. □

Examples 3.8.6.

1. The partial order $(\{1, 2, 3, 4, 5, 6\}, |)$ is isomorphic to $(B, \subseteq)$, where B is the set

$$\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 4\}, \{5\}, \{1, 2, 3, 6\}\}.$$

See Figure 3.10.

2. A set of propositional formulas in n variables, partially ordered by logical entailment $\vDash$, is isomorphic to a set of Boolean combinations of n suitable sets, partially ordered by inclusion. Compare Figure 3.9 to Figure 3.11.

Exercises

1. Show that no partial ordering is a strict partial ordering.
2. Are there partial orderings that are also equivalence-relations?
3. Are there relations that are both symmetric and anti-symmetric?

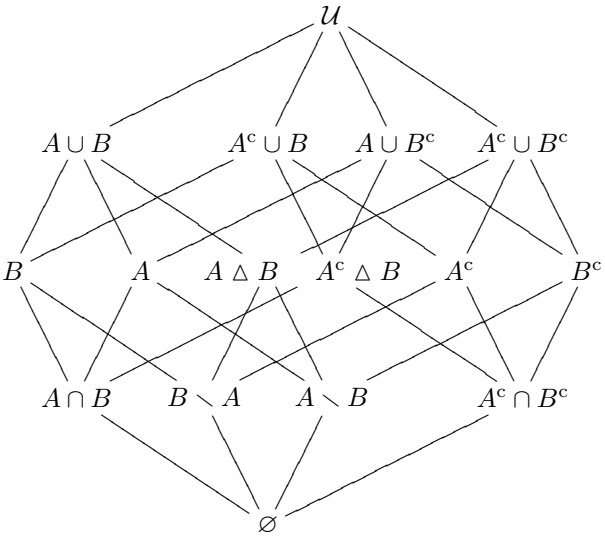


Figure 3.11. A partial order of sets. (The sets A and B here should be *independent* in the sense that all Boolean combinations here are distinct.)

4. Write down the ordered pairs that belong to $|$, considered as a relation on $\{1, 2, 3, 4, 5, 6\}$. Can you add pairs to this relation so that it becomes a linear ordering?

5. More generally, if R is a partial order on a finite set A, is there a linear ordering S on A such that $R \subseteq S$?

6. Find sets A and B such that all of the Boolean combinations depicted in Figure 3.11 are distinct.

3.9. Infinitary Boolean operations

The union of two sets is the set comprising everything that is in one or the other of the sets. There is no reason to restrict unions to two sets. Instead of writing $A \cup B$, we might write

$$\bigcup \{A, B\}.$$

This is the *union* of the single set $\{A, B\}$, whose elements happen to be the sets A and B. Then $\bigcup\{A, B, C\}$ is $A \cup B \cup C$, and so forth. If $\mathcal{S}$ is a class of sets, then the **union** of $\mathcal{S}$ is the class

$$\{x\colon \exists y\ (y \in \mathcal{S}\ \&\ x \in y)\};$$

this is denoted by

$$\bigcup \mathcal{S}.$$

Unions in this new sense are **infinitary,** in the sense that the set $\mathcal{S}$ may be infinite.

We shall need the following for Theorem 4.8.9.

Axiom 3.9.1 (Union)**.** *The union of a set is a set.*

As there are infinitary unions, so there are **infinitary intersections:** If $\mathcal{S}$ is a class of sets, then

$$\bigcap \mathcal{S} = \{x\colon \forall y\ (y \in \mathcal{S} \Rightarrow x \in y)\}. \tag{3.54}$$

So $A \cap B$ is $\bigcap\{A, B\}$, and so forth.

Theorem 3.9.2. *The intersection of a non-empty set of sets is a set.*

Proof. If $\mathcal{S}$ contains A, then

$$\bigcap \mathcal{S} = \{x \in A\colon \forall y\ (y \in \mathcal{S} \Rightarrow x \in y)\},$$

which is a set by the Axiom of Separation, 1.2.3. □

By strict application of (3.54), $\bigcap \varnothing$ is the class of everything that belongs to some set; but this class is not a set.

The following will be useful in the next chapter, starting in § 4.1.

Theorem 3.9.3. *Let $\mathcal{S}$ be a set of sets, one of which is A. Then*

$$\bigcap \mathcal{S} \subseteq A \subseteq \bigcup \mathcal{S}.$$

Proof. Exercise. □

Sometimes, in an infinitary union $\bigcup \mathcal{S}$ (or an intersection $\bigcap \mathcal{S}$), the set $\mathcal{S}$ is given as the range of a function. Say $f\colon A \to \mathcal{P}(B)$. Then we can write

$$\bigcap f[A] = \bigcap_{x \in A} f(x)$$

and $\bigcup f[A] = \bigcup_{x \in A} f(x)$.

Examples 3.9.4.

1. $\mathbb{R} = \bigcup_{n \in \mathbb{N}} (-1 - n, n + 1)$;
2. $\bigcap_{n \in \mathbb{N}} [n, \infty) = \varnothing$;
3. $\bigcap_{n \in \mathbb{N}} [-1/(n+1), 1/(n+1)] = \{0\}$.

Completeness

It is now possible to prove the completeness of our proof-system for first-order logic in a countable signature.

Theorem 3.9.5 (Completeness)**.** *Our proof-system for first-order logic in a countable signature is complete.*

Proof. Suppose Γ is a set of sentences that does not formally entail σ. Then Γ must be consistent (why?). We shall show that Γ has a model. It will then follow that Γ does not logically entail σ (why?).

Let C be a set $\{c_k\colon k \in \mathbb{N}\}$ of new constants. We consider two cases.

Suppose first that $\Gamma \cup \{c_i \neq c_j\colon i < j\}$ is inconsistent. Then there is some greatest n such that $\Gamma \cup \{c_i \neq c_j\colon i < j < n\}$ is consistent (why?). Hence

$$\Gamma \cup \{c_i \neq c_j\colon i < j < n\} \vdash c_0 = c_n \vee \cdots \vee c_{n-1} = c_n.$$

We now extend Γ to a *maximal* consistent set Σ of sentences of $\mathcal{L} \cup \{c_k\colon k < n\}$. We do this as follows. Since we are working in a countable signature $\mathcal{L}$, we can, by Theorem 3.6.4, list the sentences of $\mathcal{L}$ as σ_0, σ_1, ... Now we define a list of *sets* of sentences recursively as follows. We let $\Gamma_0 = \Gamma$. Supposing Γ_n has been defined, we let Γ_{n+1} be $\Gamma_n \cup \{\sigma_n\}$, if this is consistent; otherwise, Γ_{n+1} is $\Gamma_n \cup \{\neg\sigma_n\}$. By Lemma 3.5.18 and induction, each set Γ_n is consistent.

Now define

$$\Sigma = \bigcup_{n \in \mathbb{N}} \Gamma_n.$$

By Lemma 3.5.17, this set is consistent. Indeed, every finite subset of Σ can be written as $\{\tau_0, \ldots, \tau_{n-1}\}$ for some n in $\mathbb{N}$. Each sentence τ_k belongs to some set $\Gamma_{f(k)}$. Let m be the greatest element of $\{f(0), \ldots, f(n-1)\}$ (how?). Then $\{\tau_0, \ldots, \tau_{n-1}\} \subseteq \Gamma_m$, so it is consistent.

Suppose $\Sigma \vdash \varphi(c_k)$ whenever $k < n$. Then

$$\Sigma \vdash c_k = c_n \Rightarrow \varphi(c_n)$$

whenever $k < n$, and therefore

$$\Sigma \vdash c_0 = c_n \vee \cdots \vee c_{n-1} = c_n \Rightarrow \varphi(c_n),$$
$$\Sigma \vdash \varphi(c_n),$$
$$\Sigma \vdash \forall x\, \varphi(x)$$

by Generalization. Contrapositively, if $\Sigma \vdash \exists x\, \varphi(x)$, then $\Sigma \vdash \varphi(c_k)$ for some k that is less than n. This enables us to make $\{c_k \colon k < n\}$ into a model of Σ (how?).

In the other case, in producing Σ, whenever we add $\exists x\, \varphi(x)$, we must also add $\varphi(c_n)$ for some n such that c_n has not already been used. □

The proof can be adapted to the case where $\mathcal{L}$ is uncountable by means of Theorem 4.9.8.

Corollary 3.9.6 (Compactness Theorem)**.** *If every finite subset of a set* Γ *of sentences has a model, then* Γ *has a model.*

Proof. If Γ has no model, then $\Gamma \vDash \bot$, so $\Gamma \vdash \bot$, hence $\Gamma_0 \vdash \bot$ for some finite subset Γ_0 of Γ. Then $\Gamma_0 \vDash \bot$, so Γ_0 has no model. □

Exercises

1. Find $\bigcup \varnothing$ and $\bigcup\{\varnothing\}$.
2. Can you define $\bigcap \varnothing$?
3. Find a set $\mathcal{S}$ of sets such that $\bigcup \mathcal{S} = \bigcap \mathcal{S}$.
4. Prove Theorem 3.9.3.
5. Prove the infinitary analogues of some propositions in § 3.4: Suppose $f \colon A \to B$, and $\mathcal{S} \subseteq \mathcal{P}(A)$, and $\mathcal{T} \subseteq \mathcal{P}(B)$. Then:

a) $f[\bigcup \mathcal{S}] = \bigcup\{f[X] : X \in \mathcal{S}\}$;
b) $f[\bigcap \mathcal{S}] \subseteq \bigcap\{f(X) : X \in \mathcal{S}\}$;
c) the last inclusion is an equality if f is injective;
d) $f^{-1}[\bigcup \mathcal{T}] = \bigcup\{f^{-1}[X] : X \in \mathcal{T}\}$;
e) $f^{-1}[\bigcap \mathcal{T}] = \bigcap\{f^{-1}[X] : X \in \mathcal{T}\}$.

6. Supply the missing details of the proof of the Completeness Theorem.

4. Numbers

4.0. The Peano axioms

In a book called *The Principles of Arithmetic, Presented by a New Method* [55], originally written in Latin and published in 1889, Giuseppe Peano describes the positive integers by means of nine strings of symbols—strings that he calls *axioms.* In our terminology, three of Peano's axioms say that equality of positive integers is an equivalence-relation; another says that everything equal to a positive integer is a positive integer. The remaining five axioms have more mathematical content, and versions of them are sometimes listed by themselves[1] as *the* axioms for the positive integers; these axioms may or may not be called *the Peano axioms.* Two of these axioms say that 1 is a positive integer and that every positive integer has a successor that is a positive integer.

The remaining three of Peano's axioms correspond to the three statements at the end of § 1.2, except that the latter statements concern the non-negative integers, rather than just the positive integers. The difference is of little mathematical importance. In model-theoretic terms, Peano's axioms amount to the assertion that there is a model of three particular sentences.[2] Two of these sentences are first order; the third is second order. I propose to make this assertion as follows: it is the Axiom of Infinity, since, as we noted in § 3.6, $\mathbb{N}$ must be infinite.

Axiom 4.0.1 (Infinity)**.** *In the signature* $\{0, {}^+\}$*, there is a structure* $\mathbb{N}$ *such that:*

1) $\mathbb{N} \vDash \forall x\ x^+ \neq 0$;

2) $\mathbb{N} \vDash \forall x\ \forall y\ (x^+ = y^+ \Rightarrow x = y)$;

3) $(\mathbb{N}, A) \vDash P0\ \&\ \forall x\ (Px \Rightarrow P(x^+)) \Rightarrow \forall x\ Px$*, whenever* $A \subseteq \mathbb{N}$*, and* P *is a singulary predicate interpreted as* A *in* $\mathbb{N}$.

[1] For example, in [29, pp. 988 f.] or [31, § 1].

[2] Before Peano, Dedekind recognized that the natural numbers have this property, and that all structures with this property are isomorphic [12, II: §§ 71, 132].

Throughout this book, $\mathbb{N}$ is simply such a structure as is named in this axiom. Let us refer to the sentence $\forall x\ x^+ \neq 0$ as **Axiom Z,** since it says that *Z*ero is not a successor. Then $\forall x\ \forall y\ (x^+ = y^+ \Rightarrow x = y)$ is **Axiom U,** since it says that successors are *U*nique when they exist. Finally, there is **Axiom I,** or the **Axiom of Induction,** a *second-order* sentence that can be written formally as

$$\forall P\ (P0 \,\&\, \forall x\ (Px \Rightarrow P(x^+)) \Rightarrow \forall x\ Px),$$

where P is a singulary *predicate-variable*. Collectively, Axiom Z, Axiom U, and Axiom I can be called **the Peano Axioms.**

Axiom Z is that the immediate predecessor of 0 does *not* exist as an element of $\mathbb{N}$. The Axiom of Induction is that a set contains all natural numbers, provided that it contains 0 and contains the successor of each natural number that it contains. Later we shall define the binary operation $(x, y) \mapsto x + y$ on $\mathbb{N}$ so that $x^+ = x + 1$.

