A minimalist introduction to mathematics

Alexandru Buium

Department of Mathematics and Statistics, University of New Mexico, Albuquerque, NM 87131, USA
E-mail address: buium@math.unm.edu
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>7</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td><strong>Part 1. Logic</strong></td>
<td>19</td>
</tr>
<tr>
<td>Chapter 1. Languages</td>
<td>21</td>
</tr>
<tr>
<td>Chapter 2. Reference</td>
<td>29</td>
</tr>
<tr>
<td>Chapter 3. Syntax</td>
<td>35</td>
</tr>
<tr>
<td>Chapter 4. Semantics</td>
<td>41</td>
</tr>
<tr>
<td>Chapter 5. Witnesses</td>
<td>45</td>
</tr>
<tr>
<td>Chapter 6. Tautologies</td>
<td>47</td>
</tr>
<tr>
<td>Chapter 7. Theories</td>
<td>53</td>
</tr>
<tr>
<td>Chapter 8. Proofs</td>
<td>59</td>
</tr>
<tr>
<td>Chapter 9. Argot</td>
<td>65</td>
</tr>
<tr>
<td>Chapter 10. Strategies</td>
<td>69</td>
</tr>
<tr>
<td>Chapter 11. Fallacies</td>
<td>73</td>
</tr>
<tr>
<td>Chapter 12. Examples</td>
<td>75</td>
</tr>
<tr>
<td><strong>Part 2. Mathematics</strong></td>
<td>83</td>
</tr>
<tr>
<td>Chapter 13. ZFC</td>
<td>85</td>
</tr>
<tr>
<td>Chapter 14. Sets</td>
<td>89</td>
</tr>
<tr>
<td>Chapter 15. Maps</td>
<td>93</td>
</tr>
<tr>
<td>Chapter 16. Relations</td>
<td>97</td>
</tr>
<tr>
<td>Chapter 17. Operations</td>
<td>103</td>
</tr>
<tr>
<td>Chapter 18. Integers</td>
<td>107</td>
</tr>
<tr>
<td>Chapter 19. Induction</td>
<td>111</td>
</tr>
</tbody>
</table>
Chapter 20. Rationals 115
Chapter 21. Combinatorics 117
Chapter 22. Sequences 119
Chapter 23. Reals 121
Chapter 24. Complexes 123
Chapter 25. Residues 125
Chapter 26. $p$-adics 129
Chapter 27. Algebra 131
Chapter 28. Geometry 135
Chapter 29. Analysis 141
Chapter 30. Metamodels 145
Chapter 31. Categories 149

Part 3. Mathematical logic 153
Chapter 32. Models 155
Chapter 33. Incompleteness 159
Bibliography 163
Preface

This is a one semester undergraduate introduction to pure (i.e. deductive) mathematics. A special emphasis will be put on the following question: *How much of pure mathematics depends on intuition?* If intuition is viewed as that which humans have and “machines” don’t then the above question becomes: *How much of pure mathematics can be “understood” by a “machine”?* And if intuition is viewed as the only possible source of error/uncertainty built into mathematical knowledge then the above questions translate into *How certain is the knowledge provided by pure mathematics?* Historically these are basic questions not only from a philosophical but also from a practical point of view, especially in relation to the problem of “automation of thinking”. Indeed questions like these have been asked repeatedly long before the advent of the computer age, most notably by Leibniz, Boole, Hilbert, Gödel, Turing. And work on these questions played a crucial role in the advent of the computers themselves. On the other hand there is only one scientific way to answer the above question on intuition and that is by direct experiment: one needs to minimize the amount of intuition built into pure mathematics and see what happens. This experiment, performed at an undergraduate level, is what this course is about. And the introduction to mathematics that follows is minimalist in precisely the above sense. A minimalist introduction is not the simplest possible introduction. The simplest introduction to a subject is that which is most liberal in the choice of allowed background and tools. On the contrary, a minimalist introduction is one that is most restrictive in terms of background and tools available.

