Introductory Notes on the Foundations of Mathematics

David Pierce

December 1, 2009

Preface

[2006.01.16: These notes are being edited, following their use in the first semester of 2005/6.]

These notes concern the foundations of mathematics in two ways:

($*$) these notes are about concepts and techniques that all mathematicians use, implicitly or explicitly;

($\dagger$) these notes (or parts of them) are 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 these notes page after page as if they constituted an easy novel. They might constitute 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 these notes should 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.

[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.

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 these notes 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 chess-game at first. Depending on how seriously you take mathematics, you can see these notes 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 [14]—see the bibliography at the end of these notes. This translation is available in print and in various places around the Web.) The present notes do 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,

[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 OED [28], 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, although it does claim that she comes from a different base than he, because the feminine form derived from the base of he was too much like the masculine form.

[3] Euclid practiced mathematics in Alexandria around 300 BCE, probably having learned mathematics in Athens from the students of Plato [14, vol. I, pp. 1 f.].

you will jump around, reading what you are interested in, perhaps with the guidance of a teacher. Indeed, probably 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 doesn't *tell* you, but he *shows* you what proofs of propositions are.

The present notes contain more than just propositions and their proofs; but they *do* contain these. Each proof here is labelled as such, and ends with a little box. (The first example is on p. 10.) The propositions and proofs in these notes 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 (or deductions). 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] These notes *tell* you, as well as show 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 *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 these notes 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 integers. 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 can't define everything precisely until we have the notion

[4]Perhaps the invention can be attributed to Hilbert [7, §07, n. 110].

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

The topics of these notes 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 these notes. 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 notes. Yet my supposedly rigorous account of the integers depends on all of the machinery that the notes develop 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 $\mathcal{A}\mathcal{M}\mathcal{S}$-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 $\mathcal{A}\mathcal{M}\mathcal{S}$ is the American Mathematical Society. The original TeX program was expanded into LaTeX and independently into $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX; then the benefits of both expansions were combined into $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.

The original TeX program distinguishes between ordinary text and mathematical text. In ordinary text, in these notes, words are *italicized* for the usual sorts of reasons: they (or rather 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

[5] See [24, p. 1].

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] 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.

The LaTeX program provides an easy way to make numbered lists. So as not to have too many numerals around, I often replace the usual list

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$$

with the alternative

$$* \quad \dagger \quad \ddagger \quad \S \quad \P \quad \| \quad ** \quad \dagger\dagger \quad \ddagger\ddagger$$

that is provided in LaTeX. Another reason to use these symbols[7] is to avoid the suggestion of ranking. I may start numbered lists with 0 instead of 1.

Labelled proofs here end with boxes, as noted above; labelled examples end with bullets (the first is on p. 31).

Acknowledgments

In these notes, 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. Andreas and I revised our respective notes, with Belgin's advice, the following year. 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. Now, at the beginning of 2005, I am revising the notes again, keeping in mind the experience of Ayşe, Mahmut and myself, along with impressions from students. Advice from my friend Steve Thomas is also proving useful for this revision.

Many of the topics dealt with in these notes are also covered by basic texts like [13] or [34]. I am not trying to write such a book as these are, but I find it useful

[6]The distinction between the use and the *mention* of a word (or symbol) is attributed to Quine in [7, § 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 [7, § 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."

[7]In the order given, the first five symbols are an asterisk, a dagger, a double dagger, a section-sign, and a pilcrow.

to look at them. The preface of [34] 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 [7] and [5]; Ali Nesin's book [29] 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 [41] or [26]. I use these books, but try to give more elementary exercises than they do.

For my notes on natural numbers, [25] is inspirational.

As a student, I appreciated the style of Spivak [39]: not condescending, but treating the reader as a fellow mathematician.

Thanks to Şükrü Yalçınkaya and Vural Cam for the photographic representations of the digits 1 and 0 on the cover; the pictures were made at Perge and at Termessos; the column at Perge is in the *Corinthian order.*

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." [33, p. 55]

Contents

List of Figures

Chapter 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 these notes refer to as propositional logic can also be called *propositional calculus*.

$A\,\alpha$	**a**lpha	$H\,\eta$	**ē**ta	$N\,\nu$	**n**u	$T\,\tau$	**t**au
$B\,\beta$	**b**eta	$\Theta\,\theta$	**th**eta	$\Xi\,\xi$	**x**i	$\Upsilon\,\upsilon$	**u**psilon
$\Gamma\,\gamma$	**g**amma	$I\,\iota$	**i**ota	$O\,o$	**o**micron	$\Phi\,\phi$	**ph**i
$\Delta\,\delta$	**d**elta	$K\,\kappa$	**k**appa	$\Pi\,\pi$	**p**i	$X\,\chi$	**ch**i
$E\,\epsilon$	**e**psilon	$\Lambda\,\lambda$	**l**ambda	$P\,\rho$	**r**ho	$\Psi\,\psi$	**ps**i
$Z\,\zeta$	**z**eta	$M\,\mu$	**m**u	$\Sigma\,\sigma,\varsigma$	**s**igma	$\Omega\,\omega$	**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 (ʽ) over an initial vowel (or ρ) is transcribed as a preceeding (or following) h; the smooth-breathing mark (ʼ) and the three tonal accents (ά, α̂, 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 these notes.

Section 1.1 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 that 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. 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 [8, 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 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 these notes, 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 [44, p. 442], called them *αἰτήματα*, that is, requests, demands, or assumptions.) An **axiom** is usually a proposition that satisfies two criteria:

(∗) it is *self-evident*;

(†) it is useful for proving other propositions.

[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 [7, 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 [14, vol. 1, p. 280] for some commentary.

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 [18, p. 15], with my own formatting:

> We hold these truths to be self-evident,
>
> (∗) that all men are created equal,
>
> (†) that they are endowed by their Creator with certain unalienable rights,
>
> (‡) that among these are life, liberty and the pursuit of happiness.
>
> (§) That to secure these rights, governments are instituted among men, deriving their just powers from the consent of the governed.
>
> (¶) 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.

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*** (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*).

[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 [50, ch. 18]; this did not prevent a later American invasion.

[6] *πᾶν ἀναγκαῖον ἢ φάναι ἢ ἀποφάναι.*

[7] *ἀδύνατον ἅμα εἶναι καὶ μὴ εἶναι.*

Aristotle's examples of common notions are the Laws of *Contradiction* and of the *Excluded Middle;* they are discussed further in Book *Γ* (IV), which 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 (*θεωρεῖ*) 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 varlığı ve ona özü gereği ait olan ana nitelikleri inceleyen bir bilim vardır.

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 ἐπισκοποὐντοι*) tries to say something concerning them,—if [they] are true or not—not the geometer (*γεωμέτρησ*), not the arithmetician (*ἀριθμητικός*).
>
> But some of the physicists (*φυσικοὶ*)[9] [were] doing this appropriately (*εἰκότως*).
>
> For, they thought they alone were doing research (*σκοπεῖν*) concerning all nature (*ἡ φύσις*) and concerning being.

[8]The whole Greek sentence, as given in [3], is *Ἔστιν ἐπιστήμη τισ ἣ θεωρεῖ τὸ ὂν ᾗ ὂν 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.

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

> 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, and now principles:

> [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. 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***:

> Neither does [any]thing admit to being between a contradiction, but it is necessary either to affirm or deny one of one, whatever.[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.

The continuation of this passage is in § 1.8. If we follow Aristotle, it seems that, as mathematicians, 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

[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.*

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.) In former times, finer distinctions were considered. Writes Pappus of Alexandria, a few centuries after Aristotle:[12]

> 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.

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 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. A class is 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 (0.1) above or (1.1) below, the expressions on either side of the *sign of equality* (that is, =) can be called **members** of the equation.)

A **class** is determined by a *property.* There is no precise definition of property; I shall just say that, for every property, there is a class whose members are

[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 [45, pp. 564–567], where also are found the text and translation from which the quotation is adapted.

[13]Ivor Thomas [45, p. 567] uses inquiry here; but there is *no* word in the Greek original corresponding to this or proposition.

[14]One writer [26] seems to use collection more generally even than class.

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.

A **set** is a class that *is* a member of some classes, though it may fail to be a member of others. 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. Later in this section, there is an example of a class that is not a set. (The recognition of a distinction between classes and sets is only about a hundred years old.)

A class can be indicated in writing by 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*. In fact, it is a *set*. In particular, this set **contains** a, b, and c (and nothing else) as elements.

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

($*$) $\mathbf{C}$ contains d;

(†) d is an element of $\mathbf{C}$;

(‡) d is a member of $\mathbf{C}$;

(§) d is in $\mathbf{C}$.

Any of these can be expressed by the symbolism

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

Here the symbol $\in$ is derived from the Greek ε, which corresponds to the first letter of the Latin ELEMENTVM. 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 words 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 also, we shall *define* infinite and finite. Meanwhile, the distinction between the finite and the infinite *will* be used in Theorem 1.4.1.

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

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

and we can say also[15] that $\mathbf{D}$ **includes** $\mathbf{C}$ or that $\mathbf{C}$ is a **subset** of $\mathbf{D}$. If $\mathbf{C}$ is *not* a subset of $\mathbf{D}$, we can write

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

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:

1.2.1 Axiom (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 $A \neq B$.

I say above that a class is determined 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.) If P is a predicate, then the corresponding class can be denoted

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

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.

Often, in place of Px, 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[16] example of a class that is not a set:

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

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

[16]From 1903; see for example [26, I.2.3, p. 6], where both Russell and Zermelo are attributed.

Proof. Call this class $\mathbf{R}$, and suppose it *is* a set. Then $\mathbf{R}$ is a member of itself, or not, by the Law of the Excluded Middle, because by definition, sets are the sorts of things that *can be* members of classes. If $\mathbf{R} \in \mathbf{R}$, then this very proposition ($\mathbf{R} \in \mathbf{R}$) shows that $\mathbf{R}$ 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 $\mathbf{R} \notin \mathbf{R}$. Therefore $\mathbf{R} \notin \mathbf{R}$. This proposition ($\mathbf{R} \notin \mathbf{R}$) 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, which 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,[17] as noted on p. iii. The proof shows that there is a class to which the predicate in Line (1.3) neither applies nor fails to apply. So there is a violation of the Law of the Excluded Middle—or rather, there is an example of a class that is not a *real thing*.

A way to avoid creating classes that are not sets is the following. Suppose $\mathcal{U}$ is some set, and P is a predicate. Another axiom[18] of set-theory is that the class of elements *of* $\mathcal{U}$ with the property symbolized by P is a set:

1.2.3 Axiom (Separation)**.** *The class* $\{x \in \mathcal{U} : Px\}$ *is a set.*

The letter $\mathcal{U}$ here 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 is over two meters tall. Then $\{x \in \mathcal{U} : Px\}$ is the set of people now taller than two meters.

Mathematical examples of sets of the form $\{x \in \mathcal{U} : Px\}$ will come up throughout these notes.

In the mathematical study of sets, it turns out that there is no need to consider classes that contain anything other than sets. Here is why:

If A and B are sets, then they have a **union**, which is the set comprising every element of A or B (or both); this union is denoted

$$A \cup B.$$

(See § 3.0.) We do have one set, namely the empty set. If A is a set, then we suppose that we can form the set

$$\{A\},$$

which contains only A. Such a set, with a unique element, is called a **singleton.** (See § 3.2.) Hence, from any set A, we can form the union

$$A \cup \{A\};$$

this is the **(set-theoretic) successor** of A and can be denoted

$$A'.$$

[17] 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.

[18] The following Axiom of Separation is also called the **Axiom of Comprehension**.

This idea of successsors can be used to give the following **inductive 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:

(∗) 0 is a natural number;

(†) if n is a natural number and is a set, then n' is a natural number.

If n is a set, then n' is a set. Hence, every natural number obtained by one of the two rules is a set. Therefore, all natural numbers are sets, and every natural number has a successor, which is a natural number.

The definition of the natural numbers is inductive, because it allows **proof by induction** in the following sense. Suppose P names a possible property of natural numbers, and:

(∗) $P0$;

(†) if Pn, then $P(n')$, for every natural number n.

Then every natural number must have the property (named by) P. Here, Pn is the **inductive hypothesis**. The method of **proof by induction** is first used in Lemma 1.2.5 below. In general, an inductive proof consists of two steps:

(∗) the **base step,** in which $P0$ is proved;

(†) the **inductive step,** in which $P(n')$ is proved from the inductive hypothesis Pn.

It is perhaps 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. The class of natural numbers is then denoted

$$\omega.$$

Note well that this symbol is not a w, a double u; it is an *omega*. To remember this, 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**[19] **natural numbers**. The first five von-Neumann natural numbers are:

$$0,\ \{0\},\ \{0,\{0\}\},\ \{0,\{0\},\{0,\{0\}\}\},\ \{0,\{0\},\{0,\{0\}\},\{0,\{0\},\{0,\{0\}\}\}\}.$$

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

[19] In fact, the definition is traced to Zermelo in 1916 in [26, II.3.8, p. 54].

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 being inductive: these are given by the next two theorems:

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

Proof. By definition, every successor of a natural number contains that number; but 0 is empty. □

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

Proof. Let P be the predicate

____ includes all of its elements.

Since 0 has no elements, it includes all of its elements, so $P0$. This completes the base step of our 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 $k \subseteq n'$. (This conclusion will be part of Lemma 3.1.3.) Therefore $P(n')$. This completes the induction. □

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

Proof. Suppose k and n are natural numbers, and $k' = n'$. Then

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

In particular, $k \in n \cup \{n\}$ and $n \in k \cup \{k\}$. If $k = n$, we are done. If $k \neq n$, 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. □

We can call n the **immediate predecessor** of n'. If n is a natural number different from 0, then n itself has an immediate predecessor; we have just shown that this predecessor is *unique*, and we can denote it 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

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

(If $n = 0$, then this is the empty set.) If we do not happen to care about whether each natural number is such a set, then we can denote the set of natural numbers by

$$\mathbb{N};$$

this is the usual notation when one is not that 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

$$n^+ \tag{1.5}$$

or $n + 1$, such that:

($*$) 0 is not the successor of any element of $\mathbb{N}$;

(†) elements of $\mathbb{N}$ with the same successor are the same;

(‡) $\mathbb{N}$ is included in every class that contains 0 and that contains n^+ if it contains some n in $\mathbb{N}$.

We shall show in Chapter 4 that all properties of $\mathbb{N}$ follow from these.

1.3 Algebra of the integers

Now that we have, in the previous section, a precise definition of the natural numbers, I want to review some things 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 the set $\mathbb{N}$, whose members form the list

$$(0, 1, 2, 3, \dots).$$

As we have seen, every natural number n has a successor, which usually denoted $n+1$. Some mathematicians start the list of natural numbers at 1 instead of 0; but I shall just say that the members of the set $\{1, 2, 3, \dots\}$ 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 $-n$, 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 $-n$, although this number is itself negative only if n is positive.

The set of integers is commonly denoted[20]

$$\mathbb{Z}.$$

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

($*$) $x + y$ (the **sum** of x and y, which here are **addends**),

[20] 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*.

(†) $-x$ (**minus-x**, the **additive inverse** or **negative** of x), and

(‡) $x \cdot y$ (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

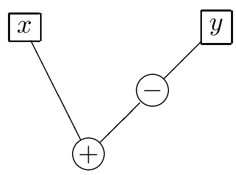
$$xy.$$

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*[21] y from x produces a **difference**, which is denoted

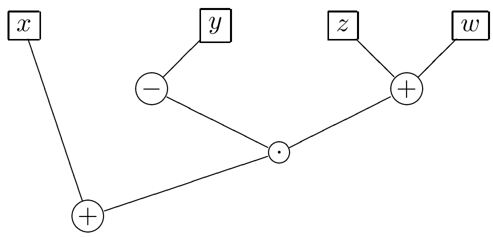
$$x - y$$

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 computing $x - y$ can be indicated by a **tree**,[22] 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

$$x + -y \cdot (z + w). \tag{1.6}$$

I shall refer to such a **string** of symbols as an *arithmetic term*[23] (The Greek

[21] 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 [28], 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.

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

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

word[24] for number is ἀριθμός, which is ARITHMOS in Latin letters. Our general definition[25] of term comes in § 3.5.)

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

- the symbols $+$, $-$ and $\cdot$ (a dot);
- **variables,** such[26] as x, y and z;
- symbols for certain integers, such as 12, 0 and -137—such symbols can be called **numerals**[27] or **(numeral) constants**[28];
- the parentheses (and).

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

($*$) every variable is an arithmetic term;

(†) every numeral is an arithmetic term;

(‡) if t is an arithmetic term, then so is $-t$;

(§) if t_0 and t_1 are arithmetic terms, then so are $(t_0 + t_1)$ and $(t_0 \cdot t_1)$.

Some writers add another condition to this definition:

(¶) nothing else is an arithmetic term.

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

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

($*$) every variable is in A;

(†) every numeral is in A;

(‡) if t is in A, then $-t$ is in A;

(§) 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:

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

---

[24]Strictly, the Greek word ἀριθμός refers to *a number of things*, in particular, more than one;—certainly not zero or 'fewer' than zero. See [22].

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

[26]The convention of using letters from the end of the Latin alphabet for 'unknown quantities' dates back to Descartes; see [10]. 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_0, x_1, x_2 and so forth, except that we can't precisely explain the words and so forth yet.

[27]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 might be thought of as the single symbol 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 31 below.

[28]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.

Proof. Let A be the set of arithmetic terms with 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 inductive definition of arithmetic terms, every term is in A. □

By the formal definition of arithmetic terms, the string on Line (1.6) above is not 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**. That our terms *are* uniquely readable has 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

$$x(y + z) = xy + xz, \tag{1.7}$$

and we shall say that the two members of this equation **represent** the same **polynomial**. Also, Equation (1.7) 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.[29] A Diophantine equation is an example of an *(arithmetic) formula.* For example, the equation

$$y^2 = 4x^3 - ax - b \tag{1.8}$$

(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

[29] Diophantus wrote the *Arithmetica*, in thirteen books, of which six have come down to us [45, 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 [45, pp. 526–535].

(c, d) of integers such that $d^2 = 4c^3 - ac - b$. Formula (1.8) is not an identity, because not every pair of integers satisfies it. (For example, if (c, d) and (c, d') satisfy it, then we must have $d' = \pm d$; there is no other possibility.)[30]

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.

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 (1.7) 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 $z = -14$:

$$\begin{aligned} 5(17 + -14) &= 5 \cdot 3 = 15; \\ 5 \cdot 17 + 5 \cdot -14 &= 85 - 70 = 15. \end{aligned}$$

But we can't check the property for all integers, since there are infinitely many.

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 didn't need to know all of the properties like the distributive property, just to be able to *define* the notion of a polynomial.

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

$$(\mathbb{Z}, +, -, \cdot). \tag{1.9}$$

Structures are defined generally in §§ 3.2 and 3.5. The structure on Line (1.9) is the set $\mathbb{Z}$ equipped with certain specified operations, namely addition, additive inversion and multiplication. Now, $\mathbb{Z}$ also has the named[31] elements 0 and 1. Moreover, $\mathbb{Z}$ is equipped with the *relation* $<$ called 'less-than'. (Relations are defined generally in § 3.2.) So we may think of the integers as composing the structure

$$(\mathbb{Z}, +, -, \cdot, 0, 1, <). \tag{1.10}$$

[30] Equations like (1.8) 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 [37, Example III.2.4, pp. 59 f.].

[31] 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 $-(1 + \cdots + 1)$.

We now have some new arithmetic formulas, the simplest being

$$x < y,$$

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

- $x > y$ is read as x is greater than y, and means $y < x$;
- $x \leqslant y$ means $x < y$ or $x = y$: that is, $x \leqslant y$ is satisfied by those (a, b) such that $a < b$ or $a = b$;
- $x \geqslant y$ 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 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 integersnon-negative — satisfy $0 \leqslant x$ and are the natural numbers, composing the set $\mathbb{N}$ as we said in § 1.2.

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** 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

$$\mathbb{Q};$$

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. 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*; we shall give a version of Euclid's proof 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) $(x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2$.

1.4 Some proofs

We have two proofs so far, officially: 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 able to prove the distributive property of the integers. By some standards—ultimately, the standards of these notes—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* [14].

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

($*$) that there are infinitely many prime numbers;

(†) that the diagonal and side of a (geometrical) square have no common measure;

(‡) 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 described in § 1.1.

Infinity of primes

Without more ado, we can state and prove:

1.4.1 Proposition. *There are infinitely many prime numbers.*[32]

Proof. Suppose there were only finitely many prime numbers. Say there were n primes (where $n \in \mathbb{N}$). Then we could list the primes thus:

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

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

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

would be indivisible by each prime p_i. Therefore this sum would have a prime factor not on our list of primes. This would contradict our assumption that our list contained 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; it is also given in § 4.5 below.) Nor have we defined what 'infinitely many' means. (We shall in § 4.0.)

Still, by some standards, we *have* given a proof.[33] The proof is by the technique of contradiction. (So was the proof of Theorem 1.2.2.) To prove a certain statement by **contradiction**, one assumes that the statement is false, and then one shows that this assumption leads to absurdity.

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**.

1.4.2 Lemma. *The product of two integers is*

(∗) even*, if one of the integers is even;*

(†) 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. □

[32] 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 $\mathbb{N}$.

[33] A proof with a similar level of detail is offered to the general reader in [17, § 12].

The following is a fundamental property[34] of $\mathbb{N}$; we shall use it here and there before proving it in Chapter 4. (It is a consequence of the properties at the end of § 1.2, but it cannot be proved by induction alone.)

1.4.3 Lemma (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*.*

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[35] alludes to a proof similar to ours.

1.4.4 Proposition. *The Diophantine equation*

$$x^2 = 2y^2 \tag{1.11}$$

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,

$${a_0}^2 = 2{a_1}^2. \tag{1.12}$$

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); say $a_0 = 2a_2$. Then ${a_0}^2 = 4{a_2}^2$; this with Equation (1.12) implies[36] $2{a_1}^2 = 4{a_2}^2$, hence

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

Thus (a_1, a_2) is also a solution of Equation (1.11). 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

$$a_0, a_1, a_2, a_3, \dots$$

of integers a_k such that (a_k, a_{k+1}) is a solution of Equation (1.11) for each natural number k. (Strictly, the existence of such a sequence is only justified by

[34] 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 square-integral area: If there were such a triangle, then there would be a smaller one, and so on. See [49, II.IX, pp. 75 ff.].

[35] In the *Prior Analytics*; the passage is quoted and discussed at [44, pp. 110 f.].

[36] The properties of equality that allow this conclusion are discussed in detail in [43, Ch. III, pp. 54–67].

the Recursion Theorem, which is 4.1.1 below.) But we may also assume (why?) that each integer a_k is *positive*, so that

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

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

$$ka \leqslant b < (k+1)a. \tag{1.13}$$

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

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

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

For the sake of completeness, we can extend this analysis to arbitrary integers. Every integer a has an **absolute value**, which is denoted $|a|$ 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 $\operatorname{rem}(b, a)$ satisfying two requirements:

(∗) $0 \leqslant \operatorname{rem}(b, a) < |a|$;

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

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

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

1.4.5 Proposition. *Any two integers have a greatest common divisor (unless both integers are zero). 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. We may also assume $|a| \geqslant |b|$. We *recursively* define a sequence of natural numbers in the following way. (Recursive definitions in general are defined precisely in § 4.1.) Let $a_0 = |a|$ and $a_1 = |b|$. Suppose $a_0, \dots, a_{i+1}$ have been defined. Then let

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

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

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

The technique of Proposition 1.4.5 for calculating this number is the **Euclidean algorithm**.[37] A modern formulation of this algorithm is found in [12]:

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

assuming $0 < b \leqslant a$.

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

$$\mathbb{R},$$

that 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 [9, 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[38]

$$\surd 2,$$

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

1.4.6 Corollary. *The real number $\surd 2$ 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

[37] The word algorithm is an 'erroneous refashioning' [28], 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.

[38] 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 [10, p. 77]. Note also that $\surd(4+5) = \sqrt{4+5} = 3$, while $\surd 4 + 5 = 7$.

worked with them *informally* in this way, as when we defined $\leqslant$ on p. 18.) 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 $\mathbb{Z}$.

1.5 Excursus on anthyphaeresis

We have now proved three important propositions about integers. In this optional section, an alternative proof of Proposition 1.4.4 is developed; a version of this proof may 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[39]

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

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

1.5.1 Lemma. *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 $a : b :: a - kc : b - kd$. □

1.5.2 Lemma. *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 the Inequality (1.13) yields the claim. □

1.5.3 Proposition. *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 $a_2 = \mathrm{rem}(a_0, a_1)$; we shall show that there is *no* proportion

$$a_0 : a_1 :: a_1 : a_2. \tag{1.14}$$

Now, $a_2 < a_1$, so we may assume $a_1 < a_0$ (otherwise (1.14) is false). We may also assume $a_2 \neq 0$. Suppose now, if possible, that (1.14) is true. By

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

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,

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

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 (1.14) 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**,[40] generating a sequence $a_0, a_1, a_2, \dots$, possibly finite, of non-negative real numbers, and a corresponding sequence $n_0, n_1, \dots$ 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 $2, 2, 2, \dots$, never ending.

That the Ancients found interest in such sequences can be inferred from certain old texts: see the brief discussion at [44, pp. 508 f.]. In modern notation, we have

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

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

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

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

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

although we can't here say exactly what this *means*.

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

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 $p \nmid 1 + x$.

(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) 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 $FB : BC :: BC : BE$.)

(9) 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.

1.6 Parity

Here we develop one possible approach to the so-called *Boolean connectives*, which will be defined in § 1.7. We 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

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

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

1.6.1 Lemma. *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:

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

Proof. Exercise. □

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

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

Proof. Exercise. □

Finally, applying the parity-operation twice is the same as applying it once:[41]

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

Proof. Exercise. □

We 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:

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

Next, we define two more operations. The following are also identities, by definition:

$$\ominus x = x \oplus 1, \tag{1.15}$$

$$x \sqcup y = (x \odot y) \oplus (x \oplus y). \tag{1.16}$$

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

1.6.5 Theorem. *The equation*

$$x \sqcup y = \ominus(\ominus x \odot \ominus y) \tag{1.17}$$

is an identity.

Proof. There are two ways we can proceed. One is to 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,

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

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

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, 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 (1.17), 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 Equation (1.17) 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 Equation (1.17). The proof did not *begin* with this equation; it began with one of the *members* of the equation and showed that it was equal to a new term. Then the *other* member of Equation (1.17) was shown to be equal to the same term. To write the proof as follows would *not* be good style:

$$\left.\begin{aligned} x \sqcup y &\stackrel{?}{=} \ominus(\ominus x \odot \ominus y), \\ (x \odot y) \oplus (x \oplus y) &\stackrel{?}{=} ((x \oplus 1) \odot (y \oplus 1)) \oplus 1, \\ \mathrm{p}((x \odot y) + (x \oplus y)) &\stackrel{?}{=} \mathrm{p}(\mathrm{p}(\mathrm{p}(x + 1)\,\mathrm{p}(y + 1)) + 1), \\ \dots &\stackrel{?}{=} \dots, \\ \mathrm{p}(xy + x + y) &= \mathrm{p}(xy + x + y). \end{aligned}\right\} \tag{1.18}$$

Do not write proofs this way! What's wrong with this style of writing? It does not show the connexion between consecutive lines. The Equations (1.18) don't tell the reader, for example, that $\ominus(\ominus x \odot \ominus y) = ((x \oplus 1) \odot (y \oplus 1)) \oplus 1$. In fact, the equations tell us *nothing* that can be assumed to be correct.

Think of the following example:

$$\left.\begin{aligned} -1 &\stackrel{?}{=} 1 \\ (-1)^2 &\stackrel{?}{=} (1)^2 \\ 1 &= 1. \end{aligned}\right\} \tag{1.19}$$

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

If you is *searching* for a proof of (1.17), then you might possibly write something like the Equations (1.18). 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 (1.19) 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,[42] let us refer to the set $\{0, 1\}$ as $\mathbb{B}$. In the last section, we defined some operations that convert integers into elements of $\mathbb{B}$. Considering the elements of $\mathbb{B}$ as integers, we shall now restrict those operations on $\mathbb{Z}$ so as to apply *only* to elements of $\mathbb{B}$. In so doing, we shall change their names:

on $\mathbb{Z}$:	$\otimes$	$\oplus$	$\ominus$	$\sqcup$
on $\mathbb{B}$:	$\wedge$	$\nleftrightarrow$	$\neg$	$\vee$

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

(∗) $\wedge$ is **conjunction**;

(†) $\neg$ is **negation**;

(‡) $\vee$ is **(inclusive) disjunction**;

(§) $\nleftrightarrow$ is **exclusive disjunction** or **(material) non-equivalence**.

[42] See for example [4, III.12, **[47]**, p. 51].

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

P	Q	$P \wedge Q$	$P \vee Q$	$P \not\leftrightarrow Q$
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:

(¶) **(material) implication** or the **conditional**: $\rightarrow$;

(‖) **(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

$$P \not\leftrightarrow Q \sim \neg(P \leftrightarrow Q), \tag{1.20}$$

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

- $\wedge$, $\neg$, $\vee$, $\not\leftrightarrow$, $\rightarrow$, $\leftrightarrow$ (or other connectives, should we choose to define them);
- the **constants** 0 and 1;
- **variable** from the list P_0, P_1, P_2, ...;
- the parentheses (and).

Then the Boolean terms are determined by the following rules:

($*$) variables and constants are Boolean terms;

(†) if F is a Boolean term, then so is $\neg F$;

(‡) if F and G are Boolean terms, then so is $(P * Q)$, where $*$ is one of the connectives $\wedge$, $\vee$, $\not\leftrightarrow$, $\rightarrow$, $\leftrightarrow$.

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 form 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.

- $\neg$ has priority over all other connectives;
- $\wedge$ and $\vee$ have priority over $\rightarrow$, $\leftrightarrow$, and $\nleftrightarrow$;
- in case of two instances of $\rightarrow$, the one on the *right* has priority[43];
- in case of two instances of $\wedge$ or of $\vee$ or of $\nleftrightarrow$, the one on the right has priority.[44]

Also, instead of writing variables P_k, we may use P, Q and R instead. Similarly, we may use letters like F, G and H to stand for formulas.[45]

1.7.1 Examples. By the order of operations,

(∗) the Boolean term denoted by $P \rightarrow Q \vee R$ is $(P \rightarrow (Q \vee R))$;

(†) $\neg P \wedge Q$ is $((\neg P) \wedge Q)$;

(‡) $P \wedge Q \vee R$ is ambiguous; the writer must say whether $(P \wedge Q) \vee R$ or $P \wedge (Q \vee R)$ is intended;

(§) $P \wedge Q \wedge R$ is $(P \wedge (Q \wedge R))$;

(¶) $P \wedge Q \wedge R \vee P$ is ambiguous;

(‖) $P \rightarrow Q \rightarrow R$ is $P \rightarrow (Q \rightarrow R)$;

(∗∗) $P \nleftrightarrow Q \nleftrightarrow R$ is $(P \nleftrightarrow (Q \nleftrightarrow R))$;

(††) $P \rightarrow Q \wedge R \rightarrow S$ is $(P \rightarrow ((Q \wedge R) \rightarrow S))$. •

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) Which Boolean terms, if any, are denoted by the following?—

(a) $P \wedge \neg Q \nleftrightarrow R \vee P$;

(b) $P \rightarrow Q \nleftrightarrow R$;

(c) $P_0 \rightarrow P_1 \rightarrow P_2 \rightarrow P_3$;

[43] 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*.

[44] We could just as well give priority to the one on the left; we just want to allow ourselves to let strings like $P \wedge Q \wedge R$ denote Boolean terms.

[45] The symbols P_0, P_1 and so on are the variables that can appear officially in Boolean terms. The symbols P, Q and so on are variables that we use to *talk about* Boolean terms: they are *syntactical variables* in the sense of [7, § 08]. Likewise, F and so on are not literally formulas; we use them as syntactical variables for formulas.

(d) $P_0 \to P_1 \to \dots \to P_n$.

(2) The following closed formulas are names of which elements of $\mathbb{B}$?—

(a) $1 \to 1 \to 1$,

(b) $1 \to 0 \to 1$,

(c) $(0 \to 1) \leftrightarrow 1$,

(d) $\neg(0 \nleftrightarrow 1) \leftrightarrow (0 \leftrightarrow 1)$,

(e) $\neg\neg\neg 0$,

(f) $(1 \lor 0) \land 0$,

(g) $(1 \lor (0 \land 0)$.

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 the parts of speech called *conjunctions*.