Lemma 4.0.2. *Every non-zero natural number is a successor. Symbolically,*

$$\mathbb{N} \vDash \forall x\ (x = 0 \vee \exists y\ y^+ = x).$$

Proof. Let A be the set of natural numbers comprising 0 and the successors. That is, $A = \{0\} \cup \{x \in \mathbb{N} : \exists y\ y^+ = x\}$. Then $0 \in A$ by definition. Also, if $n \in A$, then n^+ is a successor, so $n^+ \in A$. By induction, $A = \mathbb{N}$. □

In the last proof, the full inductive hypothesis $n \in A$ was not needed; only $n \in \mathbb{N}$ was needed.

Lemma 4.0.3. *Every natural number is distinct from its successor:*

$$\mathbb{N} \vDash \forall x\ x^+ \neq x.$$

Proof. Let $A = \{x \in \mathbb{N} : x^+ \neq x\}$. Now, 0^+ is a successor and is therefore distinct from 0 by Axiom Z. Hence $0 \in A$. Suppose $n \in A$. Then $n^+ \neq n$. Therefore $n^{++} \neq n^+$ by the contrapositive of Axiom U; so $n^+ \in A$. By induction, $A = \mathbb{N}$. □

4.1. Recursion

To able to say much more about the natural numbers, we should introduce the usual arithmetic operations. We need not do this by axioms; we can *define* the operations. There are at least two ways to do this. The approach that I propose to take starts with the following theorem. Its proof is difficult, but once we have the theorem, then we can freely define many useful operations and functions.

Theorem 4.1.1 (Recursion)**.** *Suppose A is a set with an element b, and $f\colon A \to A$. Then there is a* unique *function h from $\mathbb{N}$ to A such that $h(0) = b$ and*

$$h(n^+) = f(h(n)) \tag{4.1}$$

for all n in $\mathbb{N}$.

Proof. We seek h as a particular subset of $\mathbb{N} \times A$. Let $\mathcal{B}$ be the set whose elements are the subsets C of $\mathbb{N} \times A$ such that, if $(x, y) \in C$, then either

1) $(x, y) = (0, b)$ or else

2) C has an element (u, v) such that $(x, y) = (u^+, f(v))$.

Let $R = \bigcup \mathcal{B}$; so R is a relation from $\mathbb{N}$ to A. Since $(0, b) \in \mathcal{B}$, we have $0\ R\ b$. If $n\ R\ y$, then $(n, y) \in C$ for some C in $\mathcal{B}$, but then $C \cup \{(n^+, f(y))\} \in \mathcal{B}$ by definition of $\mathcal{B}$, so $(n^+)\ R\ f(y)$. Therefore R is the desired function h, provided it is a *function* from $\mathbb{N}$ to A. Proving this has two stages.

1. For all n in $\mathbb{N}$, there is y in A such that $n\ R\ y$. Indeed, let D be the set of such n. Then we have just seen that $0 \in D$, and if $n \in D$, then $scrn \in D$. By induction, $D = \mathbb{N}$.

2. For all n in $\mathbb{N}$, if $n\ R\ y$ and $n\ R\ z$, then $y = z$. Indeed, let E be the set of such n. Suppose $0\ R\ y$. Then $(0, y) \in C$ for some C in $\mathcal{B}$. Since 0 is not a successor, we must have $y = b$, by definition of $\mathcal{B}$. Therefore $0 \in E$. Suppose $n \in E$, and $(n^+)\ R\ y$. Then $(n^+, y) \in C$ for some C in $\mathcal{B}$. Again since 0 is not a successor, we must have $(n^+, y) = (m^+, f(v))$ for some (m, v) in C. Since succession is injective, we must have $m = n$. Since $n \in E$, we know v is *unique* such that $n\ R\ v$. Since $y = f(v)$, therefore y is unique such that $(n^+)\ R\ y$. Thus $n^+ \in E$. By induction, $E = \mathbb{N}$.

So R is the desired function h. Finally, h is unique by induction. □

In the statement of Theorem 4.1.1, (A, f, b) is a structure in the signature $\{^+, 0\}$. Also, Equation (4.1) is that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\ ^+\ } & \mathbb{N} \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ A & \xrightarrow[\ f\ ]{} & A \end{array}$$

That is, from the $\mathbb{N}$ on the left to the B on the right, there are two different routes, but each one yields the same result. In fact, the theorem is simply that there is a unique *homomorphism* from $(\mathbb{N}, ^+, 0)$ to (A, f, b).

A **recursive definition,** or a **definition by recursion,** is a definition of a function on $\mathbb{N}$ that is justified by Theorem 4.1.1. Informally, we can define such a function h by specifying $h(0)$ and by specifying how $h(n^+)$ is obtained from $h(n)$.

Sections 4.2 and 4.4 will provide several important examples of recursive definitions. Such definitions are sometimes[3] called *inductive definitions*, or *definitions by induction*. However, this terminology is misleading when Axiom I is called the Axiom of Induction. Logically, the Recursion Theorem is equivalent to the three Peano Axioms together; the Recursion Theorem is strictly stronger than the Induction Axiom, in the sense that there are models of Axiom I that do not satisfy Theorem 4.1.1. The remainder of this section is devoted to proving this.

Let us say that a structure **admits (definition by) recursion** if it satisfies the Recursion Theorem. That is, a structure $\mathfrak{A}$ in the signature $\{^+, 0\}$ admits recursion if and only if, for any other structure $\mathfrak{B}$ in this signature, there is a unique homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$.

Similarly, structures that satisfy the Induction Axiom can be said to **admit (proof by) induction.**

Theorem 4.1.2. *All structures that admit recursion are isomorphic.*

Proof. Suppose $\mathfrak{A}$ and $\mathfrak{B}$ admit recursion. Then there are unique homomorphisms f from $\mathfrak{A}$ to $\mathfrak{B}$ and g from $\mathfrak{B}$ to $\mathfrak{A}$. Hence the composition $g \circ f$ is a homomorphism from $\mathfrak{A}$ to itself; so it is the unique such homomorphism. But id_A is also such a homomorphism. Therefore $g \circ f = \mathsf{id}_A$. Similarly, $f \circ g = \mathsf{id}_B$. Therefore $g = f^{-1}$, by Theorem 3.3.4. □

Corollary 4.1.3. *All structures that admit recursion satisfy the Peano axioms; in particular, they admit induction.*

Proof. By the theorem, every structure that admits recursion is isomorphic to $(\mathbb{N}, ^+, 0)$. This satisfies the Peano axioms; hence so does every structure isomorphic to it. □

However, there are structures that admit induction, but not recursion:[4]

[3] Dedekind calls them definitions by induction in [12, Theorem 126, p. 85], which corresponds to the Recursion Theorem above.

[4] Apparently Peano himself did not recognize the distinction between proof by induction and definition by recursion; see the discussion of Landau [31, p. x]. Burris [6, p. 391] does not acknowledge the distinction. Stoll [48, p. 72] uses the term 'definition by weak recursion', although he observes that the validity of such a definition does *not obviously* follow from

Example 4.1.4. On $\mathbb{B}$, define a singulary operation s by $s(0) = 1$ and $s(1) = 0$. Then $(\mathbb{B}, s, 0)$ admits induction,[5] but there is *no* function $g : \mathbb{B} \to \mathbb{N}$ such that $g(0) = 0$ and $g(s(n)) = (g(n))^+$ for all n in $\mathbb{B}$.

Exercises

1. Prove the Recursion Theorem by showing that, if $\mathcal{C}$ is the set of all subsets D of A such that

   1) $(0, b) \in D$, and
   2) if $(u, v) \in D$, then $(u^+, f(v)) \in D$,

   then $\bigcap \mathcal{C}$ is the desired function h.

2. Prove directly (without Theorem 4.1.2) that Axiom Z is a consequence of the Recursion Theorem. (For example, if in $\mathfrak{A}$ the successor-operation is surjective, show that there is no homomorphism from $\mathfrak{A}$ into $\mathbb{N}$.)

4.2. Arithmetic operations

By recursion, we can define addition, multiplication and exponentiation.[6] First, we define the binary operation $+$ of **addition** on $\mathbb{N}$ by defining, for each n in $\mathbb{N}$, the singulary operation $y \mapsto n + y$. This operation is given by the rules:

1) $n + 0 = n$;
2) $n + m^+ = (n + m)^+$.

---

the Induction Axiom. However, Stoll does not *prove* (as we have done in Example 4.1.4) that the Induction Axiom is consistent with the negation of the Recursion Theorem.

[5] The structure $(\mathbb{B}, s, 0)$ in Example 4.1.4 also satisfies Axiom U, but not Axiom Z. If we define $t : \mathbb{B} \to \mathbb{B}$ so that $t(n) = 1$ for each n in $\mathbb{B}$, then $(\mathbb{B}, t, 0)$ satisfies the Induction Axiom and Axiom Z, but not Axiom U. Later we shall have natural examples of structures satisfying Axiom Z and Axiom U, but not admitting induction.

[6] We can also define addition and multiplication using only the Induction Axiom, not the Recursion Theorem. The method is used by Landau [31]. As a result, the operations can be defined on structures that do not satisfy all of the Peano Axioms. For example, let n be a positive integer, and on $\mathbb{Z}$ let $\equiv$ be congruence *modulo* n. if $x \equiv y$, then $x + 1 \equiv y + 1$ (though by the standards of this chapter, we cannot quite prove this yet). Hence we can define a successor-operation s on $\mathbb{Z}/\equiv$, namely $[x] \mapsto [x + 1]$. The resulting structure $(\mathbb{Z}/\equiv, s, [0])$ satisfies the Induction Axiom; therefore it can be equipped with an addition and a multiplication that satisfy the theorems of this section. Thus we get arithmetic ***modulo*** n. We can define exponentiation on $\mathbb{Z}/\equiv$ by $x^1 = x$ and $x^{k+1} = x^k \cdot x$ if and only if n is 1, 2, 6, 42, or 1806. If we try the definition in case $n = 3$, we get $2^1 = 2$, $2^2 = 2 \cdot 2 = 1$, so $2^{s(2)} = 2$, $2^{s(s(2))} = 1$—but also $s(s(2)) = 1$, so $2^{s(s(2))} = 2^1 = 2$.

Lemma 4.2.1. $\mathbb{N}$ *satisfies*
1) $\forall x\ 0 + x = x$,
2) $\forall x\ \forall y\ y^+ + x = (y + x)^+$.

Proof. By definition of addition, $0 + 0 = 0$. Suppose $0 + n = n$. Then

$$\begin{aligned} 0 + n^+ &= (0 + n)^+ && \text{[by definition of addition]} \\ &= n^+. && \text{[by inductive hypothesis]} \end{aligned}$$

This completes an induction showing $\vDash \forall x\ 0 + x = x$.

For the second claim, as the base step of an induction, we have

$$\begin{aligned} m^+ + 0 &= m^+ && \text{[by the first claim]} \\ &= (m + 0)^+; && \text{[again by the first claim]} \end{aligned}$$

so $\forall y\ y^+ + 0 = (y + 0)^+$.

Now, as an inductive hypothesis, suppose $\forall y\ y^+ + n = (y + n)^+$. Then, for all m in $\mathbb{N}$, we have

$$\begin{aligned} m^+ + n^+ &= (m^+ + n)^+ && \text{[by definition of addition]} \\ &= (m + n)^{++} && \text{[by inductive hypothesis]} \\ &= (m + n^+)^+ && \text{[again by definition of addition].} \end{aligned}$$

This completes an induction showing $\forall x\ \forall y\ y^+ + x = (y + x)^+$. □

The second part of the proof showed $\mathbb{N} = \{x : \forall y\ y^+ + x = (y + x)^+\}$: We have proved the identity

$$y^+ + x = (y + x)^+ \tag{4.2}$$

in $\mathbb{N}$ by **induction on** x. Induction on y here does not work directly. Indeed, suppose $A = \{y \in \mathbb{N} : \forall x\ y^+ + x = (y + x)^+\}$. To prove that $0 \in A$, we have to show that $0^+ + n = (0 + n)^+$. From the first part of the theorem, we know that $(0 + n)^+ = n^+$; but we cannot yet say anything about $0^+ + n$. We could prove $\forall x\ 0^+ + x = x^+$ by induction; but it would be more efficient just to start over and prove Identity (4.2) by induction on x.

To prove some identities below, one has to choose the right variable to work with.

Theorem 4.2.2. *On* $\mathbb{N}$*, the following hold.*
1. $\forall x\ x^+ = x + 1$.

2. *Addition is* ***commutative:***

$$\forall x\ \forall y\ x + y = y + x.$$

3. *Addition is* ***associative:***

$$\forall x\ \forall y\ \forall z\ (x + y) + z = x + (y + z).$$

4. *Addition admits* ***cancellation:***

$$\forall x\ \forall y\ \forall z\ (x + z = y + z \Rightarrow x = y).$$

We may henceforth write $n + 1$ instead of n^+.

The **binomial coefficients** $\binom{n}{m}$ can be given recursively as follows. First we define $m \mapsto \binom{0}{m}$ by

$$\binom{0}{m} = \begin{cases} 1, & \text{if } m = 0, \\ 0, & \text{if } m \neq 0. \end{cases}$$

Then, in terms of of $m \mapsto \binom{n}{m}$, we define $m \mapsto \binom{n+1}{m}$ recursively by

$$\binom{n+1}{m} = \begin{cases} 1, & \text{if } m = 0, \\ \binom{n}{k} + \binom{n}{k+1}, & \text{if } m = k + 1. \end{cases}$$

(See also Exercises 6 and 7 in § 4.5.)