It should be clear by now that this course drastically differs from most textbooks introducing pure mathematics. Indeed most such textbooks are oriented towards helping students achieve a smooth transition from the mathematics of calculation to the mathematics of concepts and proofs. Such a transition is best achieved by maximizing the role of intuition; on the contrary, as already mentioned, we will work here at minimizing this role. Our first move will be to minimize the amount of concepts we are ready to accept. So, unlike in most textbooks, we will begin by asking the students to first “forget” all the mathematics they ever knew. The student will have to act as if he/she does not know what the symbols 1, 2, 3,... stand for or what the words implies, contradiction, line, plane, etc. refer to; then the course will introduce each of these symbols/words in a non-circular manner and build mathematics from scratch. The building is being done through proofs. Now most textbooks introduce proofs semantically (essentially model theoretically) using the intuition of “real life ontology” or, alternatively, the intuition of “set theoretic ontology”. In the case of the latter, for instance, the mathematical objects are understood to “actually exist out there” as “eternal objects” organized into “actually infinite aggregates”, creating a sort of “maximal ontology”. None of this
intuition of the “out there” or of “actual infinity” is available to a machine. So in this course we will adopt instead a “minimal ontology” according to which the only things “admitted into existence” will be symbols written, say, on paper: everywhere in our proofs semantics will be replaced by syntax! A direct consequence of this will be that the concepts of truth and falsehood will be banned from all of our discussion of mathematics. It will not make sense, in this course, to say that sentences about integers, for instance, are true or false: the only thing that we will allow ourselves to say about such sentences will be that they are either provable, or disprovable, or neither. The set of integers itself will not be a collection of entities called integers but, rather, a mere symbol, $\mathbb{Z}$, which is a “witness” (in a precise syntactic sense) for a certain theorem affirming the existence of an ordered ring with a certain property.

Once mathematics has been reconstructed on a syntactic basis we will be able to revisit, at this new level, the ideas of semantics, model theory, and truth; this will be done at the very end of the course in the form of a formalism “raised to the second power”.

To compensate for the radical formalism which we chose to adopt the text will be kept quite short and will be interspersed with numerous remarks and exercises. The remarks will address various philosophical and historical issues hopefully making the exposition more pleasant; on the other hand the exercises are an integral part of the presentation and are often quite challenging.

Alexandru Buium
Albuquerque, 2013
Introduction

This Introduction offers a general discussion of the problematic and contents of the course. This discussion is not logically necessary for the understanding of the rest of the course and therefore may be skipped.

1. Mathematics versus logic. Mathematics is a chapter of logic. Logic organizes language into systems called theories. Then mathematics can be viewed as one among many theories; as a theory mathematics is viewed today as coinciding with set theory. Its main objects are certain special types of set theoretic constructions such as numbers, figures, and limits, leading to algebra, geometry, and analysis respectively. This viewpoint on mathematics emerged from work of Cantor [2], Russell [6], and Hilbert [5] at the turn of the 20th century; it evolved from a logicist to a formalist approach; this evolution roughly corresponds to the gradual elimination of semantics from set theory (see below). The viewpoint that mathematics is, essentially, set theory was adopted by Bourbaki [1] who, in the middle of the 20th century, provided such a presentation of mathematics in a series of now 9 classical monographs; in spite of various critical reactions to this project, today’s (pure) mathematics is, essentially, Bourbaki mathematics.

Logic is then a prerequisite for mathematics and must be distinguished from the subject called “mathematical logic” which, in its turn, is a chapter of mathematics itself. Mathematical logic models (mirrors) logic within mathematics. This viewpoint was initiated by Hilbert who was one of champions of formalism. Hilbert’s program (proposed in 1920) was to prove, within mathematics, that mathematics does not lead to contradictions (it is consistent) and can prove or disprove any of its statements (it is complete). This program received a serious blow from Gödel (in the 1930s) who proved in particular two mathematical theorems whose translations into English are as follows: 1) consistency of mathematics cannot be proved within mathematics; and 2) if mathematics is consistent then it is incomplete. On the other hand work by many people, including Gödel, showed that, in spite of the failure of Hilbert’s original program, the formalist approach can be successfully pursued provided goals less ambitious than Hilbert’s are being put forward. Our approach in this course will be along the lines of a (rather radical) formalism.

Note that mathematical logic has logic as a prerequisite: in order to even talk about mathematical logic one needs mathematics (i.e. set theory) which in its turn grounded in logic. If we use the symbol \( \subset \) to indicate containment then schematically one can represent the above discussion as follows:

\[
\{ \text{mathematical logic} \} \subset \{ \text{mathematics} \} \subset \{ \text{logic} \}
\]

2. Sets and ontological assumptions. Ontology is about the question “What exists?”; or rather about deciding what should be declared as “existing”.