In traditional grammar, of English at any rate,[46] conjunctions are *coordinating* or *subordinating*. An example of a subordinating conjunction is the word if. Coordinating conjunctions might be called *cumulative*, *disjunctive*,[47] *adversative*, or *transitional*; examples of such conjunctions, are, respectively, and, or, but and then.

Our main interest here is in how conjunctions affect the truth of statements, especially statements in mathematics. Aristotle defines truth in the *Metaphysics* (IV, vii, 1: 1011 b 26). A literal translation of his words[48] 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, isn't, or what isn't, is; it is true to say that what is, is, and what is not, is not.'

I propose (inspired by Tarski [42]) 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:

[46] I have consulted [21] in making these observations.
[47] Or *alternative*.
[48] The text is in [3].

> 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:

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

We can now analyse certain compound statements. Let A and B be statements. Then 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 $P \wedge Q$ takes the value 1 if and only if P takes the value 1 and Q takes the value 1. If 1 represents truth, then the connective $\wedge$ represents the conjunction and. The proposition A and B and the propositional formula $F \wedge G$ can alike be called **conjunctions**. Note well, however, that the proposition A and B belongs to *our* ordinary language, while the formula $F \wedge G$ belongs to propositional logic.

Similarly, A or B is true if and only if A is true or B is true. Also, $P \vee Q$ takes the value 1 if and only if P takes the value 1, or Q takes the value 1. So the connective $\vee$ represents the conjunction or. The proposition A or B and the propositional formula $F \vee G$ 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 $\not\leftrightarrow$.

The sentence Not-A is true if and only if A is false; and $\neg P$ takes the value 1 if and only if P takes the value 0. If now 0 represents falsity, then $\neg$ represents not. Both Not-A and $\neg F$ 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:

$$\begin{gathered}A \text{ and } B\\ A\text{, but } B\\ A;\ B\end{gathered}$$

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

$$A \ \&\ B.$$

One could write also $A \wedge B$; but I prefer to reserve $\wedge$ for use in propositional formulas as defined in the previous section. The sentence $A \ \&\ B$ here is not a propositional formula; it is just a proposition or sentence of ordinary language.

We can form some more compounds:

$$\begin{gathered}\text{If } A\text{, then } B\\ \text{When } A\text{, then } B\end{gathered}$$

A implies B
B if 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 $P \to Q$ can be analysed similarly, and we can apply the same terminology.

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, If A, then B means no more than B is true or A is false. This is why we referred to $\to$ as **material implication**[49]: Here material is opposed to formal. The idea is that, 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.)

There is a saying in English, If wishes were horses, then beggars would ride. We can't analyse this as a material implication, simply because the antecedent 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 $F \to G \to H$ as an abbreviation for the formula $F \to (G \to H)$.

In ordinary language, we can write indifferently

A if and only if B
A just in case B

[49]See the discussions in [7, § 05, n. 89, pp. 37f.] or [43, §§ 8, 9].

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

$$A \iff B.$$

The formula $P \leftrightarrow Q$ has a similar analysis and description.

Some fundamental rules of reasoning can be abbreviated thus:

$$A \ \& \ (A \implies B) \implies B; \tag{1.21}$$

$$\textsf{not-}(A \implies B) \iff A \ \& \ \textsf{not-}B. \tag{1.22}$$

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

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

(∗) The **converse** of $A \implies B$ is $B \implies A$;

(†) the **contrapositive** of $A \implies B$ is $\textsf{not-}B \implies \textsf{not-}A$.

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

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

This observation is of great value in the proving of mathematical propositions.

Exercises

(1) Find a true implication whose converse is true.

(2) Find a true implication whose converse is false.

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 *adjectives*, especially all and some. Quantifiers are a part of *predicate logic*. To see how good this logic is as a model of ordinary language, I propose first to look at ordinary adjectives in general, as they are used in English.

I here understand an **adjective** to be a word or phrase found in association with a noun—a noun that the adjective is said to *modify*. For example, I understand the **definite article,** the, and the **indefinite article,** a/an, to be adjectives. While the can be used with singular and plural nouns, a is used only with singular nouns. The articles are of use in establishing a fourfold classification of adjectives:

(∗) Most adjectives in the dictionary are **descriptive**, like green, good, better, first, second, . . . , single, double, . . . , contradictory and numerous. Any of these can be preceded by an article: the green grass; a second opinion. A descriptive adjective *describes*—names a property or quality of—the object or objects named by the associated noun: *Green grass* is grass with the property of being green. The property named by a descriptive

		dual	manifold
negative	sing.	neither	no
	pl.		no
existential	sing.	either	a/an, any, some
	pl.		some, a few, a little, a great many
universal	sing.	either	a/an, any, each, every
	pl.	both	all

Figure 1.2: Logical adjectives. The labels sing. and pl. indicate whether an adjective on that line is associated with a *singular* or a *plural* noun. The labels dual and manifold indicate whether the noun associated with an adjective in that column names an element (or elements) of a set of size *two* or *more than two*.

adjective may fail to belong strictly to the object or objects named by the associated noun; it may belong to the *relation* of these objects with others: A second opinion can be second only if there is also a *first* opinion.

(†) The **demonstrative** adjectives include this/these, that/those, which, the and the same. Note that this/these and that/those are peculiar, as adjectives, for having distinct singular and plural forms. The demonstrative adjectives indicate that a *certain*, a *particular*, a *definite* object is named by the associated noun. They cannot be preceded by an article: We cannot refer to *the this tree* or *a the mountain*.

(‡) The **quantitative** adjectives include zero, one, two, . . . , few, several, many, little, much. The name quantitative seems appropriate for these adjectives, although they will *not* be symbolized by the so-called quantifiers. Some of the quantitative adjectives are symbolized by the numerals 0, 1, 2, . . . A quantitative adjective can be preceded by the definite article, but not by the indefinite article: We can refer to *the two opinions*, but not to *a one opinion*. We can mention *a few opinions*; but I put a few in the final class:

(§) The **logical** adjectives are the remaining: neither, no, either, a/an, any, some, both, a few, a little, a great many, each, every, all. They cannot be preceded by an article.

Some grammarians[50] refer to the demonstrative, quantitative and logical adjectives as *determiners*. Determiners are distinguished from other adjectives by being more fundamental parts of language—and by never being preceded by the indefinite article.

The logical adjectives can be arranged as in Figure 1.2. The main point to note is that there are three kinds of logical adjectives, which I am calling negative, existential and universal.

In a section of the 'XVII. Meditation' of his *Devotions upon Emergent Occasions* of 1624, the clergyman and metaphysical poet John Donne uses three logical adjectives in addition to the indefinite article. The Meditation begins as follows

[50] For example, the editor of the ninth edition of the Concise Oxford Dictionary [46]; however, she treats one and two, like first, as ordinary [descriptive] adjectives.

(and here I preserve Donne's original spelling and typography, as found in [11, pp. 440f.]): '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.*

Note the 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 [38]:

> 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 ϕ, and [is] a piece of the continent might be denoted χ. 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

$$\neg\exists x\ \phi(x)\ \ \&\ \ \forall x\ \chi(x).$$

(Here I am borrowing $\neg$ from propositional logic, rather than writing out not-.) The symbol $\exists$ is the **existential quantifier**; the symbol $\forall$ is the **universal quantifier**. We have just seen that these correspond respectively to the logical adjectives 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, and let ϕ be a predicate applying (truly or falsely) to elements of $\mathcal{U}$; let A be the resulting set $\{x \in \mathcal{U} : \phi(x)\}$. We can form several equations and inequations whose members are $\varnothing$, A and $\mathcal{U}$; with quantifiers, we can describe them:

(∗) $\forall x\ \phi(x)$ means $A = \mathcal{U}$;

(†) $\exists x\ \phi(x)$ means $A \neq \varnothing$;

(‡) $\neg\exists x\ \phi(x)$ means $A = \varnothing$;

(§) $\neg\forall x\ \phi(x)$ means $A \neq \mathcal{U}$.

The set denoted

$$\{x \in \mathcal{U} : \neg\phi(x)\}$$

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

$$A^{\mathrm{c}}, \tag{1.23}$$

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

(∗) $\forall x\ \neg\phi(x)$ means $A^{\mathrm{c}} = \mathcal{U}$;

(†) $\exists x\ \neg\phi(x)$ means $A^{\mathrm{c}} \neq \varnothing$;

(‡) $\neg\exists x\ \neg\phi(x)$ means $A^{\mathrm{c}} = \varnothing$;

(§) $\neg\forall x\ \neg\phi(x)$ means $A^{\mathrm{c}} \neq \mathcal{U}$.

But we have, for example,

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

Correspondingly, we also have

$$\neg\exists x\ \phi(x) \iff \forall x\ \neg\phi(x); \tag{1.24}$$

$$\neg\forall x\ \phi(x) \iff \exists x\ \neg\phi(x). \tag{1.25}$$

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

1.9.1 Example. In calculus, a function f 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

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

Some people abbreviate this proposition to

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

By the Rules (1.24) and (1.25) above, as well as (1.22) in § 1.8, the negation of this proposition is

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

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 sin 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. •

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

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

where the notation $\mathbb{Z} \vDash \sigma$ can be read as [the proposition] σ is true in $\mathbb{Z}$; 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's roughly what it looks like: a gate that keeps you from entering, say, the Ankara subway without paying. (The *syntactic turnstile* $\vdash$ will be introduced in § 2.7.)

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

(∗) everything is in A,

(†) something is in A,

(‡) nothing is in A,

(§) not everything is in A.

The first three of these clauses are obtained from the clause thing is in A by adding, from Table 1.2, a universal, an existential and a negative logical adjective. 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 logical adjective with the meaning of not every and some... not. *Why* is there not such an adjective? This is a question for linguistics.

Some people might write the last clause on the list as Everything is 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, which does not have the intended meaning, since gold itself glitters. To avoid possible misunderstanding, it seems better to write

Not all that glitters is gold.

Turkish avoids the ambiguities possible from a misplaced not. In the Antalya *autogare*, 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

Hiç bir muz Asal muz değildir.

Should we have symbols for the other adjectives in Table 1.2, besides no, some and all? Probably not. The sentence Neither x is in A means $A = \varnothing$, provided that x ranges over a universe with just two elements (and A is a subset of this universe). The distinction between a pair and a multitude is perhaps important in a life where many things come in pairs (like married couples, teams of oxen, and eyeballs); but we need not make the distinction logically, with fundamental symbols, if we are just trying to do mathematics.

The word either is ambiguous: If I tell you that you may have either piece of cake, does this mean you can have *both*? Maybe, maybe not. Likewise, a/an 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. It's a distinction that matters to a poet.

Exercises

(1) Write a sentence equivalent to $\forall x\ \exists y\ \psi(x, y)$ that does not use $\exists$.

(2) Discuss the logical adjectives of Turkish (or some other language besides English).

Chapter 2

Propositional logic

2.0 Truth-tables

We have defined propositional formulas in § 1.7. For every *closed* propositional formula F, there is an element

$$\widehat{F}$$

of $\mathbb{B}$ that can be found in the following way. First note that F meets one of the following conditions:

(∗) F is a constant from $\mathbb{B}$ (that is, 0 or 1), or

(†) F is $\neg G$ for some closed formula G, or

(‡) F is $(G * H)$ for some closed formulas G and H, where $*$ is one of the connectives $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ and $\not\leftrightarrow$.

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

(∗) If F is in $\mathbb{B}$, then $\widehat{F}$ is F itself;

(†) if F is $\neg G$, then $\widehat{F}$ is the value of $\neg\widehat{G}$ as determined by the table in § 1.7;

(‡) if F is $(G * H)$, then $\widehat{F}$ is the value of $\widehat{G} * \widehat{H}$ as determined by the tables in § 1.7.

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

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

If the variables in a propositional formula F belong to the set $\{P_0, P_1, \dots, P_{n-1}\}$, then we can indicate this by writing F as $F(P_0, \dots, P_{n-1})$; we may also call F an n-**ary** formula.[1] A 3-ary formula would be **ternary**; 2-ary, **binary**; 1-ary, **singulary**.[2] A 0-ary or **nullary** formula would have *no* variables: it would be

[1]Here F is a syntactical variable as discussed in Chapter 1, n. 45.

[2]The word unary is often used instead of singulary. Following Quine, Church [7, § 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

closed in the sense of § 1.7. An n-ary formula is also $(n+1)$-ary, $(n+2)$-ary, and so on.

2.0.1 Examples.

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

$$F(P_0, P_1).$$

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

(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 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 F can be replaced with e; all the remaining variables of F belong to $\{P_0, \dots, P_{n-1}\}$, so F has become n-ary. In turn, other elements of $\mathbb{B}$ can be substituted for other variables in F, so as to obtain, in the end, a closed formula.

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

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

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

$$\mathbf{e} \qquad \text{or} \qquad \vec{e}.$$

(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 F). The truth-value of $F(\vec{e})$ can be denoted[3]

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

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

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.

first five Latin *distributive* numbers—corresponding to the Turkish birer, ikişer, üçer, dörder, beşer [30]—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* [28]. 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 μοναδ-.

[3] The notation is from [5, Definition 2.1.8, p. 41].

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

In general, each row of the truth-table for $F(P_0, \dots, P_{n-1})$ will look like the second row of the following:

P_0	$\dots$	P_{n-1}	F
e_0	$\dots$	e_{n-1}	$\widehat{F}(e_0, \dots, e_{n-1})$

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:

($*$) F is a sub-formula of itself;

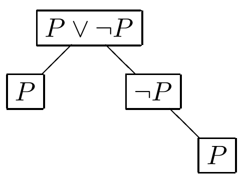
(†) F is a sub-formula of $\neg F$;

(‡) F and G are sub-formulas of $(F * G)$ (where $*$ is $\wedge$, $\vee$, $\to$, $\leftrightarrow$ or $\not\leftrightarrow$; remember that, by the convention established in § 1.7, F and G here are not just strings, but *formulas*);

(§) every sub-formula of a sub-formula of F is a sub-formula of F.

A sub-formula of F is a **proper sub-formula** if it is not F itself.

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



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

P	$\neg P$	$P \vee \neg P$
0	1	1
1	0	1

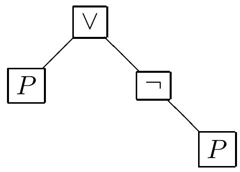
.

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

P	$P \vee \neg P$	$\neg P$	P
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. Indeed, compare the previous tree with the following:



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

$$\begin{array}{rcc} P & \leftrightsquigarrow & P \\ P \vee \neg P & \leftrightsquigarrow & \vee \\ \neg P & \leftrightsquigarrow & \neg \\ P & \leftrightsquigarrow & P \end{array}$$

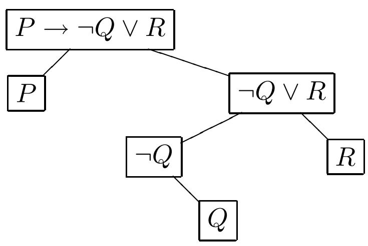
Using this correspondence, we can rewrite the last truth-table thus:

P	$\vee$	$\neg$	P
0	1	1	0
1	1	0	1

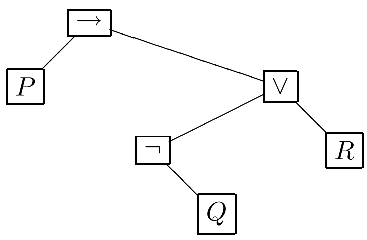
I propose to call this the **full truth-table** of $P \vee \neg P$; from it we can extract the **proper truth-table** of $P \vee \neg P$ by taking only one column headed by P, along and the column headed by $\vee$ (which corresponds to the whole formula):

P	$P \vee \neg P$
0	1
1	1

For another example, let F be the formula $P \to \neg Q \vee R$. The sub-formulas of F compose the tree



The corresponding tree of variables and connectives is:



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

P	$\to$	$\neg$	Q	$\vee$	R
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 *up* the trees drawn above, starting with the variables:

P	$\to$	$\neg$	Q	$\vee$	R
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	$\to$	$\neg$	Q	$\vee$	R
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	$\to$	$\neg$	Q	$\vee$	R
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 F itself is the last to be filled in: in this case, the second column, under $\to$. The *proper* truth-table for F is then

P	Q	R	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) $P \to (Q \to P)$;

(b) $P \land Q \land R$;

(c) $P \nleftrightarrow Q \nleftrightarrow R$;

(d) $(P \to Q \lor R) \to (\neg P \lor Q)$;

(e) $(P \to Q \lor \neg R) \land (Q \to P \land R) \to (P \to R)$;

(f) $\neg(\neg R \to P \to \neg(R \to Q))$.

How many columns has each table?

(2) What does the truth-table for a constant 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 $\widehat{F}$ for closed formulas F: that is, we have to confirm that only one value can be computed for each 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:

($*$) $\land$, $\lor$, $\to$, $\leftrightarrow$ and $\nleftrightarrow$ are **binary**, because they are used to join *two* formulas;

(†) $\neg$ is **singulary**;

(‡) 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

$$P \to \neg Q \land 1$$

(which stands for $(P \to (\neg Q \land 1))$), the arguments of $\to$ are P and $\neg Q \land 1$ (in that order); the arguments of $\land$ are $\neg Q$ and 1; the argument of $\neg$ is Q; and 1 has no argument.

By definition, each propositional formula F meets one of the following conditions:

($*$) F is a variable;

(†) F is a nullary connective;

(‡) F is $\neg G$ for some G;

(§) F is $(G * H)$ for some G and H and some binary connective $*$.

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

Let G be $(P \wedge Q)$, and let H be R. Then $(G \vee H)$ can be written as $(S \wedge T)$, where S is $(P$, and T is $Q) \vee R$. But S is not a formula (why not?); neither is T.

How do we know that, if G and H are more complicated, $(G * H)$ *still* cannot be analyzed as a different application of a binary connective? How do we know that $(G * H)$ is **uniquely readable?** Our definition of $\widehat{F}(\vec{e})$ 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. We allow the cut to come at an end: that is, we allow one of the two segments to be empty, so that the other segment is the whole string:

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

An initial segment of F that is not F itself is a **proper initial segment** of F.

2.1.2 Lemma.

($*$) *Every propositional formula has* just as many *left parentheses as right parentheses.*

($\dagger$) *If F is a variable, a constant, or a negation, then every initial segment of F has* at least as many *left parentheses as right parentheses.*

($\ddagger$) *If F is a propositional formula that is not a variable, a constant, or a negation, then every non-empty proper initial segment of 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 F that do satisfy those claims. Then, trivially, A contains all variables and constants. If A contains F, then F has at least as many left as right parentheses, hence so does $\neg F$, which means $\neg F$ is in A. Finally, suppose A contains F and G, and $*$ is a binary connective. Every non-empty proper initial segment of $(F * G)$ is either $(F * S$ for some initial segment S of G, or $(T$ for some initial segment T of F. But then S and T must have *at least* as many left as right parentheses, since F and G are in A; so $(F * S$ and $(T$ have *more* left than right parentheses. Therefore $(F * G)$ is in A. By the inductive definition of propositional formulas, A contains all of them. □

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

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

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

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 $\neg F$ or $(F*G)$. If it is $\neg F$, then its proper initial segment is $\neg F'$, where F' is a formula that is a proper initial segment of F. If the original formula is $(F*G)$, then its proper initial segment must have the form $(F' *' G')$, and then there are two possibilities:

($*$) one of F and F' is a proper initial segment of the other, or

(†) F and F' are the same formula, and G' is a proper initial segment of 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.

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

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

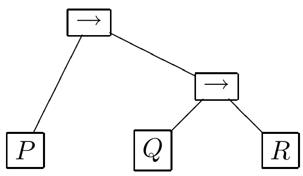
Now we know that $\widehat{F}(\vec{e})$ is well defined, so truth-tables are uniquely determined.

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 $P \to Q \to R$ for $(P \to (Q \to R))$. But we can't dispense with the parentheses in $(P \to Q) \to R$, unless we come up with a completely new system of notation.

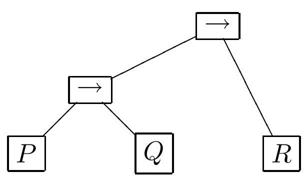
Polish notation

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

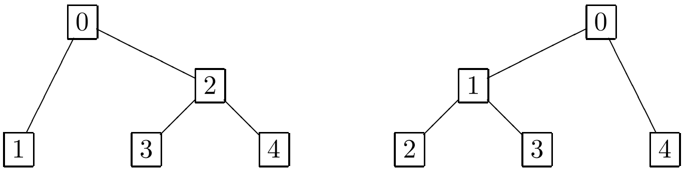
($*$) $P \to Q \to R$ becomes



(†) $(P \to Q) \to R$ 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

$$\to P \to QR; \qquad \to\to PQR.$$

These are formulas written in *Łukasiewicz* or *Polish notation.*[4]

A **signature** is a set of connectives. Our definition of propositional formulas in § 1.7 is a definition of the formulas of the signature $\{0, 1, \neg, \wedge, \vee, \to, \leftrightarrow, \not\leftrightarrow\}$ 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:

($*$) All variables are formulas of $\mathcal{L}$ in Polish notation;

(†) if $n \in \mathbb{N}$, and $*$ is an n-ary connective in $\mathcal{L}$, and if F_0, F_1, …, F_{n-1} are formulas of $\mathcal{L}$ in Polish notation, then

$$* \, F_0 F_1 \dots F_{n-1}$$

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

(The latter condition includes the case $n = 0$; in this case, the list $(F_0, \dots, F_{n-1})$ 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) For each symbol in the formula $(P \to Q \vee \neg R) \wedge (1 \to P \wedge R) \to (0 \to R)$, give the list of arguments, if it exists. Write the formula in Polish notation.

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

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

[4] Church [7, p. 38, n. 91] calls it Łukasiewicz notation, after its inventor—who was Polish; the common term today seems to be Polish notation.

2.2 Truth-equivalence

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

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

for all truth-assignments $\vec{e}$. In this case, as suggested in § 1.7, we shall write[5]

$$F \sim G;$$

and we shall say that F and G are **truth-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**.

2.2.1 Example. Are the formulas P and $(Q \lor \neg Q) \to P$ equivalent? Their full truth-tables are

P
0
1

and

$($Q	$\lor$	$\neg$	$Q)$	$\to$	P
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	Q	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 can't obviously[6] 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:

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

[5]The symbol $\sim$ is a **swung dash** or **tilde.**

[6]A one-variable polynomial of degree n has at most n zeros; so if $f(x)$ is a polynomial of degree n at most, and $0 = f(0) = f(1) = \cdots = f(n)$, then $\forall x\ f(x) = 0$. This method doesn't work for polynomials in more than one variable.

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. A proof by simplification, suitably expressed, will be an example of a *formal proof*.

Meanwhile, the problem of checking for equivalence can be formulated in other ways. If $F \sim 1$, then we write

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

and we say that F is a **tautology**.[7] (The semantic turnstile $\vDash$ was introduced in § 1.9. To be consistent with the notation in that earlier section, we might write Line (2.1) as $\mathbb{B} \vDash F$; but the variables in propositional formulas will always range over $\mathbb{B}$.) If $F \sim 0$, we call F a **contradiction**. We say F is **satisfiable** if it is not a contradiction. If both F and $\neg F$ are satisfiable, then F is a **contingency**. Hence, in the truth-table for F, if the column for F itself contains:

(∗) only 1s, then F is a tautology;

(†) only 0s, then F is a contradiction;

(‡) at least one 1, then F is satisfiable;

(§) at least one 1, and at least one 0, then F is a contingency.

Also, the following statements mean the same thing:

(∗) $F \sim G$;

(†) $\vDash F \leftrightarrow G$;

(‡) $\neg(F \leftrightarrow G)$ is not satisfiable.

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

Exercises

(1) Test for the equivalence of the following pairs of formulas by the truth-table method:

   (a) P and $Q \to P$;
   (b) P and $Q \to (P \wedge Q)$;
   (c) $P \to (Q \to R)$ and $P \to Q \to (P \to R)$.

(2) Give examples of tautologies, contradictions, and contingencies.

(3) Establish the following equivalences by truth-tables (they will constitute Lemma 2.6.1 below):

$$\begin{aligned} P \to Q &\sim \neg P \vee Q; \\ P \leftrightarrow Q &\sim (P \to Q) \wedge (Q \to P); \\ P \not\leftrightarrow Q &\sim \neg(P \leftrightarrow Q); \\ \neg\neg P &\sim P; \end{aligned}$$

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

$$\begin{aligned} \neg(P \lor Q) &\sim \neg P \land \neg Q; & \neg(P \land Q) &\sim \neg P \lor \neg Q; \\ P \land Q &\sim Q \land P; & P \lor Q &\sim Q \lor P; \\ (P \land Q) \land R &\sim P \land Q \land R; & (P \lor Q) \lor R &\sim P \lor Q \lor R; \\ P \land (Q \lor R) &\sim (P \land Q) \lor (P \land R); & P \lor (Q \land R) &\sim (P \lor Q) \land (P \lor R); \end{aligned}$$

$$\begin{aligned} P \land P &\sim P; & P \land \neg P &\sim 0; & P \lor P &\sim P; & P \lor \neg P &\sim 1; \\ P \land 1 &\sim P; & P \land 0 &\sim 0; & P \lor 0 &\sim P; & P \lor 1 &\sim 1; \end{aligned}$$

$$P \sim (P \land Q) \lor (P \land \neg Q); \qquad P \sim (P \lor Q) \land (P \lor \neg Q).$$

(4) Establish the following equivalences:

(a) $\neg P \sim 1 \nleftrightarrow P$;

(b) $P \lor Q \sim P \nleftrightarrow Q \nleftrightarrow P \land Q$;

(c) $P \nleftrightarrow Q \sim Q \nleftrightarrow P$;

(d) $(P \nleftrightarrow Q) \nleftrightarrow R \sim P \nleftrightarrow Q \nleftrightarrow R$;

(e) $P \land (Q \nleftrightarrow R) \sim P \land Q \nleftrightarrow P \land R$;

(f) $P \nleftrightarrow P \sim 0$.

(5) Is there a formula F such that $\vDash (F \to (P \leftrightarrow Q)) \land (P \lor (Q \lor F))$?

2.3 Substitution and replacement

If F is a formula for which $(e_0, \dots, e_{n-1})$ is a truth-assignment, then the constant formula $F(e_0, \dots, e_{n-1})$ 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 $(G_0, \dots, G_{n-1})$ is a list of n formulas, then from F we can obtain the formula

$$F(G_0, \dots, G_{n-1})$$

by *substitution* of G_j for each instance of P_j in 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.

2.3.1 Example. Suppose F is $P_0 \land (P_1 \to P_0)$, and G_0 is $P_0 \to P_1$, and G_1 is $P_1 \to (P_0 \lor P_2)$. Then $F(G_0, G_1)$ is

$$(P_0 \to P_1) \land ((P_1 \to (P_0 \lor P_2)) \to (P_0 \to P_1)).$$

•

Substitution is *associative* in that, if we substitute some formulas G_i into F, and then substitute some formulas H_j into the result, we get the same formula as if we substitute the H_j first into the G_i, and then the results into F. The formal statement is the following:

2.3.2 Lemma (Associativity)**.** *Suppose F is an n-ary formula, and*

$$(G_0, \dots, G_{n-1})$$

is a list of n formulas, each ℓ-ary. Let H be the formula $F(G_0, \dots, G_{n-1})$. Then H is ℓ-ary. Suppose $(K_0, \dots, K_{\ell-1})$ is a list of ℓ formulas. Then the formula

$$H(K_0, \dots, K_{\ell-1})$$

is the formula

$$F(G_0(K_0, \dots, K_{\ell-1}), \dots, G_{n-1}(K_0, \dots, K_{\ell-1})).$$

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

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

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

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

Proof. I claim that the proposition is obvious,[8] 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 $F(G_0, \dots, G_{n-1})$ also a truth-assignment for the G_j? It is, if all of the variables P_0, …, P_{n-1} actually *appear* in F; otherwise it may not be:

2.3.3 Example. Suppose F is just P_0, *considered* as a binary formula. Let G_i be P_i when $i \in \{0, 1\}$. Then $F(G_0, G_1)$ 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 G_1. •

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

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

and $(H_0, \dots, H_{n-1})$ is a list of n formulas, then

$$F(H_0, \dots, H_{n-1}) \sim G(H_0, \dots, H_{n-1}).$$

Proof. Since $F \sim G$, we have

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

for all truth-assignments $\vec{e}$ for F and G. Let F' be $F(H_0, \dots, H_{n-1})$, and let G' be $G(H_0, \dots, H_{n-1})$. Suppose $\vec{f}$ is a truth-assignment for the H_j, and let $\widehat{H}_j(\vec{f}\,) = e_j$. Then

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

[8]However, Church [7, § 15, p. 97] proves a version of this lemma by induction.

Therefore $F' \sim G'$. This completes the proof.[9] □

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

Proof. Exercise. □

2.3.6 Example. Since $P \lor \neg P$ is a tautology, so is $(P \to Q) \lor \neg(P \to Q)$. •

In ordinary language, 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:

($*$) by replacing b *with* d, or

(†) by substituting d *for* b.

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

2.3.7 Example. In $P \lor \neg P$, replacing the second occurrence of P with Q yields $P \lor \neg Q$. •

2.3.8 Theorem (Replacement)**.** *Suppose F is a sub-formula of G, and*

$$F \sim F'.$$

Let G' be the result of replacing F with F' in G. Then

$$G \sim G'.$$

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

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

and G' is $H(P_0, \dots, P_{n-1}, F')$. The remainder of the proof[10] is an exercise involving Lemma 2.3.2. □

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

Proof. Exercise. □

2.3.10 Example. Since $\vDash (P \to Q) \lor \neg(P \to Q)$ by Example 2.3.6, and

$$\neg(P \to Q) \sim P \land \neg Q,$$

we have $\vDash (P \to Q) \lor (P \land \neg Q)$. •

[9] This is also Burris's proof [5, § 2.3, pp. 46f.], although Burris's use of the fact given in Lemma 2.3.2 is not entirely explicit.

[10] Burris [5, § 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 [7, § 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.

This, in short, is the method of simplification. 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, once we have the stock of equivalences presented in § 2.6.

Exercises

(1) If $F(P)$ is $P \to P \to P$, what is $F(F(P))$?

(2) Prove Corollary 2.3.5.

(3) Prove Corollary 2.3.9.

2.4 Normal forms

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 2.4.1.

Suppose we have the truth-table for a formula $F(P_0, \dots, P_{n-1})$. Say there are m rows in which the entry for F itself is 1. Then $0 \leqslant m \leqslant 2^n$. If we ignore the other rows (namely, those rows in which the entry for F is 0), then what remains has the form

P_0	P_1	$\dots$	P_{n-1}	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 $\mathbb{B}$. (So, i is the row-number of e_j^i in the truth-table, and j is the column-number). If $0 \leqslant i < m$ and $0 \leqslant j < n$, 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 $0 \leqslant i < m$, let G^i be the conjunction

$$P_0^i \wedge \dots \wedge P_{n-1}^i.$$

The formulas G^i can be called the **normal disjunctive constituents** of F. Their disjunction,

$$G^0 \vee G^1 \vee \dots \vee G^{m-1},$$

is called a **disjunctive normal form** for F. (The other disjunctive normal forms for F are obtained by re-ordering the constituents G^i.) It is Theorem 2.4.3 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 $H_0, \dots, H_{r-1}$ is

$$H_0 \vee H_1 \vee \cdots \vee H_{r-1},$$

which can also be written

$$\bigvee_{i<r} H_i. \tag{2.3}$$

If $r = 1$, then this formula is just H_0. If $r = 0$, then, by convention,[11] the formula (2.3) is understood to be 0. In particular, the disjunctive normal form of a contradiction is 0. The conjunction

$$\bigwedge_{i<r} H_i$$

is defined analogously, and is 1 if $r = 0$.

2.4.1 Example. Here is the full truth-table of a particular disjunction:

$\neg$	$(P$	$\to$	$Q)$	$\vee$	$(R$	$\wedge$	$\neg$	$P)$
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, Q and R:

P	Q	R
1	0	0
0	0	1
1	0	1
0	1	1

The disjunctive normal form for $\neg(P \to Q) \vee (R \wedge \neg P)$ is therefore

$$(P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R).$$

•

[11] The convention is reasonable: Instead of (2.3), we could write $\bigvee\{H_0, \dots, H_{r-1}\}$; informally, this says that *at least one* of the formulas H_i is true. If $r = 0$, then there are no formulas H_i, and in particular there is no such *true* formula, so $\bigvee\{H_0, \dots, H_{r-1}\}$ is false.