The binary operation $\cdot$ of **multiplication** on $\mathbb{N}$ is given by:

1) $n \cdot 0 = 0$

2) $n \cdot (m + 1) = n \cdot m + n$.

Multiplication is also indicated by juxtaposition, so that $n \cdot m$ is nm.

Lemma 4.2.3. $\mathbb{N}$ *satisfies*

1) $\forall x\ 0x = 0$,

2) $\forall x\ \forall y\ (y + 1)x = yx + x$.

Theorem 4.2.4. *On* $\mathbb{N}$*, the following hold.*

1. $\forall x\ 1x = x$.
2. *Multiplication is commutative* $(\forall x\ \forall y\ xy = yx)$.
3. *Multiplication* ***distributes*** *over addition:*

$$\forall x\ \forall y\ \forall z\ (x + y)z = xz + yz.$$

4. *Multiplication is associative* $(\forall x\ \forall y\ \forall z\ (xy)z = x(yz))$.

Finally, exponentiation: the binary operation $(x, y) \mapsto x^y$ on $\mathbb{N}$ is given by:
1) $n^0 = 1$;
2) $n^{m+1} = n^m \cdot n$.

Theorem 4.2.5. *The following are identities in* $\mathbb{N}$*:*
1) $x^{y+z} = x^y x^z$*;*
2) $(x^y)^z = x^{yz}$*;*
3) $(xy)^z = x^z y^z$*.*

Proof. Exercise. □

Exercises

1. Prove Theorem 4.2.2. In the latter two parts, does induction work on every variable?
2. Prove that $\binom{x}{1} = x$ for all x in $\mathbb{N}$.
3. Prove Lemma 4.2.3. In the second part, does induction work on either variable?
4. Prove Theorem 4.2.4.
5. Prove Theorem 4.2.5.

4.3. Rational numbers

The positive rational numbers

The integers can be constructed from the natural numbers, and the rational numbers can be constructed from the integers. However, the *positive* rational numbers can also be constructed directly from the *positive* natural numbers, and indeed we are taught some aspects of this construction from an early age. Let us denote the set of positive natural numbers, $\{1, 2, 3, \dots\}$, by

$$\mathbb{N}^+.$$

If a and b are natural numbers, then there is a **fraction** denoted by

$$\frac{a}{b}$$

or a/b. Then there are definitions for adding and multiplying fractions:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{4.3}$$

We are taught to *reduce* fractions also: By (4.3) we compute $1/3 + 1/6 = 9/18$, which reduces to $1/2$. In particular, $9/18$ and $1/2$ are *equal* fractions. Equality of fractions may be given by

$$\frac{a}{b} = \frac{c}{d} \iff ad = cb. \tag{4.4}$$

This equation is justified by:

Theorem 4.3.1. *The relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ is an equivalence-relation.*

Proof. Reflexivity and symmetry of $\sim$ follow immediately from the corresponding properties of equality; but transitivity needs more. Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = cb$ and $cf = ed$, so

$$(ad)f = (cb)f = c(bf) = c(fb) = (cf)b = (ed)b$$

by commutativity and associativity of multiplication. By these properties and also cancellation, we can go on to conclude

$$af = eb,$$

hence $(a, b) \sim (e, f)$. □

The fraction a/b is the equivalence-class $(a, b)/\sim$, where

$$(a, b) \sim (x, y) \iff ay = bx. \tag{4.5}$$

Let us denote $(\mathbb{N}^+ \times \mathbb{N}^+)/\sim$ by

$$\mathbb{Q}^+.$$

This is the set of **positive rational numbers.**

Structure

We are free to define operations $\oplus$ and $\otimes$ on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \oplus (c, d) = (ad + cb, bd), \qquad (a, b) \otimes (c, d) = (ac, bd).$$

What makes these useful is the following:

Theorem 4.3.2. *If $a/b = a'/b'$ and $c/d = c'/d'$, then*

$$(a, b) \oplus (c, d) \sim (a', b') \oplus (c', d'),$$
$$(a, b) \otimes (c, d) \sim (a', b') \otimes (c', d').$$

Corollary 4.3.3. *On $\mathbb{Q}^+$, the equations (4.3) define two binary operations.*

Theorem 4.3.4. *On $\mathbb{Q}^+$,*

1) addition and multiplication are commutative and associative,
2) multiplication distributes over addition,
3) 1 is a ***multiplicative identity:***

$$\forall x \; 1 \cdot x = x.$$

The whole point of defining $\mathbb{Q}^+$ is the following:

Theorem 4.3.5. *There is a well-defined operation $x \mapsto x^{-1}$ on $\mathbb{Q}^+$ given by*

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

This operation is ***multiplicative inversion:***

$$\forall x \; x \cdot x^{-1} = 1.$$

Therefore, if r and s are in $\mathbb{Q}^+$, then the equation $r = s \cdot x$ has the unique solution $s^{-1}r$, which is written also as a fraction,

$$\frac{r}{s}.$$

If $a, b, c, d \in \mathbb{N}$, then

$$\frac{a/b}{c/d} = \frac{ad}{bc},$$

and in particular

$$\frac{a/1}{c/1} = \frac{a}{c}. \tag{4.6}$$

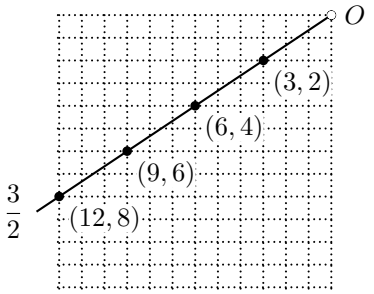


Figure 4.1. Fractions as straight lines

Numbers and fractions

By our construction, a positive natural number is not literally a positive rational number; a positive rational number is a class of ordered pairs of positive natural numbers. One way to understand this is shown in Figure 4.1, where ordered pairs of natural numbers are depicted as points in a grid; then a fraction is the class of ordered pairs lying on a particular straight line through the point O.

A fraction may not literally be a positive natural number; but there are fractions that *behave* like natural numbers:

Theorem 4.3.6. *The function $x \mapsto x/1$ is an embedding of $(\mathbb{N}^+, 1, +, \cdot)$ in $(\mathbb{Q}^+, 1/1, +, \cdot)$; that is, it is injective, it takes 1 to 1/1, and*

$$\frac{x+y}{1} = \frac{x}{1} + \frac{y}{1}, \qquad \frac{x \cdot y}{1} = \frac{x}{1} \cdot \frac{y}{1}.$$

Proof. Immediate from the definitions. □

We may therefore forget about the distinction between natural numbers and positive rational numbers: we may *identify* a natural number n with its image $n/1$ in $\mathbb{Q}^+$. By (4.6), there will be no ambiguity in writing fractions: a fraction of natural numbers as such will be the same as their fraction as positive rational numbers.

Using the idea in Figure 4.1, we can arrange the positive rational numbers along a semicircle, according to their ordering, as in Figure 4.2 (a). It is more usual to arrange the positive rational numbers along a straight line, as in Figure 4.2 (b); the point of using a semicircle is that here, if $k < m$, then m/k lies directly above k/m. Indeed, in Figure 4.3, since $BDCO$ is a semicircle, the

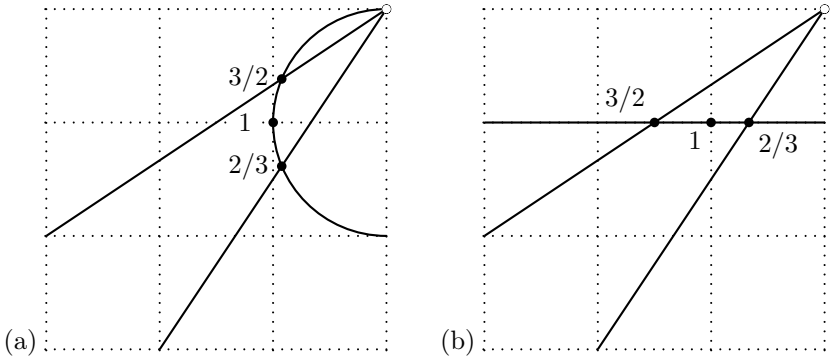


Figure 4.2. Positive rationals along a semicircle and a straight line

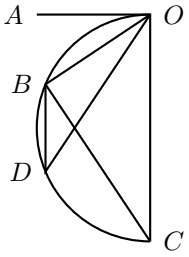


Figure 4.3. Fractions are below their reciprocals

angles AOB, OCB, and ODB are equal; if also AOB and COD are equal, then COD and ODB are equal, so the straight lines BD and OC are parallel.

The integers

In analogy with (4.5), let us define $\approx$ on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \approx (c, d) \iff a + d = b + c. \tag{4.7}$$

Then we have a direct analogue of Theorem 4.3.1:

Theorem 4.3.7. *The relation $\approx$ on $\mathbb{N} \times \mathbb{N}$ is an equivalence-relation.*

Now we can denote $(n, m)/\approx$ by

$$n - m.$$

Such an equivalence-class is just an **integer;** the set of all integers is

$$\mathbb{Z}.$$

As we have multiplication on $\mathbb{Q}^+$, so we have:

Theorem 4.3.8. *On $\mathbb{Z}$, there are a well-defined operation of addition given by*

$$(a-b)+(c-d)=(a+c)-(b+d).$$

In partial analogy with Theorem 4.3.4, we have

Theorem 4.3.9. *On $\mathbb{Z}$, addition is commutative and associative, and 0 is an **additive identity:***

$$\forall x\ 0+x=x.$$

In analogy with Theorem 4.3.5, we have

Theorem 4.3.10. *There is a well-defined operation $x \mapsto -x$ on $\mathbb{Z}$ given by*

$$-(k-n)=n-k.$$

*This operation is **additive inversion:***

$$\forall x\ x-x=0.$$

If a and b are in $\mathbb{Z}$, then the equation $a=b+x$ has the unique solution $-b+a$, which is also denoted by

$$a-b.$$

If $k,\ell,m,n \in \mathbb{N}$, then

$$(k-\ell)-(m-n)=(n+k)+(m+\ell).$$

In analogy with Theorem 4.3.6, we have

Theorem 4.3.11. *The function $x \mapsto x-0$ embeds $(\mathbb{N},0,+)$ in $(\mathbb{Z},0,+)$.*

We may identify a natural number n with its image $n-0$ in $\mathbb{Z}$. The elements of $\mathbb{Z}$ are usually depicted on a straight line extending infinitely in both directions. Alternatively, we can arrange them in a circle, as in Figure 4.4, where, if $0<n$, then $-n$ is directly to its right. The left half of the circle is the semicircle in Figure 4.2 (a).

Finally, we can extend **multiplication** on $\mathbb{N}$ to $\mathbb{Z}$ as in school, by

$$-m\cdot -n=m\cdot n, \qquad -m\cdot n=m\cdot -n=-(m\cdot n), \tag{4.8}$$

where m and n are in $\mathbb{N}$.

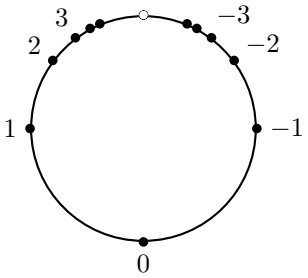


Figure 4.4. Integers on a circle

Theorem 4.3.12. *Multiplication on $\mathbb{Z}$ is commutative and associative, and it distributes over addition; also* 1 *is a multiplicative identity.*

Proof. Commutativity on $\mathbb{Z}$ with identity 1 follows immediately from commutativity on $\mathbb{N}$ with identity 1, along with the definitions (4.8). Associativity follows from considering the several cases, such as

$$(x \cdot -y) \cdot -z = -(x \cdot y) \cdot -z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot (-y \cdot -z).$$

For distributivity, we have for example, if $-y + z = w > 0$, then $z = w + y$, so $x \cdot z = x \cdot w + x \cdot y$, and therefore

$$x \cdot (-y + z) = -(x \cdot y) + x \cdot z = x \cdot -y + x \cdot z. \qquad \square$$

The rational numbers

As we obtained $\mathbb{Z}$ from $\mathbb{N}$, so we can obtain $\mathbb{Z}$ from $\mathbb{N}^+$. The difference is that the embedding of $\mathbb{N}^+$ in $\mathbb{Z}$ is $x \mapsto (x + 1) - 1$, and 0 in $\mathbb{Z}$ is $1 - 1$.

We can now obtain $(\mathbb{Q}, 0, -, +, \cdot)$ from $(\mathbb{Q}^+, +, \cdot)$ just as we obtain $(\mathbb{Z}, 0, -, +, \cdot)$ from $(\mathbb{N}^+, +, \cdot)$.