9
According to Cantor (but NOT according to this course) what exists in mathematics are the Cantor sets. According to Cantor’s original “definition” [2], a Cantor set is a “collection into a whole \( M \) of definite and separate objects \( m \) of our intuition or our thought”. Cantor allowed his sets to reach arbitrary levels of “infinity” (way beyond “countable”); this has been seen by many as assuming a rather extravagant (in some sense “maximal”) ontology. Indeed, in Cantor’s theory all individual objects and relations among them and relations among relations, etc., exist. One admits into existence all things such as: the Sun, the Moon, the movement of planets in space, space itself, the man Napoleon, electrons, feelings, Hamlet’s doubts, unicorns, revolving around, being the father of, being an emperor, the word “Napoleon”, the words “revolves around”, etc. Note that the above list comprises things belonging to both the “physical world” and the “imaginary worlds”.

On the contrary the ontology we will assume in this course will be “minimal”; simplifying a little bit what we assume as existing in the list above are only: the word “Napoleon”, the words “revolves around”, etc. (and not the man Napoleon, the revolving around, etc.) More precisely in our ontology the only things admitted into existence are symbols and their combinations i.e. collections of symbols, strings of symbols, collections of strings of symbols, and strings of strings of symbols; any of the above will be referred to as a text. Collections are non-ordered while strings are ordered. Symbols can be signs written on a piece of paper, spoken words, pictures, etc.; they are always in “finite number” but their “number” can always be increased if necessary; we will refer to this property of texts as “being (at most) metacountable”.

This course will be populated with texts. For instance in our discussion of logic we will introduce languages (which are collections of symbols), sentences (which are strings of symbols), theories (which are collections of sentences), proofs (which are strings of sentences), etc. In particular languages, sentences, theories, proofs are all texts. In our discussion of mathematics, mathematics will be, by definition, a certain theory called set theory; so mathematics will be a text. Sets will be, by definition, certain symbols; so sets themselves will be texts. Finally in our discussion of mathematical logic we will introduce formalized set theory; the latter itself will a be a set.

In our mention of the physical world above the physical world was understood as “phenomenal” rather than “noumenal”. Indeed the “physical world” is assumed here to have two aspects: one aspect is that of “world in itself” or the “noumenal” world (in Kant’s terminology); the other aspect is that of “phenomenal world” or the “world of phenomena” or the “world as it appears to us”. The “world in itself” is, in principle, an unbroken whole where there are no objects or actions, no nouns, no verbs, no space, no time, no causality; as a consequence the “world in itself” cannot be thought of and will be ignored in what follows. The phenomenal world is the physical world cut out into fragments by the cognitive apparatus of the subject; this apparatus also establishes correspondences between these fragments and symbols. The symbols are part of the “physical world” as a “phenomenal world” and everything except them in the phenomenal world will be ignored. As an example the physical “man Napoleon” is acknowledged to exist as a fragment of the physical world “cut out” from the whole by the (unconscious) cognitive apparatus of the subject. We shall ignore (forget about) the “man Napoleon” as a fragment...
of the physical world. On the other hand the subject establishes a correspondence between this fragment and a symbol, the “word Napoleon”; this symbol will be an object that we will retain and operate with.

Such an ontology is too minimalistic to be useful in dealing with more general philosophical questions, including natural sciences; but it turns out to be more than enough for dealing with mathematics.

3. Contents of the course. Part 1 of the course is about the part of logic necessary to introduce mathematics. Part 2 is about mathematics. Part 3 is about mathematical logic.

Here is a detailed outline of the ideas presented in this course.

The first part of the course is devoted to logic. The idea that rational thought obeys definite laws goes back to the classics of logic: Aristotle (4th century BC), Leibniz (17/18th century), and Boole (19th century). Now rational thought does not operate with the phenomena but rather with names/symbols given/attached to various phenomena. Symbols are concrete physical objects; they are spoken, written, or shown. They are organized in systems of symbols by certain organizational principles. The collection of all symbols in a system of symbols is referred to as a language. So in some sense logic is an analysis of languages; as such it can be viewed as part of linguistics:

\[ \{ \text{logic} \} \subset \{ \text{linguistics} \} \]

Linguistics is also interested in non-logical aspects of languages such as: morphology, phonology, etymology, psychological and neurological aspects, etc. We will not touch upon these here.