An n-ary formula is in disjunctive normal form if the formula is precisely

$$\bigvee_{i<m}\bigwedge_{j<n} P^i_j,$$

where each sub-formula P^i_j is either P_j or $\neg P_j$, but all of the constituents $\bigwedge_{j<n} P^i_j$ are distinct. Note especially that each constituent must contain the same variables.

2.4.2 Example. The formula $\neg(P \to Q) \lor (R \land \neg P)$ is equivalent to

$$(P \land \neg Q) \lor (\neg P \land \neg Q \land R) \lor (\neg P \land Q \land R),$$

but this is *not* a disjunctive normal form, since one of the constituents does not contain R. •

2.4.3 Theorem. *Every formula is equivalent to its disjunctive normal forms.*

Proof. Let us use the notation of the definition above. Write H for $\bigvee_{i<m} G^i$. Then we have to show $F \sim H$. For the truth-assignment $(e^i_0, \dots, e^i_{n-1})$, let us write $\vec{e}^{\,i}$. For arbitrary truth-assignments $\vec{f}$ for the G^i, we have

$$\widehat{G^i}(\vec{f}\,) = \begin{cases} 1, & \text{if } \vec{f} = \vec{e}^{\,i}; \\ 0, & \text{if } \vec{f} \neq \vec{e}^{\,i}. \end{cases}$$

Then

$$\widehat{H}(\vec{f}\,) = \begin{cases} 1, & \text{if } \vec{f} \in \{\vec{e}^{\,0}, \dots, \vec{e}^{\,m-1}\}; \\ 0, & \text{if } \vec{f} \notin \{\vec{e}^{\,0}, \dots, \vec{e}^{\,m-1}\}. \end{cases}$$

Hence H and F have the same truth-table. □

There is also a **conjunctive normal form;** it looks like the disjunctive form, except that the $\land$ and the $\lor$ 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.

2.4.4 Example. To obtain the conjunctive normal form of the formula in Example 2.4.1, from its truth-table we extract

P	Q	R
0	0	0
0	1	0
1	1	0
1	1	1

,

from which we read off

$$(P \lor Q \lor R) \land (P \lor \neg Q \lor R) \land (\neg P \lor \neg Q \lor R) \land (\neg P \lor \neg Q \lor \neg R).$$

•

2.4.5 Theorem. *Every formula is equivalent to its conjunctive normal form.*

Proof. Exercise. □

If F is a tautology in the variables $P_0, \dots, P_{n-1}$, then its disjunctive normal form will be the disjunction of the 2^n possible constituents

$$P_0^j \land \dots \land P_{n-1}^j.$$

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) What is the disjunctive normal form for a tautology in no variables?

(2) Find the disjunctive and conjunctive normal forms for:

  (a) $P \to (Q \to R)$;

  (b) $(\neg P \to Q) \land (\neg Q \to P) \to (\neg P \lor \neg Q)$.

(3) Show that for any formula $F(P_0, P_1, P_2, P_3)$, either the disjunctive or the conjunctive normal form has no more than 8 constituents.

(4) Show that every satisfiable n-ary formula is equivalent to a formula

$$F_0 \nleftrightarrow F_1 \nleftrightarrow \dots \nleftrightarrow F_{m-1},$$

where all of the 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 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

$$\{\land, \lor, \neg, \to, \leftrightarrow, \nleftrightarrow, 0, 1\}.$$

However, we have just seen that every formula with a truth-table is equivalent to a formula with the smaller signature $\{\land, \lor, \neg\}$. (If the formula is a contingency, then just take a conjunctive or disjunctive normal form. For a contradiction, take $P_0 \land \neg P_0$; for a tautology, $P_0 \lor \neg P_0$.)

Another way to say this is that every Boolean polynomial is represented by a formula in $\{\land, \lor, \neg\}$. 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 $\mathcal{L}$.

2.5.1 Lemma. *If $\mathcal{L}$ is an adequate signature, and $\mathcal{L}'$ is a signature that includes $\mathcal{L}$, then $\mathcal{L}'$ is adequate.*

Proof. Obvious. □

In short, if a signature is adequate, then so is any *larger* signature.

In fact, there are proper subsets of $\{\wedge, \vee, \neg\}$ that are adequate. The following was proved by Emil Post in 1921.[12]

2.5.2 Theorem. *The signature $\{\vee, \neg\}$ is adequate.*

Proof. Since $\{\wedge, \neg, \vee\}$ is adequate, it is enough to show that any formula in this signature is equivalent to a formula in $\{\wedge, \neg\}$. Suppose F is in $\{\wedge, \neg, \vee\}$. Every instance of $\wedge$ in F determines (as in § 2.1) a sub-formula of F that is a conjunction. Say this conjunction is $G \wedge H$, where G and H are sub-formulas of F. We have an equivalence

$$P \wedge Q \sim \neg(\neg P \vee \neg Q)$$

(as can be checked by truth-tables); therefore, by the Substitution Theorem, we have

$$G \wedge H \sim \neg(\neg G \vee \neg H).$$

By the Replacement Theorem, in F we can replace $G \wedge H$ with $\neg(\neg G \vee \neg H)$. In this way, we can remove all instances of $\wedge$ from F, obtaining a formula in $\{\vee, \neg\}$ that is equivalent to F. □

Similarly, we have:

2.5.3 Theorem. *The signature $\{\wedge, \neg\}$ is adequate.*

Proof. Exercise. □

2.5.4 Corollary. *The signature $\{\wedge, \nleftrightarrow, 1\}$ is adequate.*

Proof. The signature $\{\wedge, \neg\}$ is adequate, but the connective $\neg$ can be expressed in terms of $\nleftrightarrow$ and 1, since

$$\neg P \sim 1 \nleftrightarrow P$$

by § 2.2, Exercise 4a; so $\{\wedge, \nleftrightarrow, 1\}$ 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:

(∗) $\mathcal{L}'$ is known to be adequate;

(†) the elements of $\mathcal{L}'$ can be expressed in terms of $\mathcal{L}$.

[12] Post's method is different from ours; see [32, pp. 167 f.].

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 would be 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**:[13] this is defined so that

$$P \curlywedge Q \sim \neg P \land \neg Q.$$

So $\curlywedge$ is defined in terms of $\land$ and $\neg$. This fact by itself tells us *nothing* about the adequacy of $\{\curlywedge\}$; it has no relevance to the proof of the following:

2.5.5 Theorem. *The signature $\{\curlywedge\}$ is adequate.*

Proof. It is enough to write $\neg P$ and $P \land Q$ using only $\curlywedge$. We have $\neg P \sim P \curlywedge P$, and also

$$\begin{aligned} P \land Q &\sim (\neg P) \curlywedge (\neg Q) \\ &\sim (P \curlywedge P) \curlywedge (Q \curlywedge Q). \end{aligned}$$

Hence all formulas in the adequate signature $\{\land, \neg\}$ can be written in terms of $\curlywedge$. Thus $\{\curlywedge\}$ is adequate. □

Adequate n-ary connectives where $n > 2$ can also be found.

How might we show that a certain signature is *not* adequate? Note that the signature $\{\land, \neg\}$ is adequate even though it contains no nullary connectives: the two constant Boolean *polynomials* are represented in $\{\land, \neg\}$ by $P \land \neg P$ and $\neg(P \land \neg P)$ respectively.

2.5.6 Theorem. *The signature $\{\land, \nleftrightarrow\}$ is* not *adequate.*

Proof. We shall show that no formula in $\{\land, \nleftrightarrow\}$ represents 1. Now, if

$$F(P_0, P_1, P_2, \dots, P_n) \sim 1,$$

then $F(P_0, P_0, P_0, \dots, P_0) \sim 1$ by the Substitution Theorem. Since $\{\land, \nleftrightarrow\}$ contains no nullary connectives, it is enough to show that no *singulary* formula represents 1.

In $\{\land, \nleftrightarrow\}$, we can represent 0 by $P \nleftrightarrow P$. We also have

$$\begin{aligned} 0 \land 0 &\sim 0, & 0 \nleftrightarrow 0 &\sim 0, \\ 0 \land P &\sim 0, & 0 \nleftrightarrow P &\sim P, \\ P \land 0 &\sim 0, & P \nleftrightarrow 0 &\sim P, \\ P \land P &\sim P, & P \nleftrightarrow P &\sim 0. \end{aligned}$$

By the Replacement Theorem, we can create no singulary formula in $\{\land, \nleftrightarrow\}$ that is *not* equivalent to 0 or a variable. □

[13] According to Burris [5, § 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 $\{\curlywedge\}$.

Exercises

(1) Write down truth-tables for unknown formulas, and then find disjunctive normal forms for those formulas.

(2) Prove Theorem 2.5.3.

(3) Prove that $\{\neg, \to\}$ is adequate.

(4) Prove that $\neg$ by itself is *not* adequate.

(5) Prove the adequacy of the **Sheffer stroke**, the connective $|$ such that $P \mid Q \sim \neg\,(P \land Q)$.

(6) Find an adequate ternary (3-ary) connective. (See § 2.1, Exercise 3.)

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 the following lemma, which lists some fundamental properties of the Boolean connectives. (The label definitions here is not a literal account of how the connectives were defined in § 1.7.)

2.6.1 Lemma.

($*$) ***definitions:***

$$\begin{aligned} P \to Q &\sim \neg P \lor Q, \\ P \leftrightarrow Q &\sim (P \to Q) \land (Q \to P), \\ P \nleftrightarrow Q &\sim \neg(P \leftrightarrow Q); \end{aligned}$$

(†) ***double negation:***

$$\neg\neg P \sim P;$$

(‡) ***De Morgan's Laws:***

$$\neg(P \lor Q) \sim \neg P \land \neg Q, \qquad \neg(P \land Q) \sim \neg P \lor \neg Q;$$

(§) ***Commutativity:***

$$P \land Q \sim Q \land P, \qquad P \lor Q \sim Q \lor P;$$

(¶) ***Associativity:***

$$(P \land Q) \land R \sim P \land (Q \land R), \qquad (P \lor Q) \lor R \sim P \lor (Q \lor R);$$

(‖) ***Distributivity:***

$$P \land (Q \lor R) \sim (P \land Q) \lor (P \land R), \qquad P \lor (Q \land R) \sim (P \lor Q) \land (P \lor R);$$

($**$) ***redundancies:***

$$\begin{array}{cccc} P \wedge P \sim P, & P \wedge \neg P \sim 0, & P \wedge 1 \sim P, & P \wedge 0 \sim 0, \\ P \vee P \sim P, & P \vee \neg P \sim 1, & P \vee 0 \sim P, & P \vee 1 \sim 1; \end{array}$$

(††) ***new variables:***

$$P \sim (P \wedge Q) \vee (P \wedge \neg Q), \qquad P \sim (P \vee Q) \wedge (P \vee \neg Q).$$

Proof. This was § 2.2, Exercise 3. □

To reduce a formula to disjunctive normal form, using the equivalences in Lemma 2.6.1, we can:

(0) eliminate instances of $\rightarrow$, $\leftrightarrow$ and $\nleftrightarrow$;

(1) eliminate multiple negations, and make sure that the only arguments of $\neg$ are variables;

(2) eliminate conjunctions of disjunctions;

(3) eliminate redundancies; now the formula is a disjunction of conjunctions of variables and negated variables, so:

(4) add variables as necessary to obtain a disjunctive normal form.

2.6.2 Example. Suppose F is the formula $\neg(P \rightarrow Q) \vee Q$. The reduction of F to disjunctive normal form can proceed as follows:

$$\begin{aligned} F &\sim \neg(\neg P \vee Q) \vee Q && \text{[def'n of } \rightarrow\text{]} \\ &\sim (\neg\neg P \wedge \neg Q) \vee Q && \text{[de Morgan]} \\ &\sim (P \wedge \neg Q) \vee Q && \text{[double negation]} \\ &\sim (P \wedge \neg Q) \vee (Q \wedge P) \vee (Q \wedge \neg P) && \text{[new variable]} \\ &\sim (P \wedge \neg Q) \vee (P \wedge Q) \vee (\neg P \wedge Q) && \text{[commutativity]} \end{aligned}$$

•

There may be more than one way to proceed:

2.6.3 Example. Let F be $\neg(\neg P \rightarrow Q) \wedge (Q \vee \neg P)$. Then

$$\begin{aligned} F &\sim \neg(\neg\neg P \vee Q) \wedge (Q \vee \neg P) && \text{[def'n of } \rightarrow\text{]} \\ &\sim \neg(P \vee Q) \wedge (Q \vee \neg P) && \text{[double neg.]} \\ &\sim (\neg P \wedge \neg Q) \wedge (Q \vee \neg P) && \text{[De Morgan]} \\ &\sim ((\neg P \wedge \neg Q) \wedge Q) \vee ((\neg P \wedge \neg Q) \wedge \neg P) && \text{[dist.]} \\ &\sim (\neg P \wedge (\neg Q \wedge Q)) \vee (\neg P \wedge (\neg P \wedge \neg Q)) && \text{[assoc.; comm.]} \\ &\sim (\neg P \wedge 0) \vee ((\neg P \wedge \neg P) \wedge \neg Q) && \text{[red.; assoc.]} \\ &\sim \neg P \vee (\neg P \wedge \neg Q) && \text{[red.]} \\ &\sim (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg Q) && \text{[new var.]} \\ &\sim (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) && \text{[red.]} \\ &\sim \neg P. && \text{[new var.]} \end{aligned}$$

Thus, as a binary formula, F has the disjunctive normal form

$$(\neg P \wedge Q) \vee (\neg P \wedge \neg Q);$$

but F is also equivalent to a singulary formula, $\neg P$, which is trivially in disjunctive normal form. An alternative simplification of F to $\neg P$ proceeds:

$$\begin{aligned}
F &\sim \neg(P \vee Q) \wedge (Q \vee \neg P) && \text{[def'n of } \to\text{; double neg.]}\\
&\sim (\neg P \wedge \neg Q) \wedge (Q \vee \neg P) && \text{[De Morgan]}\\
&\sim \neg P \wedge (\neg Q \wedge (Q \vee \neg P)) && \text{[assoc.]}\\
&\sim \neg P \wedge ((\neg Q \wedge Q) \vee (\neg Q \wedge \neg P)) && \text{[dist.]}\\
&\sim \neg P \wedge (0 \vee (\neg Q \wedge \neg P)) && \text{[red.]}\\
&\sim \neg P \wedge (\neg Q \vee \neg P) && \text{[red.]}\\
&\sim (\neg P \vee Q) \wedge (\neg P \vee \neg Q) \wedge (\neg Q \vee \neg P) && \text{[new var.]}\\
&\sim (\neg P \vee Q) \wedge (\neg P \vee \neg Q) && \text{[red.]}\\
&\sim \neg P. && \text{[new var.]}
\end{aligned}$$

•

In the last example, the two simplifications implicitly established the two **Absorption Laws**:

$$P \wedge (P \vee Q) \sim P, \qquad P \vee (P \wedge Q) \sim P.$$

If two formulas F and G are equivalent, then we can use simplification to show this:

(0) Simplify F to a disjunctive normal form F'.

(1) Simplify G to a disjunctive normal form G'.

(2) Note that $F' \sim G'$. (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.

2.6.4 Example. The formulas $P \to Q \to R$ and $Q \to P \to R$ are equivalent, because

$$\begin{aligned}
P \to Q \to R &\sim \neg P \vee (Q \to R) && \text{[def'n of } \to\text{]}\\
&\sim \neg P \vee \neg Q \vee R && \text{[def'n of } \to\text{]}\\
&\sim \neg Q \vee \neg P \vee R && \text{[comm.]}\\
&\sim \neg Q \vee (P \to R) && \text{[def'n of } \to\text{]}\\
&\sim Q \to P \to R. && \text{[def'n of } \to\text{]}
\end{aligned}$$

(Associativity was used silently.) The reduction of each formula to disjunctive normal form would be tedious, since that normal form is

$$\begin{aligned}
&(\neg P \wedge \neg Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \vee\\
&\quad \vee (\neg P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge Q \wedge R);
\end{aligned}$$

but the conjunctive normal form is just the formula $\neg P \vee \neg Q \vee R$, found in the original simplification. •

Exercises

(1) Given a formula in normal form, how would you write down its truth-table?

(2) Use simplification to prove the following equivalences:

(a) $\neg(P \wedge Q) \vee R \sim P \wedge Q \to R$;

(b) $(P \to Q) \wedge (R \to Q) \wedge \neg Q \to \neg(P \vee R) \sim 1$;

(c) $P \to (Q \to R) \sim P \to Q \to (P \to R)$;

(d) $(P \vee R) \wedge (Q \vee \neg R) \sim (P \wedge \neg R) \vee (Q \wedge R)$;

(e) $(P_0 \vee P_1) \wedge (Q_0 \vee Q_1) \sim \bigvee_{i=0}^{1} \bigvee_{j=0}^{1} (P_i \wedge Q_j)$.

(3) For $(\neg P \to Q) \wedge (\neg Q \to P) \to (\neg P \vee \neg Q)$, find the disjunctive normal form using simplification.

(4) Use simplification to verify the equivalences listed in § 2.2, Exercise 4.

(5) Use simplification to establish the following:

(a) $P \nleftrightarrow Q \sim \neg(P \leftrightarrow Q)$;

(b) $P \leftrightarrow Q \sim P \nleftrightarrow \neg Q$.

2.7 Logical consequence and formal proofs

Simplification is a way to prove that two formulas have the same truth-table. There is more that we might want to prove:

If F is an n-ary formula such that $\widehat{F}(\vec{e})$ for all truth-assignments $\vec{e}$, then as in § 2.2 we write

$$\vDash F.$$

Suppose $(F_0, \dots, F_m)$ is a list of $m+1$ formulas, each n-ary, such that, for all n-ary truth-assignments $\vec{e}$, if $\widehat{F_i}(\vec{e}) = 1$ for each i in $\{0, \dots, m-1\}$, then $\widehat{F_m}(\vec{e}) = 1$. Then we say that F_m is a **logical consequence** of $\{F_0, \dots, F_{m-1}\}$, and we write

$$F_0, \dots, F_{m-1} \vDash F_m;$$

if $\Sigma = \{F_0, \dots, F_{m-1}\}$, then we can also write

$$\Sigma \vDash F_m.$$

Corresponding to Theorem 2.3.4, we have

2.7.1 Theorem (Substitution)**.** *If $(F_0, \dots, F_m)$ is a list of n-ary formulas such that*

$$F_0, \dots, F_{m-1} \vDash F_m,$$

and $(G_0, \dots, G_{n-1})$ is a list of n formulas, then

$$F_0(G_0, \dots, G_{n-1}),\ \dots,\ F_{m-1}(G_0, \dots, G_{n-1}) \vDash F_m(G_0, \dots, G_{n-1}).$$

Proof. Write the $F_i(G_0, \dots, G_{n-1})$ as H_i. Say $\vec{e}$ is a truth-assignment for the G_j such that $\widehat{H}_i(\vec{e}) = 1$ when $i < m$. Let $f_j = \widehat{G}_i(\vec{e})$ when $j < n$. Then $\widehat{F}_i(\vec{f}) = 1$ when $i < m$, by the associativity of substitution (that is, Lemma 2.3.2). Hence also $\widehat{H}_m(\vec{e}) = \widehat{F}_m(\vec{f}) = 1$ (since F_m is a logical consequence of $\{F_0, \dots, F_{m-1}\}$), so $H_0, \dots, H_{m-1} \vDash H_m$, which was to be proved. □

The following basic means of establishing logical consequence should be compared with Implication (1.21):

2.7.2 Lemma (Detachment)**.** *$F,\ F \to G \vDash G$.*

Proof. It is enough to show $P_0,\ P_0 \to P_1 \vDash P_1$, by the preceding Substitution Theorem. The truth-table

P_0	P_0	$\to$	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 $P_0 \to P_1$ are true. Under this assignment, P_1 is true. □

Suppose F is a formula, and Σ is a set of formulas. A **deduction** or **formal proof** of F from Σ is a finite non-empty list

$$G_0, \dots, G_\ell$$

of formulas such that G_ℓ is F, and for each k in $\{0, \dots, \ell\}$, one of the following conditions is met:

(∗) G_k is in Σ; or

(†) G_k is a tautology; or

(‡) there is j in $\{0, \dots, k-1\}$ such that $G_j \sim G_k$; or

(§) there are distinct i and j in $\{0, \dots, k-1\}$ such that G_j is $G_i \to G_k$.

If such a deduction exists, then we say that F is **deducible** or **formally provable** from Σ, and Σ is a set of **hypotheses** (singular: hypothesis) from which F is deducible; we may then write

$$\Sigma \vdash F.$$

If Σ is a finite set $\{G_0, \dots, G_{m-1}\}$, then we can also write $G_0, \dots, G_{m-1} \vdash F$; if Σ is empty, we write

$$\vdash F.$$

2.7.3 Example. $F \wedge G \vdash G$, because the following is a deduction of G from $F \wedge G$:

(0)	$F \wedge G$	[hyp.]
(1)	1	[taut.]
(2)	$\neg F \vee 1$	[red.]
(3)	$\neg F \vee \neg G \vee G$	[red.]
(4)	$\neg(F \wedge G) \vee G$	[De Morgan]
(5)	$(F \wedge G) \to G$	[def'n of $\to$]
(6)	G	[Detachment, lines 0 & 5]

Strictly, the deduction itself is just the list

$$F \wedge G,\ 1,\ \neg F \vee 1,\ \neg F \vee \neg G \vee G,\ \neg(F \wedge G) \vee G,\ (F \wedge G) \to G,\ G$$

of formulas. In fact, there is a shorter deduction of F from $F \wedge G$, namely

$$F \wedge G,\ F \wedge G \to G,\ G.$$

However, *recognizing* this as a deduction requires, in part, recognizing that $F \wedge G \to G$ is a tautology. •

2.7.4 Theorem. *For all formulas F and all finite sets Σ of formulas,*

$$\Sigma \vDash F \iff \Sigma \vdash F.$$

Proof. We shall prove

$$\begin{array}{ccc}
(F_0,\dots,F_{m-1} \vDash F_m) & \Longrightarrow & (\vDash F_0 \to F_1 \to \cdots \to F_m) \\
\Uparrow & & \Downarrow \\
(F_0,\dots,F_{m-1} \vdash F_m) & \Longleftarrow & (\vdash F_0 \to F_1 \to \cdots \to F_m)
\end{array}$$

Suppose $F_0,\dots,F_{m-1} \vDash F_m$. Then for every truth-assignment $\vec{e}$ for the F_i, either $\widehat{F}_m(\vec{e}) = 1$, or $\widehat{F}_i(\vec{e}) = 0$ for some i in $\{0,\dots,m-1\}$. If $\widehat{F}_i(\vec{e}) = 0$ and $i < m$, then $F_i \to F_{i+1} \to \cdots \to F_m$ is true at $\vec{e}$, and hence so is $F_0 \to \cdots \to F_m$. For the same reason, if $\widehat{F}_m(\vec{e}) = 1$, then $F_0 \to \cdots \to F_m$ is true at $\vec{e}$. Hence $\vDash F_0 \to \cdots \to F_m$.

Suppose $\vDash F_0 \to \cdots \to F_m$. Then, since it is a tautology, the formula $F_0 \to \cdots \to F_m$ is its own proof of itself. Hence $\vdash F_0 \to \cdots \to F_m$.

Suppose $\vdash F_0 \to \cdots \to F_m$. Let $G_0,\dots,G_\ell$ be a deduction of $F_0 \to \cdots \to F_m$. Then we have a deduction

(0)	G_0	
$\dots$	$\dots$	
$(\ell-1)$	$G_{\ell-1}$	
(ℓ)	$F_0 \to \cdots \to F_m$	
$(\ell+1)$	F_0	[hyp.]
$(\ell+2)$	$F_1 \to \cdots \to F_m$	[Detachment]
$(\ell+3)$	F_1	[hyp.]
$(\ell+4)$	$F_2 \to \cdots \to F_m$	[Detachment]
$\dots$	$\dots$	
$(\ell+2m-2)$	$F_{m-1} \to F_m$	[Detachment]
$(\ell+2m-1)$	F_{m-1}	[hyp.]
$(\ell+2m)$	F_m	[Detachment]

of F_m from $\{F_0, \dots, F_{m-1}\}$. Thus $F_0, \dots, F_{m-1} \vdash F_m$.

Suppose finally $F_0, \dots, F_{m-1} \vdash F_m$. We use the method of infinite descent. Let $G_0, \dots, G_{\ell-1}, F_m$ be a deduction of F_m from $\{F_0, \dots, F_{m-1}\}$. Let $\vec{e}$ be a truth-assignment such that $\widehat{F_i}(\vec{e}) = 1$ whenever $i < m$. Suppose if possible that $\widehat{F_m}(\vec{e}) = 0$. Then F_m is not in $\{F_0, \dots, F_{m-1}\}$, nor is F_m a tautology. Hence, by the definition of a deduction, either $F_m \sim G_i$ for some i in $\{0, \dots, \ell-1\}$, or there are i and j in $\{0, \dots, \ell-1\}$ such that G_j is $G_i \to F_m$. In the first case, G_i is false at $\vec{e}$; in the second case, either G_i or G_j is false at $\vec{e}$. In either case, $\widehat{G_k}(\vec{e}) = 0$ for some k in $\{0, \dots, \ell-1\}$. But $G_0, \dots, G_k$ is still a deduction from $\{F_0, \dots, F_{m-1}\}$, strictly shorter then the original one, but with the same property (namely that its last formula is false at $\vec{e}$). We can't take shorter deductions indefinitely. Hence $\widehat{F_m}(\vec{e}) = 1$. Therefore $F_0, \dots, F_{m-1} \vDash F_m$. □

Suppose $F_0, \dots, F_{m-1} \vDash F_m$. The proof of the last theorem shows how to write down a deduction of F_m from $\{F_0, \dots, F_{m-1}\}$. Indeed, let G_0 be the formula $F_0 \to F_1 \to \dots \to F_m$. Then G_0 must be a tautology, so the sequence

$$G_0,\ F_0,\ F_1 \to \dots \to F_m,\ F_1,\ F_2 \to \dots \to F_m,\ \dots,\ F_m$$

is a deduction from $\{F_0, \dots, F_{m-1}\}$. The problem is that this sequence is not *obviously* a deduction. To make it so, we can apply simplification to G_0, getting a chain

$$G_0 \sim G_1 \sim \dots \sim G_\ell$$

of equivalences as in § 2.6, where G_ℓ is a tautology in disjunctive or conjunctive normal form (or follows from such a tautology by a substitution). Then the sequence

$$G_\ell,\ G_{\ell-1},\ \dots,\ G_0,\ F_0,\ F_1 \to \dots \to F_m,\ F_1,\ F_2 \to \dots \to F_m,\ \dots,\ F_m \tag{2.4}$$

will be a deduction, and recognizably so; we may call it a **recognizable deduction.** I'm not giving a precise definition of recognizable. It could be done, but we might find the definition too restrictive. Informally then, recognizable deduction is:

(∗) a deduction;

(†) *clearly* a deduction to any reader that knows the rules of simplification established in § 2.6.

Not every recognizable deduction need be as long as the Deduction (2.4); there may be short-cuts:

2.7.5 Example. To show $F \lor G,\ \neg F \vdash G$, we can start with the simplification

$$\begin{aligned} F \lor G \to \neg F \to G &\sim \neg(F \lor G) \lor (\neg F \to G) \\ &\sim \neg(F \lor G) \lor (F \lor G) \end{aligned}$$

ending in a tautology derived from $\neg P \lor P$ by substitution. Then the sequence

$$
\begin{array}{cl}
\neg(F \vee G) \vee (F \vee G), & \text{[taut.]} \\
\neg(F \vee G) \vee (\neg F \to G), & \text{[def'n of } \to\text{]} \\
F \vee G \to \neg F \to G, & \text{[def'n of } \to\text{]} \\
F \vee G, & \text{[hyp.]} \\
\neg F \to G, & \text{[Det.]} \\
\neg F, & \text{[hyp.]} \\
G & \text{[Det.]}
\end{array}
$$

is a recognizable deduction of G from $F \vee G$ and $\neg F$. A shorter deduction, still recognizable, is

$$
\begin{array}{cl}
F \vee G, & \text{[hyp.]} \\
\neg F \to G, & [\to] \\
\neg F, & \text{[hyp.]} \\
G. & \text{[Det.]}
\end{array}
$$

(Curiously, it's the tail end of the first deduction.) •

Exercises

(1) Show that $F_0,\ \ldots,\ F_{m-1} \vDash G$ if and only if $\bigwedge_{k<m} F_k \vDash G$.

(2) Using an exercise from § 2.6, write a recognizable deduction of $\neg(P \vee R)$ from $P \to Q,\ R \to Q,\ \neg Q$.

(3) Convert other simplifications from § 2.6 into recognizable deductions.

(4) Write recognizable deductions for the following:

   (a) $\neg F \to 0 \vdash F$;

   (b) $F \to G_0 \vee \cdots \vee G_n,\ G_0 \to H,\ \ldots,\ G_m \to H \vdash F \to H$;

   (c) $F \vdash F \vee G$ and $F \vdash G \vee F$;

   (d) $F \to G,\ \neg G \vdash \neg F$;

   (e) $F \to G,\ G \to H \vdash F \to H$;

   (f) $F \vee G,\ \neg G \vdash F$;

   (g) $F_0 \to G_0,\ F_1 \to G_1,\ F_0 \vee F_1 \vdash G_0 \vee G_1$;

   (h) $F,\ G \vdash F \wedge G$.

(5) Assuming that $H_0, \ldots, H_m$ is a recognizable deduction of G from $F_0 \wedge F_1$, write a recognizable deduction of G from $\{F_0, F_1\}$.

2.8 Proof-systems

Deductions as defined in the preceding section are really just deductions *in a particular proof-system*. For propositional formulas, a **proof-system** consists of:

(∗) **axioms**[14], that is, certain distinguished formulas, and

(†) **rules of inference**, which are clearly described ways of obtaining new formulas from finitely many given formulas.

Then, of the proof-system of § 2.7,

(∗) the axioms are just the tautologies;

(†) the rules of inference are two:

(0) to infer, from any formula, a formula equivalent to it;

(1) (also called ***Modus Ponens***): to infer, from F and $F \to G$, the formula G.

Then the following should be an obvious generalization of what we did in § 2.7:

Suppose we have a proof-system $\mathcal{N}$ and a list $(F_0, \dots, F_m)$ of formulas. In the system $\mathcal{N}$, a **deduction** or **formal proof** of F_m from $\{F_0, \dots, F_{m-1}\}$ is a finite sequence

$$G_0, \dots, G_\ell,$$

where G_ℓ is F_m and, for each k in $\{0, \dots, \ell\}$, the formula G_k is:

(∗) an axiom of $\mathcal{N}$, or

(†) one of the formulas F_i, where $i < m$, or

(‡) a formula obtainable from (some of) the formulas in $\{G_0, \dots, G_{k-1}\}$ by one of the rules of inference of $\mathcal{N}$.

If there is such a deduction, then we write

$$F_0, \dots, F_{m-1} \vdash_{\mathcal{N}} F_m,$$

and we say that F_m is **derivable** or **formally provable** in $\mathcal{N}$ from the set $\{F_0, \dots, F_{m-1}\}$ of **hypotheses**. In case $m = 0$, we write $\vdash_{\mathcal{N}} F_0$ and say that F_0 is a **validity** of $\mathcal{N}$ (or a **theorem** of $\mathcal{N}$).

We might think of axioms as rules of inference whereby certain formulas can be inferred from *no* given formulas.

Many proof-systems are possible. Some are more useful than others. As a minimum requirement, we should like a proof-system $\mathcal{N}$ to have the following two properties:

(∗) **soundness**: if $F_0, \dots, F_{n-1} \vdash_{\mathcal{N}} G$, then $F_0, \dots, F_{n-1} \models G$;

(†) **completeness**: if $F_0, \dots, F_{n-1} \models G$, then $F_0, \dots, F_{n-1} \vdash_{\mathcal{N}} G$.

Theorem 2.7.4 is that the proof-system of § 2.7 is sound and complete.

In § 2.7, the notion of a *recognizable* deduction was kept imprecise. The Substitution Theorem 2.7.1 gives a way to add new rules of inference to our system, some of which we may want to allow in recognizable deductions. For instance, taking note of Example 2.7.3, we may want to allow the rule of inferring G from $F \wedge G$. More generally, if we know

$$F_0, \dots, F_{m-1} \models F_m,$$

[14]From the Greek ἀξίωμα, ἀξιώματοσ (honor, worth, etc.).

then we may allow the rule of inferring $F_m(G_0, \dots, G_{n-1})$ from the formulas

$$F_0(G_0, \dots, G_{n-1}), \dots, F_{m-1}(G_0, \dots, G_{n-1}),$$

for every list $(G_0, \dots, G_{n-1})$ of n formulas.