Theorem 4.3.13. *Addition and multiplication are commutative and associative on $\mathbb{Q}$, and multiplication distributes over addition. Addition has the identity* 0*, and multiplication has the identity* 1*. The operation $x \mapsto -x$ is additive inversion, and there is an operation $x \mapsto x^{-1}$ of multiplicative inversion on $\mathbb{Q} \setminus \{0\}$.*

Because of this theorem, $\mathbb{Q}$ is called a **field.**

Exercises

1. Prove Theorem 4.3.2 and Corollary 4.3.3.
2. Prove Theorem 4.3.4.
3. Prove Theorem 4.3.5.
4. Prove Theorem 4.3.7.
5. Prove Theorem 4.3.8.
6. Prove Theorem 4.3.9.
7. Prove Theorem 4.3.10.
8. Prove Theorem 4.3.11.
9. Prove Theorem 4.3.12.
10. Prove Theorem 4.3.13.

4.4. More recursion

Informally, we define $n!$, that is, **n-factorial,** by

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

More precisely, we have the recursive definition

$$0! = 1, \qquad (n+1)! = n! \cdot (n+1). \tag{4.9}$$

However, for this to be a valid definition by the Recursion Theorem as it is, we would have to express $n! \cdot (n+1)$ as a function of $n!$. Alternatively, (4.9) is a valid recursive definition by the following.

Theorem 4.4.1 (Recursion with Parameter)**.** *Suppose B is a set with an element c, and $F : \mathbb{N} \times B \to B$. Then there is a* unique *function G from $\mathbb{N}$ to B such that $G(0) = c$ and*

$$G(n+1) = F(n, G(n)) \tag{4.10}$$

for all n in $\mathbb{N}$.

Proof. Let f be the function

$$(x, b) \longmapsto (x + 1, F(x, b))$$

from $\mathbb{N} \times B$ to $\mathbb{N} \times B$. By recursion, there is a unique function g from $\mathbb{N}$ to $\mathbb{N} \times B$ such that $g(0) = (0, c)$ and

$$g(n + 1) = f(g(n))$$

for all n in $\mathbb{N}$. Now let G be $\pi \circ g$, where π is the function

$$(x, b) \longmapsto b$$

from $\mathbb{N} \times B$ to B. Then for each n in $\mathbb{N}$ we have $g(n) = (m, G(n))$ for some m in $\mathbb{N}$. We can prove by induction that $m = n$. Indeed, this is the case when $n = 0$, since $g(0) = (0, c)$. Suppose $g(n) = (n, G(n))$ for some n in $\mathbb{N}$. Then

$$g(n + 1) = f(n, G(n)) = (n + 1, F(n, G(n))). \tag{4.11}$$

In particular, the first entry in the value of $g(n + 1)$ is $n + 1$. This completes our induction.

We now know that $g(n) = (n, G(n))$ for all n in $\mathbb{N}$. Hence in particular $g(n+1) = (n+1, G(n+1))$. But we also have (4.11). Therefore we have (4.10), as desired. Finally, each of g and G determines the other. Since g is unique, so is G. □

Example 4.4.2. We can define a function f on $\mathbb{N}$ by requiring $f(0) = 0$ and $f(x + 1) = x$. This is a valid recursive definition, by Theorem 4.4.1. Note that f picks out the immediate predecessor of a natural number, when this exists.[7]

For any function f from $\mathbb{N}^+$ to M, where M is a set equipped with addition and multiplication, we can now define the sum $\sum_{k=1}^{n} f(k)$ and the product $\prod_{k=1}^{n} f(k)$ recursively as follows:

$$\sum_{k=1}^{0} f(k) = 0, \qquad \sum_{k=1}^{n+1} f(k) = \sum_{k=1}^{n} f(k) + f(n + 1),$$

$$\prod_{k=1}^{0} f(k) = 1, \qquad \prod_{k=1}^{n+1} f(k) = \prod_{k=1}^{n} f(k) \cdot f(n + 1).$$

See Exercise 1 below.

[7]Since f is unique, we now have a proof that Axiom U follows from the Recursion Theorem.

Exercises

1. Show clearly that the definitions of $\sum_{k=1}^{n} f(k)$ and $\prod_{k=1}^{n} f(k)$ are justified by Theorem 4.4.1.

2. Prove the following for all n in $\mathbb{N}$:
   a) $\sum_{k=1}^{n} k = n(n+1)/2$;
   b) $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$;
   c) $\sum_{k=1}^{n} b^{k-1} = (b^n - 1)/(b-1)$;
   d) $\sum_{k=1}^{n} (2k-1) = n^2$;
   e) $\prod_{k=1}^{n} (k/(k+1)) = 1/(n+1)$.

4.5. Ordering of the natural numbers

We can define the binary relation $\leqslant$ on $\mathbb{N}$ as the set

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} : \exists z \; x + z = y\}.$$

The associated strict relation $<$ is then $\{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leqslant y \,\&\, x \neq y\}$. Now we have to show that $\leqslant$ is the linear ordering that we expect:

Lemma 4.5.1. $\mathbb{N} \vDash \forall x \; \forall y \; (x + 1 \leqslant y + 1 \Rightarrow x \leqslant y)$.

Proof. Suppose $a + 1 \leqslant b + 1$. Then $a + 1 + c = b + 1$ for some c in $\mathbb{N}$, by definition of $\leqslant$. This means $a + c + 1 = b + 1$, by Lemma 4.2.1, so $a + c = b$, by Axiom U, and therefore $a \leqslant b$, again by the definition of $\leqslant$. □

Lemma 4.5.2. $\mathbb{N}$ *satisfies:*
1) $\forall x \; (x \leqslant 0 \Rightarrow x = 0)$*;*
2) $\forall x \; \forall y \; (x + y \leqslant x \Rightarrow y = 0)$.

Proof. Suppose $a \leqslant 0$. Then $a + b = 0$ for some b in $\mathbb{N}$. Either $a = 0$, or $a = c + 1$ for some c in $\mathbb{N}$, by Lemma 4.0.2. In the latter case, $c + b + 1 = 0$, which is absurd by Axiom Z. Hence $a = 0$, and the first claim is proved.

Now suppose $a + b \leqslant a$. Then $a + b + c = a = a + 0$ for some c, so $b + c = 0$ by cancellation (Theorem 4.2.2), which means $b \leqslant 0$. Hence $b = 0$ by the first claim. The second claim is now proved. □

Lemma 4.5.3. $\mathbb{N}$ *satisfies:*
1) $\forall x \; \forall y \; (x < y \Rightarrow x + 1 \leqslant y)$*;*

2) $\forall x\, \forall y\, (x < y + 1 \Rightarrow x \leqslant y)$.

Proof. To prove the first claim, by Lemma 4.0.2, it is enough to show

$$\forall x\, (x < 0 \Rightarrow x + 1 \leqslant 0),$$
$$\forall x\, \forall y\, (x < y + 1 \Rightarrow x + 1 \leqslant y + 1).$$

The first sentence is trivially true in $\mathbb{N}$ by Lemma 4.5.2, since the hypothesis $x < 0$ always fails: If $n < 0$, then $n \leqslant 0$, so $n = 0$, which means $\neg(n < 0)$.

For the second sentence, suppose $n < m + 1$. Then $n + \ell = m + 1$ for some ℓ; but $\ell \neq 0$, so $\ell = k + 1$ for some k. Hence $n + k + 1 = m + 1$, that is, $n + 1 + k = m + 1$, so $n + 1 \leqslant m + 1$.

The proof of the second claim is an exercise. □

Theorem 4.5.4. *On* $\mathbb{N}$*, the relation* $\leqslant$ *is a linear ordering.*

Proof. There are four properties to check:
Reflexivity: Since $n + 0 = n$, we have $n \leqslant n$ by definition.
Anti-symmetry: We show

$$n \leqslant x \,\&\, x \leqslant n \Rightarrow n = x$$

by considering that, by Lemma 4.0.2, x is either 0 or a successor. If $n \leqslant 0$ and $0 \leqslant n$, then $n \leqslant 0$, so $n = 0$ by Lemma 4.5.2. Suppose $n \leqslant m + 1$ and $m + 1 \leqslant n$. From the latter inequality, $n = m + 1 + \ell = m + \ell + 1$ for some ℓ. Hence $m + \ell + 1 \leqslant m + 1$ by the former inequality, so $m + \ell \leqslant m$ by Lemma 4.5.1. Hence $\ell = 0$ by Lemma 4.5.2, so $n = m + 1 + 0 = m + 1$.
Transitivity: We show

$$\ell \leqslant m \,\&\, m \leqslant z \Rightarrow \ell \leqslant z$$

by induction on z. If $\ell \leqslant m$ and $m \leqslant 0$, then $m = 0$ by Lemma 4.5.2, so $\ell \leqslant 0$. As an inductive hypothesis, suppose the claim holds when $z = n$. Suppose also $\ell \leqslant m$ and $m \leqslant n + 1$. There are two possibilities. If $m = n + 1$, then $\ell \leqslant n + 1$ immediately. Suppose $m < n + 1$. Then $m \leqslant n$ by Lemma 4.5.3, so $\ell \leqslant n$ by inductive hypothesis. By definition then, $\ell + k = n$ for some k, so $\ell + k + 1 = n + 1$, and therefore $\ell \leqslant n + 1$. This completes the induction.
Linearity: We show

$$x \leqslant m \vee m \leqslant x$$

by induction on x. Since $0 + m = m$, we have $0 \leqslant m$. As an inductive hypothesis, suppose the claim holds when $x = n$. Suppose $\neg(n + 1 \leqslant m)$ for some m. Then $\neg(n < m)$ by Lemma 4.5.3. By inductive hypothesis, $m \leqslant n$. Also $n \leqslant n + 1$. By transitivity, $m \leqslant n + 1$. □

Various standard properties can now be proved:

Theorem 4.5.5. *The following are true in* $\mathbb{N}$.

1. $\forall x\ \forall y\ \forall z\ (x < y \Leftrightarrow x + z < y + z)$.
2. $\forall x\ \forall y\ \forall z\ (x < y \Leftrightarrow x \cdot (z + 1) < y \cdot (z + 1))$.
3. $\forall x\ \forall y\ \exists z\ (x \leqslant y \Leftrightarrow x + z = y)$.

Exercises

1. Complete the proof of Lemma 4.5.3.
2. Prove Theorem 4.5.5.
3. Prove $\mathbb{N} \vDash \forall x\ x < 2^x$. (See § 3.6 (3.52).)
4. Prove the following in $\mathbb{N}$:
   a) $\forall x\ \forall y\ 1 + xy \leqslant (1 + x)^y$,
   b) $\forall x\ (3 < x \Rightarrow x^2 < 2^x)$.
5. Find the flaw in the following argument, where max is the function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that $\max(x, y) = y$ if $x \leqslant y$, and otherwise $\max(x, y) = x$.

   > If $\max(x, y) = 0$, then $x = y$. Suppose that $x = y$ whenever $\max(x, y) = n$. Suppose $\max(z, w) = n + 1$. Then $\max(z - 1, w - 1) = n$, so $z - 1 = w - 1$ by inductive hypothesis; therefore $z = w$. Therefore all natural numbers are equal.

6. Prove that, if $y \leqslant x$, then $\binom{x}{y} = \dfrac{x!}{y!\,(x - y)!}$.
7. Prove the **Binomial Theorem:**

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

8. Prove that every proper divisor of a positive integer is less than that integer. (A **proper divisor** is a divisor other than the number itself.)

4.6. Real numbers

From § 4.3, we have $\mathbb{Q}$ and its subset $\mathbb{Q}^+$. We can define the relation $<$ on $\mathbb{Q}$ by

$$x < y \Leftrightarrow y - x \in \mathbb{Q}^+.$$

Theorem 4.6.1. *The relation $<$ is a strict linear ordering of $\mathbb{Q}$ such that*

$$x < y \Leftrightarrow x + z < y + z,$$
$$x < y \,\&\, 0 < z \Rightarrow z \cdot x < z \cdot y.$$

Because of this and Theorem 4.3.13, $\mathbb{Q}$ is called an **ordered field.**

A linear order is **dense** if between any two distinct elements lies a third, that is,

$$\forall x\, \forall y\, \exists z\, (x < y \Rightarrow x < z \,\&\, z < y).$$

An **endpoint** of a linear order is a **maximum** or a **minimum,** that is, an element a such that no element is greater or no element is less:

$$\forall x\, x \leqslant a \vee \forall y\, a \leqslant y.$$

Theorem 4.6.2. $(\mathbb{Q}, <)$ *and* $(\mathbb{Q}+, <)$ *are dense linear orders without endpoints.*

Suppose $(A, <)$ is a dense linear order without endpoints. A **cut** of $(A, <)$ is a nonempty proper subset B of A whose every element is less than every element of its complement:

$$\forall x\, \forall y\, (x \in B \,\&\, y \in A \setminus B \Rightarrow x < y).$$

If $C \subseteq A$ and $d \in A$, then d is an **upper bound** of C if no element of C is greater than d:

$$\forall x\, (x \in C \Rightarrow x \leqslant d).$$

A **lower bound**is defined similarly. Then d is a **supremum** of C if it is a least upper bound of C, that is, d is an upper bound of C and also a lower bound of the set of upper bounds of C. Likewise, an **infimum** is a greatest lower bound.

Theorem 4.6.3. *Suprema and infima are unique when they exist. If the set of lower bounds of a subset C of a linear order has a supremum, then this is the infimum of of C.*

A linear order is **complete** if every nonempty subset with an upper bound has a supremum; it follows then that every nonempty subset with a lower bound has an infimum.