There are various types of correspondences between languages; they attach to fragments of one language fragments of another language. A familiar type of correspondences are translations such as:

English \rightarrow French

which have an interpretative role. But there are other types of correspondences playing various other (combinations of) roles: referential, descriptive, prescriptive, generative, etc. Cf. some examples below.

Symbols within a language are assembled into strings (called sentences) according to specific rules which are common to large groups of languages. The main (logical) aspects of languages are: syntax, semantics, reference, inference, truth. Syntax is the set of rules governing the way sentences are assembled from symbols; in other words sentences are the syntactically correct strings of symbols. Syntactic rules are formulated in terms of syntactic categories; examples of syntactic categories are logical categories (such as constants, variables, predicates, connectives, quantifiers, etc.) or grammatical categories (such as nouns, verbs, adjectives, etc.) Natural languages are analyzable from both the logical and the grammatical angles; but mathematics requires logical rather than grammatical categories. So we will essentially ignore the grammatical categories. Semantics (also referred to as meaning) is about what sentences “say”; it is derived from context within the language or from correspondences with other languages. Reference is “whatever there is in the physical or imaginary worlds that the symbols refer to”. Inference is a process
by which we accept “new” declarative sentences based on already accepted “old” declarative sentences; there are other types of sentences such as interrogative or imperative that do not need acceptance hence inference. Also there are sentences which are impossible to infer and whose negation is also impossible to infer from anything that is being accepted; see VI below. What inference consists of is a matter of convention: it can mean anything from “some evidence to believe” to “formal proof”. Truth is a property of declarative sentences that have a meaning; a theory of truth requires that any such sentence is either true or false; a theory of truth does not require in principle that truth be capable of being inferred: a sentence can be in principle true “objectively” without the possibility of inference. (Not all theories of truth agree here and we will actually very soon give up the concept to truth in this very course.) For instance consider the following utterances:

I. through passes not electron slit
II. colorless green ideas sleep furiously
III. it is going to be here
IV. all men are immortal
V. Napoleon was alive at the battle of Waterloo
VI. the universe is infinite

In the above I is syntactically incorrect so it is not a sentence. II is a sentence and is an example of Chomsky’s; it has no meaning in any reasonable translation so no truth value; its words have a precise reference. III is a sentence; it has an imprecise reference because “it” is ambiguous; once a reference is given to “it” it has a meaning; hence it becomes susceptible of being true or false. IV and V are sentences with meaning and reference; IV is false and V is true in any reasonable theory of truth; the falsehood of IV and the truth of V are trivially inferred from generally accepted sentences. VI is a sentence, it has meaning and reference, so it is susceptible of being true or false; its truth or falsehood can be thought of as being independent of our ability to infer it (although not all theories of truth agree on this). The above are just examples; one task of the philosophy of language is to define the concepts of syntax, semantics, reference, inference, truth, and build an explanatory theory of language and understanding based on the corresponding definitions.

Going back to reference, there are two kinds of reference: linguistics reference and non-linguistic reference. V above refers to the physical “man Napoleon” (whatever that means) rather than to the “word Napoleon”; such a reference is non-linguistic. On the other hand saying that a language \( \hat{L} \) has language \( L \) as its linguistic reference means that \( \hat{L} \) “talks about” \( L \) as a language, i.e. about the symbols, syntax, semantics, etc. of \( L \) (or group of languages like \( L \)). In this case, once we fixed \( \hat{L} \) and \( L \) we may call \( L \) the object language and \( \hat{L} \) the metalanguage. This designation is relative i.e. a language may be an object language in one designation and a metalanguage in another designation. But once such a designation has been made we will tend to treat object languages and metalanguages according to slightly different standards, as we shall explain momentarily. Linguistic reference is a correspondence between metalanguage and object language:

\[
\text{Metalanguage} \quad \rightarrow \quad \text{Object language}
\]
This kind of correspondence introduces a hierarchy among languages which is reminiscent of Russell’s theory of types; we will not discuss that theory here. The necessity of introducing the object language / metalanguage hierarchy (and indeed metallanguage, metametallanguage, etc.) was recognized by Tarski; but our metalanguage will be slightly different from Tarski’s (ours will be poorer than Tarski’s, as we shall explain later.)