In any case, we have the rule that, from a formula, we may derive an equivalent formula. This is *not* a rule of inference such as we have just described. But *Detachment* is such a rule, being derived from

$$P,\ P \to Q \vDash Q.$$

More rules can be obtained from the following:

2.8.1 Lemma.

(∗) $\neg P \to 0 \vDash P$ *(**Contradiction**);*

(†) $P \wedge Q \vDash Q$;

(‡) $P \to Q_0 \vee \dots \vee Q_n,\ Q_0 \to R,\ \dots,\ Q_m \to R \vDash P \to R$ *(**Cases**);*

(§) $P \vDash P \vee Q$ *and* $P \vDash Q \vee P$ *(**Addition**);*

(¶) $P \to Q,\ \neg Q \vDash \neg P$ *(***Modus Tollens***[15]);*

(‖) $P \to Q,\ Q \to R \vDash P \to R$ *(**Hypothetical Syllogism**[16]);*

(∗∗) $P \vee Q,\ \neg P \vDash Q$ *and* $P \vee Q,\ \neg Q \vDash P$ *(**Disjunctive Syllogism**);*

(††) $P_0 \to Q_0,\ P_1 \to Q_1,\ P_0 \vee P_1 \vDash Q_0 \vee Q_1$ *(**Constructive Dilemma**).*

Proof. These were all proved in § 1.4 (most as exercises). □

Exercises

Write deductions for the following, using Lemma 2.8.1:

(1) $P \leftrightarrow Q,\ Q \leftrightarrow R \vdash P \leftrightarrow R$;

(2) $P \nleftrightarrow Q,\ Q \nleftrightarrow R \vdash P \leftrightarrow R$.

2.9 Łukasiewicz's proof system

Here is developed a proof-system $\mathcal{L}$ (for its inventor Łukasiewicz). It is of interest for the simplicity of its definition. It involves only formulas in the signature $\{\to, \neg\}$. (We know from an exercise in § 2.5 that this signature is adequate.) The only rule of inference of $\mathcal{L}$ is Detachment. The axioms of $\mathcal{L}$ are of three kinds[17]:

[15] Latin for method [of] denying.

[16] A *syllogism* is a classical form of argument; Aristotle's definition is quoted in Appendix A. A standard example of a syllogism is: All men are mortal. Socrates is a man. Therefore Socrates is mortal.

[17] Frege had an earlier proof-system in this signature that used three additional kinds of axioms.

(0) $\vdash_{\mathcal{L}} F \to G \to F$ (**Affirmation of the Consequent**);

(1) $\vdash_{\mathcal{L}} (F \to G \to H) \to (F \to G) \to F \to H$ (**Self-Distributivity of Implication**);

(2) $\vdash_{\mathcal{L}} (\neg F \to \neg G) \to G \to F$ (**Contraposition**).

System $\mathcal{L}$ is sound by Lemma 2.7.2 and because the axioms are tautologies. To prove completeness, we shall need the following.

2.9.1 Lemma. $\vdash_{\mathcal{L}} F \to F$.

Proof. The formal proof is

$$\begin{aligned}
&F \to F \to F\\
&F \to (F \to F) \to F\\
&(F \to (F \to F) \to F) \to (F \to F \to F) \to F \to F\\
&(F \to F \to F) \to F \to F\\
&F \to F,
\end{aligned}$$

where the first three entries are axioms (0), (0), and (1) respectively, and the last two follow by Detachment. □

2.9.2 Lemma. *If $F_0, \dots, F_{n-1} \vdash_{\mathcal{L}} G \to H$, then $F_0, \dots, F_{n-1}, G \vdash_{\mathcal{L}} H$.*

Proof. Exercise. □

The converse of Lemma 2.9.2 is the following; the proof is by cases (and the method of infinite descent).

2.9.3 Theorem (Deduction). *If $F_0, \dots, F_{n-1}, G \vdash_{\mathcal{L}} H$, then*

$$F_0, \dots, F_{n-1} \vdash_{\mathcal{L}} G \to H.$$

Proof. There are three possibilities for H:

If H is an axiom of $\mathcal{L}$, or is one of the formulas F_i, then $F_0, \dots, F_{n-1} \vdash_{\mathcal{L}} H$; but also $\vdash_{\mathcal{L}} H \to G \to H$; hence $F_0, \dots, F_{n-1} \vdash_{\mathcal{L}} G \to H$ by Detachment.

If H is G, then $\vdash_{\mathcal{L}} G \to H$ by Lemma 2.9.1.

Finally, suppose $K_0, \dots, K_m$ is the formal proof in $\mathcal{L}$ of H from $F_0, \dots, F_{n-1}$ and G, and suppose the last step in the proof is by Detachment. (If it's not, then we have already treated this possibility.) Then K_i is F, and K_j is $F \to H$, for some formula F, and for some i and j less than m. If $G \to K_i$ and $G \to K_j$ can be deduced in $\mathcal{L}$ from $\{F_0, \dots, F_{n-1}\}$, then, by Detachment and the Self-Distributivity Axiom, so can $G \to H$. Also, both K_i and K_j have shorter deductions than H in $\mathcal{L}$. Hence, if $G \to H$ cannot be deduced, then neither can $G \to K$ for some K with a shorter deduction than H, which would be absurd. □

2.9.4 Lemma. *The following are validities of $\mathcal{L}$:*

(1) $\neg G \to G \to F$;

(2) $\neg\neg F \to F$;

(3) $F \to \neg\neg F$;

(4) $(F \to G) \to \neg G \to \neg F$;

(5) $F \to \neg G \to \neg(F \to G)$.

(6) $(F \to G) \to (\neg F \to G) \to G$.

Proof. (1) The following is a formal proof in $\mathcal{L}$ from $\neg G$:

$$\neg G,\ \neg G \to (\neg F \to \neg G),\ \neg F \to \neg G,\ \neg F \to \neg G \to (G \to F),\ G \to F.$$

So $\neg G \vdash_{\mathcal{L}} G \to F$. By the Deduction Theorem, the claim follows.

(2) By part (1) (and Lemma 2.9.2) we have $\neg\neg F \vdash_{\mathcal{L}} \neg F \to \neg\neg\neg F$. Use contraposition to get $\neg\neg F \vdash_{\mathcal{L}} F$, then use the Deduction Theorem to get the claim.

The remaining parts are an exercise. □

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.

2.9.5 Theorem. *Let F be an n-ary formula in the signature $\{\to, \neg\}$. Let $\vec{e}$ be a truth-assignment for F. Define*

$$P_i' = \begin{cases} P_i, & \text{if } e_i = 1; \\ \neg P_i, & \text{if } e_i = 0; \end{cases} \quad \text{and} \quad F' = \begin{cases} F, & \text{if } \widehat{F}(\vec{e}) = 1; \\ \neg F, & \text{if } \widehat{F}(\vec{e}) = 0. \end{cases}$$

Then $P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} F'$.

Proof. If F is P_i, then P_i' is F', so $P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} F'$.

Now we can suppose F is not just a variable, and use infinite descent. So, assume F' is *not* deducible in $\mathcal{L}$ from $P_0', \ldots, P_{n-1}'$. There are two cases:

Say F is $\neg G$ for some formula G. Then

$$F' = \begin{cases} G', & \text{if } \widehat{F}(\vec{e}) = 1; \\ \neg\neg G', & \text{if } \widehat{F}(\vec{e}) = 0. \end{cases}$$

Hence G' is also not deducible; but G is shorter then F.

Say F is $G \to H$ for some formulas G and H. Then

$$P_0', \ldots, P_{n-1}' \vdash_{\mathcal{L}} G', H'.$$

There are three sub-cases to consider, according as

($*$) G' is $\neg G$, or

(†) H' is H, or

(‡) G' is G and H' is $\neg H$.

Details are an exercise. This completes the proof. □

2.9.6 Corollary. *The proof-system $\mathcal{L}$ is complete.*

Proof. Suppose $F_0, \ldots, F_{m-1} \vDash F_m$, the formulas being n-ary. Let G be the tautology $F_0 \to \cdots \to F_m$. Then for all n-ary truth-assignments $\vec{e}$, we have

$$P_0' \ldots, P_{n-1}' \vdash_{\mathcal{L}} G.$$

If $n = 0$, we are done. If $n > 0$, then by the Deduction Theorem we have

$$P_0' \ldots, P_{n-2}' \vdash_{\mathcal{L}} P_{n-1} \to G, \neg P_{n-1} \to G,$$

so $P_0' \ldots, P_{n-2}' \vdash_{\mathcal{L}} G$ by Lemma 2.9.4 (6). Continuing, we find $\vdash_{\mathcal{L}} G$, so $F_0, \ldots, F_{m-1} \vdash_{\mathcal{L}} F_m$. □

Exercises

(1) Prove Lemma 2.9.2.

(2) Prove parts (3), (4), (5) and (6) of Lemma 2.9.4.

(3) Supply the missing details in the proof of Theorem 2.9.5.

Chapter 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*.

Suppose $\mathcal{U}$ is some large set—a **universal set**, which will include all of the other sets that we shall work with. By the Axiom of Comprehension, 1.2.3, if P is a predicate applying (truly or falsely) to the elements of $\mathcal{U}$, then we can form a set

$$\{x \in \mathcal{U} : Px\}. \tag{3.1}$$

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**. We may replace the set A with other sets, but for now, our only individual variable will be x. (We shall allow more variables in § 3.2.)

First note that we can write A as

$$\{x \in \mathcal{U} : x \in A\}$$

(the set of x in $\mathcal{U}$ such that x is in A). This is not very interesting; but we can create more interest by combining $\in$-formulas, by means of Boolean connectives,

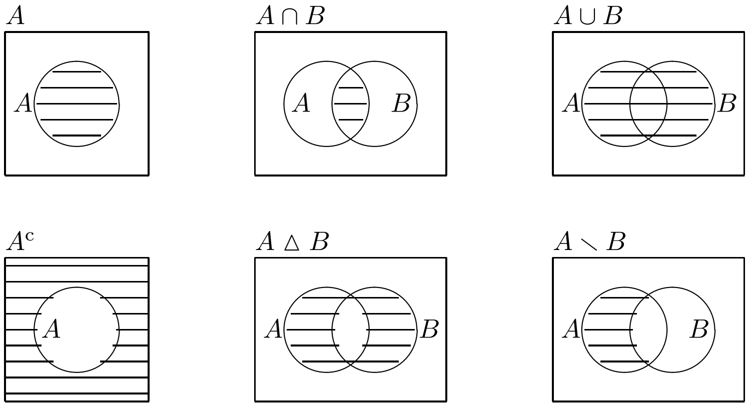


Figure 3.1: Venn diagrams of combinations of sets

so as to create new $\in$-formulas. We have already done this once, in § 1.9. From the formula $x \in A$, we obtain $\neg(x \in A)$, that is, $x \notin A$; this formula defines the **complement** of A in $\mathcal{U}$:

$$\{x \in \mathcal{U} : x \notin A\} = A^{\mathrm{c}}.$$

Suppose also $B \subseteq \mathcal{U}$. Using both of the formulas $x \in A$ and $x \in B$, we obtain the following standard combinations:

- $\{x \in \mathcal{U} : x \in A \wedge x \in B\} = A \cap B$, the **intersection** of A and B; it contains everything that is in *both* A and B;
- $\{x \in \mathcal{U} : x \in A \vee x \in B\} = A \cup B$, the **union** of A and B; it contains everything that is in (at least) *one* of A and B (the union was defined first in § 1.2);
- $\{x \in \mathcal{U} : x \in A \nleftrightarrow x \in B\} = A \mathbin{\triangle} B$, the **symmetric difference** of A and B; it contains everything that is in *exactly one* of A and B;
- $\{x \in \mathcal{U} : x \in A \wedge x \notin B\} = A \smallsetminus B$, the **difference** of A and B; it 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 $\smallsetminus$, along with $\varnothing$, stand for **Boolean operations**.

Note some alternative formulations:

$$A \cap B = \{x \in A : x \in B\};$$
$$A \smallsetminus B = \{x \in A : x \notin B\}.$$

Hence also

$$A^{\mathrm{c}} = \mathcal{U} \smallsetminus A.$$

If $A \cap B = \varnothing$, then A and B are called **disjoint**.

We now have a sort of correspondence between propositional logic and set-theory:

$$\begin{array}{ccc} \land & \leftrightsquigarrow & \cap \\ \lor & \leftrightsquigarrow & \cup \\ \nleftrightarrow & \leftrightsquigarrow & \triangle \\ \neg & \leftrightsquigarrow & {}^{\mathrm{c}} \\ 0 & \leftrightsquigarrow & \varnothing \end{array}$$

In the remainder of this section, we shall see how thorough-going this correspondence is.

Let us give ourselves an infinite list

$$(A_0, A_1, A_2, \dots)$$

of subsets of $\mathcal{U}$. We may let letters like A, B, and C stand for members of this list. If F is an n-ary propositional formula, then, by substituting for each variable P_k the formula $x \in A_k$, we obtain the $\in$-formula

$$F(x \in A_0,\ \dots,\ x \in A_{n-1}). \tag{3.2}$$

Abbreviate this as $\phi(x)$. The latter is a *formula* determining[1] a subset

$$\{x \in \mathcal{U} : \phi(x)\} \tag{3.3}$$

of $\mathcal{U}$. (Compare Line (3.1) above.) This subset is a **Boolean combination** of the sets A_k. It consists precisely of those elements c of $\mathcal{U}$ such that

$$\widehat{F}(\vec{e}) = 1,$$

where the n-ary truth-assignment $\vec{e}$ is defined so that

$$e_k = \begin{cases} 1, & \text{if } c \in A_k, \\ 0, & \text{if } c \notin A_k, \end{cases} \tag{3.4}$$

for each k in $\{0, \dots, k-1\}$. So we can express membership in Boolean combinations of sets by means of truth-tables:

3.0.1 Example. From the truth-table

P	$\to$	Q
0	1	0
1	0	0
0	1	1
1	1	1

,

by considering the lines where the formula $P \to Q$ takes the value 1, we can conclude that the set $\{x \in \mathcal{U} : x \in A \to x \in B\}$ consists of those c in $\mathcal{U}$ such that one of the following holds:

($*$) $c \notin A$ & $c \notin B$, or

[1] By the Axiom of Separation, 1.2.3. See also § 3.9. However, the existence of the set named in Line (3.3) is not really an axiom so much as a *definition* of the objects that we are studying. Indeed, Theorem 3.0.2, along with Exercise 1, will show that, in effect, we are studying *equivalence-classes* of propositional formulas.

(†) $c \notin A$ & $c \in B$, or

(‡) $c \in A$ & $c \in B$.

Alternatively, from the line of the truth-table where $P \to Q$ takes the value 0, we conclude that the set $\{x \in \mathcal{U} : x \in A \to x \in B\}$ 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 sets A and B are equal if

$$c \in A \iff c \in B \tag{3.5}$$

for all c in $\mathcal{U}$. The *converse* of this axiom is obviously true: If two sets are equal, then in particular, they have the same members. Hence, if

$$\{x \in \mathcal{U} : x \in A \leftrightarrow x \in B\} = \mathcal{U}, \tag{3.6}$$

then, for all c in $\mathcal{U}$, the proposition $c \in A$ is true if and only if the proposition $c \in B$ is true—that is, Equivalence (3.5) holds, so $A = B$ by the Axiom of Extension. Conversely, if $A = B$, then the Axiom gives us Equation (3.6). In short, the Axiom gives us the equivalence

$$A = B \iff \{x \in \mathcal{U} : x \in A \leftrightarrow x \in B\} = \mathcal{U}.$$

Being nullary Boolean connectives, the constants 0 and 1 are also $\in$-formulas; so we can form sets $\{x \in \mathcal{U} : 0\}$ and $\{x \in \mathcal{U} : 1\}$. The former contains nothing, so it must be *the* empty set; the latter contains every element of $\mathcal{U}$, and nothing else, so it must be $\mathcal{U}$. In short,

$$\{x \in \mathcal{U} : 0\} = \varnothing;$$
$$\{x \in \mathcal{U} : 1\} = \mathcal{U}.$$

Another consequence of the Axiom of Extension is:

3.0.2 Theorem. *Suppose F_0 and F_1 are n-ary propositional formulas such that*

$$F_0 \sim F_1.$$

When $e \in \mathbb{B}$, let $\phi_e(x)$ be the $\in$-formula $F_e(x \in A_0, \ldots, x \in A_{n-1})$. Then

$$\{x \in \mathcal{U} : \phi_0(x)\} = \{x \in \mathcal{U} : \phi_1(x)\}.$$

Proof. If $c \in \mathcal{U}$, let the n-ary truth-assignment $\vec{e}$ be as defined by the Rule (3.4) above. Then

$$\begin{aligned} c \in \{x \in \mathcal{U} : \phi_0(x)\} &\iff \widehat{F_0}(\vec{e}) = 1 \\ &\iff \widehat{F_1}(\vec{e}) = 1 \iff c \in \{x \in \mathcal{U} : \phi_1(x)\}. \end{aligned}$$

By the Axiom of Extension, the equality of the sets follows. □

Example (3.0.1 continued)**.** Because $P \to Q \sim \neg P \vee Q$, the two sets $\{x \in \mathcal{U} : x \in A \to x \in B\}$ and $\{x \in \mathcal{U} : x \notin A \vee x \in B\}$ are equal. •

We can say more. The following should be compared with Theorem 2.3.8:

3.0.3 Theorem (Replacement)**.** *Suppose F is a sub-formula of the n-ary formula G, so that G itself is $H(P_0, \dots, P_{n-1}, F)$ for some formula H. Let*

$$B = \{x \in \mathcal{U} : F(x \in A_0,\ \dots,\ x \in A_{n-1})\}.$$

Then the set $\{x \in \mathcal{U} : G(x \in A_0,\ \dots,\ x \in A_{n-1})\}$ is equal to

$$\{x \in \mathcal{U} : H(x \in A_0,\ \dots,\ x \in A_{n-1},\ x \in B)\}.$$

Proof. Exercise. □

3.0.4 Corollary. *For all $\in$-formulas $\phi(x)$ and $\psi(x)$,*

$$\begin{aligned}
\{x \in \mathcal{U} : \phi(x) \wedge \psi(x)\} &= \{x \in \mathcal{U} : \phi(x)\} \cap \{x \in \mathcal{U} : \psi(x)\},\\
\{x \in \mathcal{U} : \phi(x) \vee \psi(x)\} &= \{x \in \mathcal{U} : \phi(x)\} \cup \{x \in \mathcal{U} : \psi(x)\},\\
\{x \in \mathcal{U} : \phi(x) \nleftrightarrow \psi(x)\} &= \{x \in \mathcal{U} : \phi(x)\} \vartriangle \{x \in \mathcal{U} : \psi(x)\},\\
\{x \in \mathcal{U} : \neg\phi(x)\} &= \{x \in \mathcal{U} : \phi(x)\}^{\mathrm{c}}.
\end{aligned}$$

Proof. Let $A = \{x \in \mathcal{U} : \phi(x)\}$ and $B = \{x \in \mathcal{U} : \psi(x)\}$, and let H be the binary formula $P_0 \wedge P_1$. Then

$$\begin{aligned}
&\{x \in \mathcal{U} : \phi(x) \wedge \psi(x)\} &&\\
&= \{x \in \mathcal{U} : H(\phi(x), \psi(x))\} && \text{[by def'n of } H\text{]}\\
&= \{x \in \mathcal{U} : H(x \in A,\ x \in B)\} && \text{[by Replacement]}\\
&= \{x \in \mathcal{U} : x \in A \wedge x \in B\} && \text{[by def'n of } H\text{]}\\
&= A \cap B && \text{[by def'n of } \cap\text{]}\\
&= \{x \in \mathcal{U} : \phi(x)\} \cap \{x \in \mathcal{U} : \psi(x)\} && \text{[by def'n of } A \text{ and } B\text{]}.
\end{aligned}$$

The other identities are established likewise. □

Example (3.0.1 continued again)**.** We now have

$$\begin{aligned}
\{x \in \mathcal{U} : x \in A \to x \in B\} &= \{x \in \mathcal{U} : x \notin A \vee x \in B\}\\
&= \{x \in \mathcal{U} : x \notin A\} \cup \{x \in \mathcal{U} : x \in B\}\\
&= A^{\mathrm{c}} \cup B,
\end{aligned}$$

and similarly, $\{x \in \mathcal{U} : x \in A \to x \in B\} = (A^{\mathrm{c}} \cap B^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap B) \cup (A \cap B)$. 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. •

3.0.5 Example. From the truth-table

P	$\wedge$	$(Q$	$\vee$	$R)$
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 $\{x \in \mathcal{U} : x \in A \wedge (x \in B \vee x \in C)\}$ 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 $A \cap \{x \in \mathcal{U} : x \in B \vee x \in C\}$, which is $A \cap (B \cup C)$. •

3.0.6 Lemma. *The following are set-theoretic identities:*

($*$) ***definition:***

$$A \mathbin{\triangle} B = (A \cup B) \smallsetminus (A \cap B) \tag{3.7}$$
$$= (A \smallsetminus B) \cup (B \smallsetminus A), \tag{3.8}$$
$$A \smallsetminus B = A \cap B^{\mathrm{c}}; \tag{3.9}$$

(†) ***double complementation:***

$$A^{\mathrm{cc}} = A; \tag{3.10}$$

(‡) ***De Morgan's Laws:***

$$\begin{aligned}(A \cup B)^{\mathrm{c}} &= A^{\mathrm{c}} \cap B^{\mathrm{c}},\\ (A \cap B)^{\mathrm{c}} &= A^{\mathrm{c}} \cup B^{\mathrm{c}};\end{aligned} \tag{3.11}$$

(§) ***Commutativity:***

$$A \cap B = B \cap A, \qquad A \cup B = B \cup A; \tag{3.12}$$

(¶) ***Associativity:***

$$(A \cap B) \cap C = A \cap (B \cap C), \qquad (A \cup B) \cup C = A \cup (B \cup C), \tag{3.13}$$

(‖) *mutual* ***Distributivity*** *of* $\cap$ *and* $\cup$*:*

$$\begin{aligned}A \cap (B \cup C) &= (A \cap B) \cup (A \cap C),\\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C);\end{aligned} \tag{3.14}$$

($**$) ***redundancies:***

$$\varnothing^{\mathrm{c}} = \mathcal{U}, \qquad \mathcal{U}^{\mathrm{c}} = \varnothing; \tag{3.15}$$
$$A \cap A = A, \quad A \cap A^{\mathrm{c}} = \varnothing, \quad A \cap \mathcal{U} = A, \quad A \cap \varnothing = \varnothing, \tag{3.16}$$
$$A \cup A = A, \quad A \cup A^{\mathrm{c}} = \mathcal{U}, \quad A \cup \varnothing = A, \quad A \cup \mathcal{U} = \mathcal{U}, \tag{3.17}$$

(††) ***new set:***

$$A = (A \cap B) \cup (A \cap B^{c}); \tag{3.18}$$

(‡‡) ***Absorption:***

$$\begin{aligned} A \cap (A \cup B) &= A, \\ A \cup (A \cap B) &= A. \end{aligned} \tag{3.19}$$

Proof. Most of these identities are immediate from the equivalences in § 2.6 by means of Theorem 3.0.2 and Corollary 3.0.4. Identity (3.9) uses the definition of $\smallsetminus$. The rest are exercises. □

We can now prove other set-theoretic identities by a process of simplification parallel to the one we use for logical equivalences:

3.0.7 Theorem. *The equations*

$$A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C), \tag{3.20}$$
$$A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C) \tag{3.21}$$

are identities of sets.

Proof. For (3.20), we have the chain of identities

$$\begin{aligned} A \smallsetminus (B \cap C) &= A \cap (B \cap C)^{c} && \text{[def'n of } \smallsetminus\text{]} \\ &= A \cap (B^{c} \cup C^{c}) && \text{[De Morgan]} \\ &= (A \cap B^{c}) \cup (A \cap C^{c}) && \text{[distributivity]} \\ &= (A \smallsetminus B) \cup (A \smallsetminus C) && \text{[def'n of } \smallsetminus\text{].} \end{aligned}$$

Equation (3.21) 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 Identity (3.9) for example, it is enough to prove $A \smallsetminus B \subseteq A \cap B^{c}$ and $A \cap B^{c} \subseteq A \smallsetminus B$. To prove the former, suppose $c \in A \smallsetminus B$. Then $c \in A$, but $c \notin B$. Hence also $c \in B^{c}$. Hence $c \in A \cap B^{c}$. Therefore $A \smallsetminus B \subseteq A \cap B^{c}$. The other inclusion can be proved similarly.

Exercises

(1) Prove the converse of Theorem 3.0.2 in the following sense: Show that, if F and G are not equivalent, then there is a set $\mathcal{U}$ with subsets A_k such that $\{x \in \mathcal{U} : F(x \in A_0, \dots, x \in A_{n-1})\} \neq \{x \in \mathcal{U} : G(x \in A_0, \dots, x \in A_{n-1})\}$. (*Suggestion:* Let $\mathcal{U}$ be a set of truth-assignments, and let A_k comprise those $\vec{e}$ such that $e_k = 1$.)

(2) Complete the proof of Theorem 3.0.3 and its corollary, 3.0.4.

(3) Complete the proof of Lemma 3.0.6.

(4) Complete the proof of Theorem 3.0.7.

(5) Prove that $(A \smallsetminus B) \cup (B \smallsetminus A) = A \vartriangle B$.

(6) Prove that $(A \cap B) \cup (A \cup B)^{\mathrm{c}} = \{x : x \in A \leftrightarrow x \in B\}$.

(7) Prove the following set-theoretic identities:

(a) $\mathcal{U} = A \cup A^{\mathrm{c}}$

(b) $\varnothing = A \cap A^{\mathrm{c}}$

(c) $(A \smallsetminus B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B$

(d) $B^{\mathrm{c}} \smallsetminus A^{\mathrm{c}} = A \smallsetminus B$

(e) $A \smallsetminus (B \smallsetminus C)^{\mathrm{c}} = (A \cap B) \smallsetminus C$

3.1 Inclusions and implications

A natural generalization of Theorem 3.0.2 is:

3.1.1 Theorem. *Suppose F_0 and F_1 are n-ary propositional formulas such that*

$$F_0 \vDash F_1.$$

When $e \in \mathbb{B}$, let $\phi_e(x)$ be the $\in$-formula $F_e(x \in A_0, \ \ldots, \ x \in A_{n-1})$. Then

$$\{x \in \mathcal{U} : \phi_0(x)\} \subseteq \{x \in \mathcal{U} : \phi_1(x)\}.$$

Proof. Exercise. □

Some of the rules of inference in Lemma 2.8.1 now translate into **tautological** inclusions (inclusions that are true for all sets):

3.1.2 Lemma. *The following inclusions are tautological:*

$$A \cap B \subseteq B; \tag{3.22}$$
$$A \subseteq A \cup B; \tag{3.23}$$
$$(A \cup B) \cap A^{\mathrm{c}} \subseteq B. \tag{3.24}$$

Proof. The first two inclusions are translations (justified by Theorem 3.1.1) of the logical consequences $P \wedge Q \vDash Q$ and $P \vDash P \vee Q$; the last inclusion is a translation of the rule of Disjunctive Syllogism, in view of § 2.8, Exercise 1. □

Rules involving $\to$, such as the Hypothetical Syllogism and the Constructive Dilemma, can be expressed set-theoretically as implications:

3.1.3 Lemma. *The following implications are tautological:*

$$A \subseteq B \ \& \ B \subseteq C \implies A \subseteq C; \tag{3.25}$$
$$A \subseteq B \ \& \ C \subseteq D \implies A \cup C \subseteq B \cup D \ \& \ A \cap C \subseteq B \cap D. \tag{3.26}$$

Proof. Suppose $A \subseteq B$ and $B \subseteq C$ and $d \in A$. Then $d \in B$, so $d \in C$. Thus $A \subseteq C$.

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. □

Implication (3.25) justifies abbreviating the proposition $A \subseteq B \ \& \ B \subseteq C$ by

$$A \subseteq B \subseteq C.$$

By Identities (3.16) and (3.17) above, Implication (3.26) has the special cases:

$$A \subseteq B \ \& \ A \subseteq C \implies A \subseteq B \cap C, \tag{3.27}$$
$$A \subseteq B \ \& \ C \subseteq B \implies A \cup C \subseteq B. \tag{3.28}$$

Their converses are a part of the following:

3.1.4 Lemma. *The following are true for all sets:*

($*$) $A \subseteq B \cap C \implies A \subseteq B$;

(†) $A \cup B \subseteq C \implies A \subseteq C$;

(‡) $A \cap B = \varnothing \ \& \ A \subseteq B \implies A = \varnothing$;

(§) $A^{\mathrm{c}} \subseteq A \iff A^{\mathrm{c}} = \varnothing \iff A = \mathcal{U}$;

(¶) $A \smallsetminus B = \varnothing \iff A \subseteq B$.

Proof. Suppose $A \subseteq B \cap C$. Since $B \cap C \subseteq B$ by Lemma 3.1.2, we get $A \subseteq B$ by Lemma 3.1.3. The remaining implications are exercises. □

We are now equipped to prove some non-obvious claims:

3.1.5 Example. Suppose $A^{\mathrm{c}} \cup (B \mathbin{\triangle} C) \subseteq A \cap B^{\mathrm{c}} \cap C$. Then

$$A \cap (B \cup C) = (A \cup B) \cap C. \tag{3.29}$$

Indeed, to see this, note first

$$\begin{aligned} A^{\mathrm{c}} &\subseteq A^{\mathrm{c}} \cup (B \mathbin{\triangle} C) && \text{[by Lemma 3.1.2]} \\ &\subseteq A \cap B^{\mathrm{c}} \cap C && \text{[by assumption]} \\ &\subseteq A. && \text{[by Lemma 3.1.2]} \end{aligned}$$

Then $A^{\mathrm{c}} \subseteq A$ by Lemma 3.1.3, and therefore

$$A = \mathcal{U}$$

by Lemma 3.1.4. By the same lemmas, and Lemma 3.0.6, our assumption now gives us

$$(B \smallsetminus C) \cup (C \smallsetminus B) = B \mathbin{\triangle} C \subseteq B^{\mathrm{c}} \cap C = B \smallsetminus C;$$

therefore $C \smallsetminus B \subseteq B \smallsetminus C$, that is,

$$C \cap B^{\mathrm{c}} \subseteq B \cap C^{\mathrm{c}}.$$

Say $a \in C \cap B^c$. Then $a \in B^c$. But also, $a \in B \cap C^c$, so $a \in B$. Thus $a \in B^c \cap B = \varnothing$, which is absurd. So $C \cap B^c$ 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

$$C \cap B^c \subseteq B \cap C^c \implies C \cap B^c = \varnothing.$$

But if $C \cap B^c \subseteq B \cap C^c$, then

$$C \cap B^c \subseteq (B \cap C^c) \cap (C \cap B^c) = B \cap (C^c \cap C) \cap B^c = \varnothing.$$

Thus there is no need to look at individual elements of $C \cap B^c$, as in the proof above.

Whatever minor adjustments we make, the proof in Example 3.1.5 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 (3.1.5 continued)**.** We can analyze the given Boolean combinations of A, B, and C as follows. First note that

$$\begin{aligned} A^c &= (A^c \cap B^c) \cup (A^c \cap B) \\ &= (A^c \cap B^c \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B \cap C), \end{aligned}$$

while

$$\begin{aligned} B \mathbin{\triangle} C &= (B \cap C^c) \cup (B^c \cap C) \\ &= (A^c \cap B \cap C^c) \cup (A \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A \cap B^c \cap C). \end{aligned}$$

Therefore

$$\begin{aligned} A^c \cup (B \mathbin{\triangle} C) = (A^c \cap B^c \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A^c \cap B \cap C^c) \cup \\ \cup (A^c \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C) \end{aligned}$$

The six constituents of this union are disjoint, and the whole set $A^c \cup (B \mathbin{\triangle} C)$ is assumed to be a subset of its last constituent, $A \cap B^c \cap C$; therefore the first five constituents are empty. We aim to prove Equation (3.29). Analyzing the two members of this equation, we have

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ &= (A \cap B \cap C^c) \cup (A \cap B \cap C) \cup (A \cap B^c \cap C), \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \\ &= (A \cap B^c \cap C) \cup (A \cap B \cap C) \cup (A^c \cap B \cap C). \end{aligned}$$

Under the assumption, two constituents in each case are empty, and each member of Equation (3.29) 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) Complete the proof of Lemma 3.1.3.

(3) Complete the proof of Lemma 3.1.4.