Theorem 4.6.4. *As a linear order, $\mathbb{Q}$ is not complete.*

Proof. The set of positive rationals x such that $x^2 < 2$ has no supremum in $\mathbb{Q}$ (why not?). □

Suppose A is a dense linear order without endpoints. Let $\bar{A}$ be the set of cuts of A. If $b \in A$, let

$$\mathrm{pred}(b) = \{x \in A \colon x < b\},$$

the set of **predecessors** of b in A; then $\mathrm{pred}(b) \in \bar{A}$.

Theorem 4.6.5. *Suppose A is a dense linear order without endpoints. Then $\bar{A}$, with respect to inclusion, is a dense linear order without endpoints and is complete with respect to this ordering; also the function $x \mapsto \mathrm{pred}(x)$ from A to $\bar{A}$ is an embedding of orders.*

Proof. We already know inclusion is a partial ordering of $\bar{A}$. If B and C are distinct cuts of A, then we may assume $C \setminus B$ has an element d; but then d is an upper bound of B, and $B \subset C$. Thus inclusion linearly orders $\bar{A}$.

If $\mathcal{D}$ is a set of cuts of A, then $\bigcup \mathcal{D}$ is also a cut and is the supremum of $\mathcal{D}$.

In A, if $x < y$, then $\mathrm{pred}(x) \subseteq \mathrm{pred}(y)$ and moreover $\mathrm{pred}(x) \subset \mathrm{pred}(y)$ since $x \in \mathrm{pred}(y) \setminus \mathrm{pred}(x)$. □

If A is a dense linear order without endpoints, then $\bar{A}$ is called the **completion**[8] of A. We can now denote the completion of $\mathbb{Q}$ by

$$\mathbb{R};$$

this is the set of **real numbers.** The challenge is to define addition and multiplication on $\mathbb{R}$ and show they have the usual properties. We can define addition on $\mathbb{R}$ by

$$X + Y = \bigcup \{\mathrm{pred}(x + y) \colon \mathrm{pred}(x) \subseteq X \,\&\, \mathrm{pred}(y) \subseteq Y\}.$$

It is easier to define multiplication first on the completion of $\mathbb{Q}^+$, which we can denote by

$$\mathbb{R}^+.$$

[8] Strictly, to justify this terminology, one should show that $\bar{A}$ is somehow minimal among the complete dense linear orders without endpoints in which A embeds, and moreover all such minimal orders are somehow isomorphic.

Here we define multiplication by

$$X \cdot Y = \bigcup \{\text{pred}(xy) \colon \text{pred}(x) \subseteq X \,\&\, \text{pred}(y) \subseteq Y\}.$$

One then extends multiplication to $\mathbb{R}$, just as it is extended from $\mathbb{Q}^+$ to $\mathbb{Q}$. Ultimately one obtains:

Theorem 4.6.6. $(\mathbb{R}, +, \cdot, <)$ *is an ordered field, the function* $x \mapsto \text{pred}(x)$ *from* $\mathbb{Q}$ *to* $\mathbb{R}$ *is an embedding of ordered fields.*

Now we can refer to $\mathbb{R}$ as the[9] **complete ordered field.** We consider $\mathbb{Q}$ as an ordered subfield of $\mathbb{R}$.

Theorem 4.6.7. $\mathcal{P}(\mathbb{N}) \preccurlyeq \mathbb{R}$*; in particular,* $\mathbb{R}$ *is uncountable.*

Proof. There is an embedding h of ${}^{\mathbb{N}^+}\mathbb{B}$ in $\mathbb{R}$ given by

$$h(e_k \colon k \in \mathbb{N}^+) = \sup \left\{ \sum_{k=1}^{n} \frac{e_k}{3^k} \colon k \in \mathbb{N} \right\}. \qquad \square$$

Exercises

1. Prove Theorem 4.6.1.
2. Prove Theorem 4.6.2.
3. Prove Theorem 4.6.3.
4. Prove Theorem 4.6.4.

4.7. Well-ordered sets

Suppose $(\Omega, \leqslant)$ is a linear order, and $A \subseteq \Omega$. A **least** element of A is an infimum of A that also belongs to A. By Theorem 4.6.3, least elements are unique when they exist. *The* least element—if it exists—of A can be denoted by

$$\min(A).$$

The linear order $(\Omega, \leqslant)$:

1) **is well-ordered** if every non-empty subset of Ω has a least element;

[9] Again the use of the definite article the should be justified by a uniqueness proof.

2) **admits (proof by) strong induction** if $A = \Omega$ whenever A is a subset of Ω such that
$$\text{pred}(b) \subseteq A \implies b \in A$$
for all b in Ω;
3) **admits (definition by) strong recursion** if, for every set B and function h from $\mathcal{P}(B)$ to B, there is a unique function G from Ω to B such that
$$G(c) = h(G[\text{pred}(c)])$$
for all c in Ω.

We shall see presently that these three conditions are equivalent. Meanwhile, we can observe that $(\mathbb{N}, \leqslant)$ satisfies one of the conditions.

Lemma 4.7.1. $\text{pred}(n+1) = \text{pred}(n) \cup \{n\}$ *for all* n *in* $\mathbb{N}$.

Proof. Since $n < n+1$, we have $\text{pred}(n) \cup \{n\} \subseteq \text{pred}(n+1)$. For the reverse inclusion, suppose $a \in \text{pred}(n+1)$, so that $a < n+1$. Then $a \leqslant n$ by Lemma 4.5.3, so $a = n$ or $a < n$; in either case, $a \in \text{pred}(n) \cup \{n\}$. Thus, $\text{pred}(n+1) \subseteq \text{pred}(n) \cup \{n\}$. □

Theorem 4.7.2. $(\mathbb{N}, \leqslant)$ *admits strong induction.*

Proof. Suppose A is a subset of $\mathbb{N}$ that contains n whenever it includes $\text{pred}(n)$. By induction, we shall show that $\text{pred}(n) \subseteq A$ for all n in $\mathbb{N}$; from this, it will follow that $A = \mathbb{N}$.

Since $\text{pred}(0) = \varnothing$, and $\varnothing \subseteq A$, this means $0 \in A$ by assumption. As an inductive hypothesis, suppose $\text{pred}(n) \subseteq A$. Then $n \in A$ by assumption, so $\text{pred}(n) \cup \{n\} \subseteq A$, that is, $\text{pred}(n+1) \subseteq A$ by Lemma 4.7.1. This completes the induction. Hence, for all n, we have $n \in \text{pred}(n+1) \subseteq A$, so $n \in A$. Thus $A = \mathbb{N}$. □

Example 4.7.6 will show one use of strong induction.

The linearly ordered set $(\Omega, \leqslant)$ is well-ordered if and only if every subset with no least element is empty. This formulation will be used in proving the following theorem. Also, a subset A of Ω has no least element if and only if

$$\forall x\ (\text{pred}(x) \cap A = \varnothing \Rightarrow x \notin A),$$

that is, $\forall x\ (\text{pred}(x) \subseteq \Omega \setminus A \Rightarrow x \in \Omega \setminus A)$.

Theorem 4.7.3. *The following are equivalent conditions on a linear order.*

1. *It is well-ordered.*
2. *It admits strong induction.*
3. *It admits strong recursion.*

Proof. Let $(\Omega, \leqslant)$ be a linear order. We shall show that, if it admits strong induction *or* strong recursion, then it is well-ordered, and if it is well-ordered, then it admits strong induction *and* strong recursion. Then the claim will follow from the equivalences

$$\boldsymbol{P} \vee \boldsymbol{Q} \Rightarrow \boldsymbol{R} \sim (\boldsymbol{P} \Rightarrow \boldsymbol{R}) \,\&\, (\boldsymbol{Q} \Rightarrow \boldsymbol{R}), \quad \boldsymbol{R} \Rightarrow \boldsymbol{P} \,\&\, \boldsymbol{Q} \sim (\boldsymbol{R} \Rightarrow \boldsymbol{P}) \,\&\, (\boldsymbol{R} \Rightarrow \boldsymbol{Q}).$$

Suppose $(\Omega, \leqslant)$ admits strong induction, but A is a subset of Ω with no least element. We shall show that A is empty. If $a \in \Omega$, and $\mathrm{pred}(a) \subseteq \Omega \smallsetminus A$, then $a \in \Omega \smallsetminus A$, since a is not a least element of A. By strong induction, $\Omega = \Omega \smallsetminus A$, so $A = \varnothing$. Thus $(\Omega, \leqslant)$ is well-ordered.

Suppose $(\Omega, \leqslant)$ admits strong recursion, but A is a subset of Ω with no least element. Let

$$C = \{x \in \Omega \colon \exists y \, (y \in A \,\&\, y \leqslant x)\}.$$

Then C has no least element (exercise). For each e in $\mathbb{B}$, let G_e be the function from Ω to $\mathbb{B}$ given by

$$G_e(x) = \begin{cases} 0, & \text{if } x \notin C; \\ e, & \text{if } x \in C. \end{cases}$$

So G_1 is the characteristic function of C on Ω in the sense of § 3.6, but G_0 is the constant function $x \mapsto 0$ on Ω. Let h be the function from $\mathcal{P}(\mathbb{B})$ to $\mathbb{B}$ given by

$$h(X) = 1 \iff 1 \in X,$$

that is,

$$h(X) = \begin{cases} 0, & \text{if } X \in \big\{\varnothing, \{0\}\big\}; \\ 1, & \text{if } X \in \big\{\{1\}, \{0, 1\}\big\}. \end{cases}$$

Then $G(a) = h(G[\mathrm{pred}(a)])$ for all a in Ω, whether G is G_0 or G_1 (exercise). By strong recursion, there is a *unique* such function G, so $G_0 = G_1$. Therefore $C = \varnothing$. Thus $(\Omega, \leqslant)$ is well-ordered.

Now, conversely, suppose $(\Omega, \leqslant)$ is well-ordered. First, let A be a subset of Ω such that, if $\mathrm{pred}(a) \subseteq A$, then $a \in A$, for all a in A. Consequently, if $\mathrm{pred}(a) \cap (\Omega \smallsetminus A) = \varnothing$, then $a \notin \Omega \smallsetminus A$. Then $\Omega \smallsetminus A$ has no least element, so it is empty, and $A = \Omega$. Thus $(\Omega, \leqslant)$ admits strong induction.

Finally, using that $(\Omega, \leqslant)$ admits strong induction, we shall follow the proof of the Recursion Theorem, 4.1.1, to prove that $(\Omega, \leqslant)$ admits strong recursion. Suppose B is a set, and $h\colon \mathcal{P}(B) \to B$. Let $\mathcal{S}$ be the set of relations R from Ω to B such that, if $(a, b) \in R$, then there is a function f from $\mathrm{pred}(a)$ to B such that

$$b = h(f[\mathrm{pred}(a)]).$$

Let $T = \bigcup \mathcal{S}$. We show first that T is a function G from Ω to B, that is, for all x in Ω,

$$\exists!\, y\ x\ T\ y.$$

Suppose, as a strong inductive hypothesis, that this is true when $x \in \mathrm{pred}(a)$. Then there is a function f from $\mathrm{pred}(a)$ to B such that

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

Then $(a, h(f[\mathrm{pred}(a)])) \in T$ by definition of T; moreover, if $(a, b) \in T$, then $b = h(f[\mathrm{pred}(a)])$. By strong induction, T is a function G from Ω to B. If now $a \in \Omega$, and $f = G \restriction \mathrm{pred}(a)$, then we must have $G(a) = h(f[\mathrm{pred}(a)])$, again by definition of T; so $G(a) = h(G[\mathrm{pred}(a)])$.

Suppose also $G'\colon \Omega \to B$ and $G'(a) = h(G'[\mathrm{pred}(a)])$ for all a in Ω. Let

$$D = \{x \in \Omega\colon G(x) = G'(x)\}.$$

If $\mathrm{pred}(a) \subseteq D$, then $G'(a) = h(G'[\mathrm{pred}(a)]) = h(G[\mathrm{pred}(a)]) = G(a)$, so $a \in D$. By strong induction, $D = \Omega$, so $G' = G$. Thus G is the only function on Ω in $\mathcal{S}$, and $(\Omega, \leqslant)$ admits strong recursion. □

Corollary 4.7.4. *$(\mathbb{N}, \leqslant)$ is well-ordered and admits strong recursion.*

Proof. Theorem 4.7.2. □

Interrelations

What is the force of the word strong in strong induction and strong recursion?