Sentences in metalanguage will be called metasentences; meaning in metalanguage will be called metameaning, etc. Assuming we have fixed an object language and a metalanguage we will adopt the following principles (which are appropriate for introducing logic and mathematics although are not all appropriate for introducing other sciences or analyzing natural languages):

1) carefully distinguish between the symbols of object language and the same symbols viewed as belonging to metalanguage;
2) ignore the meaning and reference of sentences in the object language;
3) take into consideration the meaning and reference of metasentences in metalanguage;
4) control syntax of sentences in the object languages (as well as translations between various object languages) through metasentences in metalanguage;
5) adopt a self-referential approach to controlling the syntax of metalanguages; this is in order to avoid the introduction of a metametallanguage, etc.
6) inference of sentences in the object language will be called proof and will be a rigid process whose rules are spelled out in metalanguage; inference of metasentences in metalanguage will be called metaproof and will obey less strict rules (which should be spelled out, again, in metalanguage, or if ambiguity arises, in metametallanguage); metaproofs must be finitistic (in the sense of Hilbert and Weyl i.e. “reducible to a quantifier free formulation”) and should reduce to verifying (via case by case inspection) that rules and definitions are applied correctly. In particular no metasentence involving quantifiers “over infinite domains” can be metaproved.
7) ban truth predicates from both the object language and the metalanguage; so the words true and false will be banned from both object languages and metalanguage; or if used they will be declared meaningless.

By 1 and 7 above we dispose of a class of classical paradoxes. Indeed consider the “liar’s paradox” which is the following sentence in English: “The sentence that you reading now is false’. If one assumes the sentence is true it looks like its content says it is false. And if one assumes the sentence is false it looks like its content says it is true. There are two sources of the above paradox. One is the use of the words true and false equipped with their meaning. Another one is the identification of English as object language with English as metalanguage. In this course we will adopt, as already mentioned, a viewpoint which eliminates both sources of the above paradox: this is done through 1 and 7 above.

Another reason why we want to operate with an object language and a metalanguage level is that object languages (like English, theoretical physics, mathematics) usually have a complicated structure and their meaning is acquired through translation into other complicated object languages (like history/literature, experimental physics, philosophy); whereas the metalanguage that controls their syntax has a relatively simple structure (it refers to these object languages alone, hence, essentially, to marks on a piece of paper) and its meaning is acquired through translation
into other simple languages (like the ones governing simple children games or elementary computer programs). Think of the meaning and possibility of inference of the sentence

1) “Radiation is quantized”

in English compared to the metasentence in “MetaEnglish”:

2) The word “radiation” occurs in the sentence “radiation is quantized”

The meaning of (and so the possibility to infer) the sentence 1 is problematic: it depends on the translation of the sentence into the language of theoretical physics; there may be several translations into one such language and there are several physical theories to choose from; deciding which theory to use depends on translations between various theoretical physics languages and the language of data coming from experimental physics; the decision may depend also upon translations into usual English and interactions of these with sentences expressing issues in the politics of science, etc. On the other hand the metameaning of (and the possibility to infer) the metasentence 2 above is arguably less problematic: the metameaning depends on the language describing the search of a word in a sentence and as such 2 has an obvious meaning and is trivial to infer. This being the case one can defer the analysis of meaning and inference from a complicated/problematic level to an arguably simple/unproblematic level. (The meaning and inference of 2 is not as unproblematic as it seems: see Wittgenstein [8].)

The next step in the discussion of languages is the discussion of inference (also called deduction). If truth were allowed as a predicate inference would be required to be such that sentences inferred from true sentences must themselves be true. However, since truth of sentences is not defined, we should view inference as a substitute for the guarantee of truth. Let us fix in our discussion an object language and a metalanguage. A collection of sentences in the object language obtained via inference from a given list of sentences called specific axioms will be called a theory. The sentences of a theory will be called theorems. Inference is defined in terms of sentences referred to as background axioms. The process of inference of sentences will be called proof; technically proofs are strings of sentences formed according to certain rules. A key syntactic object behind inference will be a certain class of constants called witnesses; this way of proceeding goes back to Hilbert (cf. Weyl’s exposition of Hilbert’s theory in [7]). The word witness used here is borrowed from model theory but our use of witnesses is not model theoretic (it precedes, as in Hilbert, set theory).