(4) Prove the following tautological inclusions:

(a) $A \cap (A \smallsetminus B)^{c} \subseteq B$
(b) $A \smallsetminus C \subseteq (A \smallsetminus B) \cup (B \smallsetminus C)$
(c) $(A \smallsetminus B)^{c} \cap (B \smallsetminus C)^{c} \subseteq (A \smallsetminus C)^{c}$
(d) $A \smallsetminus C \subseteq (A \smallsetminus (B \smallsetminus C)^{c}) \cup (A \smallsetminus B)$
(e) $A \subseteq A \smallsetminus (B \cap B^{c})$
(f) $(A^{c} \smallsetminus A)^{c} \subseteq A$
(g) $A^{c} \subseteq A^{c} \smallsetminus A$
(h) $(A \cup B) \smallsetminus C \subseteq (A \smallsetminus C) \cup (B \smallsetminus C)$
(i) $B^{c} \subseteq (A \smallsetminus B) \cup (A^{c} \smallsetminus B)$
(j) $A \smallsetminus B \subseteq B^{c}$
(k) $B \smallsetminus A \subseteq B$

(5) Prove the following implications:

(a) $\mathcal{U} \subseteq B \implies \mathcal{U} = B$
(b) $A \subseteq B \;\&\; A \subseteq (B \smallsetminus C)^{c} \implies A \subseteq C$
(c) $A^{c} \subseteq B \cap B^{c} \implies A = \mathcal{U}$
(d) $A \subseteq B \;\&\; A \subseteq B^{c} \implies A = \varnothing$
(e) $A^{c} = \mathcal{U} \implies A \subseteq B$
(f) $A \subseteq B \implies A \cap C \subseteq B \cap C$

(6) Prove the following equivalences:

(a) $A \subseteq B \iff A^{c} \cup B = \mathcal{U}$
(b) $A \nsubseteq B \iff A \cap B^{c} \neq \varnothing$
(c) $A \subseteq B \iff B^{c} \subseteq A^{c}$
(d) $A \subseteq (B \smallsetminus C)^{c} \iff A \cap B \subseteq C$

(7) Simplify $(A^{c} \cap B^{c} \cap C^{c}) \cup (A^{c} \cap B^{c} \cap C) \cup (A^{c} \cap B \cap C^{c}) \cup (A^{c} \cap B \cap C) \cup (A \cap B \cap C^{c}) \cup (A \cap B^{c} \cap C)$ to the form $A^{c} \cup (B \mathbin{\triangle} C)$.

(8) Compose an example like 3.1.5.

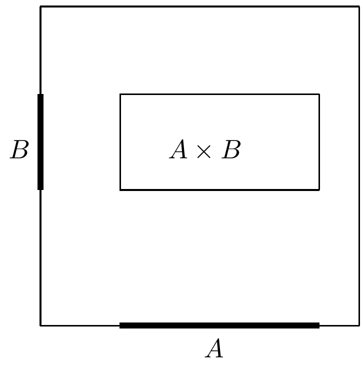


Figure 3.2: Cartesian product

3.2 Cartesian products, and relations

Suppose $\phi(x)$ is an $\in$-formula as in § 3.0, Line (3.2). We can say that this formula **defines**, in $\mathcal{U}$, the set $\{x \in \mathcal{U} : \phi(x)\}$; and this set can be called the **interpretation** of $\phi(x)$ in $\mathcal{U}$. The interpretation of $\phi(x)$ may change if $\mathcal{U}$ changes. For example, the interpretation of $x \notin A$ in $\mathcal{U}$ is $\mathcal{U} \smallsetminus A$, 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

$$x \in A \wedge y \in B$$

defines a set. It *does* define a set, which is denoted

$$A \times B$$

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

$$(a, b)$$

and called an **ordered pair**. Such objects will have the property that

$$(a, b) = (a', b') \iff a = a' \ \& \ b = b'; \tag{3.30}$$

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. A completely different way of producing sets is usually taken as an axiom:

3.2.1 Axiom (Pairing)**.** *For any two objects (possibly not distinct), there is a set whose elements are precisely those objects. That is, for all a and b, the set*

$$\{a, b\}$$

exists.

This axiom involves an existential statement. In particular, the axiom can be written formally as

$$\forall x\ \forall y\ \exists z\ \forall w\ (w \in z \leftrightarrow w = x \lor w = y).$$

When one formalizes set-theory in this way, one usually understands the variables (here x, y, z, and w) to range only over *sets.* We are not being so restrictive, for now.

If $a = b$, then the set $\{a, b\}$ is just

$$\{a\},$$

which contains nothing but a and can be called a **singleton.** (We saw this notion in § 1.2.) If $a \neq b$, then $\{a, b\}$ is an **(unordered) pair** or a **doubleton.**

3.2.2 Lemma. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \iff a = c\ \&\ b = d.$

Proof. Exercise. □

Now we can define ordered pairs so as to have the desired Property (3.30): by definition,

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Note well that we make this definition solely so that ordered pairs will have Property (3.30). It is true but unimportant[2] that $\{a\} \in (a, b)$—except that, in 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

$$A \times B = \{(x, y) \in \mathcal{U} \times \mathcal{U} : x \in A \land y \in B\}.$$

Suppose now F is a $2n$-ary propositional formula. Then we have the binary $\in$-formula

$$F(x \in A_0,\ \dots,\ x \in A_{n-1},\ y \in A_0,\ \dots,\ y \in A_{n-1}). \tag{3.31}$$

Call this $\phi(x, y)$. Its interpretation in $\mathcal{U}$ is a subset of $\mathcal{U} \times \mathcal{U}$, namely

$$\{(x, y) \in \mathcal{U} \times \mathcal{U} : \phi(x, y)\}, \tag{3.32}$$

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 $\{0, \dots, n-1\}$. As special cases, we have

$$\{(x, y) \in \mathcal{U} \times \mathcal{U} : x \in A\} = A \times \mathcal{U};$$
$$\{(x, y) \in \mathcal{U} \times \mathcal{U} : y \in B\} = \mathcal{U} \times B.$$

[2] Some discussion of this point is in [16, § 6].

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 Line (3.32), we can now replace $\phi(x, y)$ with the formula

$$\begin{multline} F((x,y) \in A_0 \times \mathcal{U},\ \dots,\ (x,y) \in A_{n-1} \times \mathcal{U}, \\ (x,y) \in \mathcal{U} \times A_0,\ \dots,\ (x,y) \in \mathcal{U} \times A_{n-1}), \quad (3.33) \end{multline}$$

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 $\cap$, $\cup$, $\vartriangle$, and $\smallsetminus$, but not over ${}^{\mathrm{c}}$, so that, for example,

$$\begin{aligned} A \times B \cap C &= (A \times B) \cap C; \\ A \times B^{\mathrm{c}} &= A \times (B^{\mathrm{c}}). \end{aligned}$$

Then we have:

3.2.3 Theorem. *The following are set-theoretic identities:*

$$\begin{aligned} A \times (B \cap C) &= A \times B \cap A \times C, & (A \cap B) \times C &= A \times C \cap B \times C, \\ A \times (B \cup C) &= A \times B \cup A \times C, & (A \cup B) \times C &= A \times C \cup B \times C, \\ \mathcal{U} \times A^{\mathrm{c}} &= (\mathcal{U} \times A)^{\mathrm{c}}, & A^{\mathrm{c}} \times \mathcal{U} &= (A \times \mathcal{U})^{\mathrm{c}}. \end{aligned}$$

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, we have

$$\begin{aligned} A \times (B \cap C) &= \{(x, y) \in \mathcal{U} \times \mathcal{U} : x \in A \wedge y \in B \cap C\} \\ &= \{(x, y) \in \mathcal{U} \times \mathcal{U} : x \in A \wedge y \in B \wedge y \in C\} \\ &= \{(x, y) \in \mathcal{U} \times \mathcal{U} : (x \in A \wedge y \in B) \wedge (x \in A \wedge y \in C)\} \\ &= \{(x, y) \in \mathcal{U} \times \mathcal{U} : (x, y) \in A \times B \wedge (x, y) \in A \times C\}, \end{aligned}$$

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:

$$\begin{gathered} x \in A \wedge y \in B \cap C, \qquad x \in A \wedge y \in B \wedge y \in C, \\ (x \in A \wedge y \in B) \wedge (x \in A \wedge y \in C), \qquad (x, y) \in A \times B \wedge (x, y) \in A \times C \end{gathered}$$

—while the last formula defines $(A \times B) \cap (A \times C)$. $\square$

The identity for $A \times B^{\mathrm{c}}$ is not so neat: see Exercise 3. Part of the last theorem can be generalized:

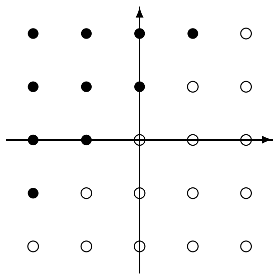


Figure 3.3: The less-than relation on $\mathbb{Z}$

3.2.4 Theorem. *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

$$x \in A \wedge y \in B \wedge x \in C \wedge y \in D,$$

which is equivalent to

$$x \in A \wedge x \in C \wedge y \in B \wedge y \in D,$$

which is the interpretation of $(A \cap C) \times (B \cap D)$. □

For $A \times B \cup C \times D$ and $(A \times B)^{\mathrm{c}}$, see Exercise 5.

We have observed that the formulas on Lines (3.31) and (3.33) 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 G is an n-ary propositional formula, then we have a binary $\in$-formula

$$G((x, y) \in R_0,\ \ldots,\ (x, y) \in R_{n-1}).$$

We have binary analogues of Theorems 3.0.2 and 3.1.1 (which I shall not write down).

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 $R = \{(x, y) \in \mathcal{U} \times \mathcal{U} : x\ R\ y\}$.

3.2.5 Example. 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:

(∗) If $R \subseteq A \times B$, then R is a relation **from** A **to** B; also, A is the **domain** of R, and B is the **co-domain**.

(†) There are n-ary relations 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

$$x_0 \in A_0 \land \ldots \land x_{n-1} \in A_{n-1};$$

its interpretation in $\mathcal{U}$ can be denoted

$$A_0 \times \cdots \times A_{n-1}.$$

This is a subset of $\underbrace{\mathcal{U} \times \cdots \times \mathcal{U}}_{n}$, which we can also denote

$$\mathcal{U}^n.$$

The elements of $\mathcal{U}^n$ are just the **(ordered)** n**-tuples**

$$(c_0, \ldots, c_{n-1}) \qquad \text{or} \qquad \vec{c}$$

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 3.2.2.

(2) Complete the proof of Theorem 3.2.3.

(3) Prove the identity $A \times B^{\mathrm{c}} = A \times \mathcal{U} \smallsetminus \mathcal{U} \times B$.

(4) Prove the identities:

  (a) $(A \vartriangle B) \times C = A \times C \vartriangle B \times C$;
  (b) $(A \smallsetminus B) \times C = A \times C \smallsetminus B \times C$.

(5) Prove the identities:

  (a) $A \times B \cup C \times D = ((A \cup C) \times (B \cup D) \smallsetminus A^{\mathrm{c}} \times D^{\mathrm{c}}) \smallsetminus C^{\mathrm{c}} \times B^{\mathrm{c}}$;
  (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:

($*$) For every a in A there is some b in B such that $(a, b) \in R$.

($\dagger$) If R contains both (a, b) and (a, c), then $b = c$.

One might abbreviate these properties as follows:

($*$) $(\forall x \in A)\ (\exists y \in B)\ x \mathrel{R} y$.

($\dagger$) $(\forall x \in A)\ (\forall y \in B)\ (\forall z \in B)\ (x \mathrel{R} y \ \&\ x \mathrel{R} z \implies y = z)$.

Alternatively, R is a function if it has the property:

($*$) For every a in A, there is a *unique* b in B such that $a \mathrel{R} b$.

Unique existence—existence of exactly one—is sometimes abbreviated by the quantifier

$$\exists!.$$

Then the last property can be abbreviated:

($*$) $(\forall x \in A)\ (\exists!\ y \in B)\ a \mathrel{R} b$.

Often a function is denoted by a letter like f; then, instead of writing $(a, b) \in f$, or $a \mathrel{f} b$, one writes

$$f(a) = b.$$

Suppose f is a function from A to B. This can be indicated by

$$f : A \longrightarrow B \qquad \text{or} \qquad A \xrightarrow{f} B.$$

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.

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

$$\mathsf{id}_A.$$

More generally, if $k < n$, then there is an n-ary operation

$$(x_0, \dots, x_{n-1}) \longmapsto x_k$$

on A. (This operation is id_A if $n = 1$ and $k = 0$.) But there are all sorts of operations besides these:

3.3.1 Examples.

(∗) In §1.2, the successor of a number n in $\mathbb{N}$ is denoted n^+ or $n+1$. This means there is a function $x \mapsto x^+$ from $\mathbb{N}$ to itself; this is a singulary operation on $\mathbb{N}$.

(†) The operations $+$ and $\cdot$ named in § 1.3 are binary operations on $\mathbb{Z}$ and can be denoted $(x, y) \mapsto x + y$ and $(x, y) \mapsto xy$ respectively.

(‡) Hence any arithmetic term t in an n-tuple $(x_0, \dots, x_n)$ of variables determines the n-ary operation $\vec{x} \mapsto t$ on $\mathbb{Z}$.

(§) 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 $f : A \to B$. Then f is:

(∗) **surjective** or **onto,** if every element of B is $f(a)$ for *at least* one a in A;

(†) **injective** or **one-to-one,** if every element of B is $f(a)$ for *at most* one a in A;

(‡) **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:

(∗) surjective, if $(\forall y \in B)\ (\exists x \in A)\ f(x) = y$;

(†) injective, if $(\forall x \in A)\ (\forall y \in A)\ (f(x) = f(y) \implies x = y)$.

3.3.2 Examples.

(∗) id_A is a bijection.

(†) 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 $\mathbb{R}$.

(‡) The tangent-function $x \mapsto \tan x$ from $\mathbb{R}$ to $\mathbb{R}$ is surjective, but not injective.

(§) The cubing function $x \mapsto x^3$ from $\mathbb{R}$ to $\mathbb{R}$ is bijective. •

Again suppose $f : A \to B$. The **range** of f is the set

$$\{y \in B : (\exists x \in A)\ f(x) = y\};$$

this is a subset of the co-domain of f, and can be denoted

$$\{f(x) : x \in A\},$$

or more simply

$$f(A).$$

Since this notation suggests—usually wrongly—that A is actually an *element* of the domain of f, I shall also use the notation

$$f[A].$$

A function is surjective if and only if its range is equal to its co-domain.

3.3.3 Examples.

(∗) The co-domain of $x \mapsto \sin x$ is usually considered to be $\mathbb{R}$, although the range of the function is the interval $[-1, 1]$.

(†) The function $x \mapsto 1 + x^2$, as a function on $\mathbb{R}$, has range $[1, \infty)$. •

Suppose also $g : B \to C$. The **composition** of f and g is

$$\{(x, z) \in A \times C : g(f(x)) = z\};$$

This can be denoted

$$g \circ f,$$

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:

3.3.4 Theorem. *Suppose $A \neq \varnothing$ and $f : A \to B$.*

(0) *The function f is injective if and only if $g \circ f = \mathsf{id}_A$ for some function g from B to A.*

(1) *The function f is surjective if and only if $f \circ g = \mathsf{id}_B$ for some function g from B to A.*

(2) *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. (0) 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 $\{(f(x), x) : x \in A\}$ 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 $B \smallsetminus f[A]$ 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.

(1) 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 (2), are left as an exercise. □

3.3.5 Theorem. *Suppose $f : A \to B$ 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

$$f^{-1}.$$

A bijection can also be called an **invertible** function.

In general, if $f : A \to B$ and $C \subseteq A$, then $f \cap (C \times B)$ is a function from C to B; this can be denoted by

$$f \upharpoonright C;$$

it is the **restriction** of f to C, and its range is $f[C]$.

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 following relations,

- prove whether it is always a function; and
- prove whether it is always *not* a function:

(a) $f \cup g$;
(b) $f \cap g$;
(c) $f \circ g^{-1}$;
(d) $f^{-1} \circ g$.

(5) Let $f : A \to B$ and $g : B \to C$.

(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 Deeper into functions

Induced functions

If $f : A \to B$ 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?

3.4.1 Axiom (Power-set)**.** *If A is a set, then the class of subsets of A is a set.*

The set of subsets of A can be denoted

$$\mathcal{P}(A);$$

it is called the **power-set** of A.

3.4.2 Examples.

(∗) $\mathcal{P}(\varnothing) = \{\varnothing\}$, that is, $\mathcal{P}(0) = 1$ in the definition of von Neumann;
(†) $\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$, that is, $\mathcal{P}(1) = 2$.
(‡) $\varnothing \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$ for all sets A.

Hence, if $f : A \to B$, then the function $X \mapsto f[X]$ has the domain $\mathcal{P}(A)$ and the co-domain $\mathcal{P}(B)$.

3.4.3 Lemma. *Suppose $f : A \to B$. 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, $x \in f[Y]$. □

3.4.4 Theorem. *Suppose $f : A \to B$. Then*

$$f[X \cup Y] = f[X] \cup f[Y], \tag{3.34}$$
$$f[X \cap Y] \subseteq f[X] \cap f[Y] \tag{3.35}$$

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 (3.28). 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 (3.34).

For (3.35), 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 (3.27). □

3.4.5 Example. The inclusion (3.35) can be strict. For example, if f is $\{(0, 0), (1, 0)\}$ and $X = \{0\}$ and $Y = \{1\}$, then $X \cap Y = \varnothing$, but $f[X] \cap f[Y] = \{0\}$. •

3.4.6 Theorem. *Suppose $f : A \to B$.*

(1) The following are equivalent:

- ($*$) *f is injective.*
- (†) *$f[X \cap Y] = f[X] \cap f[Y]$ 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:

- ($*$) *f is bijective.*
- (†) *$f[X^{\mathrm{c}}] = (f[X])^{\mathrm{c}}$ for all subsets X of A.*

Proof. Exercise. □

If $f : A \to B$, and $C \subseteq B$, then A has the subset

$$\{x \in A : f(x) \in C\},$$

which can be denoted

$$f^{-1}[C].$$

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:

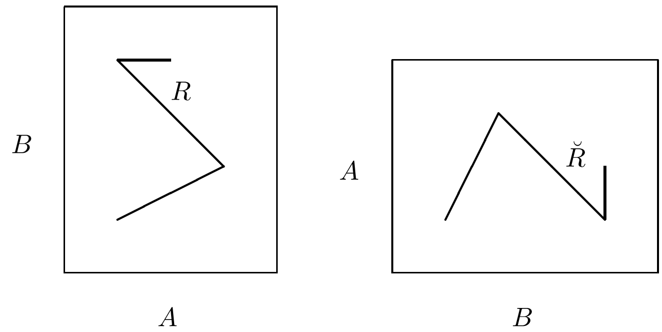


Figure 3.4: Converse of a relation

3.4.7 Theorem. *Suppose $f : A \to B$. Then*

$$f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y], \tag{3.36}$$
$$f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y], \tag{3.37}$$
$$f^{-1}[X^{\mathrm{c}}] = (f^{-1}[X])^{\mathrm{c}}, \tag{3.38}$$
$$f^{-1}[X \smallsetminus Y] = f^{-1}[X] \smallsetminus f^{-1}[Y] \tag{3.39}$$

for all subsets X and Y of A.

Proof. Exercise. Note that, by adequacy of the signature $\{\wedge, \neg\}$, the other equations follow from (3.37) and (3.38). □

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

$$S \circ R.$$

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 follow Tarski [43, § 28, p. 92] (and Suppes [41, § 3.1, Definition 7, p. 63]) and write

$$R/S$$

for $S \circ R$.

The relation R from A to B has a **converse**, namely, the relation

$$\{(y, x) \in B \times A : x\ R\ y\}$$

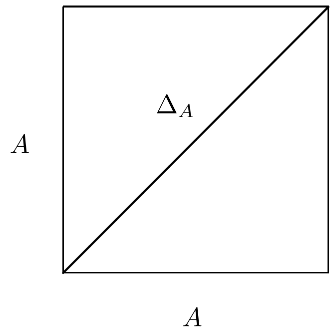


Figure 3.5: Diagonal on a set

from B to A; it can be denoted

$$\breve{R}.$$

(See Figure 3.4.) This is sometimes denoted R^{-1}, but this 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

(∗) **full**, if $\Delta_A \subseteq R/\breve{R}$;

(†) **functional**, if $\breve{R}/R \subseteq \Delta_B$.

3.4.8 Theorem. *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:

3.4.9 Theorem. *Suppose $f : A \to B$.*

(∗) *f is surjective if and only if $\Delta_B \subseteq \breve{f}/f$;*

(†) *f is injective if and only if $f/\breve{f} \subseteq \Delta_A$;*

(‡) *f is bijective if and only if $\breve{f}/f = \Delta_B$ and $f/\breve{f} = \Delta_A$.*

Proof. Exercise. □

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* $\mathcal{L}$ for *a first-order logic* consists of *constants*, *function-symbols*, and *predicates*. A *structure* in the signature $\mathcal{L}$ is a non-empty set A along with a function that takes:

($*$) each constant of $\mathcal{L}$ to an element of A;

(†) each function-symbol of $\mathcal{L}$ to an operation on A;

(‡) 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*[3] 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 standing for particular elements of A can be used as *parameters* in terms and formulas.

3.5.1 Example. The set $\mathbb{Z}$ of integers can be understood as a structure in the signature $\{+, -, \cdot, 0, 1, <\}$ (see § 1.3 (1.10)); a term in this signature (with parameters from $\mathbb{Z}$ as desired) is an *arithmetic term* as defined in § 1.3. (However, the general definition of terms given below will use Polish notation as in § 2.1.) 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 $(A, \mathfrak{I})$—which can also be referred to as $\mathfrak{A}$—where:

[3]From the Greek ἄτομοσ uncuttable, not compound, from τόμοσ a slice.

(∗) A is a non-empty set, which is called the **universe** of the structure;

(†) $\mathfrak{I}$ is a function, written also

$$s \longmapsto s^{\mathfrak{A}},$$

whose domain $\mathcal{L}$ is called the **signature** of the structure;

(‡) $s^{\mathfrak{A}}$ is either an element of A or an n-ary operation or relation on A for some positive n, for each s in $\mathcal{L}$.

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 some structure *different* from $\mathfrak{A}$ has the same universe and the same signature).

3.5.2 Examples. The following are structures:

(1) $(\mathbb{N}, {}^{+}, 0)$ (see § 1.2), or more briefly $\mathbb{N}$;

(2) the power-set structure on a non-empty set Ω, namely

$$(\mathcal{P}(\Omega), \cap, \cup, {}^{\mathrm{c}}, \varnothing, \Omega, \subseteq);$$

(3) the **truth-structure**[4]

$$(\mathbb{B}, \land, \lor, \neg, 0, 1, \vDash),$$

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 $\mathfrak{I}$ is as above in the structure $(A, \mathfrak{I})$, and s is an element of $\mathcal{L}$, then:

(∗) $s^{\mathfrak{A}}$ is called the **interpretation** in $\mathfrak{A}$ of s;

(†) s is called a **symbol** for $s^{\mathfrak{A}}$.

So s is one of the following, according to its interpretation:

(∗) a **constant**;

(†) an **n-ary function-symbol** for some positive n in ω;

(‡) 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:

(∗) I am following the old convention[5] of denoting the universe of a structure by a Roman letter, and the structure itself by the corresponding Fraktur or

[4] The name truth-structure is my invention.

[5] Used for example in [6]. Recent writers (as in [27] or [35]) use 'calligraphic' letters, not Fraktur:

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 (taken in [20]) is to use an ordinary letter like A for a structure, and then $\operatorname{dom}(A)$ for its universe. (Here dom stands for *domain*.)

Gothic letter. One might not bother to make a typographical distinction between a 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).

(†) Similarly, it is not always easy or convenient to distinguish in writing between a symbol and its interpretation.

(‡) In a structure $(A, \mathfrak{I})$, the **interpretation-function** $\mathfrak{I}$ could be considered to carry, within itself, the universe A. In any case, A and $\mathfrak{I}$ 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).

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

$$x_0, x_1, x_2, \dots$$

of **variables** (that is, of **individual variables**: variables standing for *individual* elements of a universe). Then, by definition,

(∗) all variables are terms of $\mathcal{L}$;

(†) all constants of $\mathcal{L}$ are terms of $\mathcal{L}$;

(‡) if f is an n-ary function-symbol in $\mathcal{L}$, and $(t_0, \dots, t_{n-1})$ is a list of n terms of $\mathcal{L}$, then
$$ft_0 \cdots t_{n-1}$$
is a term of $\mathcal{L}$; if f is binary, then ft_0t_1 may also be written
$$(t_0\ f\ t_1).$$
Finally, singulary function-symbols are sometimes written as superscripts on their arguments: examples include n^+ in § 1.2, Line (1.5), and A^{c} in § 1.9, Line (1.23).

The **atomic formulas** are defined similarly:

(∗) if t_0 and t_1 are terms of $\mathcal{L}$, then the equation
$$t_0 = t_1$$
is an atomic formula of $\mathcal{L}$;

(†) if R is an n-ary predicate of $\mathcal{L}$, and $(t_0, \dots, t_{n-1})$ 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
$$t_0\ R\ t_1.$$

Finally, **formulas** in general can be defined:

(∗) atomic formulas of $\mathcal{L}$ are formulas of $\mathcal{L}$;

(†) if ϕ is a formula of $\mathcal{L}$, then so is $\neg\phi$;

(‡) if ϕ and χ are formulas of $\mathcal{L}$, then $(\phi \wedge \chi)$ is a formula of $\mathcal{L}$;

(§) if ϕ is a formula of $\mathcal{L}$, and x is an individual variable, then $\exists x\ \phi$ 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, $\neg$ and $\wedge$. One will generally want to use an adequate signature for propositional logic, like $\{\neg, \wedge\}$. 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 (1.24) and (1.25) in § 1.9.

It is standard to write a formula $\neg(t_0 = t_1)$ as $t_0 \neq t_1$.

Interpretations of formulas

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:

(∗) if $k < n$, then the variable x_k is an n-ary term, and as such is interpreted in $\mathfrak{A}$ as the n-ary operation $\vec{x} \mapsto x_k$ on A (here necessarily $n > 0$);

(†) 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 (or just as $c^{\mathfrak{A}}$, if $n = 0$);

(‡) 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 (or as $f^{\mathfrak{A}}(t_0{}^{\mathfrak{A}}, \dots, t_{k-1}{}^{\mathfrak{A}})$, if $n = 0$).

3.5.3 Example. In $\mathbb{Z}$, the two 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 (1.7).) •

Interpretations of formulas take longer to define precisely, but the idea is that $\neg$, $\wedge$, 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 an $\mathcal{L}$-structure $\mathfrak{A}$ as an n-ary relation $\phi^{\mathfrak{A}}$ on A. This relation $\phi^{\mathfrak{A}}$ is the **solution-set** in $\mathfrak{A}$ of the formula ϕ. In particular:

$$(t_0 = t_1)^{\mathfrak{A}} = \{\vec{x} \in A^n : t_0{}^{\mathfrak{A}}(\vec{x}) = t_1{}^{\mathfrak{A}}(\vec{x})\}, \tag{3.40}$$

$$(Rt_0 \cdots t_{k-1})^{\mathfrak{A}} = \{\vec{x} \in A^n : (t_0{}^{\mathfrak{A}}(\vec{x}), \dots, t_{k-1}{}^{\mathfrak{A}}(\vec{x})) \in R^{\mathfrak{A}}\}. \tag{3.41}$$

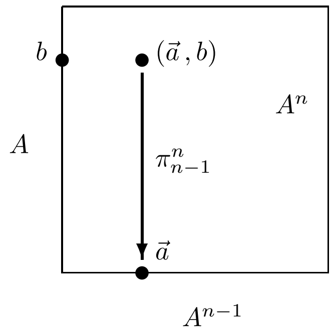


Figure 3.6: Projection

3.5.4 Example. The interpretation of $((x_0 \cdot x_0) + (x_1 \cdot x_1)) = 25$ (or just ${x_0}^2 + {x_1}^2 = 25$) in $\mathbb{R}$ is a circle of radius 5 and center $(0, 0)$; 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. •

In the sense described in § 3.2, a nullary relation is a truth-value; if $n = 0$, then Equations (3.40) and (3.41) can be written as the equivalences

$$(t_0 = t_1)^{\mathfrak{A}} = 1 \iff {t_0}^{\mathfrak{A}} = {t_1}^{\mathfrak{A}}; \tag{3.42}$$
$$(Rt_0 \cdots t_{k-1})^{\mathfrak{A}} = 1 \iff ({t_0}^{\mathfrak{A}}, \dots, {t_{k-1}}^{\mathfrak{A}}) \in R^{\mathfrak{A}}. \tag{3.43}$$

Quantifiers complicate matters, such as the defining of the arity of a formula. Assume for the moment that we *have* defined this, and that ϕ and ψ are arbitrary n-ary formulas, whose interpretations $\phi^{\mathfrak{A}}$ and $\psi^{\mathfrak{A}}$ are n-ary relations on A. Then

$$(\neg\phi)^{\mathfrak{A}} = A^n \smallsetminus \phi^{\mathfrak{A}} = (\phi^{\mathfrak{A}})^{\mathrm{c}};$$
$$(\phi \wedge \psi)^{\mathfrak{A}} = \phi^{\mathfrak{A}} \cap \psi^{\mathfrak{A}}.$$

If also $n > 0$, then $(\exists x_{n-1}\ \phi)^{\mathfrak{A}}$ is an $(n-1)$-ary relation on A, namely the set of all $(a_0, \dots, a_{n-2})$ in A^{n-1} such that $(a_0, \dots, a_{n-2}, b) \in \phi^{\mathfrak{A}}$ for *some* b in A. This means

$$(\exists x_{n-1}\ \phi)^{\mathfrak{A}} = \pi^n_{n-1}[\phi^{\mathfrak{A}}], \tag{3.44}$$

where π^n_{n-1} is the function

$$(x_0, \dots, x_{n-2}, x_{n-1}) \longmapsto (x_0, \dots, x_{n-2}) \tag{3.45}$$

from A^n to A^{n-1}; such a function can be called a **projection**. (See Figure 3.6 and § 3.7.) Note then that the formula $\exists x_{n-1}\ \phi$ should be considered as $(n-1)$-ary, not n-ary, even though it contains the variable x_{n-1}. The point is that this variable is not *free* in the formula; it is only *bound*.

The set of **free variables** in a formula is defined recursively:

(∗) $\mathrm{fv}(\phi)$ is the set of variables appearing in ϕ, if ϕ is atomic;

(†) $\mathrm{fv}(\neg\phi) = \mathrm{fv}(\phi)$;

(‡) $\mathrm{fv}(\phi \wedge \psi) = \mathrm{fv}(\phi) \cup \mathrm{fv}(\psi)$;

(§) $\mathrm{fv}(\exists x\ \phi) = \mathrm{fv}(\phi) \smallsetminus \{x\}$.

Thus quantifiers **bind** variables, making them not free.

3.5.5 Example. Suppose R and S are binary predicates. Then

$$\mathrm{fv}(\exists x\ (x\ R\ y \wedge x\ S\ z)) = \{y, z\},$$

but $\mathrm{fv}(\exists x\ x\ R\ y \wedge x\ S\ z) = \mathrm{fv}(\exists x\ x\ R\ y) \cup \mathrm{fv}(x\ S\ z) = \{y\} \cup \{x, z\} = \{x, y, z\}$. Thus parentheses make a difference. •

Suppose $\mathrm{fv}(\phi) \subseteq \{x_k : k < n\}$. Then ϕ is n**-ary,** and so is $\exists x_k\ \phi$, no matter what k is. If $k < n$, then let π^n_k be the function

$$(x_0, \dots, x_{n-1}) \longmapsto (x_0, \dots, x_{k-1}, x_{k+1}, \dots, x_{n-1})$$

from A^n to A^{n-1}; the function π^n_{n-1} defined on Line (3.45) above is a special case. By definition then,

$$(\exists x_k\ \phi)^{\mathfrak{A}} = \begin{cases} \phi^{\mathfrak{A}}, & \text{if } n \leqslant k; \\ (\pi^n_k)^{-1}[\pi^n_k[\phi^{\mathfrak{A}}]], & \text{if } k < n. \end{cases}$$

In particular, if $k < n$, then $(\exists x_k\ \phi)^{\mathfrak{A}}$ is the set of $\vec{a}$ in A^n such that

$$(a_0, \dots, a_{k-1}, b, a_{k+1}, \dots, a_{n-1}) \in \phi^{\mathfrak{A}}$$

for some b in A.