Structures that admit induction or recursion have a signature that includes $\{^+, 0\}$. Structures that admit strong induction or strong recursion have a signature that includes $\{\leqslant\}$. The next theorem establishes one possible connexion between these two kinds of structures:

Theorem 4.7.5. *Suppose $(\Omega, {}^+, 0)$ admits induction and has a partial ordering $\leqslant$ such that $a < a^+$ for all a in Ω. Then $\leqslant$ is a linear ordering, and $\mathbb{N}$ and Ω are isomorphic as structures in the signature $\{^+, 0, \leqslant\}$: in particular, $(\Omega, \leqslant)$ admits strong induction.*

Proof. Since $(\mathbb{N}, {}^+, 0)$ admits recursion, there is a homomorphism h from $(\mathbb{N}, {}^+, 0)$ to $(\Omega, {}^+, 0)$. In particular,

$$h(m)^+ = h(m+1)$$

for all m in $\mathbb{N}$. We shall first show that the function h is also a homomorphism from $(\mathbb{N}, <)$ to $(\Omega, <)$; that is,

$$\forall x\ (x < n \Rightarrow h(x) < h(n)) \tag{4.12}$$

for all n in $\mathbb{N}$. This is trivially true when $n = 0$. Suppose it is true when $n = m$, and now $a < m + 1$. Then $a \leqslant m$. Either $a = m$ or $a < m$.

1. If $a = m$, then $h(a) = h(m) < h(m)^+ = h(m+1)$.
2. If $a < m$, then by inductive hypothesis, $h(a) < h(m) < h(m)^+ = h(m+1)$.

In either case, $h(a) < h(m+1)$. Thus (4.12) is true when $n = m + 1$. By induction, it is true for all n in $\mathbb{N}$.

Also, h is surjective, by induction in $(\Omega, {}^+, 0)$. Indeed, $0 \in h[\mathbb{N}]$, and if $a \in h[\mathbb{N}]$, then $a = h(n)$ for some n in $\mathbb{N}$, so $a^+ = h(n)^+ = h(n+1)$, and $a^+ \in h[\mathbb{N}]$.

Since h is a bijection, it is an isomorphism from $\mathbb{N}$ to Ω in the signature $\{{}^+, 0\}$. To complete the proof, it is enough to show that h^{-1} is order-preserving. If $h(m) \leqslant h(n)$, then $\neg(h(n) < h(m))$, so $\neg(n < m)$ by (4.12); hence, $m \leqslant n$. □

Thus, roughly,

$$\text{induction } \&\ \text{ordering } \Longrightarrow \text{ strong induction.} \tag{4.13}$$

It is sometimes suggested[10] that strong induction can be proved from induction alone. It cannot; there has to be an ordering, as in the theorem, and induction alone does not guarantee that there is such an ordering. Example 4.1.4 gives a structure that admits induction, but has no ordering such that $\forall x\ x < x + 1$.

Strong induction on $\mathbb{N}$ is called strong because it involves a stronger *hypothesis* than ordinary induction. To prove $\mathbb{N} \vDash \forall x\ \varphi(x)$ by induction, one proves two things, as described in § 1.2:

1. $\mathbb{N} \vDash \varphi(0)$.
2. $\mathbb{N} \vDash \forall x\ (\varphi(x) \Rightarrow \varphi(x+1))$.

The inductive hypothesis is here is $\varphi(x)$. To make the proof by strong induction, one proves one thing:

1. $\mathbb{N} \vDash \forall x\ (\forall y\ (y < x \Rightarrow \varphi(y)) \Rightarrow \varphi(x))$.

[10] For example, Epp [18, § 4.4, p. 213] says that the two methods of proof are equivalent; but the proofs use hidden assumptions.

Here the **strong inductive hypothesis** is $\forall y\ (y < x \Rightarrow \varphi(y))$. If x is 0, then this hypothesis is trivially true; if x is not 0, then x is a successor. Hence we can analyse a proof by strong induction into two steps, as with ordinary induction:

1. $\mathbb{N} \vDash \varphi(0)$.
2. $\mathbb{N} \vDash \forall x\ (\forall y\ (y \leqslant x \Rightarrow \varphi(y)) \Rightarrow \varphi(x+1))$.

In this formulation, the strong inductive hypothesis is $\forall y\ (y \leqslant x \Rightarrow \varphi(y))$, that is,

$$\varphi(0)\ \&\ \varphi(1)\ \&\ \ldots\ \&\ \varphi(x);$$

this is a stronger assumption than $\varphi(x)$ alone. Sometimes this stronger assumption is just what one needs:

Example 4.7.6. To prove that every natural number other than 1 has a prime divisor, it seems not enough to use induction. If n has prime divisors, what does that say about $n+1$? But every positive integer divides 0, so 0 has prime divisors. Suppose $n > 0$, and all of the numbers in the set $\{2, 3, 4, \ldots, n\}$ have prime divisors. If $n+1$ is prime, then it is its own prime divisor. If n is composite, then it has a divisor in the set just named, by Exercise 8 in § 4.5. By strong inductive hypothesis, this divisor has a prime divisor, which is then a divisor of $n+1$.

From the theorem, there follows a connexion between recursion and strong recursion:

Corollary 4.7.7. *Every structure $(\Omega, {}^+, 0)$ that admits recursion has a partial ordering $\leqslant$ such that $a < a+1$ for all a in Ω. If $\leqslant$ is any such ordering on Ω, then $\leqslant$ is linear, and $(\Omega, \leqslant)$ admits strong recursion.*

Proof. Every structure that admits recursion satisfies the Peano axioms, by Corollary 4.1.3; in particular, it has a linear ordering as defined in § 4.5, so it admits strong recursion by Corollary 4.7.4. If $\leqslant$ is just a partial ordering of the structure such that $\forall x\ x < x+1$, then the theorem applies, showing that the structure is isomorphic to $\mathbb{N}$ and so admits strong recursion. □

In short then,

$$\text{recursion} \implies \text{strong recursion}. \tag{4.14}$$

That is, logically, recursion is at least as strong as strong recursion. The converses of (4.14) and (4.13) fail. To show this, some more definitions will be useful. Let $(\Omega, \leqslant)$ be a well-ordered set. We can use 0 as a name for $\min(\Omega)$. An element a of Ω is a **limit** if

1) $a \neq 0$, and

2) $\forall x\ \exists y\ (x < a \Rightarrow x < y < a)$.

In short, a is a limit if it is not zero and has no immediate predecessor.

Examples 4.7.8.

1. $(\mathbb{N}, \leqslant)$ has no limits.
2. Extend $\leqslant$ so that it well-orders $\mathbb{N} \cup \{\infty\}$ by defining $n < \infty$ for all n in $\mathbb{N}$. Then ∞ is a limit.

A **greatest** element of a subset A of Ω is a supremum of A that belongs to A. Suppose Ω itself has no greatest element. Then every element a of Ω has a successor, a^+, given by

$$x^+ = \min(\{y \in \Omega \colon x < y\}).$$

In this case, the limits of Ω are just those elements not in $\{0\} \cup \{x^+ \colon x \in \Omega\}$, that is, the non-zero elements of Ω that are not successors.

Theorem 4.7.9. *Every well-ordered set with no greatest element and no limits admits induction and recursion.*

Proof. We shall show that such structures satisfy the Peano axioms. In such structures, we always have $0 \leqslant x < x^+$. In particular, $0 \neq x^+$. Thus Axiom Z is satisfied. Also, if $a < b$, then $a^+ \leqslant b < b^+$; so Axiom U is satisfied. Finally, suppose A is a proper subset of such a structure Ω, and $0 \in A$. Then $\Omega \setminus A$ has a least element b, which is not 0, so it must be a successor c^+. Then $c \in A$, but $c^+ \notin A$. Contrapositively, if $0 \in A$, and $\forall x\ (x \in A \Rightarrow x^+ \in A)$, then $A = \Omega$. That is, Axiom I is satisfied. □

If a well-ordered set does have a greatest element, then this can have no successor, so induction and recursion are meaningless. If the well-ordered set Ω has no greatest element, but does have limits, let ℓ be its *least* limit. Then $\mathrm{pred}(\ell)$ satisfies the hypotheses of Theorem 4.7.9, so it admits induction and recursion; but the whole structure Ω does not (exercise).[11]

Exercises

1. Supply the missing details in the proof of Theorem 4.7.3.

[11] Rotman [43] gives an intuitive argument, based tacitly on induction and the ordering, for why $\mathbb{N}$ is well-ordered; then he claims to *prove* induction, seemingly from well-ordering alone. The hidden assumption is that every non-zero element of $\mathbb{N}$ is a successor.

2. Show that there are well-ordered sets with no greatest element that do not admit induction or recursion.

3. Find a formula $\psi(x, y)$ containing no quantifiers such that the sentence $\forall x\ \exists y\ \psi(x, y)$ is logically equivalent to $\forall x\ (\forall y\ (y < x \Rightarrow \varphi(y)) \Rightarrow \varphi(x))$.

4.8. Ordinal numbers

A class that includes each of its elements is called **transitive.** So **C** is transitive if and only if

$$A \in B\ \&\ B \in \mathbf{C}\ \implies\ A \in \mathbf{C}.$$

By the definition given in § 1.2, an **ordinal,** or **ordinal number,** is a *set* that is transitive and is *strictly* well-ordered by membership. The class of ordinals is denoted by

$$\mathbf{ON}.$$

The Greek letters α, β, γ, ... will henceforth denote ordinals.

Lemma 4.8.1. ON *is transitive, that is, every element of an ordinal is an ordinal. Also every ordinal* properly *includes its elements.*

Proof. Suppose $\alpha \in \mathbf{ON}$ and $b \in \alpha$. Then $b \subseteq \alpha$ by transitivity of α, so b is well-ordered by membership. Suppose $c \in b$ and $d \in c$. Then $c \in \alpha$, so $c \subseteq \alpha$, and hence $d \in \alpha$. Since $d \in c$ and $c \in b$, and all are elements of α, where membership is a transitive relation, we have $d \in b$. Thus b is transitive, so it is an ordinal. Therefore $\alpha \subseteq \mathbf{ON}$. So **ON** is transitive.

Finally, $b \subset \alpha$ simply because membership is a *strict* ordering of α. □

Lemma 4.8.2. *Every ordinal contains every ordinal that it properly includes.*

Proof. Suppose $\beta \subset \alpha$. Then $\alpha \setminus \beta$ contains some γ. Then $\beta \subseteq \gamma$; indeed, if $\delta \in \beta$, then, since $\gamma \notin \beta$, we have $\gamma \notin \delta$ (by transitivity of β) and $\gamma \neq \delta$, so $\delta \in \gamma$ (since α is strictly linearly ordered by membership). Suppose $\beta \subset \gamma$. Then $\gamma \setminus \beta$ contains some δ, so by what we have just shown, $\beta \subseteq \delta$. But $\delta \subset \gamma$ by the last lemma, so γ was not the least element of $\alpha \setminus \beta$ (since δ must be less). Therefore the least element of $\alpha \setminus \beta$ must be β; in particular, $\beta \in \alpha$. □

Theorem 4.8.3 (Burali-Forti Paradox [5])**. ON** *is transitive and well-ordered by membership; so it is not a set.*

Proof. Because membership is a *strict* ordering of an ordinal, membership is irreflexive on **ON**. Because each ordinal is transitive, membership is a transitive relation on **ON**. Let α and β be two distinct ordinals such that $\beta \notin \alpha$. By strong induction in α, we have $\alpha \in \beta$. Indeed, say $\gamma \in \alpha$ and $\gamma \subseteq \beta$. Then $\gamma \neq \beta$, so $\gamma \in \beta$ by the last lemma. Therefore **ON** is strictly linearly ordered by membership. In particular, if $\alpha \in \mathbf{ON}$, then $\alpha \neq \mathbf{ON}$; so **ON** is not an ordinal.

If a is a set of ordinals with an element β, then the least element of a is the least element of $a \cap \beta$, if this set is nonempty; otherwise it is β. Thus **ON** is well-ordered by membership. Since however **ON** is not an ordinal, it must not be a set. □

Since, on **ON** and hence on every ordinal, the relations of membership and proper inclusion are the same, these can be denoted by $<$.

Theorem 4.8.4. ON *contains* 0 *and is closed under* $x \mapsto x \cup \{x\}$.

For $\alpha \cup \{\alpha\}$, we may write

$$\alpha';$$

this is the **successor** of α. The operation $x \mapsto x'$ on **ON** is **succession.** By the definition in § 1.2, ω is the class of ordinals that neither *are* limits nor *contain* limits.[12]

An alternative form of the Axiom of Infinity, 4.0.1, is the following.

Axiom 4.8.5 (Infinity [second form])**.** *A— of InfinityAxiom of I—* ω *is set.*

This formulation *implies* the earlier one, by the following.

Theorem 4.8.6. ω *contains* 0 *and is closed under succession, and the following hold.*

1. 0 *is not a successor.*

[12] One could say, 'ω is the class of ordinals that neither *are* nor *contain* limits'; but this would violate the principles laid down in [22, Cases] and reaffirmed in [21]. In the original sentence, the second instance of *limits* is the direct object of *contain,* so it is notionally in the 'objective case'; but the first instance of *limits* is is not an object of *are* (which does not take objects), but is in the 'subjective case', like the subject, *that,* of the relative clause. On similar grounds, the common expression 'x is less than or equal to y' is objectionable, unless *than,* like *to,* is construed as a preposition. However, allowing *than* to be used as a preposition can cause ambiguity: does 'She likes tea better than me' mean 'She likes tea better than she likes me', or 'She likes tea better than I do'? There it is recommended in [22, Than 6] and (less strongly) in [21] that *than* not be used as a preposition. Then '$x \leqslant y$' should be read as 'x is less than y or [x is] equal to y.'