We end our discussion of logic on a more philosophical note by discussing two aspects of language namely: its relation with psychology and its relation with the “world in itself”.

We start by looking at one aspect of the study language that has relevance to psychology; this is related to an important example of correspondence between languages coming from Chomsky’s work [3],

\[
\text{deep structure } \rightarrow \text{ surface structure}
\]

in which surface structure is, very roughly speaking, what we hear/see when one speaks/reads a natural language (such as English) and deep structure is a language
which our minds actually operate with; the arrow consists of successive compositions of syntactical operations such as ellipses, permutations, etc., applied to grammatical categories (nouns, verbs, adjectives, prepositions, etc.) rather than to the logical categories of constants, variables, predicates, connectives, quantifiers, etc. This correspondence is neither descriptive nor prescriptive but, rather, generative; this kind of correspondence between languages will not concern us in this course (although it may be the key to the semantics of metalanguage which IS of concern to us). The mechanisms behind this scheme are referred to by Chomsky as universal grammar. Universal grammar is believed to be innate, largely the same for all humans, and may explain linguistics competence (e.g. the effortless “reinvention” of language by children based on very little empirical material).

A few words now about the relation between language and the world in itself. An interesting philosophical question (which we will NOT explore in this course) is whether the syntactic structure of sentences in a language corresponds to the structure of the world in itself. When natural languages are being considered and familiar situations in the world are looked at then a correspondence between the two seems to be operating almost by definition. (Cf. Wittgenstein’s thesis [8] that the structure of a fragment of the world needs to be similar to the structure of a sentence describing that fragment in order to even make sense of the claim that the sentence describes that fragment.) For instance consider the sentence in English:

(i) “The cause of death of hominid A is the stone thrown by hominid B”

It looks like the constants hominid A and hominid B correspond to two “physical” hominids, the functional symbol death of corresponds (unfortunately) to a “physical” event, and so do the functional symbols the cause of and the stone thrown by; the equality is seems to be related to a “physical” fact too. This correspondence of syntactic structure with the structure of the world in itself must have had an important value in the evolutionary process that lead to language. Indeed, by Darwin’s theory, a hominid who (by some random accident in his genetic material) would have had the ability to see the murder scene according to (i) will have had a better chance of survival, say, in an encounter with a hominid like B, and hence would have had a better chance to pass on his genetic material to his offspring. But such a correspondence cannot be easily taken for granted or extrapolated from examples as above. Indeed the scene described by (i) has other possible descriptions that do not involve two hominids one of which murders the other. Here are other descriptions:

(i’) “The cause of death of hominid A is its property of attracting rocks”

(i”) “The hominid population decreased due to its translation movement with respect to a fixed rock”

A hominid whose genes generated the wiring responsible for (i’) would not survive very long and hence would have a low chance of passing on his genes to his offspring; this is maybe why our minds favor (i) over (i’) in decoding a scene like the one we are contemplating. The sentence (i”) may be what a tiny extraterrestrial visitor who landed on our rock would see in the murder scene; in (i”) the two individual hominids have disappeared, cause/effect has shifted from individual events to more global events, etc. For the world in itself the scene may look quite different: the hominids, the rock, and the space-time surrounding them including the Earth, Moon, Sun and all the stars from the Big Bang to the Big End, should be seen as
forming a "continuum", the objects have no boundaries that separate them from space-time, nor is movement something separate from what moves, nor is causation meaningful. The murder disappears from the picture and there is no sentence to express the situation. For a sentence to exist mind has to break down the world in itself into artificial fragments; if the world in itself is an unbroken whole there is no sentence to express it.