If $k = n-1$, then $\exists x_k\ \phi$ is also $(n-1)$-ary and, as such, can be interpreted in $\mathfrak{A}$ as on Line (3.44) above; now we can see this as an application of the following rule.

Suppose again that ϕ is n-ary. Then ϕ is also $(n+1)$-ary. Suppose that, as such, ϕ has the interpretation X in A. Then, as an n-ary formula, ϕ has the interpretation $\pi^{n+1}_n[X]$.

3.5.6 Example. As a binary formula, $\exists x_1\ {x_0}^2 + {x_1}^2 = 25$ is interpreted in $\mathbb{R}$ as $\{(x, y) \in \mathbb{R}^2 : -5 \leqslant x \leqslant 5\}$, which is $[-5, 5] \times \mathbb{R}$; as singulary, the formula has the interpretation $[-5, 5]$. •

Truth of sentences

By our definition, some formulas are *nullary*. Such formulas are called **sentences.** If σ is a sentence, then $\sigma^{\mathfrak{A}}$ is a truth-value, as we have noted. In particular, if $\sigma^{\mathfrak{A}} = 1$, then σ is called **true in** $\mathfrak{A}$, and we write

$$\mathfrak{A} \vDash \sigma; \tag{3.46}$$

otherwise, σ is **false in** $\mathfrak{A}$, and we write

$$\mathfrak{A} \nvDash \sigma.$$

Thus, a structure in signature $\mathcal{L}$ is a **context** in which a sentence of $\mathcal{L}$ is true or false. If σ is true in $\mathfrak{A}$, we may also say that $\mathfrak{A}$ **satisfies** σ.

For an alternative (but equivalent) method of defining truth, we need **parameters,** that is, constants standing for elements of the universe of a structure. We have been working with an arbitrary structure $\mathfrak{A}$ in an arbitrary signature $\mathcal{L}$. If to this signature we add a parameter for every element of A, then we get a signature called $\mathcal{L}(A)$. Then $\mathfrak{A}$ can be considered, in the obvious way, as a structure with this larger signature: if $b \in A$, then b is also considered as a constant (belonging to $\mathcal{L}(A)$) whose interpretation $b^{\mathfrak{A}}$ in $\mathfrak{A}$ is just b itself.

Any formula can be made into a sentence by substitution of constants for its *free* variables. Now, we have defined the set of free variables of a formula; but that does not mean that every element of that set is free where it appears in the formula; it might be *bound.* (Look again at Example 3.5.5.) If ϕ is a formula, and x is a variable, and c is a constant, then the result of replacing every *free* occurrence of x in ϕ with c is denoted

$$\phi^x_c;$$

this is defined recursively as follows:

(∗) if ϕ is atomic, then ϕ^x_c is just the result of replacing *every* occurrence of x with c;

(†) $(\neg\phi)^x_c$ is $\neg(\phi^x_c)$;

(‡) $(\phi \wedge \psi)^x_c$ is $(\phi^x_c) \wedge (\phi^x_c)$;

(§) $(\exists x\ \phi)^x_c$ is $\exists x\ \phi$ (that is, the formula does not change);

(¶) $(\exists y\ \phi)^x_c$ is $\exists y\ (\phi^x_c)$, if y is a different variable from x.

Then a particular occurrence of x in ϕ is **free** if it is replaced by c in the formation of ϕ^x_c; otherwise, the occurrence is **bound.**

If ϕ is a formula of $\mathcal{L}$, and $b \in A$, then ϕ^x_b is a formula of $\mathcal{L}(A)$. We can use Equivalences (3.42) and (3.43) to define truth of atomic sentences of $\mathcal{L}(A)$ in $\mathfrak{A}$. If σ is an arbitrary sentence of $\mathcal{L}(A)$ for which truth in $\mathfrak{A}$ is defined, then

$$\mathfrak{A} \models \neg\sigma \iff \mathfrak{A} \not\models \sigma;$$

if also τ is a sentence of $\mathcal{L}(A)$ for which truth is defined, then

$$\mathfrak{A} \models (\sigma \wedge \tau) \iff \mathfrak{A} \models \sigma\ \&\ \mathfrak{A} \models \tau.$$

Finally, if $\{x\} \subseteq \mathrm{fv}(\phi)$, and truth of ϕ^x_a is defined for all a in A, then

$$\mathfrak{A} \models \exists x\ \phi \iff \{a \in A : \mathfrak{A} \models (\phi^x_a)\} \neq \varnothing.$$

We now have a recursive definition of truth of sentences in structures. The definition can be extended in an obvious way to allow other Boolean connectives. For example,

$$\begin{aligned} \mathfrak{A} \models (\sigma \to \tau) &\iff \mathfrak{A} \not\models \sigma \vee \mathfrak{A} \models \tau \\ &\iff \mathfrak{A} \models \neg\sigma \vee \mathfrak{A} \models \tau. \end{aligned}$$

Likewise,

$$\mathfrak{A} \models \forall x\ \phi \iff \{a \in A : \mathfrak{A} \models (\phi^x_a)\} = A.$$

Using the definition of truth, we can define interpretations of formulas. First, note that we can perform more than one substitution at once. If ϕ is n-ary, and $\vec{c}$ is an n-tuple of constants, then, instead of writing

$$\phi^{x_0}_{c_0} \cdots {}^{x_{n-1}}_{c_{n-1}},$$

we can write

$$\phi[c_0, \dots, c_{n-1}]$$

or just $\phi[\vec{c}]$. Then

$$\phi^{\mathfrak{A}} = \{\vec{a} \in A^n : \mathfrak{A} \models \phi[\vec{a}]\}.$$

Strictly, the last equation is a *theorem,* namely the theorem that our two ways of defining interpretations are equivalent.

If a formula is described as

$$\phi(u_0, \dots, u_{n-1}),$$

this means that its set of free variables is a subset of $\{u_0, \dots, u_{n-1}\}$. In this case, the formula

$$\phi(c_0, \dots, c_{n-1})$$

is just $\phi(u_0, \dots, u_{n-1})^{u_0}_{c_0} \cdots {}^{u_{n-1}}_{c_{n-1}}$.

3.5.7 Example. The sentence

$$\neg(\neg\exists x_0\ \neg(Px_0 \wedge \neg Qx_0) \wedge (\neg\exists x_0\ \neg Px_0 \wedge \exists x_0\ \neg Qx_0)).$$

is true in every structure in the signature $\{P, Q\}$, where P and Q are singulary predicates. To prove this, note first that the sentence is just an official version of

$$\forall x\ (Px \to Qx) \to (\forall x\ Px \to \forall x\ Qx).$$

To prove that this is true in all structures in $\{P, Q\}$, it is enough to show that $\mathfrak{A} \models (\forall x\ Px \to \forall x\ Qx)$ whenever $\mathfrak{A} \models \forall x\ (Px \to Qx)$. So suppose

$$\mathfrak{A} \models \forall x\ (Px \to Qx). \tag{3.47}$$

It is now enough to show that, if also $\mathfrak{A} \models \forall x\ Px$, then $\mathfrak{A} \models \forall x\ Qx$. So suppose

$$\mathfrak{A} \models \forall x\ Px. \tag{3.48}$$

Let $a \in A$. Then $\mathfrak{A} \models Pa$, by (3.48). But $\mathfrak{A} \models (Pa \to Qa)$, by (3.47). Hence $\mathfrak{A} \models Qa$. Since a was arbitrary, we have $\mathfrak{A} \models \forall x\ Qx$. •

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 $\mathfrak{A}$.

The notation for truth in Line (3.46) is standard, although an alternative notation such as $\vDash_{\mathfrak{A}} \sigma$ might be preferable, in order to avoid confusion with the notion of *logical consequence,* now to be introduced by analogy with § 2.7.

Suppose Σ is a set of sentences of a first-order signature $\mathcal{L}$, and $\mathfrak{A}$ is a structure in $\mathcal{L}$. Then $\mathfrak{A}$ is a **model** of Σ if every sentence in Σ is true in $\mathcal{L}$. A sentence τ of $\mathcal{L}$ is a **logical consequence** of Σ if τ is true in every model of Σ; in this case, we can write

$$\Sigma \vDash \tau.$$

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[6] that the theory of $\mathbb{N}$ in the signature $\{^+, +, \cdot, 0, 1\}$ cannot be *recursively* axiomatized: there is no program that can generate a complete set of axioms for the theory. By Mojżesz Presburger's earlier work,[7] the theory of $\mathbb{N}$ in the signature $\{^+, +, 0, 1\}$ *is* recursively axiomatizable [27, § 3.1, pp. 81–84]: the axioms are

(∗) $\forall x\ x^+ \neq 0$ (that is, $\forall x\ \neg(x^+ = 0)$);

(†) $\forall x\ \forall y\ (x^+ = y^+ \to x = y)$;

(‡) $\forall x\ x + 0 = x$;

(§) $\forall x\ x + 1 = x^+$;

(¶) $\forall x\ x + y^+ = (x + y)^+$;

(‖) $\phi(0) \land \forall x\ (\phi(x) \to \phi(x^+)) \to \forall x\ \phi(x)$, for all formulas $\phi(x)$ 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:

(∗) To show that a particular set of sentences axiomatizes a complete theory;

(†) 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.

[6] Published in 1931; available in English in [48].

[7] 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. [15, pp. 73–74]

If T is a theory in a signature $\mathcal{L}$, then two n-ary formulas $\phi(\vec{x}\,)$ and $\psi(\vec{x}\,)$ of $\mathcal{L}$ are **T-equivalent** if

$$T \vDash \forall x_0 \ \cdots \forall x_{n-1} \ (\phi(x_0, \dots, x_{n-1}) \leftrightarrow \psi(x_0, \dots, x_{n-1})).$$

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 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.

First-order logic has a *compactness theorem,*[8] namely that if every finite subset of a set of sentences has a model, then the whole set has a model. Propositional logic has a similar theorem; second-order logic does not. This is a reason why model-theorists work mostly with first-order logic.

Exercises

(1) Letting P and Q be singulary predicates, determine, from the definition of $\vDash$, whether the following hold. (A method is shown in Example 3.5.7.)

- ($*$) $(\exists x\ Px \to \exists x\ Qx) \vDash \forall x\ (Px \to Qx)$;
- (†) $(\forall x\ Px \to \exists x\ Qx) \vDash \exists x\ (Px \to Qx)$;
- (‡) $\exists x\ (Px \to Qx) \vDash (\forall x\ Px \to \exists x\ Qx)$;
- (§) $\{\exists x\ Px,\ \exists x\ Qx\} \vDash \exists x\ (Px \wedge Qx)$;
- (¶) $\exists x\ Px \to \exists y\ Qy \vDash \forall x\ \exists y\ (Px \to Qy)$.

(2) Let $\mathcal{L} = \{R\}$, where R is a binary predicate, and let $\mathfrak{A}$ be the $\mathcal{L}$-structure $(\mathbb{Z}, \leqslant)$. Determine $\phi^{\mathfrak{A}}$ if ϕ is:

- ($*$) $\forall x_1\ (Rx_1x_0 \to Rx_0x_1)$;
- (†) $\forall x_2\ (Rx_2x_0 \vee Rx_1x_2)$.

[8]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 [19] in 1948 in *his* doctoral dissertation at Princeton. [20, p. 318]

(3) 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:

 (∗) $\{0\}$;
 (†) $\{1\}$;
 (‡) $\{a \in \mathbb{R} : 0 < a\}$;
 (§) $\{(a, b) \in \mathbb{R}^2 : a < b\}$.

(4) Show that the following sets are definable in $(\omega, +, \cdot, \leqslant, 0, 1)$:

 (∗) the set of even numbers;
 (†) the set of prime numbers.

(5) 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 $\phi^{(\mathbb{Z},<)} = R$.

3.6 Equipollence

By the definitions of the previous section, a non-empty set is a structure in the empty signature.

If a set is finite, then in principle we can count its elements. Two finite sets then have the same **size** if they have the same number of elements. What if the sets are infinite? We can't count them separately; but in theory we can count one of the sets by using the elements of the other:

Two sets are **equipotent** or **equipollent**[9] if there is a bijection from one to the other. If A and B are equipollent, we can write

$$A \approx B.$$

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

$$A \prec B; \tag{3.49}$$

in this case, B is **strictly larger** than A.

3.6.1 Examples.

(1) If $A \neq \varnothing$, then $\varnothing \prec A$.

(2) $\mathbb{Z} \approx \{x \in \mathbb{Z} : \exists y\ 2y = x\}$. •

[9] The Latin participles POTENT- and POLLENT- both mean *able*.

It is a remarkable fact,[10] to be proved below in Theorem 3.6.3, that Sentence (3.49) may hold even when both A and B are infinite.

The following gives some justification for the name power-set.

3.6.2 Theorem. *If $n \in \mathbb{N}$, and a set A has n elements, then $\mathcal{P}(A) \approx \mathbb{B}^n$.*

Proof. We can consider A as a set

$$\{a_0, \dots, a_{n-1}\}.$$

Let f be the function from $\mathcal{P}(A)$ to $\mathbb{B}^n$ given by

$$f(B) = (e_0, \dots, e_{n-1}),$$

where

$$e_i = \begin{cases} 1, & \text{if } a_i \in B; \\ 0, & \text{if } a_i \notin B. \end{cases}$$

Let g be the function from $\mathbb{B}^n$ to $\mathcal{P}(A)$ given by

$$g((e_0, \dots, e_{n-1})) = \{a_i : e_i = 1\}.$$

Then $g \circ f = \mathsf{id}_{\mathcal{P}(A)}$ and $f \circ g = \mathsf{id}_{\mathbb{B}^n}$. So f is a bijection by Theorem 3.3.4. $\square$

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[11] 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. Then for all sets A, the function

$$f \longmapsto \{x \in A : f(x) = 1\}$$

[10] Discovered by Cantor.

[11] Many writers will give this function the domain $\{1, 2, \dots, n\}$ instead of $\{0, 1, \dots, n-1\}$.

is a bijection from ${}^{A}\mathbb{B}$ to $\mathcal{P}(A)$ whose inverse is $Z \mapsto \chi_Z$, 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; the letter chi may cause confusion, but it stands for the Greek *χαρακτήρ*.) Thus

$$\mathcal{P}(A) \approx {}^{A}\mathbb{B}$$

for all sets A. The inequality

$$n < 2^n \tag{3.50}$$

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:

3.6.3 Theorem. *$A \prec \mathcal{P}(A)$ 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 $\{x \in A : x \notin f(x)\}$ 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 $\mathcal{P}(A)$. □

Suppose $A \preccurlyeq B$ and $B \preccurlyeq A$; do we then have $A \approx B$? In fact we do, by Theorem 4.8.11, but the proof is not easy.

3.7 Equivalence-relations

Let R be a binary relation on a set A. The following are some properties that R might have. Now, R *does* have these properties, for example, if R is Δ_A (as defined in § 3.4). In any case, we say that R is:

(∗) **reflexive,** if $(A, R) \vDash \forall x\; x\; R\; x$;

(†) **symmetric,** if $(A, R) \vDash \forall x\; \forall y\; (x\; R\; y \to y\; R\; x)$;

(‡) **transitive,** if $(A, R) \vDash \forall x\; \forall y\; \forall z\; (x\; R\; y \land y\; R\; z \to x\; R\; z)$.

An alternative formulation can be given in terms of the notions of § 3.4. The relation R is:

(∗) reflexive if and only if $\Delta_A \subseteq R$;

(†) symmetric if and only if $R = \breve{R}$;

(‡) transitive if and only if $R/R \subseteq R$.

A reflexive, symmetric, transitive relation is called an **equivalence-relation**.

3.7.1 Examples.

(1) Truth-equivalence (§ 2.2) is an equivalence-relation on 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 on the first-order formulas of $\mathcal{L}$.)

(2) If R is a relation from A to B, then $R/\breve{R}$ is an equivalence-relation on A.

(3) If n is an integer, then **congruence *modulo*** n is an equivalence-relation on $\mathbb{Z}$. This is the relation consisting of pairs (a, b) such that

$$a \equiv b \pmod{n}$$

that is, $n \mid a - b$.

(4) 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.)

(5) 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.)

(6) Equipollence is an equivalence-relation (on any set of sets).

(7) If $k < n$, and A is a set, then there is an equivalence-relation $\sim^n_k$ on A^n given by

$$\vec{a} \sim^n_k \vec{b} \iff \bigwedge_{\substack{j<n \\ j \neq k}} a_j = b_j,$$

that is, $\vec{a} \sim^n_k \vec{b} \iff \pi^n_k(\vec{a}\,) = \pi^n_k(\vec{b}\,)$, where π^n_k is as in § 3.5. •

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:

3.7.2 Lemma. *If an equivalence-relation on A is given, then*

$$[b] = [c] \iff [b] \cap [c] \neq \varnothing$$

for all b and c in A.

Proof. Exercise. □

The **quotient** of A by the equivalence-relation $\sim$ is the set $\{[b] : b \in A\}$, which can be denoted

$$A/{\sim};$$

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 $\pi_\sim$. Suppose also $f : A \to B$. 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?**

$$\begin{tikzcd}
A \arrow[r, "\pi_\sim"] \arrow[d, "f"'] & A/\sim \arrow[dl, "g"] \\
B &
\end{tikzcd}$$

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.

3.7.3 Theorem. *Suppose E is an equivalence-relation on A, and $f : A \to B$. The following conditions are equivalent:*

(∗) $E \subseteq f/\breve{f}$;

(†) $x \mathrel{E} y \implies f(x) = f(y)$ *for all x and y in A;*

(‡) *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 3.7.4 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.**

3.7.4 Examples. The following parallel Examples 3.7.1:

(1) If F is an n-ary propositional formula in a signature $\mathcal{L}$, then there is a function $\vec{e} \mapsto \widehat{F}(\vec{e})$ or $\widehat{F}$ from $\mathbb{B}^n$ to $\mathbb{B}$. Hence there is a function $F \mapsto \widehat{F}$ 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, $F \sim G$ if and only if $\widehat{F} = \widehat{G}$. Hence there is a well-defined injection $F/\sim \mapsto \widehat{F}$ from $\mathrm{Fm}^n(()\mathcal{L})/\sim$ to ${}^{\mathbb{B}^n}\mathbb{B}$; if $\mathcal{L}$ is adequate, then this function is also surjective.

(2) If $f : A \to B$, then $A/(f/\breve{f}) = \{\{a \in A : f(a) = b\} : b \in f(A)\}$.

(3) If $n > 0$, then the distinct elements of the quotient of $\mathbb{Z}$ by congruence *modulo* n are $[0]$, $[1]$, $[2]$, …, $[n-1]$.

(4) 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.)

(5) 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.)

(6) The equipollence-class of a set A can be called the **cardinality** of A and denoted
$$|A|.$$
Equipollent sets are sets having the same equipollence-class; such sets can also be said to have the same cardinality.

(7) 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:

(∗) if B and C are in P, and $B \cap C \neq \varnothing$, then $B = C$;

(†) every element of A is an element of some element of P.

3.7.5 Theorem. *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.

Proof. Exercise. □

Exercises

(1) Prove Lemma 3.7.2.

(2) Prove Theorem 3.7.3.

(3) Prove Theorem 3.7.5.

(4) 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 $|A/F| = 7$?

(5) Define an equivalence-relation $\sim$ on $\mathbb{Z}$ so that there is a bijection from $\mathbb{Z}/{\sim}$ to $\mathbb{N}$.

(6) 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.

(7) Suppose R is a reflexive and symmetric relation on A, but $R \nsubseteq R/R$. Can you find an equivalence-relation S on A such that $R \subseteq S$?

3.8 Orderings

Let R be a binary relation on A. The following possible properties complement those given in § 3.7. The relation R is:

(∗) **irreflexive,** if $(A, R) \vDash \forall x\ \neg(x\ R\ x)$;

(†) **anti-symmetric,** if $(A, R) \vDash \forall x\ \forall y\ (x\ R\ y \wedge y\ R\ x \rightarrow x = y)$.

Figure 3.7: The remains of the temple at Assos: an example of the Doric order of architecture. Think of the columns, *when arranged properly,* as an order in our sense. Now the columns are only partially ordered!

Again we have alternative characterizations. The relation R is:

($*$) irreflexive if and only if $R \cap \Delta_A = \varnothing$;

(†) anti-symmetric if and only if $R \cap \breve{R} \subseteq \Delta_A$.

A reflexive, anti-symmetric, transitive relation on a non-empty set is called a **partial ordering.** A set with a partial ordering is a **partially ordered set** or a **partial order.** Thus an order is a kind of structure in a signature consisting of a binary predicate. A **strict partial ordering** is an irreflexive, anti-symmetric, transitive relation on a non-empty set. Note then that a strict partial order is technically *not* a partial order (see Exercise 1). In any case, in my terminology, an *order* is a kind of *structure* (see Figure 3.7); an *ordering* is the *relation* that is part of an order. However, this terminological distinction is not of great importance.

3.8.1 Examples.

(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 3.7.4.) If we understand $\vDash$ as a binary relation, then $(\mathrm{Fm}^n(()\mathcal{L})/{\sim}, \vDash)$ is a partial order. The case $n = 2$ can be depicted as in Figure 3.8.

(4) $(\mathbb{Z}, \mid)$ is a partial order.

(5) (A, Δ_A) is a partial order.

(6) $(A, \varnothing)$ is a strict partial order.

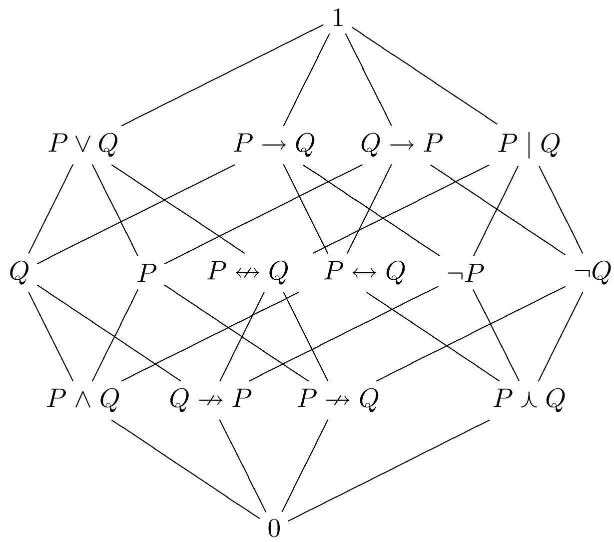


Figure 3.8: In this depiction of the set of (truth-equivalence-classes of) propositional formulas in two variables, $F \vDash G$ if an only if G can be reached from F by travelling upwards along the drawn lines. The new connective $\nrightarrow$ here has the obvious meaning.

(7) The relation $\preccurlyeq$ on sets is not a partial ordering; but we shall see in § 4.8 that it 'induces' a partial ordering of *cardinalities.* •

3.8.2 Lemma.

($*$) *If* (A, R) *is a partial ordering, then* $(A, R \smallsetminus \Delta_A)$ *is a strict partial ordering.*

(†) *If* (A, S) *is a strict partial ordering, then* $(A, S \cup \Delta_A)$ *is a partial ordering.*

Proof. Exercise. □

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 **total order** (or a **linear order**) if

$$(A, R) \vDash \forall x \; \forall y \; (x \; R \; y \vee y \; R \; x),$$

that is,

$$R \cup \breve{R} = A^2.$$

If $\leqslant$ is a total ordering, then the associated strict total ordering can be denoted by $<$, and *vice versa.*

3.8.3 Example. $(\mathbb{Z}, \leqslant)$ is a total order; $(\mathbb{Z}, <)$ is a strict total order. •

Suppose (A, R) and (B, S) are partial orders, and $f : A \to B$. Then f is **order-preserving** if

$$x \mathrel{R} y \implies f(x) \mathrel{S} f(y)$$

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

$$\mathfrak{A} \vDash \phi(a_0, \dots, a_{n-1}) \implies \mathfrak{B} \vDash \phi(f(a_0), \dots, f(a_{n-1}))$$

for all atomic formulas $\phi(x_0, \dots, x_{n-1})$ of $\mathcal{L}$ and all a_i in A, for all n in $\mathbb{N}$. Moreover, 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). 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.*

3.8.4 Examples. Here are some kinds of homomorphisms and isomorphisms:

(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) Any function from a non-empty set to another is a homomorphism of sets. Equipollence is isomorphism of sets.

(3) By Theorem 3.4.7, if $f : A \to B$, then $X \mapsto f^{-1}[X]$ is a homomorphism from $(\mathcal{P}(B), \cap, \cup, {}^{c})$ to $(\mathcal{P}(A), \cap, \cup, {}^{c})$.

(4) 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.

3.8.5 Theorem. *For every partial order (A, R), there is a set Ω and a subset B of $\mathcal{P}(\Omega)$ such that $(A, R) \cong (B, \subseteq)$. In fact, Ω can be A.*

Proof. Let f be the function $x \mapsto \{y \in A : y \mathrel{R} x\}$ from A to $\mathcal{P}(A)$. Then f is injective: Indeed, suppose c and d are elements of A. If $c \mathrel{R} d$ and $d \mathrel{R} c$, then $c = d$ since R is anti-symmetric. Suppose $c \neq d$. Then we may assume $\neg(c \mathrel{R} d)$. 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 $c \mathrel{R} d$. If $e \in f(c)$, then $e \mathrel{R} c$, so $e \mathrel{R} d$ since R is transitive; hence $e \in f(d)$. Thus $f(c) \subseteq f(d)$. This shows that f is order-preserving.

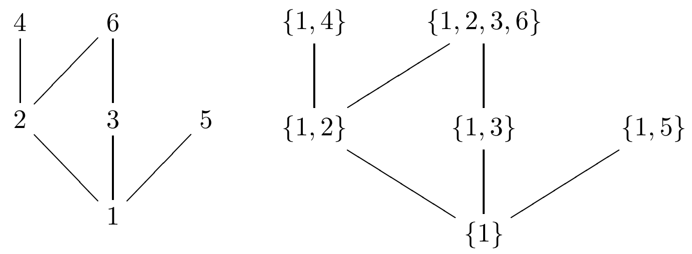


Figure 3.9: Two isomorphic partial orders:

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 $(B, \subseteq)$. □

3.8.6 Examples.

(1) The partial ordering $(\{1, 2, 3, 4, 5, 6\}, |)$ 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 3.9.

(2) A set of propositional formulas in n variables, partially ordered by logical consequence (that is, by $\vDash$), is isomorphic to a set of Boolean combinations of n suitable sets, partially ordered by inclusion. Compare Figure 3.8 to Figure 3.10. •

Exercises

(1) Show that no partial ordering is a strict partial ordering.

(2) Are there partial orders that are also equivalence-relations?

(3) Are there relations that are both symmetric and anti-symmetric?

(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 total ordering?

(5) More generally, if R is a partial order on a finite set A, is there a total 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 3.10 are distinct.

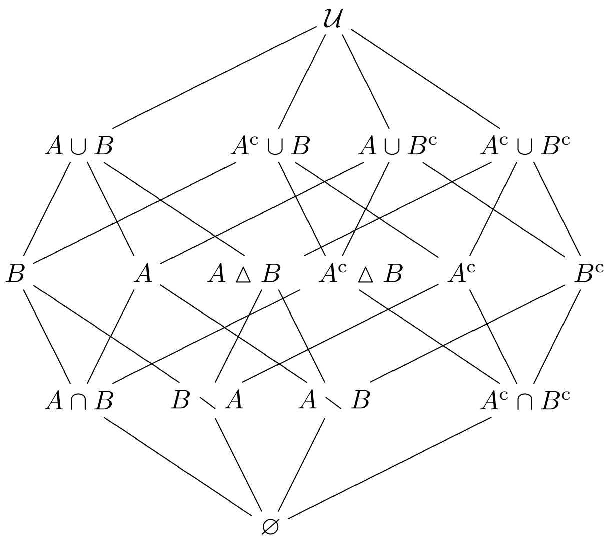


Figure 3.10: A partial order of sets. (The sets A and B here should be *independent* in the sense that all Boolean combinations here are distinct.)

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 set of sets, then the **union** of $\mathcal{S}$ is the class

$$\{x : \exists y\ (y \in \mathcal{S} \land x \in y)\};$$

this is denoted

$$\bigcup \mathcal{S}.$$

Unions in the latter sense are **infinitary,** in the sense that the set $\mathcal{S}$ may be infinite. Note that no universal set is specified in the definition of $\bigcup \mathcal{S}$. The union of a set of sets is generally considered to be a set itself:

3.9.1 Axiom (Union)**.** *Infinitary unions are sets.*

As there are infinitary unions, so there are **infinitary intersections:** If $\mathcal{S}$ is a set of sets, one of which is A, then

$$\bigcap \mathcal{S} = \{x \in A : \forall y\ (y \in \mathcal{S} \to x \in y)\}. \tag{3.51}$$

So $A \cap B$ is $\bigcap\{A, B\}$, and so forth.

3.9.2 Theorem. *The intersection of a non-empty set of sets is a set.*

Proof. By the Axiom of Separation, 1.2.3, the right member of Equation (3.51) is a set. □

The following will be useful in the next chapter, starting in § 4.1.

3.9.3 Theorem. *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 $f : A \to \mathcal{P}(B)$. Then we can write

$$\bigcap f[A] = \bigcap_{x \in A} f(x)$$

and $\bigcup f[A] = \bigcup_{x \in A} f(x)$.

3.9.4 Examples.

(1) $\mathbb{R} = \bigcup_{n \in \mathbb{N}} (-1 - n, n + 1)$;
(2) $\bigcap_{n \in \mathbb{N}} [n, \infty) = \varnothing$;
(3) $\bigcap_{n \in \mathbb{N}} [-1/(n + 1), 1/(n + 1)] = \{0\}$. •

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 $f : A \to B$, 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) $f^{-1}[\bigcap \mathcal{T}] = \bigcap \{f^{-1}[X] : X \in \mathcal{T}\}$.

Chapter 4

Numbers

4.0 The Peano axioms

In a book called *The Principles of Arithmetic, Presented by a New Method* [47], 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 *natural numbers,* rather than just the positive integers. In model-theoretic terms, Peano's axioms amount to the assertion that a certain structure is a model of the theory axiomatized by certain sentences. (However, one of these sentences is second order.) I propose to make this an assertion about the natural numbers as follows:

4.0.1 Axiom (Existence of $\mathbb{N}$)**.** *In the signature* $\{0, {}^+\}$*, there is a structure* $\mathbb{N}$ *such that:*

(∗) $\mathbb{N} \vDash \forall x\; x^+ \neq 0$*;*

(†) $\mathbb{N} \vDash \forall x\; \forall y\; (x^+ = y^+ \to x = y)$*;*

(‡) $(\mathbb{N}, A) \vDash P0 \land \forall x\; (Px \to P(x^+)) \to \forall x\; Px$*, whenever* $A \subseteq \mathbb{N}$*, and* P *is a singulary predicate.*

(In the last line, it should be understood that A is to be considered as the interpretation of P in $\mathbb{N}$.) Henceforth, $\mathbb{N}$ is simply such a structure as named in this Axiom.

I shall refer to the sentence $\forall x\; x^+ \neq 0$ as **Axiom Z,** since it says that Zero is not a successor. Then $\forall x\; \forall y\; (x^+ = y^+ \to x = y)$ is **Axiom U,** since it says

[1] For example, in [23, pp. 988 f.] or [25, § 1].

that successors are Unique when they exist. Finally, there is **Axiom I,** or the **Axiom of Induction,** a *second-order* sentence that can be written formally as

$$\forall P\ (P0 \land \forall x\ (Px \to P(x^+)) \to \forall x\ Px),$$

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 $x^+ = x + 1$.

In § 1.2, I gave an informal definition of the set ω of von-Neumann natural numbers. The definition is such that the structure $(\omega, ', \varnothing)$ satisfies the Axiom of Induction automatically. In Theorems 1.2.4 and 1.2.6, we proved that this structure satisfies Axiom Z and Axiom U. Thus we *proved* the Axiom of Existence of $\mathbb{N}$, 4.0.1—on the assumption that ω exists. Now I want to justify this assumption by means of another set-theoretic axiom:

4.0.2 Axiom (Infinity)**.** *There is a set Ω, consisting only of sets, such that $\varnothing \in \Omega$, and for all sets A, if $A \in \Omega$, then $A' \in \Omega$.*

Let Ω be so. Then Ω contains all of what we have called the von-Neumann natural numbers; but it may contain other things. We can throw out these other things, obtaining ω itself, by taking an appropriate intersection. That is, we can make the definition

$$\omega = \bigcap \{x \in \mathcal{P}(\Omega) : \varnothing \in x \land \forall y\ (y \in x \to y \cup \{y\} \in x)\}. \tag{4.1}$$

Now we can *prove* that ω has the properties claimed for it in § 1.2:

4.0.3 Theorem. *$(\omega, ', \varnothing)$ is a model of the Peano axioms.*

Proof. Let $\mathcal{S}$ be the set whose intersection is defined to be ω in Equation 4.1. Then ω is a set by Theorem 3.9.2.