2. *Succession on* ω *is injective.*

3. $(\omega, 0, ')$ *admits induction.*

Proof. 1. Successors are nonempty.

2. If α and β are distinct ordinals, then we may assume $\alpha \in \beta$, so that $\beta \notin \alpha'$; but $\beta \in \beta'$, so $\alpha' \neq \beta'$.

3. Suppose A is a proper subset of ω. Then $\omega \smallsetminus A$ has a least element α. Either $\alpha = 0$ or else $\alpha = \beta'$ for some β in A. Hence A either does not contain 0 or else is not closed under succession. □

The first form of the Axiom implies the second form, once we have the following.

Axiom 4.8.7 (Replacement)**.** *The image of a set under a function is a set.*

In proving the Recursion Theorem 4.1.1, we never need that A and f are sets; they need only be classes. By the Theorem then, there is a homomorphism from $(\mathbb{N}, 0, ^+)$ into $(\mathbf{ON}, 0, ')$; the image of $\mathbb{N}$ under this homomorphism is ω, so ω is a set.

Theorem 4.8.8. $\omega \in \mathbf{ON}$.

We now have ordinals beyond ω, namely ω', ω'', and so on. These are usually written as $\omega + 1$, $\omega + 2$, and so on. By recursion, there is a function $n \mapsto \omega + n$ from ω into **ON**; the image of ω under this function is denoted by one of

$$\omega + \omega, \qquad\qquad \omega \cdot 2.$$

Continuing these ideas, we can develop an arithmetic of ordinals, according to which we can list the ordinals as

$$0, 1, 2, 3, \ldots; \omega, \omega + 1, \omega + 2, \ldots; \omega \cdot 2, \ldots; \omega^2, \ldots; \omega^\omega; \ldots$$

Thus we have a way to extend the ordinary list first, second, third, ... of ordinal numbers.

Theorem 4.8.9. *For every set of ordinals, there is an ordinal that is greater than every ordinal in the set. Indeed, the union of a set of ordinals is the supremum of the set.*

Exercises

1. Prove Theorem 4.8.8.

2. Prove Theorem 4.8.9.

4.9. Cardinal numbers

By the definition in § 3.6, if A is a finite set, then $A \approx n$ for some n in ω. By Theorem 3.6.2, this n is unique; so we can call it the **cardinality** of A, and we may write

$$|A| = n. \tag{4.15}$$

We aim to define a cardinality $|A|$ for all sets A.

Lemma 4.9.1. *If A is finite, and there is a surjective function from A onto B, then B is finite.*

Proof. Use induction on the cardinality of A. The claim is trivially true if $|A| = 0$. Suppose it is true when $|A| = n$, but now $|A| = n + 1$, and f is a surjection from A onto B. We may assume that A is just pred(). Let $c = f(n)$. There are two possibilities:

1. If also $c = f(m)$ for some m in pred(n), then $f \restriction \text{pred}(n)$ is still surjective on B, so B is finite by inductive hypothesis.

2. Suppose $f[\text{pred}(n)] \subseteq B \setminus \{c\}$. Then $f \restriction \text{pred}(n)$ is a surjection on $B \setminus \{c\}$, so this set is finite, again by inductive hypothesis. In this case, there is a bijection h from pred(k) onto $B \setminus \{c\}$ for some k in $\mathbb{N}$. Then $h \cup \{(k, c)\}$ is a bijection from pred$((k + 1))$ onto B, so B is finite.

The induction is complete. □

Theorem 4.9.2. *Suppose $A \preccurlyeq B$. If B is finite, then A is finite.*

Proof. It is enough to show that if $A \subseteq B$, and B is finite, then A is finite. If A is empty, then $|A| = 0$. Suppose A contains c. Define f from B to A by:

$$f(x) = \begin{cases} x, & \text{if } x \in A; \\ c, & \text{if } x \notin A. \end{cases}$$

Then f is surjective, so the claim follows by Lemma 4.9.1. □

Contrapositively, if $A \preccurlyeq B$, and A is infinite, then so is B. Hence we can show that a set A is infinite if we can find an injective function G from ω to A. Does the converse hold? That G is injective means precisely that

$$G(n+1) \in A \setminus \{G(0), \ldots, G(n)\}$$

for all n in ω. Now, if A is infinite, then in each case the set

$$A \setminus \{G(0), \ldots, G(n)\}$$

is not empty by Lemma 4.9.1, so there is some hope that the function G exists. Does strong recursion (that is, Corollary 4.7.4) give us such a function G? It does, *if* there is a function $h : \mathcal{P}(A) \to A$ such that $h(X) \notin X$ when $X \neq A$. However, we have no reason, so far, to assert that such a function exists. That functions like h exist is a consequence of:

Axiom 4.9.3 (Choice)**.** *For every set A, there is a function $f\colon \mathcal{P}(A) \to A$ such that $f(C) \in C$ whenever $C \neq 0$.*

It was proved by Gödel that this axiom is consistent with our other axioms; it was proved by Paul Cohen [10] that the Axiom of Choice is not *entailed* by our other axioms.

A function f as in the Axiom of Choice is called a **choice-function.**

Theorem 4.9.4. *If A is infinite, then $\omega \preccurlyeq A$.*

Proof. Let f be a choice-function for A, and define h on $\mathcal{P}(A) \setminus \{A\}$ by

$$h(X) = f(A \setminus X).$$

Then strong recursion gives us the desired embedding of ω in A, as suggested above. □

Now we can prove the converse of Theorem 3.6.2.

Corollary 4.9.5. *Every infinite set is equipollent to a proper subset of itself.*

Proof. If A is infinite, we may assume $\omega \subseteq A$, and then we can define f on A by

$$f(x) = \begin{cases} x+1, & \text{if } x \in \omega, \\ x, & \text{if } x \in A \setminus \omega. \end{cases}$$

This shows $A \approx A \setminus \{0\}$, a proper subset. □

Similarly, we have:

Corollary 4.9.6. *If A is infinite, then $A \cup \{A\} \approx A$.*

Proof. The claim is trivially true if $A \in A$; so suppose $A \notin A$, and f is an injection from ω to A. Define a function g from $A \cup \{A\}$ to A by:

$$g(x) = \begin{cases} f(0), & \text{if } x = A; \\ x, & \text{if } x \in A \setminus f[\omega]; \\ f(f^{-1}(x) + 1), & \text{if } x \in f[\omega]. \end{cases}$$

Then g is a bijection. □

The converse of this theorem is true, a proper subset of $A \cup \{A\}$. Suppose if possible that $A = A \cup \{A\}$. Then $A \in A$, which is very strange, and which is ruled out by:

Axiom 4.9.7 (Foundation)**.** *Every non-empty set A has a subset that has no elements in common with A:*

$$\exists X \, (X \in A \mathbin{\&} X \cap A = \varnothing)$$

for all non-empty sets A.

Here, if we replace A with $\{A\}$, then this set has the single element A, so $A \cap \{A\} = \varnothing$, which means $A \notin A$.

Theorem 4.9.8. *Every set is equipollent with some ordinal.*

Proof. Supposing f is a choice-function for A, define h as in the proof of Theorem 4.9.4. Let $\mathbf{C}$ be the class of ordinals α for which there is a function g from α to A given by

$$g(\beta) = h(g[\beta]).$$

Such a function g is unique (by Strong Recursion) and can be denoted by g_β. Moreover, if β and γ are both in $\mathbf{C}$ and $\beta \leqslant \gamma$, then $g_\beta \subseteq g_\gamma$. Therefore, if $\mathbf{C}$ has no upper bound in $\mathbf{ON}$, then $\bigcup_{\beta \in \mathbf{C}} g_\beta$ is an embedding of $\mathbf{ON}$ in A, which is absurd, since $\mathbf{ON}$ is a proper class. Hence $\mathbf{C}$ has a least upper bound, say γ; then $\bigcup_{\beta < \gamma} g_\beta$ is a bijection from γ to A. □

This theorem lets us adapt the proof of the Completeness Theorem, 3.9.5, to the case where $\mathcal{L}$ is uncountable: we just to index the sentences of $\mathcal{L}$ by the

ordinals less than some ordinal, and then we can obtain the sets Γ_α by transfinite recursion.

Our main purpose now is to define $|A|$, the **cardinality** of A, as the *least* ordinal that is equipollent with A. Then the cardinalities are well-ordered; in particular, we have:

Corollary 4.9.9 (Schröder–Bernstein Theorem[13])**.** *For all sets A and B,*

$$A \preccurlyeq B \ \&\ B \preccurlyeq A \implies A \approx B.$$

The **cardinals** or **cardinal numbers** are the ordinals that are cardinalities of some set. The cardinals compose the class

CN.

Most infinite ordinals are *not* cardinals; but by strong recursion, there is an order-preserving bijection

$$\alpha \longmapsto \aleph_\alpha$$

from the class of ordinals to the class of infinite cardinals. Here $\aleph$ is the Hebrew letter *aleph.* By definition, $\aleph_\beta$ is the least infinite cardinal that is greater than each of the cardinals $\aleph_\alpha$ such that $\alpha < \beta$. If β is a limit ordinal, then by Theorem 4.8.9, $\aleph_\beta$ is just $\bigcup_{\alpha<\beta} \aleph_\alpha$; but if $\beta = \gamma + 1$, then $\aleph_\beta$ is the least cardinal κ such that

$$\aleph_\gamma < \kappa \leqslant |\mathcal{P}(\aleph_\gamma)|.$$

Theorem 4.9.10. $\mathbb{R} \approx \mathcal{P}(\mathbb{N})$.

Proof. By Theorem 4.6.7 and the Schröder–Bernstein Theorem, it is enough to show that $[0,1) \preccurlyeq {}^{\mathbb{N}^+}\mathbb{B}$, where $[0,1) = \{x \in \mathbb{R} \colon 0 \leqslant x < 1\}$. Given an element a of $[0,1)$, we can, by strong recursion, define a function $k \mapsto a_k$ from $\mathbb{N}^+$ to $\mathbb{B}$ so that, for each n in $\mathbb{N}^+$,

$$\sum_{k=1}^{n} \frac{a_k}{2^k} \leqslant a < \sum_{k=1}^{n} \frac{a_k}{2^k} + \frac{1}{2^n}.$$

The function $a \mapsto (a_k \colon k \in \mathbb{N}^+)$ is injective. Indeed, suppose a and b are distinct elements of $[0,1)$. For some n in $\mathbb{N}^+$ we have

$$\frac{1}{|a-b|} < 2^n,$$

[13] This theorem is commonly attributed to Schröder and Bernstein, who, according to [48, p. 81], proved the theorem independently in the 1890s. But the theorem is attributed to Cantor in [38, § 8.3, p. 171].

so $1/2^n < |a - b|$. If $(a_1, \ldots, a_{n-1}) = (b_1, \ldots, b_{n-1})$, then $a_n \neq b_n$. □

We know $|\mathbb{R}| = \aleph_\alpha$ for some nonzero ordinal α; but we do not know what α is. The set $\mathbb{R}$ is called the **continuum,** and the statement that $|\mathbb{R}| = \aleph_1$ is called the **Continuum Hypothesis.** Gödel showed that there are models of the axioms of set-theory in which the Continuum Hypothesis is true; Cohen, false.

Exercises

1. Prove that the union of two finite sets is finite, and if A and B are finite, then $|A \cup B| + |A \cap B| = |A| + |B|$.
2. If $A \preccurlyeq \omega$ and $B \approx \omega$, show that $A \times B \approx \omega$.
3. Show that, if $A \preccurlyeq \omega$, and $n \in \omega$, then $A^n \preccurlyeq N$.
4. Show that, if $A \preccurlyeq \omega$, then $\bigcup_{n \in \omega} A^n \preccurlyeq N$.
5. Show that $\mathbb{R}$ is equipollent with the set of functions from $\mathbb{N}$ to $\mathbb{N}$.
6. Show that $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$.
7. A real number α is **algebraic** if there is no positive integer n for which there is an n-tuple $\vec{a}$ of rational numbers such that

$$\sum_{k<n} a_k \alpha^k + \alpha^n = 0.$$

A real number that is not algebraic is **transcendental.** Show that there are uncountably many transcendental numbers.

A. Aristotle's *Analytics*

Below is a translation from the first few pages of the Aristotelian work called the Prior Analytics. *Like all of Aristotle's extant works, the text appears to consist of students' lecture notes; perhaps these notes were never edited by Aristotle himself.*

I only want to observe three features of the text:

1) the absence of any special notation;

2) the definition of proposition*;*

3) the use of proofs.

The translation here is mine, from the text in the Loeb edition [2]. Some of the wording is from the English translation by Tredennick in that edition, but there are deviations. For example, where I have 'proposition', Tredennick has 'premiss'. The typography is entirely my own, based on the conception of the text as *lecture-notes; the Greek text indicates no special line-breaks. Likewise, my English is highly abbreviated and 'telegraphic', as is the original Greek.*

Here then is Aristotle:

First, to say what our study (σκέψις) is *about* and *of*:

1) it is about demonstration (ἀπόδειξις), and
2) it is of demonstrative science (ἐπιστήμη ἀποδεικτικῆ).