- ($*$) By definition, every element of $\mathcal{S}$ contains $\varnothing$; so ω contains $\varnothing$, the proof of Theorem 1.2.4 is valid, and ω satisfies Axiom Z.
- (†) Every element of $\mathcal{S}$ also contains the set-theoretic successor of every set that it contains; so ω satisfies Axiom U, by the proof of Theorem 1.2.6.
- (‡) Finally, if A contains $\varnothing$, and contains the successor of its every element, then $A \in \mathcal{S}$, and therefore $\omega \subseteq A$ by Theorem 3.9.3; so ω satisfies Axiom I.

Thus $(\omega, ', \varnothing)$ is a structure satisfying the Peano axioms. □

We have now given a precise definition of the class ω defined informally in § 1.2.[2] We also observed in § 1.2 that, in ω, every non-zero von-Neumann natural number is a successor; this is true generally in every model $\mathbb{N}$ of the Peano axioms, by the Axiom of Induction:

[2] More precisely, we have given two definitions—one less formal, one more—of structures satisfying the Peano axioms. That only one structure can fit the definitions will be a consequence of Theorem 4.1.2.

4.0.4 Lemma. *Every non-zero natural number is a successor. Symbolically,*

$$\mathbb{N} \vDash \forall x\ (x = 0 \lor \exists y\ y^+ = x).$$

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.

4.0.5 Theorem. *The successor-operation is a bijection between* $\mathbb{N}$ *and* $\mathbb{N} \smallsetminus \{0\}$*; in particular,*

$$\mathbb{N} \approx \mathbb{N} \smallsetminus \{0\}.$$

Proof. Exercise. □

By the definition suggested by Richard Dedekind[3] in 1882, a set is **infinite** if it is equipollent with a proper subset of itself. (See also § 4.8.) Then we have:

4.0.6 Corollary. $\mathbb{N}$ *is infinite.*

Proof. Immediate from the theorem. □

4.0.7 Lemma. *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. But how? There are several possible approaches. 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.

4.1.1 Theorem (Recursion)**.** *Suppose B is a set with an element c, and $f : B \to B$. Then there is a* unique *function g from $\mathbb{N}$ to B such that $g(0) = c$ and*

$$g(n^+) = f(g(n)) \tag{4.2}$$

for all n in $\mathbb{N}$.

[3] See Dedekind's note on [9, p. 63].

Proof. Recall from § 3.3 that a function from $\mathbb{N}$ to B is literally, by definition, a subset of $\mathbb{N} \times B$. Let $\mathcal{S}$ be the set whose members are the subsets R of $\mathbb{N} \times B$ that have the following two properties:

(1) $(0, c) \in R$;

(2) $(n, t) \in R \implies (n^+, f(t)) \in R$, for all (n, t) in $\mathbb{N} \times B$.

In one line, we can write

$$\mathcal{S} = \{R \in \mathcal{P}(\mathbb{N} \times B) : 0 \; R \; c \wedge \forall (x, t) \; (x \; R \; t \to x^+ \; R \; f(t))\}.$$

So the members of $\mathcal{S}$ have the properties required of g, except perhaps the property of being a function.

The set $\mathcal{S}$ is non-empty, since $\mathbb{N} \times B$ itself is in $\mathcal{S}$. Let g be the intersection $\bigcap \mathcal{S}$. Then $g \in \mathcal{S}$ (exercise).

We shall show that g is a function with domain $\mathbb{N}$. To do this, we shall show by induction that, for all n in $\mathbb{N}$, there is a unique t in B such that $(n, t) \in g$.

For the base step of our induction, we note first that $(0, c) \in g$. To finish the base step, we shall show that, for every t in B, if $(0, t) \in g$, then $t = c$. Suppose $t \neq c$. Then neither Property (1) nor Property (2) requires $(0, t)$ to be in a given member of $\mathcal{S}$. That is, if $R \in \mathcal{S}$, then $R \smallsetminus \{(0, t)\}$ still has these two properties; so, this set is in $\mathcal{S}$. In particular, $g \smallsetminus \{(0, t)\} \in \mathcal{S}$. But g is included in every member of $\mathcal{S}$, by Theorem 3.9.3; in particular,

$$g \subseteq g \smallsetminus \{(0, t)\}.$$

Therefore $(0, t) \notin g$. By contraposition, the base step is complete.

As an inductive hypothesis, let us suppose that $n \in \mathbb{N}$ and that there is a unique t in B such that $(n, t) \in g$. Then $(n^+, f(t)) \in g$. To complete our inductive step, we shall show that, for every u in B, if $(n^+, u) \in g$, then $u = f(t)$. There are two possibilities for u:

($*$) If $(n^+, u) = (y^+, f(v))$ for some (y, v) in g, then $n^+ = y^+$, so $n = y$ by Axiom U; this means $(n, v) \in g$, so $v = t$ by inductive hypothesis, and therefore $u = f(v) = f(t)$.

(†) If $(n^+, u) \neq (y^+, f(v))$ for any (y, v) in g, then (as in the base step) $g \smallsetminus \{(n^+, u)\} \in \mathcal{S}$, so $g \subseteq g \smallsetminus \{(n^+, u)\}$, which means $(n^+, u) \notin g$.

Therefore, if $(n^+, u) \in g$, then $(n^+, u) = (y^+, f(v))$ for some (y, v) in g, in which case $u = f(t)$. Therefore $f(t)$ is unique such that $(n^+, f(t)) \in g$.

Our induction is now complete; by Axiom I, we may conclude that g is a function on $\mathbb{N}$ with the required properties (1) and (2). If h is also such a function, then $h \in \mathcal{S}$, so $g \subseteq h$, which means $g = h$ since both are functions on $\mathbb{N}$. So g is unique. □

In the statement of Theorem 4.1.1, (B, f, c) is a structure in the signature $\{{}^+, 0\}$. Also, Equation (4.2) is that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{N} \arrow[r, "+"] \arrow[d, "g"'] & \mathbb{N} \arrow[d, "g"] \\
B \arrow[r, "f"'] & B
\end{tikzcd}$$

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 (B, f, c).

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 g by specifying $g(0)$ and by specifying how $g(n^+)$ is obtained from $g(n)$.

Sections 4.2 and 4.4 will provide several important examples of recursive definitions. Such definitions are sometimes[4] 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**.

4.1.2 Theorem. *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. □

4.1.3 Corollary. *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:[5]

[4] Dedekind calls them definitions by induction in [9, Theorem 126, p. 85], which corresponds to the Recursion Theorem above.

[5] Apparently Peano himself did not recognize the distinction between proof by induction and definition by recursion; see the discussion on [25, p. x]. Burris does not acknowledge the distinction; see [5, p. 391]. Stoll [40, p. 72] uses the term 'definition by weak recursion', although he observes that the validity of such a definition does *not obviously* follow from 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.

4.1.4 Example. On $\mathbb{B}$, define a singulary operation s by $s(0) = 1$ and $s(1) = 0$. Then $(\mathbb{B}, s, 0)$ admits induction,[6] 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) If g and $\mathcal{S}$ are as in the proof of the Recursion Theorem, prove that $g \in \mathcal{S}$.

(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 The arithmetic operations

By recursion, we can define addition, multiplication and exponentiation.[7] 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:

$(*)$ $n + 0 = n$;

$(\dagger)$ $n + m^+ = (n + m)^+$.

4.2.1 Lemma. $\mathbb{N}$ *satisfies*

$(*)$ $\forall x\ 0 + x = x$,

$(\dagger)$ $\forall x\ \forall y\ y^+ + x = (y + x)^+$.

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 $\models \forall x\ 0 + x = x$.

For the second claim, as the base step of an induction, we have

$$\begin{aligned} m^+ + 0 &= m^+ && \text{[by the first claim]} \\ &= (m + 0)^+; && \text{[again by the first claim]} \end{aligned}$$

[6]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.

[7]We can also define addition and multiplication using only the Induction Axiom, not the Recursion Theorem. The method is shown, for example, in [25]. 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 can't quite prove this yet). Hence we can define a successor-operation s, namely

$$[x] \longmapsto [x + 1] : \mathbb{Z}/{\equiv} \longrightarrow \mathbb{Z}/{\equiv}.$$

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. (The result is arithmetic ***modulo*** n.) We *cannot* in general define exponentiation on $\mathbb{Z}/{\equiv}$. If we try to do this in case $n = 3$, we get $2^0 = 1$, $2^1 = 2$, $2^2 = 2 \cdot 2 = 1$, so $2^{s(2)} = 2$—but also $s(2) = 0$, so $2^{s(2)} = 2^0 = 1$.

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

$$y^+ + x = (y+x)^+ \tag{4.3}$$

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 (4.3) by induction on x.

To prove some identities below, one has to choose the right variable to work with.

4.2.2 Theorem. $\mathbb{N}$ *satisfies*

(∗) $\forall x\ x^+ = x + 1$*;*

(†) $\forall x\ \forall y\ x + y = y + x$ *[that is, + is* ***commutative****];*

(‡) $\forall x\ \forall y\ \forall z\ (x+y)+z = x+(y+z)$ *[that is, + is* ***associative****];*

(§) $\forall x\ \forall y\ \forall z\ (x+z = y+z \to x = y)$ *[that is, + admits* ***cancellation****].*

Proof. Exercise. □

The **binomial coefficients** $\binom{n}{m}$ are given by a two-stage recursion:

(∗) $\binom{0}{0} = 1$, and $\binom{0}{m^+} = 0$.

(†) $\binom{n^+}{0} = 1$, and $\binom{n^+}{m^+} = \binom{n}{m} + \binom{n}{m^+}$.

(See also Exercises 6 and 7 in § 4.5.)

The binary operation $\cdot$ of **multiplication** on $\mathbb{N}$ is given by:

(∗) $n \cdot 0 = 0$

(†) $n \cdot m^+ = n \cdot m + n$.

Multiplication is also indicated by juxtaposition, so that $n \cdot m$ is nm.

4.2.3 Lemma. $\mathbb{N}$ *satisfies*

(∗) $\forall x\ 0x = 0$*,*

(†) $\forall x\ \forall y\ y^+x = yx + x$*.*

Proof. Exercise. □

4.2.4 Theorem. $\mathbb{N}$ *satisfies*

($*$) $\forall x\ 1x = x$,

(†) $\forall x\ \forall y\ xy = yx$ *[that is, $\cdot$ is commutative]*,

(‡) $\forall x\ \forall y\ \forall z\ (x + y)z = xz + yz$ *[that is, $\cdot$* ***distributes*** *over +]*,

(§) $\forall x\ \forall y\ \forall z\ (xy)z = x(yz)$ *[that is, $\cdot$ is associative]*.

Proof. Exercise. □

Finally, exponentiation: the binary operation $(x, y) \mapsto x^y$ on $\mathbb{N}$ is given by:

($*$) $n^0 = 1$;

(†) $n^{m^+} = n^m \cdot n$.

4.2.5 Theorem. *The following are identities in* $\mathbb{N}$*:*

($*$) $x^{y+z} = x^y x^z$;

(†) $(x^y)^z = x^{yz}$;

(‡) $(xy)^z = x^z y^z$.

Proof. Exercise. □

Exercises

(1) Prove Lemma 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 The integers and the rational numbers

In Examples 3.7.1 and 3.7.4, I mentioned equivalence-relations $\sim$ on $\mathbb{N} \times \mathbb{N}$ and $\approx$ on $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$ and corresponding bijections:

($*$) $[a, b] \longmapsto a - b$ from $\mathbb{N}^2/\sim$ to $\mathbb{Z}$;

(†) $[a, b] \longmapsto a/b$ from $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})/\approx$ to $\mathbb{Q}$.

We couldn't properly prove these claims then, since we didn't have precise definitions of the structures involved. Now that we have defined $\mathbb{N}$ axiomatically, we can use the observations in § 3.7 to justify a *definition* of $\mathbb{Z}$ and $\mathbb{Q}$ in terms of $\mathbb{N}$.

4.3.1 Lemma. *On $\mathbb{N} \times \mathbb{N}$, let $\sim$ be the relation given by*

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

Then $\sim$ is an equivalence-relation. If $(a_0, b_0) \sim (a_1, b_1)$ and $(c_0, d_0) \sim (c_1, d_1)$, then

(∗) $(a_0 + c_0, b_0 + d_0) \sim (a_1 + c_1, b_1 + d_1)$;

(†) $(b_0, a_0) \sim (b_1, a_1)$;

(‡) $(a_0c_0 + b_0d_0, b_0c_0 + a_0d_0) \sim (a_1c_1 + b_1d_1, b_1c_1 + a_1d_1)$.

Proof. Exercise. For the last part, show that each member is equivalent to $(a_1c_0 + b_1d_0, b_1c_0 + a_1d_0)$. □

Letting $\sim$ be as in Lemma 4.3.1, we now define $\mathbb{Z}$ to be $\mathbb{N} \times \mathbb{N}/{\sim}$. Let the $\sim$-class of (a, b) be denoted

$$a - b.$$

By Theorem 3.7.3 and Lemma 4.3.1, we can define the operations $+$, $-$, and $\cdot$ on $\mathbb{Z}$ by the following rules, where $a, b, c, d \in \mathbb{N}$. I use superscripts on the symbols (as described in § 3.5) as a reminder of which structure is being considered:

(∗) $(a - b) +^{\mathbb{Z}} (c - d) = (a +^{\mathbb{N}} c) - (b +^{\mathbb{N}} d)$;

(†) $-^{\mathbb{Z}}(a - b) = b - a$;

(‡) $(a - b) \cdot^{\mathbb{Z}} (c - d) = (a \cdot^{\mathbb{N}} c +^{\mathbb{N}} b \cdot^{\mathbb{N}} d) - (b \cdot^{\mathbb{N}} c +^{\mathbb{N}} a \cdot^{\mathbb{N}} d)$.

Alternatively,

(∗) Addition on $\mathbb{Z}$ is $(x - y, z - w) \mapsto (x + z) - (y + w)$;

(†) additive inversion on $\mathbb{Z}$ is $x - y \mapsto y - x$;

(‡) multiplication on $\mathbb{Z}$ is $(x - y, z - w) \mapsto (xz + yw) - (yz + xw)$.

Note that, by the current precise definition, an integer like $5 - 3$ is *not* the natural number 2; it is not a natural number at all; it is the equivalence-class

$$\{(2, 0), (3, 1), (4, 2), (5, 3), \dots\},$$

which is $\{(x, y) \in \mathbb{N}^2 : x = y + 2\}$. The distinction is just a technical detail, because of the following:

4.3.2 Theorem. *Let i be the function $x \mapsto x - 0$ from $\mathbb{N}$ to $\mathbb{Z}$. Then i is injective. Also, i is a homomorphism from $(\mathbb{N}, +, \cdot)$ to $(\mathbb{Z}, +, \cdot)$, that is,*

(∗) $i(a +^{\mathbb{N}} b) = i(a) +^{\mathbb{Z}} i(b)$;

(†) $i(a \cdot^{\mathbb{N}} b) = i(a) \cdot^{\mathbb{Z}} i(b)$

for all a and b in $\mathbb{N}$. On $\mathbb{Z}$, addition and multiplication are commutative and associative, and multiplication distributes over addition. Finally,

$$a +^{\mathbb{Z}} (-^{\mathbb{Z}}a) = 0 - 0 = i(0)$$

for all a in $\mathbb{Z}$.

Proof. Exercise. □

On $\mathbb{Z}$, define the binary operation $-$ by the identity

$$x - y = x + (-y).$$

4.3.3 Lemma. *If $a, b \in \mathbb{N}$, then the integer $a - b$ is $(a - 0) -^{\mathbb{Z}} (b - 0)$.*

Proof. Exercise. □

Now we can identify the natural numbers with their images in $\mathbb{Z}$, considering the natural number n to be equal to the integer $n - 0$.

We can define the **rational numbers** similarly:

4.3.4 Lemma. *On $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, let $\approx$ be the relation given by*

$$(a, b) \approx (c, d) \iff ad = bc.$$

Then $\approx$ is an equivalence-relation. If $(a_0, b_0) \approx (a_1, b_1)$ and $(c_0, d_0) \approx (c_1, d_1)$, then

(∗) $(a_0 d_0 \pm b_0 c_0, b_0 d_0) \approx (a_1 d_1 \pm b_1 c_1, b_1 d_1)$;

(†) $(a_0 c_0, b_0 d_0) \approx (a_1 c_1, b_1 d_1)$;

(‡) $(b_0, a_0) \approx (b_1, a_1)$ *and* $(0, a_0) \approx (0, 1)$ *if* $a_0 \neq 0$.

Proof. Exercise. □

Letting $\approx$ be as in Lemma 4.3.4, we define $\mathbb{Q}$ to be $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})/{\approx}$. Let the $\approx$-class of (a, b) be denoted

$$\frac{a}{b}$$

or a/b. By Theorem 3.7.3 and Lemma 4.3.4, we can define the operations $+$, $-$, and $\cdot$ on $\mathbb{Q}$, and $x \mapsto x^{-1}$ on $\mathbb{Q} \smallsetminus \{0/1\}$, by the following rules, where $a, b, c, d \in \mathbb{Z}$:

(∗) $a/b \pm c/d = (ad \pm bc)/bd$;

(†) $(a/b)(c/d) = ac/bd$;

(‡) $(a/b)^{-1} = b/a$ if $a \neq 0$.

4.3.5 Theorem. *The function $x \mapsto x/1$ is an injective homomorphism from $(\mathbb{Z}, +, -, \cdot\,)$ to $(\mathbb{Q}, +, -, \cdot\,)$. On $\mathbb{Q}$, addition and multiplication are commutative and associative, and multiplication distributes over addition. Finally,*

$$a \cdot a^{-1} = \frac{1}{1}$$

for all a in $\mathbb{Q} \smallsetminus \{0/1\}$.

Proof. Exercise. □

Now we can identify the integers with their images in $\mathbb{Q}$, considering the integer x to be equal to the rational number $x/1$.

Exercises

(1) Prove Lemma 4.3.1.

(2) Prove Theorem 4.3.2.

(3) Prove Lemma 4.3.3.

(4) Prove Lemma 4.3.4.

(5) Prove Theorem 4.3.5.

4.4 Recursion generalized

How can we define $n!$, called **n-factorial?** Informally, we write

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

A formal recursive definition should be able to take care of the dots. We say $0! = 1$, and $(n^+)! = n^+ \cdot n!$. But for this to be a valid definition by the Recursion Theorem, we would have to express $n^+ \cdot n!$ as a function of $n!$.

In fact our definition of $n!$ is valid by the following.

4.4.1 Theorem (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*

$$G(n^+) = F(n, G(n)) \tag{4.4}$$

for all n in $\mathbb{N}$.

Proof. Let f be the function

$$(x, b) \longmapsto (x^+, F(x, b))$$

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

$$g(n^+) = f(g(n))$$

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

$$g(n^+) = f(n, G(n)) = (n^+, F(n, G(n))). \tag{4.5}$$

In particular, the first entry in the value of $g(n^+)$ is n^+. This completes our induction.

We now know that $g(n) = (n, G(n))$ for all n in $\mathbb{N}$. Hence in particular $g(n^+) = (n^+, G(n^+))$. But we also have (4.5). Therefore we have (4.4), as desired. Finally, each of g and G determines the other. Since g is unique, so is G. □

4.4.2 Example. We can define a function f on $\mathbb{N}$ by requiring $f(0) = 0$ and $f(x^+) = x$. 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.[8]

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 $\sum_{k=0}^{n} f(k)$ and the product $\prod_{k=0}^{n} f(k)$ recursively as follows:

$$(*)\quad \sum_{k=0}^{0} f(k) = f(0) \text{ and } \sum_{k=0}^{n^+} f(k) = \sum_{k=0}^{n} f(k) + f(n^+);$$

$$(\dagger)\quad \prod_{k=0}^{0} f(k) = f(0) \text{ and } \prod_{k=0}^{n^+} f(k) = \left(\prod_{k=0}^{n} f(k)\right) f(n^+).$$

See Exercise 1 below.

Exercises

(1) Show clearly that the definitions of $\sum_{k=0}^{n} f(k)$ and $\prod_{k=0}^{n} f(k)$ are justified by Theorem 4.4.1.

(2) Prove the following for all n in $\mathbb{N}$:

(a) $\sum_{k=0}^{n}(k+1) = (n^2+3n+2)/2$;
(b) $\sum_{k=0}^{n}(k+1)^2 = (2n^3+9n^2+13n+6)/6$;
(c) $\sum_{k=0}^{n} b^k = (b^{n+1}-1)/(b-1)$;
(d) $\sum_{k=0}^{n}(2k+1) = (n+1)^2$;
(e) $\prod_{k=0}^{n}((k+1)/(k+2)) = 1/(n+2)$.

4.5 The 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 $\{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leqslant y \wedge x \neq y\}$. Now we have to show that $\leqslant$ is the total ordering that we expect:

4.5.1 Lemma. $\mathbb{N} \vDash \forall x\ \forall y\ (x^+ \leqslant y^+ \to x \leqslant y)$.

Proof. Suppose $a^+ \leqslant b^+$. Then $a^+ + c = b^+$ for some c in $\mathbb{N}$, by definition of $\leqslant$. This means $(a+c)^+ = b^+$, by Lemma 4.2.1, so $a + c = b$, by Axiom U, and therefore $a \leqslant b$, again by the definition of $\leqslant$. □

4.5.2 Lemma. $\mathbb{N}$ *satisfies:*

$(*)$ $\forall x\ (x \leqslant 0 \to x = 0)$*;*

$(\dagger)$ $\forall x\ \forall y\ (x + y \leqslant x \to y = 0)$.

[8]Since f is unique, we now have a proof that Axiom U follows from the Recursion Theorem.

Proof. Suppose $a \leqslant 0$. Then $a + b = 0$ for some b in $\mathbb{N}$. Either $a = 0$, or $a = c^+$ for some c in $\mathbb{N}$, by Lemma 4.0.4. In the latter case, $(c + b)^+ = 0$, 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. □

4.5.3 Lemma. $\mathbb{N}$ *satisfies:*

(∗) $\forall x\, \forall y\, (x < y \to x^+ \leqslant y)$;

(†) $\forall x\, \forall y\, (x < y^+ \to x \leqslant y)$.

Proof. To prove the first claim, by Lemma 4.0.4, it is enough to show

$$\forall x\, (x < 0 \to x^+ \leqslant 0),$$
$$\forall x\, \forall y\, (x < y^+ \to x^+ \leqslant y^+).$$

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 $n < m^+$. Then $n + \ell = m^+$ for some ℓ; but $\ell \neq 0$, so $\ell = k^+$ for some k. Hence $n + k^+ = m^+$, that is, $n^+ + k = m^+$, so $n^+ \leqslant m^+$.

The proof of the second claim is an exercise. □

4.5.4 Theorem. *On* $\mathbb{N}$*, the relation* $\leqslant$ *is a total ordering.*

Proof. There are four properties to check:

Reflexivity: Since $n + 0 = n$, we have $n \leqslant n$ by definition.

Anti-symmetry: We can use Lemma 4.0.4. If $n \leqslant 0$ and $0 \leqslant n$, then $n \leqslant 0$, so $n = 0$ by Lemma 4.5.2. Suppose $n \leqslant m^+$ and $m^+ \leqslant n$. From the latter inequality, $n = m^+ + \ell = (m + \ell)^+$ for some ℓ. Hence $(m + \ell)^+ \leqslant m^+$ by the former inequality, so $m + \ell \leqslant m$ by Lemma 4.5.1. Hence $\ell = 0$ by Lemma 4.5.2, so $n = m^+ + 0 = m^+$.

Transitivity: If $n \leqslant m$ and $m \leqslant 0$, then $m = 0$ by Lemma 4.5.2, so $n \leqslant 0$, so $n = 0$. As an inductive hypothesis, suppose

$$\forall x\, \forall y\, (x \leqslant y \wedge y \leqslant \ell \to x \leqslant \ell).$$

Suppose also $n \leqslant m$ and $m \leqslant \ell^+$. There are two possibilities. If $m = \ell^+$, then $n \leqslant \ell^+$. Suppose $m < \ell^+$. Then $m \leqslant \ell$ by Lemma 4.5.3, so $n \leqslant \ell$ by inductive hypothesis. By definition then, $n + k = \ell$ for some k, so $n + k^+ = \ell^+$, and therefore $n \leqslant \ell^+$. This completes the induction.

Totality: We shall prove $x \leqslant y \vee y \leqslant x$ by induction on x. Since $0 + m = m$ for all m, we have $\forall y\; 0 \leqslant y$. As an inductive hypothesis, suppose

$$\forall y\, (n \leqslant y \vee y \leqslant n).$$

To complete the induction, suppose $\neg(n^+ \leqslant m)$ for some m. Then $\neg(n < m)$ by Lemma 4.5.3. By inductive hypothesis, $m \leqslant n$. Also $n \leqslant n + 1 = n^+$. By transitivity, $m \leqslant n^+$.

The proof is complete. $\square$

Various standard properties can now be proved:

4.5.5 Theorem. $\mathbb{N}$ *satisfies:*

($*$) $\forall x\ 0 \leqslant x$;

($\dagger$) $\forall x\ \forall y\ \forall z\ (x < y \leftrightarrow x + z < y + z)$;

($\ddagger$) $\forall x\ \forall y\ \forall z\ (x < y \rightarrow x \cdot z^{+} < y \cdot z^{+})$;

($\S$) $\forall x\ \forall y\ \exists z\ (x \leqslant y \leftrightarrow x + z = y)$.

Proof. Exercise. $\square$

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 (3.50).)

(4) Prove the following in $\mathbb{N}$.

($*$) $\forall x\ \forall y\ 1 + xy \leqslant (1 + x)^y$

($\dagger$) $\forall x\ (3 < x \rightarrow x^2 < 2^x)$

(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 $\dbinom{x}{y} = \dfrac{x!}{y!\,(x-y)!}$.

(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. (By **proper divisor,** I mean a divisor other than the number itself.)

4.6 The real numbers

Recall from § 4.3 that every integer is a difference $x - y$ of two natural numbers, and every rational number is a quotient u/v of two integers.

4.6.1 Lemma. *There is a well-defined subset P of $\mathbb{Z}$ consisting of those differences $a - b$ of natural numbers a and b such that $b < a$. There is a unique strict total ordering $<$ of $\mathbb{Z}$ such that*

$$x < y \iff y - x \in P$$

for all x and y in $\mathbb{Z}$. The injection $x \mapsto x - 0 : \mathbb{N} \to \mathbb{Z}$ is order-preserving.

4.6.2 Lemma. *There is a well-defined subset P of $\mathbb{Q}$ consisting of those quotients a/b of integers a and b such that $0 < ab$. There is a unique strict total ordering $<$ of $\mathbb{Q}$ such that*

$$x < y \iff y - x \in P$$

for all x and y in $\mathbb{Q}$. The injection $x \mapsto x/1 : \mathbb{Z} \to \mathbb{Q}$ is order-preserving.

A **cut** of a total order $(X, \leqslant)$ is a subset $\mathfrak{a}$ such that:

($*$) $\varnothing \subset \mathfrak{a} \subset X$;

($\dagger$) $x < y \land y \in \mathfrak{a} \implies x \in \mathfrak{a}$;

($\ddagger$) $\forall y\ (y \in \mathfrak{a} \to y \leqslant x) \implies x \notin \mathfrak{a}$.

The set $\mathbb{R}$ of **real numbers** is the set of cuts of $\mathbb{Q}$. On $\mathbb{R}$, the operations $+$ and $\cdot$ and the relation $<$ can be defined so that the expected algebraic properties are true. Details are an exercise.

4.6.3 Theorem. *The function $x \mapsto \{y \in \mathbb{Q} : y < x\} : \mathbb{Q} \to \mathbb{R}$ is an injective homomorphism from $(\mathbb{Q}, +, \cdot, <)$ to $(\mathbb{R}, +, \cdot, <)$.*

Proof. Exercise. □

If $a, b \in \mathbb{R}$, then $[a, b)$ is the set $\{x \in \mathbb{R} : a \leqslant x < b\}$.

4.6.4 Theorem. *Suppose the real number a is in $[0, 1)$. Then there is a unique function $k \mapsto a_k : \mathbb{N} \to \mathbb{B}$ such that*

$$\sum_{k=0}^{n} \frac{a_k}{2^{k+1}} \leqslant a < \sum_{k=0}^{n} \frac{a_k}{2^{k+1}} + \frac{1}{2^{n+1}}$$

for all n in $\mathbb{N}$.

Proof. Exercise. □

With notation as in the theorem, we can write

$$a = \sum_{k \in \mathbb{N}} \frac{a_k}{2^{k+1}};$$

this is a **binary expansion** of a.

4.7 Well-ordered sets

Suppose $(\Omega, \leqslant)$ is a total order. Then we can define a function $x \mapsto \operatorname{pred} x$ from Ω to $\mathcal{P}(\Omega)$ by the rule
$$\operatorname{pred} x = \{y \in \Omega : y < x\}.$$
Then $\operatorname{pred} a$ is the set of **predecessors** of a. Suppose $A \subseteq \Omega$. An element b of Ω is a **least** or **minimal element** of A if $b \in A$, but $b \leqslant c$ if $c \in A$. That is, an element b of Ω is a least element of A if and only if
$$b \in A \ \ \& \ \ A \cap \operatorname{pred} a = \varnothing.$$

4.7.1 Lemma. *Least elements are unique when they exist.*

Proof. Exercise. □

The least element—if it exists—of a subset A can be denoted
$$\min A.$$

The total order $(\Omega, \leqslant)$:

(∗) **is well-ordered** if every non-empty subset of Ω has a least element;

(†) **admits (proof by) strong induction** if $A = \Omega$ whenever A is a subset of Ω such that
$$\operatorname{pred} b \subseteq A \implies b \in A$$
for all b in Ω;

(‡) **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
$$G(c) = h(G[\operatorname{pred} c])$$
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.

4.7.2 Lemma. $\operatorname{pred}(n^+) = \operatorname{pred} n \cup \{n\}$ *for all n in $\mathbb{N}$.*

Proof. Since $n < n^+$, we have $\operatorname{pred} n \cup \{n\} \subseteq \operatorname{pred}(n^+)$. For the reverse inclusion, suppose $a \in \operatorname{pred}(n^+)$, so that $a < n^+$. Then $a \leqslant n$ by Lemma 4.5.3, so $a = n$ or $a < n$; in either case, $a \in \operatorname{pred} n \cup \{n\}$. Thus, $\operatorname{pred}(n^+) \subseteq \operatorname{pred} n \cup \{n\}$. □

4.7.3 Theorem. $(\mathbb{N}, \leqslant)$ *admits strong induction.*

Proof. Suppose A is a subset of $\mathbb{N}$ that contains n whenever it includes $\operatorname{pred} n$. By induction, we shall show that $\operatorname{pred} n \subseteq A$ for all n in $\mathbb{N}$, and then $A = \mathbb{N}$.

Since $\operatorname{pred} 0 = \varnothing$, and $\varnothing \subseteq A$, this means $0 \in A$ by assumption. As an inductive hypothesis, suppose $\operatorname{pred} n \subseteq A$. Then $n \in A$ by assumption, so $\operatorname{pred}(n^+) = \operatorname{pred} n \cup \{n\} \subseteq A$ by Lemma 4.7.2. This completes the induction. Hence, for all n, we have $n \in \operatorname{pred}(n^+) \subseteq A$, so $n \in A$. Thus $A = \mathbb{N}$. □

Example 4.7.7 will show one use of strong induction.

The totally 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

$$\forall x\ (\operatorname{pred} x \cap A = \varnothing \to x \notin A),$$

that is, $\forall x\ (\operatorname{pred} x \subseteq \Omega \smallsetminus A \to x \in \Omega \smallsetminus A)$.

4.7.4 Theorem. *The following are equivalent conditions on a total order:*

($*$) *It is well-ordered.*

(†) *It admits strong induction.*

(‡) *It admits strong recursion.*

Proof. Let $(\Omega, \leqslant)$ be a total 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.