Next, to define:

1) *proposition* (πρότασις), *term* (ὅρος), and *syllogism* (συλλογισμός), and
2) which kinds [of syllogism] are *complete* (τέλειος) and *incomplete* (ἀτελής).

After these:

3) what it is for one thing *to be or not to be wholly* (τὸ ἐν ὅλῳ εἶναι ἢ μὴ εἶναι) in another, and
4) what we mean by *being predicated* (κατηγορεῖσθαι) of all or of none.

A **proposition** is a statement affirming (καταφατικός) or denying (ἀποφατικός) something of something. It is *universal* (καθόλου), *particular* (ἐν μερει), or *indefinite* (ἀδιόριστος).

1) By **universal**, I mean applying (ὑπάρχειν) to all or none;

2) by **particular**, applying to some, or not to some, or not to all;
3) by **indefinite**, applying or not applying, without reference to whole or part, as in 'The same science studies contraries' or 'Pleasure is not good.'

[*I skip some further discussion of propositions.*]

A **term** is what a proposition is divided into, namely
1) that which is predicated, and
2) that of which it is predicated,

[a form of] to be or not to be being added or removed.

A **syllogism** is a 'piece of language' (λόγος) in which, some things being assumed (τεθέντων τινῶν), because of these (τῷ ταῦτα εἶναι), something different from what was laid down (τα κειμένα) necessarily follows. By saying:
1) 'because of these', I mean it follows *through* these (διὰ ταῦτα);
2) 'it follows through these', no additional term is needed for the necessity to come about.

I call a syllogism:
1) **complete**, if it needs nothing else, apart from what it [already] contains, for the necessary [conclusion] to be evident;
2) **incomplete**, if it needs one or more [propositions] not included among the [given] propositions, although they are necessary through the terms that have been laid down.

These are the same:
1) for *this* **to be wholly** in *that*;
2) for *that* to be predicated of all of *this*.

We say that [*that* is] predicated of all [of *this*] when nothing of *this* can be taken of which *that* cannot be said. Similarly if [*that*] is predicated of *none* [of *this*].

Now, every proposition is
1) an application (ὑπάρχειν), or
2) a *necessary* (ἐξ ἀνάνκης) application, or
3) a *potential* (τοῦ ἐνδέχεσθαι) application.

Of these,
1) some are affirmative (καταφατικός),
2) some negative (ἀποφατικός),

according to each application.

Again, of the affirmative and negative, some are universal, some particular, some indefinite.

A universal
1) *negative* (στερητικός) application is necessarily convertible (ἀντιστρέφειν) in terms; for example, if no pleasure is a good thing, then no good thing is a pleasure;

2) *affirmative* (κατηγορικός) is necessarily convertible, not universally, but particularly. For example, if every pleasure is good, then some good is a pleasure.

Of the particular:

1) the *affirmative* is necessarily convertible particularly; for, if some pleasure is good, then some good will be a pleasure;
2) the *negative,* not necessarily; for it does not follow that, if man does not apply to some animal, then animal does not apply to some man.

First, let the proposition AB be negative universal. If then A applies to nothing of B, then B will apply to nothing of A. For if to something, say C, then it will not be true that A applies to nothing of B, for C is of B.

If A applies to all B, then B applies to some A. For if not, then A will apply to no B; but it was supposed to apply to all.

Similarly if the proposition is particular:

If A to some of B, then B to some of A necessarily applies; for if not, then A to nothing of B.

But if some of B does not apply to A, there is no necessity that some of A should not be B. For example, suppose B is animal and A is man; man not to every animal, but animal to every man applies.

Bibliography

[1] Aristoteles. *Metafizik*. Sosyal Yayınlar, Cağaloğlu–İstanbul, 1996. Second printing. Turkish translation by Ahmet Arslan.

[2] Aristotle. *Categories, On Interpretation, and Prior Analytics*, volume 325 of *Loeb Classical Library*. Harvard University Press and William Heinemann Ltd, Cambridge, Massachusetts and London, 1973. with an English translation by H. P. Cooke and H. Tredennick.

[3] Aristotle. *The Metaphysics, Books I–IX*, volume XVII of *Loeb Classical Library*. Harvard University Press and William Heinemann Ltd., Cambridge, Massachusetts, and London, 1980. with an English translation by Hugh Tredennick. First printed 1933.

[4] George Boole. *Collected Logical Works. Volume II: The Laws of Thought*. The Open Court Publishing Company, Chicago and London, 1940. First published 1854. With a note by Philip E.B. Jourdain.

[5] Cesare Burali-Forti. A question on transfinite numbers (1897). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 104–12. Harvard University Press, 1976.

[6] Stanley N. Burris. *Logic for Mathematics and Computer Science*. Prentice Hall, Upper Saddle River, New Jersey, USA, 1998.

[7] C. C. Chang and H. J. Keisler. *Model theory*. North-Holland Publishing Co., Amsterdam, 1973. Studies in Logic and the Foundations of Mathematics, Vol. 73.

[8] Ian Chiswell and Wilfrid Hodges. *Mathematical logic*, volume 3 of *Oxford Texts in Logic*. Oxford University Press, Oxford, 2007.

[9] Alonzo Church. *Introduction to mathematical logic. Vol. I*. Princeton University Press, Princeton, N. J., 1956.

[10] Paul J. Cohen. *Set theory and the continuum hypothesis*. W. A. Benjamin, Inc., New York-Amsterdam, 1966.

[11] R. G. Collingwood. *An Autobiography*. Clarendon Press, Oxford, 1978. With a new introduction by Stephen Toulmin; originally written 1938; reprinted 2002.

[12] Richard Dedekind. *Essays on the theory of numbers. I: Continuity and irrational numbers. II: The nature and meaning of numbers*. authorized translation by Wooster Woodruff Beman. Dover Publications Inc., New York, 1963.

[13] Descartes. *The Geometry of René Descartes*. Dover Publications, Inc., New York, 1954. Translated from the French and Latin by David Eugene Smith and Marcia L. Latham, with a facsimile of the first edition of 1637.

[14] René Descartes. *Meditations on First Philosophy*. Hackett, Indianapolis, 1979. translated from the Latin by Donald A. Cress.

[15] René Descartes. *Söylem, Kurallar, Meditasyonlar*. İdea, İstanbul, 1996. translated by Aziz Yardımlı.

[16] John Donne. *The Complete Poetry and Selected Prose of John Donne*. The Modern Library, New York, 1952. Edited with an introduction by Charles M. Coffin.

[17] Lou van den Dries and Yiannis N. Moschovakis. Is the Euclidean algorithm optimal among its peers? *Bulletin of Symbolic Logic*, 10(3):390–418, September 2004.

[18] Susanna S. Epp. *Discrete Mathematics with Applications*. PWS Publishing Company, Boston, Massachusetts, USA, 1995. 2nd edition.

[19] Euclid. *The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix*. Dover Publications Inc., New York, 1956. Translated with introduction and commentary by Thomas L. Heath, 2nd ed.

[20] Anita Burdman Feferman and Solomon Feferman. *Alfred Tarski: life and logic*. Cambridge University Press, Cambridge, 2004.

[21] H. W. Fowler. *A Dictionary of Modern English Usage*. Oxford University Press, second edition, 1982. revised and edited by Ernest Gowers.

[22] H. W. Fowler. *A Dictionary of Modern English Usage*. Wordsworth Editions, Ware, Hertfordshire, UK, 1994. reprint of the original 1926 edition.

[23] Paul R. Halmos. *Naive set theory*. Springer-Verlag, New York, 1974. Reprint of the 1960 edition, Undergraduate Texts in Mathematics.

[24] G. H. Hardy. *A mathematician's apology*. Cambridge University Press, Cambridge, 1992. With a foreword by C. P. Snow, Reprint of the 1967 edition.

[25] Richard D. Heffner. *A Documentary History of the United States*. New American Library, New York, 3rd edition, 1976. Expanded and Revised Bicentennial Edition.

[26] Leon Henkin. The completeness of the first-order functional calculus. *J. Symbolic Logic*, 14:159–166, 1949.

[27] Wilfrid Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.

[28] Jacob Klein. *Greek mathematical thought and the origin of algebra*. Dover Publications Inc., New York, 1992. Translated from the German and with notes by Eva Brann, Reprint of the 1968 English translation.

[29] Morris Kline. *Mathematical thought from ancient to modern times*. Oxford University Press, New York, 1972.

[30] Donald E. Knuth. *The TEXbook*, volume A of *Computers & Typesetting*. Addison Wesley Publishing Company, Reading, Massachusetts, USA, June 1986. Seventh printing.

[31] Edmund Landau. *Foundations of Analysis. The Arithmetic of Whole, Rational, Irrational and Complex Numbers*. Chelsea Publishing Company, New York, N.Y., third edition, 1966. translated by F. Steinhardt; first edition 1951; first German publication, 1929.

[32] Azriel Levy. *Basic set theory*. Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1979 original [Springer, Berlin].

[33] David Marker. *Model theory: an introduction*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[34] Murray et al., editors. *The Compact Edition of the Oxford English Dictionary*. Oxford University Press, 1973.

[35] Ali Nesin. *Önermeler Mantığı*. İstanbul Bilgi Üniversitesi Yayınları, 2001.

[36] Filiz Öktem. *Uygulamalı Latin Dili [Practical Latin Grammar]*. Sosyal Yayınlar, İstanbul, 1996.

[37] Giuseppe Peano. The principles of arithmetic, presented by a new method (1889). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 83–97. Harvard University Press, 1976.

[38] Bruno Poizat. *A course in model theory*. Universitext. Springer-Verlag, New York, 2000. An introduction to contemporary mathematical logic, Translated from the French by Moses Klein and revised by the author.

[39] Emil L. Post. Introduction to a general theory of elementary propositions. *Amer. J. Math.*, 43(3):163–185, July 1921.

[40] Paul Reps and Nyogen Senzaki, editors. *Zen Flesh, Zen Bones*. Shambala, Boston, 1994. A Collection of Zen and Pre-Zen Writings.

[41] Kenneth A. Ross and Charles R.B. Wright. *Discrete mathematics. 4th ed.* Upper Saddle River, NJ: Prentice Hall. xiv, 684 p. $ 113.04 , 1999.

[42] Philipp Rothmaler. *Introduction to model theory*, volume 15 of *Algebra, Logic and Applications*. Gordon and Breach Science Publishers, Amsterdam, 2000. prepared by Frank Reitmaier, translated and revised from the 1995 German original by the author.

[43] Joseph J. Rotman. *A First Course in Abstract Algebra*. Prentice Hall Inc., Upper Saddle River, NJ, 2 edition, 2000.

[44] Bertrand Russell. Letter to Frege (1902). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 124–5. Harvard University Press, 1976.

[45] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[46] *Simon and Garfunkel*. Öykü Yayıncılık, Sultanahmet, İstanbul, 1987. Words and music of songs of Paul Simon and Art Garfunkel; Turkish translation by Devrim Eker.

[47] Michael Spivak. *Calculus. 2nd ed.* Berkeley, California: Publish or Perish, Inc. XIII, 647 pp., 1980.

[48] Robert R. Stoll. *Set theory and logic*. Dover Publications Inc., New York, 1979. corrected reprint of the 1963 edition.

[49] Patrick Suppes. *Axiomatic set theory*. Dover Publications Inc., New York, 1972. Unabridged and corrected republication of the 1960 original with a new preface and a new section (8.4).

[50] J. B. Sykes, editor. *The Concise Oxford Dictionary of Current English*. Clarendon Press, Oxford, sixth edition, 1976. Based on the Oxford English Dictionary and its Supplements. First edited by H. W. Fowler and F. G. Fowler.

[51] Alfred Tarski. Truth and proof. *Scientific American*, pages 63–77, 1969.

[52] Alfred Tarski. *Introduction to Logic and to the Methodology of Deductive Sciences*. Dover, 1995. An unabridged republication of the 9th printing, 1961, of the 1946 second, revised edition of the work originally published by Oxford University Press, New York, in 1941.

[53] Ivor Thomas, editor. *Selections illustrating the history of Greek mathematics. Vol. I. From Thales to Euclid*. Harvard University Press, Cambridge, Mass., 1951. With an English translation by the editor.

[54] Ivor Thomas, editor. *Selections illustrating the history of Greek mathematics. Vol. II. From Aristarchus to Pappus*. Harvard University Press, Cambridge, Mass, 1951. With an English translation by the editor.

[55] Jean van Heijenoort. *From Frege to Gödel. A source book in mathematical logic, 1879–1931*. Harvard University Press, Cambridge, Mass., 1967.

[56] Jean van Heijenoort, editor. *Frege and Gödel. Two fundamental texts in mathematical logic*. Harvard University Press, Cambridge, Mass., 1970.

[57] John von Neumann. On the introduction of transfinite numbers (1923). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 346–354. Harvard University Press, 1976.

[58] André Weil. *Number theory.* Birkhäuser Boston Inc., Boston, MA, 1984. An approach through history, From Hammurapi to Legendre.

[59] Howard Zinn. *A People's History of the United States: 1492–Present.* Harper Collins, New York, 2nd edition, 1995.

Symbols

Index