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 $\operatorname{pred} a \subseteq \Omega \smallsetminus A$, 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

$$C = \{x \in \Omega : \exists y\ (y \in A \wedge y \leqslant x)\}.$$

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,

$$h(X) = \begin{cases} 0, & \text{if } X \in \{\varnothing, \{0\}\}; \\ 1, & \text{if } X \in \{\{1\}, \{0,1\}\}. \end{cases}$$

Then $G(a) = h(G[\operatorname{pred} a])$ 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 $\operatorname{pred} a \subseteq A$, then $a \in A$, for all a in A. Consequently, if $\operatorname{pred} a \cap (\Omega \smallsetminus A) = \varnothing$, 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 $h : \mathcal{P}(B) \to B$. Let $\mathcal{S}$ be the set of relations R from Ω to B such that

$$(a, h(f[\operatorname{pred} a])) \in R$$

whenever $f : \operatorname{pred} a \to B$ and $f \subseteq R$. Then $\mathcal{S}$ is non-empty, since it contains $\Omega \times B$ itself. Let $G = \bigcap \mathcal{S}$. Then $G \in \mathcal{S}$ (exercise). Let

$$A = \{x \in \Omega : \exists!\, y\ (x, y) \in G\}.$$

Suppose $\operatorname{pred} a \subseteq A$. Then $G \cap (\operatorname{pred} a \times B)$ is the *unique* function f from $\operatorname{pred} a$ to B such that $f \subseteq G$. Hence (exercise) $h(f[\operatorname{pred} a])$ is the *unique* b in B such that $(a, b) \in G$. Therefore $a \in A$. By strong induction, $A = \Omega$, so G is a function from Ω to B. Also,

$$G(a) = h(G[\operatorname{pred} a])$$

for all a in Ω, since $G \in \mathcal{S}$. Suppose G' is another function on Ω in $\mathcal{S}$. Let

$$D = \{x \in \Omega : G(x) = G'(x)\}.$$

If $\operatorname{pred} a \subseteq D$, then $G'(a) = h(G'[\operatorname{pred} a]) = h(G[\operatorname{pred} a]) = G(a)$, 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. □

4.7.5 Corollary. $(\mathbb{N}, \leqslant)$ *is well-ordered and admits strong recursion.*

Proof. Theorem 4.7.3. □

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 connexion between these two kinds of structures:

4.7.6 Theorem. *Suppose* $(\Omega, {}^+, 0)$ *admits induction and has a partial ordering* $\leqslant$ *such that* $a < a^+$ *for all* a *in* Ω. *Then* $\leqslant$ *is a total 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,

$$h(m)^+ = h(m^+)$$

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,

$$\forall x\ (x < n \to h(x) < h(n)) \tag{4.6}$$

for all n in $\mathbb{N}$. Sentence (4.6) is trivially true when $n = 0$. Suppose it is true when $n = m$, and now $a < m^+$. Then $a \leqslant m$. Either $a = m$ or $a < m$.

(∗) If $a = m$, then $h(a) = h(m) < h(m)^+ = h(m^+)$.

(†) If $a < m$, then by inductive hypothesis, $h(a) < h(m) < h(m^+)$.

In either case, $h(a) < h(m^+)$. Thus (4.6) is true when $n = m^+$. 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 $a^+ = h(n)^+ = h(n^+)$, 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 (4.6); hence, $m \leqslant n$. □

Thus, roughly,

$$\text{induction \& ordering} \implies \text{strong induction.} \tag{4.7}$$

It is sometimes suggested[9] that strong induction can be proved from induction alone. It cannot; there has to be an ordering around, as in the theorem. Example 4.1.4 gives a structure that admits induction, but has no ordering such that $\forall x\ x < x^+$.

Strong induction on $\mathbb{N}$ is called strong because it involves a stronger *hypothesis* than ordinary induction. To prove $\mathbb{N} \vDash \forall x\ \phi(x)$ by induction, one proves two things, as described in § 1.2:

(∗) $\mathbb{N} \vDash \phi(0)$;

(†) $\mathbb{N} \vDash \forall x\ (\phi(x) \to \phi(x^+))$.

The inductive hypothesis is here is $\phi(x)$. To make the proof by strong induction, one proves one thing:

(∗) $\mathbb{N} \vDash \forall x\ (\forall y\ (y < x \to \phi(y)) \to \phi(x))$.

Here the **strong inductive hypothesis** is $\forall y\ (y < x \to \phi(y))$. 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:

(∗) $\mathbb{N} \vDash \phi(0)$;

(†) $\mathbb{N} \vDash \forall x\ (\forall y\ (y \leqslant x \to \phi(y)) \to \phi(x^+))$.

In this formulation, the strong inductive hypothesis is $\forall y\ (y \leqslant x \to \phi(y))$, that is, $\phi(0) \wedge \phi(1) \wedge \ldots \wedge \phi(x)$; this is a stronger assumption than $\phi(x)$ alone. Sometimes this stronger assumption is just what one needs:

4.7.7 Example. 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 $n + 1$.

[9]For example, [13, § 4.4, p. 213] says that the two methods of proof are equivalent; but the proofs use hidden assumptions.

From the theorem follows a connexion between recursion and strong recursion:

4.7.8 Corollary. *Every structure* $(\Omega, {}^+, 0)$ *that admits recursion has a partial ordering* $\leqslant$ *such that* $a < a^+$ *for all* a *in* Ω. *If* $\leqslant$ *is any such ordering on* Ω, *then* $\leqslant$ *is total, 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 total ordering as defined in § 4.5, so it admits strong recursion by Corollary 4.7.5. If $\leqslant$ is just a partial ordering of the structure such that $\forall x\ x \leqslant x^+$, then the theorem applies, showing that the structure is isomorphic to $\mathbb{N}$ and so admits strong recursion. □

In short then,

$$\text{recursion} \implies \text{strong recursion.} \tag{4.8}$$

That is, logically, recursion is at least as strong as strong recursion. The converses of Implications (4.8) and (4.7) 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:

(∗) $a \neq 0$;

(†) $\forall x\ \exists y\ (x < a \to x < y < a)$.

In short, a is a limit if it is not zero and has no immediate predecessor.

4.7.9 Examples.

(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 Ω is an element a such that $\forall x\ x \leqslant a$. Suppose Ω has no greatest element. Then we can define the **successor-operation** $x \mapsto x^+$ on Ω by

$$x^+ = \min\{y \in \Omega : x < y\}.$$

In this case, the limits of Ω are just those elements not in $\{0\} \cup \{x^+ : x \in \Omega\}$, that is, the non-zero elements of Ω that are not successors.

4.7.10 Theorem. *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, $\forall x\ 0 \leqslant x < x^+$ by definition of successor; so Axiom Z is satisfied. Also, if $a < b$, then $a^+ \leqslant b < b^+$, again by definition of successor; so Axiom U is satisfied. Finally, suppose A is a proper subset of such a structure Ω, and $0 \in A$. Then $\Omega \smallsetminus A$ 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 $\forall x\ (x \in A \to x^+ \in A)$, 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 $\operatorname{pred} \ell$

satisfies the hypotheses of Theorem 4.7.10, so it admits induction and recursion; but the whole structure Ω does not (exercise).[10]

Ordinals

Theorem 4.7.6 gives us that $\subseteq$ is a total ordering of ω, and $(\omega, \subseteq)$ is well-ordered. By Lemma 1.2.5, if $n \in \omega$, then $n \subseteq \omega$. This observation gives an easy way to obtain the least element of a subset A of ω:

$$\min A = \bigcap A.$$

Moreover, on ω, the relation $\subset$ is precisely $\in$:

4.7.11 Theorem. *On ω, strict inclusion is containment.*

Proof. We have $n \in n \cup \{n\} = n'$ for all n in ω. Also, $\in$ is a strict partial ordering:

Irreflexivity: As the base of an induction, note $\varnothing \notin \varnothing$. Now suppose $m' \in n'$. Then $m' \in n \cup \{n\}$. If $m' = n$, then $m \in n$. If $m' \in n$, then $m' \subseteq n$ by Lemma 1.2.5, so $m \in n$. In either case, $m \in n$. Contrapositively, if $m \notin n$, then $m' \notin n'$. In particular, if $m \notin m$, then $m' \notin m'$. This completes the induction.

Anti-symmetry: Say $m \in n$. Then $m \subseteq n$, but $m \neq n$ by irreflexivity, so $m \subset n$. Hence $n \nsubseteq m$, so $n \notin m$.

Transitivity: If $\ell \in m$ and $m \in n$, then also $m \subset n$, so $\ell \in n$.

By Theorem 4.7.6, there is an isomorphism from $(\omega, \subset)$ to $(\omega, \in)$ that takes 0 to 0 and n' to n'; so this isomorphism is id_ω. This completes the proof. □

Now we can rewrite Examples 4.7.9 in a neater way:

4.7.12 Examples.

(1) $(\omega, \subseteq)$ has no limits.

(2) ω is a limit in $(\omega', \subseteq)$. •

A set that *includes* its every element is called **transitive;** that is, a set Ω is transitive if and only if

$$A \in B \ \& \ B \in \Omega \implies A \in \Omega.$$

A transitive set that is strictly well-ordered by containment is called an **ordinal number** or an **ordinal.** Then ω is an ordinal; so are all of its elements; so is the successor of every ordinal. The *class* of ordinals would be an ordinal itself, if it were a set; then it would contain itself, so it would strictly include itself. Therefore the class of ordinals is not a set. Still, it is well-ordered, and parts of it can be listed:

$$0, 1, 2, 3, \dots; \omega, \omega', \omega'', \dots$$

[10] Rotman [36] 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.

There is an arithmetic of ordinals, according to which we can list the ordinals as

$$0, 1, 2, 3, \dots; \omega, \omega + 1, \omega + 2, \dots; \omega \cdot 2, \dots; \omega^2, \dots; \omega^\omega; \dots$$

Thus we have a way to extend the ordinary list first, second, third,... of ordinal numbers.

Exercises

(1) Prove Lemma 4.7.1.

(2) Supply the missing details in the proof of Theorem 4.7.4.

(3) Show that there are well-ordered sets with no greatest element that do not admit induction or recursion.

(4) Find a formula $\psi(x, y)$ containing no quantifiers such that the sentence $\forall x\ \exists y\ \psi(x, y)$ is logically equivalent to $\forall x\ (\forall y\ (y < x \to \phi(y)) \to \phi(x))$.

4.8 Cardinality

Infinite sets are defined in § 4.0 as sets equipollent with proper subsets of themselves. Finite sets could be defined as sets that are not infinite; but it is more interesting and perhaps more natural to say that a set A is **finite** if

$$A \approx \operatorname{pred} n$$

for some n in $\mathbb{N}$. We may then write

$$|A| = n. \tag{4.9}$$

This is not an equation in the usual sense, since we have not given a meaning to $|A|$ by itself. In § 3.7, it was suggested that the equipollence-class of a set can be called the *cardinality* of the set; but Formula (4.9) is also read as saying that the **cardinality** of A is n. If $\operatorname{pred} n \approx \operatorname{pred} k$, then it would be nice to have $n = k$; also, finite sets should not be infinite. In fact, both of these conditions hold:

4.8.1 Theorem. *Finite sets are not infinite.*

Proof. It is enough to prove by induction that no set $\operatorname{pred} n$ is infinite. The set $\operatorname{pred} 0$ is empty, so it has no proper subsets that it can be equipollent with; hence it is not infinite. Suppose $\operatorname{pred} n$ is not infinite. Say f is an injective function from $\operatorname{pred}(n^+)$ into itself. Define g from $\operatorname{pred} n$ into itself by

$$g(x) = \begin{cases} f(x), & \text{if } f(x) \neq n; \\ f(n), & \text{if } f(x) = n. \end{cases}$$

(See Figure 4.1.) Then g is injective (exercise). Hence g is surjective, by inductive hypothesis. Therefore f is surjective (exercise). Consequently, $\operatorname{pred}(n^+)$ is not infinite. □

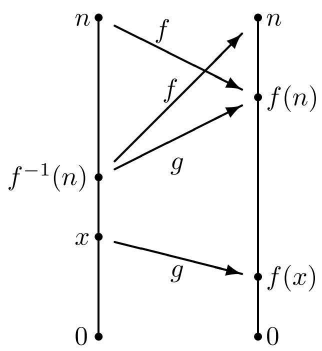


Figure 4.1: Functions used in the proof of Theorem 4.8.1.

4.8.2 Theorem. *On* $\mathbb{N}$*, the relation* $\leqslant$ *is just* $\{(x, y) : \operatorname{pred} x \preccurlyeq \operatorname{pred} y\}$.

Proof. If $m \leqslant n$, then $\operatorname{pred} m \subseteq \operatorname{pred} n$, so $\operatorname{pred} m \preccurlyeq \operatorname{pred} n$.

Suppose conversely that f is an injection from $\operatorname{pred} m$ into $\operatorname{pred} n$; we want to show $m \leqslant n$. Supposing $n \leqslant m$, it will be enough to show $m = n$. (So we shall give nearly a proof by contradiction, except that we are not quite assuming the negation of what we want to prove.)

Since $n \leqslant m$, we have $\operatorname{pred} n \subseteq \operatorname{pred} m$, so $f \restriction \operatorname{pred} n$ is an injection of $\operatorname{pred} n$ into itself. Hence $f \restriction \operatorname{pred} n$ is also a surjection, by Theorem 4.8.1, and f is also a surjection onto $\operatorname{pred} n$. In particular, for every a in $\operatorname{pred} m$, there is b in $\operatorname{pred} n$ such that $f(a) = f(b)$; but then $a = b$ since f is injective, so $a \in \operatorname{pred} n$. Thus $\operatorname{pred} m \subseteq \operatorname{pred} n$, so $\operatorname{pred} m = \operatorname{pred} n$ and $m = n$. In short, if $\operatorname{pred} m \preccurlyeq \operatorname{pred} n$, then $m \leqslant n$. □

4.8.3 Lemma. *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 $|A| = n^+$, and f is a surjection from A onto B. We may assume that A is just $\operatorname{pred}(n^+)$. Let $c = f(n)$. There are two possibilities:

(∗) If also $c = f(m)$ for some m in $\operatorname{pred} n$, then $f \restriction \operatorname{pred} n$ is still surjective on B, so B is finite by inductive hypothesis.

(†) Suppose $f[\operatorname{pred} n] \subseteq B \smallsetminus \{c\}$. Then $f \restriction \operatorname{pred} n$ is a surjection on $B \smallsetminus \{c\}$, so this set is finite, again by inductive hypothesis. In this case, there is a bijection h from $\operatorname{pred} k$ onto $B \smallsetminus \{c\}$ for some k in $\mathbb{N}$. Then $h \cup \{(k, c)\}$ is a bijection from $\operatorname{pred}(k^+)$ onto B, so B is finite.

The induction is complete. □

4.8.4 Theorem. *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 4.8.3. $\square$

4.8.5 Theorem. *If A is infinite, then $\mathbb{N} \preccurlyeq A$.*

Proof. There is a non-surjective injection $s : A \to A$. Let $c \in A \smallsetminus s[A]$. Then (A, s, c) satisfies Axiom Z and Axiom U. Now let

$$\mathcal{S} = \{C \in \mathcal{P}(A) : c \in C \wedge s[C] \subseteq C\}.$$

Then $\mathcal{S}$ contains A itself, so $\mathcal{S}$ is non-empty; so we can let $B = \bigcap \mathcal{S}$. Then $(B, s \restriction B, c)$ satisfies all three Peano axioms (exercise). By Theorem 4.1.2, there is an isomorphism from $(\mathbb{N}, {}^+, 0)$ to $(B, s \restriction B, c)$; this function is an injection from $\mathbb{N}$ to A. $\square$

By Theorem 4.8.4, if $A \preccurlyeq B$, and A is not finite, then B is not finite. Below we shall show that the non-infinite sets are precisely the infinite sets; but this will require a new set-theoretic axiom. Without this, we can still prove:

4.8.6 Theorem. *Suppose $A \preccurlyeq B$. If A is infinite, then B is infinite.*

Proof. Suppose the functions $f : A \to B$ and $g : A \to A$ are injections. Then $f \circ g \circ f^{-1}$ is an injection from $f[A]$ to B. Let $C = B \smallsetminus f[A]$, and let h be the union $(f \circ g \circ f^{-1}) \cup \mathsf{id}_C$. Then h is an injection from B to itself. If $c \notin g[A]$, then $f(c) \notin h[B]$. $\square$

By this theorem, we can show that a set A is infinite if we can find an injective function G from $\mathbb{N}$ to A. That G is injective means precisely that

$$G(n^+) \in A \smallsetminus \{G(0), \dots, G(n)\}$$

for all n in $\mathbb{N}$. Now, if A is *not* finite, then in each case the set

$$A \smallsetminus \{G(0), \dots, G(n)\}$$

is not empty by Lemma 4.8.3, so there is some hope that the function G exists. Does strong recursion (that is, Corollary 4.7.5) 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:

4.8.7 Axiom (Choice)**.** *For every set A, there is a function $f : \mathcal{P}(A) \to A$ such that $f(C) \in C$ whenever $C \neq 0$.*

A function f as in the axiom is called a **choice-function.**

4.8.8 Theorem. *Every set is either finite or infinite.*

Proof. Suppose A is not finite. Let f be a choice-function for A, and let h be the function $X \mapsto f(A \smallsetminus X)$ on $\mathcal{P}(A)$. By strong recursion, there is a function G from $\mathbb{N}$ to A such that

$$G(n) = h(G[\operatorname{pred} n]) = f(A \smallsetminus G[\operatorname{pred} n])$$

For all n in $\mathbb{N}$. Since $G[\operatorname{pred} n]$ is finite by Lemma 4.8.3, the set $A \smallsetminus G[\operatorname{pred} n]$ is non-empty, so $G(n) \notin G[\operatorname{pred} n]$. In particular, if $m < n$, then $G(m) \neq G(n)$. Thus, G is injective. □

It is a remarkable result of twentieth-century mathematics that neither the Axiom of Choice, nor its negation, is a consequence of of the other set-theoretic axioms that we have been using.

4.8.9 Theorem. *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 $\mathbb{N}$ to A. Define a function g from $A \cup \{A\}$ to A by:

$$g(x) = \begin{cases} f(0), & \text{if } x = A; \\ x, & \text{if } x \in A \smallsetminus f[\mathbb{N}]; \\ f(f^{-1}(x) + 1), & \text{if } x \in f[\mathbb{N}]. \end{cases}$$

Then g is a bijection. □

The converse of this theorem is true, by definition of infinite, *if* every set A is 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:

4.8.10 Axiom (Foundation). *Every non-empty set A has a subset that has no elements in common with A:*

$$\exists X\ (X \in A \wedge X \cap A = \varnothing)$$

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 $A \notin A$.

We haven't yet proved that $\preccurlyeq$ is a partial ordering of the cardinalities. This we now do.

4.8.11 Theorem (Schröder–Bernstein[11]). *$A \preccurlyeq B \ \&\ B \preccurlyeq A \implies A \approx B$ for all sets A and B.*

Proof. Suppose $f : A \to B$ and $g : B \to A$ are injections. We recursively define a function

$$n \longmapsto (A_n, B_n)$$

[11] This theorem is commonly attributed to Schröder and Bernstein, who, according to [40, p. 81], proved the theorem independently in the 1890s. But the theorem is attributed to Cantor in [31, § 8.3, p. 171].

from $\mathbb{N}$ to $\mathcal{P}(A) \times \mathcal{P}(B)$ by requiring $(A_0, B_0) = (A, B)$, and $(A_{n+1}, B_{n+1}) = (g[B_n], f[A_n])$. Since f and g are injective, we have

$$f[(A_n \smallsetminus A_{n+1})] = f[A_n] \smallsetminus f[A_{n+1}] = B_{n+1} \smallsetminus B_{n+2}$$

by Theorem 3.4.6, and likewise $g[(B_n \smallsetminus B_{n+1})] = A_{n+1} \smallsetminus A_{n+2}$. Also

$$f[\bigcap\{A_n : n \in \mathbb{N}\}] = \bigcap\{B_{n+1} : n \in \mathbb{N}\}$$

by Exercise 5 in § 3.9. Now define $h : A \to B$ by

$$h(x) = \begin{cases} f(x), & \text{if } x \in A_{2n} \smallsetminus A_{2n+1}; \\ g^{-1}(x), & \text{if } x \in A_{2n+1} \smallsetminus A_{2n+2}; \\ f(x), & \text{if } x \in \bigcap\{A_n : n \in \mathbb{N}\}. \end{cases}$$

Then h is a bijection. □

We now know that if A is finite, and B is infinite, then the successor $A \cup \{A\}$ is finite, and

$$A \prec A' \prec \mathbb{N} \preccurlyeq B.$$

So $\mathbb{N}$ has the least infinite cardinality, which is a least upper bound for the finite cardinalities.

It is possible, using the Axiom of Choice, to show that every set A can be well-ordered by some relation $\leqslant$, and then $(A, \leqslant)$ is isomorphic to $(\alpha, \subseteq)$ for some ordinal number α. In particular then, the class of cardinalities is well-ordered. In another adjustment of terminology, the **cardinality** of a set can also be defined now as the least ordinal that is equipollent with the set. The **cardinal numbers** are then the ordinals that are cardinalities of some set. Most infinite ordinals are *not* cardinals; but there is an order-preserving bijection

$$\alpha \longmapsto \omega_\alpha$$

from the class of ordinals to the class of infinite cardinals. In particular, ω_0 is just ω. Sometimes ω_α is written $\aleph_\alpha$; here $\aleph$ is the Hebrew letter *aleph.*

Exercises

(1) Supply the missing details in the proof of Theorem 4.8.1.

(2) Prove that the union of two finite sets is finite, and if A and B are finite, then $|A \cup B| + |A \cap B| = |A| + |B|$.

(3) Complete the proof of Theorem 4.8.5.

(4) If $A \preccurlyeq \mathbb{N}$ and $B \approx \mathbb{N}$, show that $A \times B \approx \mathbb{N}$.

(5) Show that, if $A \preccurlyeq \mathbb{N}$, and $n \in \mathbb{N}$, then $A^n \preccurlyeq N$.

(6) Show that, if $A \preccurlyeq \mathbb{N}$, then $\bigcup_{n\in\mathbb{N}} A^n \preccurlyeq N$.

4.9 Uncountable sets

If $A \preccurlyeq \mathbb{N}$, then A is called **countable.** If $A \approx \mathbb{N}$, then A is **countably infinite.** If $\mathbb{N} \prec A$, then A is called **uncountable.**

By Theorem 3.6.3, we know that uncountable sets exist, at least in principle.

The set $\mathbb{R}$ of real numbers is also called the **continuum,** and its cardinality is denoted by $\mathfrak{c}$.

4.9.1 Theorem. *The cardinality of* $\mathcal{P}(\mathbb{N})$ *is* $\mathfrak{c}$*; in particular,* $\mathbb{R}$ *is uncountable.*

Proof. By Theorem 4.6.4, each real number a in $[0, 1)$ has a uniquely determined binary expansion

$$\sum_{k\in\mathbb{N}} \frac{a_k}{2^{k+1}}.$$

Different numbers have different expansions. Also 1 can be given the expansion $\sum_{k\in\mathbb{N}} 1/2^{k+1}$. Hence we have an embedding

$$a \longmapsto \{k \in \mathbb{N} : a_k = 1\}$$

from $[0, 1]$ to $\mathcal{P}(\mathbb{N})$. This is not a surjection (why not?). However, each subset A of $\mathbb{N}$ determines a *ternary* expansion, namely

$$\sum_{i\in\mathbb{N}} \frac{e_i}{3^{i+1}},$$

where

$$e_i = \begin{cases} 1, & \text{if } i \in A; \\ 0, & \text{if } i \notin A. \end{cases}$$

This is an element of $[0, 1]$, and a different set A would determine a different element. So we have an injection from $\mathcal{P}(\mathbb{N})$ into $[0, 1]$. By the Schröder–Bernstein Theorem, we have

$$\mathcal{P}(\mathbb{N}) \approx [0, 1].$$

But also, $[0, 1] \subseteq \mathbb{R}$; while $\mathbb{R} \preccurlyeq [0, 1]$, since for example the function

$$x \longmapsto \begin{cases} \frac{2x-1}{x}, & \text{if } 0 < x \leqslant \frac{1}{2}; \\ \frac{2x-1}{1-x}, & \text{if } \frac{1}{2} < x < 1 \end{cases}$$

is a bijection from $(0, 1)$ to $\mathbb{R}$. Thus $[0, 1] \approx \mathbb{R}$. By transitivity of equipollence, we are done. □

The special symbol $\mathfrak{c}$ is used for the cardinality of $\mathbb{R}$ because the set-theoretic axioms introduced so far do *not* determine an ordinal α such that $\omega_\alpha \approx \mathbb{R}$. In particular, the **Continuum Hypothesis** is

$$\mathfrak{c} = \omega_1; \tag{4.10}$$

but this can be neither proved nor disproved from what we know. (There are models of our axioms in which (4.10) is true, and models in which it is false—on the assumption that there are models of our axioms at all, and *this* is something that we cannot prove either.)

If we only want to show $\mathbb{N} \prec \mathbb{R}$, we can use the following *diagonal* argument. Suppose f is a function from $\mathbb{N}$ into $[0,1]$. If $n \in \mathbb{N}$, write

$$f(n) = \sum_{i \in \mathbb{N}} \frac{a_{n,i}}{10^{i+1}},$$

where $a_{n,i} \in 10$. Now define

$$b_i = \begin{cases} 5, & \text{if } a_{i,i} \neq 5; \\ 0, & \text{if } a_{i,i} = 5. \end{cases}$$

Then $f(n)$ is never equal to $\sum_{i \in \mathbb{N}} b_i/10^{i+1}$; so f is not surjective.

Exercises

(1) Show that $\mathbb{R}$ is equipollent with the set of functions from $\mathbb{N}$ to $\mathbb{N}$.

(2) Show that $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$.

(3) 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.

Appendix 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:

(∗) the absence of any special notation;

(†) the definition of *proposition*;

(‡) the use of *proofs*.

The translation here is mine, from the text in [2]. Some of the wording is from the English translation by Tredennick that accompanies that text, 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*:

(∗) it is about demonstration (*ἀπόδειξισ*), and

(†) it is of demonstrative science (*ἐπιστήμη ἀποδεικτικῆ*).

Next, to define:

(∗) *proposition* (*πρότασισ*), *term* (*ὅροσ*), and *syllogism* (*συλλογισμόσ*), and

(†) which kinds [of syllogism] are *complete* (*τέλειοσ*) and *incomplete* (*ἀτελήσ*).

After these:

(‡) what it is for one thing *to be or not to be wholly* (*τὸ ἐν ὅλῳ εἶναι ἢ μὴ εἶναι*) in another, and

(§) 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*).

(∗) By **universal**, I mean applying (*ὑπάρχειν*) to all or none;

(†) by **particular**, applying to some, or not to some, or not to all;

(‡) 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

(∗) that which is predicated, and

(†) 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:

(∗) 'because of these,' I mean it follows *through* these (*διὰ ταῦτα*);

(†) 'it follows through these,' no additional term is needed for the necessity to come about.

I call a syllogism:

(∗) **complete**, if it needs nothing else, apart from what it [already] contains, for the necessary [conclusion] to be evident;

(†) **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:

(∗) for *this* **to be wholly** in *that*;

(†) 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

(∗) an application (*ὑπάρχειν*), or

(†) a *necessary* (*ἐξ ἀνάνκησ*) application, or

(‡) a *potential* (*τοῦ ἐνδέχεσθαι*) application.

Of these,

(∗) some are affirmative (*καταφατικόσ*),

(†) some negative (*ἀποφατικόσ*),

according to each application.

Again, of the affirmative and negative, some are universal, some particular, some indefinite.

A universal

(∗) *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;

(†) *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:

(∗) the *affirmative* is necessarily convertible particularly; for, if some pleasure is good, then some good will be a pleasure;

(†) 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. Translated by H. P. Cooke and H. Tredennick.

[3] Aristotle. *The Metaphysics, Books I–IX*, volume XVII of *Loeb Classical Library*. Harvard University Press, Cambridge, Massachusetts, USA, 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] Stanley N. Burris. *Logic for Mathematics and Computer Science*. Prentice Hall, Upper Saddle River, New Jersey, USA, 1998.

[6] 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.

[7] Alonzo Church. *Introduction to mathematical logic. Vol. I*. Princeton University Press, Princeton, N. J., 1956.

[8] R. G. Collingwood. *An Autobiography*. Clarendon Press, c. 1938. Reprinted 2002.

[9] Richard Dedekind. *Essays on the theory of numbers. I:Continuity and irrational numbers. II:The nature and meaning of numbers*. Dover Publications Inc., New York, 1963.

[10] René 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.

[11] 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.

[12] 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.

[13] Susanna S. Epp. *Discrete Mathematics with Applications.* PWS Publishing Company, Boston, Massachusetts, USA, 1995. 2nd edition.

[14] 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.

[15] Anita Burdman Feferman and Solomon Feferman. *Alfred Tarski: life and logic.* Cambridge University Press, Cambridge, 2004.

[16] Paul R. Halmos. *Naive set theory.* Springer-Verlag, New York, 1974. Reprint of the 1960 edition, Undergraduate Texts in Mathematics.

[17] G. H. Hardy. *A mathematician's apology.* Cambridge University Press, Cambridge, 1992. With a foreword by C. P. Snow, Reprint of the 1967 edition.

[18] Richard D. Heffner. *A Documentary History of the United States.* New American Library, New York, 3rd edition, 1976. Expanded and Revised Bicentennial Edition.

[19] Leon Henkin. The completeness of the first-order functional calculus. *J. Symbolic Logic*, 14:159–166, 1949.

[20] Wilfrid Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, 1993.

[21] Homer C House and Susan Emolyn Harman. *Descriptive English Grammar.* Prentice-Hall, Englewood Cliffs, N.J., USA, second edition, 1950. Revised by Susan Emolyn Harman. Twelfth printing, 1962.

[22] 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.

[23] Morris Kline. *Mathematical thought from ancient to modern times.* Oxford University Press, New York, 1972.

[24] Donald E. Knuth. *The TEXbook*, volume A of *Computers & Typesetting.* Addison Wesley Publishing Company, Reading, Massachusetts, USA, June 1986. Seventh printing.

[25] Edmund Landau. *Foundations of Analysis. The Arithmetic of Whole, Rational, Irrational and Complex Numbers.* Chelsea Publishing Company, New York, N.Y., 1951. Translated by F. Steinhardt.

[26] Azriel Levy. *Basic set theory.* Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1979 original [Springer, Berlin; MR0533962 (80k:04001)].

[27] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. An introduction.

[28] Murray et al., editors. *The Compact Edition of the Oxford English Dictionary*. Oxford University Press, 1973.

[29] Ali Nesin. *Önermeler Mantığı*. İstanbul Bilgi Üniversitesi Yayınları, 2001.

[30] Filiz Oktem. *Uygulamalı Latin Dili*. Sosyal Yayınlar, Eylül 1996.

[31] 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.

[32] Emil L. Post. Introduction to a general theory of elementary propositions. *Amer. J. Math.*, 43(3):163–185, July 1921.

[33] Paul Reps and Nyogen Senzaki, editors. *Zen Flesh, Zen Bones*. Shambala, Boston, 1994. A Collection of Zen and Pre-Zen Writings.

[34] Kenneth A. Ross and Charles R.B. Wright. *Discrete mathematics. 4th ed.* Upper Saddle River, NJ: Prentice Hall. xiv, 684 p. $ 113.04 , 1999.

[35] 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.

[36] Joseph J. Rotman. *A First Course in Abstract Algebra*. Prentice Hall Inc., Upper Saddle River, NJ, 2 edition, 2000.

[37] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[38] *Simon and Garfunkel*. Öykü Yayıncılık, Sultanahmet, İstanbul, 1987. Words and music of songs of Paul Simon and Art Garfunkel; Turkish translation by Devrim Eker.

[39] Michael Spivak. *Calculus. 2nd ed.* Berkeley, California: Publish Perish, Inc. XIII, 647 p. , 1980.

[40] Robert R. Stoll. *Set theory and logic*. Dover Publications Inc., New York, 1979. Corrected reprint of the 1963 edition.

[41] 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).

[42] Alfred Tarski. Truth and proof. *Scientific American*, pages 63–77, 1969.

[43] 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.

[44] 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.

[45] 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.

[46] Della Thompson, editor. *The Concise Oxford Dictionary of Current English.* Clarendon Press, Oxford, ninth edition edition, 1995.

[47] Jean van Heijenoort. *From Frege to Gödel. A source book in mathematical logic, 1879–1931.* Harvard University Press, Cambridge, Mass., 1967.

[48] Jean van Heijenoort, editor. *Frege and Gödel. Two fundamental texts in mathematical logic.* Harvard University Press, Cambridge, Mass., 1970.

[49] André Weil. *Number theory.* Birkhäuser Boston Inc., Boston, MA, 1984. An approach through history, From Hammurapi to Legendre.

[50] Howard Zinn. *A People's History of the United States: 1492–Present.* Harper Collins, New York, 2nd edition, 1995.

Symbols

Index