Here is another example. Consider the sentence in English:

(ii) "The cause of planet movement around the Sun is the attraction of the Sun"

This was contested by Newton’s contemporaries (including Leibniz) as being an empty (metaphysical) statement because the word attraction is just an anthropomorphic metaphor (actually borrowed from the metaphysics of Christianity along the idea that attraction is identifiable with the love of God). But the success of this statement made it acceptable after Newton’s time until Einstein’s general theory offered another statement:

(ii’) "The cause of planet movement around the Sun is the bending of space-time by the Sun"

This is, of course, an equally empty statement because bending is just another anthropomorphic metaphor (borrowed from everyday life). The success of Einstein’s theory did not come from the sentence (ii’) itself but from the prediction power of its metaphorical content. But if the world in itself is an indivisible whole, planets and Sun and their relative movements are a continuum that cannot be a priori broken into constants (such as planets, Sun), functional symbols (such as the cause of, the attraction of) and equality is. Breaking the world in itself into objects (constants, variables, and more generally terms; or noun phrases) and relations among them (relational predicates; or verb phrases) is an operation executed (unconsciously) by our minds which are wired to act so; this was clearly understood by Hume and, in a deeper way, by Kant. After Darwin it became clear that this particular wiring came to be through a natural selection process based on extrapolation from examples like (i) above. The extrapolation referred to generates, among other things, functional symbols such as the cause of in (ii) which is anthropomorphic and has no correspondent in the world in itself. Natural sciences are full of anthropomorphic constants and predicates (space, time, force, causality) which are probably just extrapolations from situations as in (i) to situations as in (ii); at best these predicates should be viewed as metaphors.

The second part of the course is devoted to mathematics. Mathematics will be introduced as being the same as a specific theory (in the sense of logic) called set theory. The first move will then be to introduce the axioms of set theory (called the ZFC axioms) and to introduce sets themselves which will be defined as the constants of set theory. (In one version of set theory there are no other sets except the witnesses.) Then we will introduce some of the basic concepts of set theory: maps, relations, operations. The next step will be to introduce the basic types of numbers: integer numbers, rational numbers, real numbers, complex numbers, numbers mod $p$, and the $p$-adic numbers. (Here $p$ is any prime number.) The collections of such numbers are denoted by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Z}_p$ respectively. Denoting by arrows what we will call ring homomorphisms we have the following connections between various types of numbers:
As the picture suggests the integers $\mathbb{Z}$ are the most basic numbers; the existence of the integers will follow from the ZFC axioms; then we will construct the rest of the numbers via standard constructions in set theory. The part of mathematics that abstracts the behavior of numbers is algebra. Geometry then deals with figures. Finally analysis deals with limits, more generally with the infinite (both large and small). The course will provide a quick introduction to some of the basic objects of algebra, geometry, and analysis. These 3 branches of mathematics are closely interconnected; and in each of these branches one is lead to consider all the types of numbers referred to above. A somewhat special chapter of mathematics is mathematical logic (which will be quickly introduced in the third part of the course); it can be viewed as a special chapter of algebra but its flavor is different from that of main stream algebra.

We end our discussion here by looking at the connections between mathematics and the physical world (phenomenal world, natural world). Roughly this comes about as follows. Natural sciences are, themselves, organized as languages. It turns out that there are interesting translations from the languages of natural sciences into the language of mathematics. These translations are not unique and finding new such translations may amount to revolutions in the natural sciences. (Translations into the language of mathematics can be referred to as mathematical models, or simply metamodels, and will be very briefly discussed towards the end of the course.) Throughout history there was a close relationship between the development of mathematics (which in this course is the same as pure mathematics) and the development of translations into mathematics (which constitute applied mathematics). The dynamics of this relationship is somewhat surprising. Indeed pure mathematics seems to have been constantly anticipating the needs of applied mathematics. For example the theory of conic sections of Apollonius turned out, much later, to be exactly what was needed in the theory of planetary motion of Kepler and Newton; and the matrix algebra of the 19th century British algebraists turned out to be exactly what was needed for the development of the 20th century quantum mechanics. The parts of pure mathematics that found the most spectacular applications turned out to be precisely those parts which were considered the “most beautiful”; this link between aesthetics and applicability is an interesting puzzle in the history of science.
Part 1

Logic
CHAPTER 1

Languages

Logic is the analysis of language with special emphasis on syntax, semantics, reference, inference, truth. We start a general discussion of these now; more details will be given in subsequent chapters.

Example 1.1. (Logical analysis) We will introduce here two languages, English and Formal, and we will analyze their interconnections.

Let us start with a discussion of English. The English language is the collection $L_{Eng}$ of all English words (plus separators such as parentheses, commas, etc.) We treat words as individual symbols (and ignore the fact that they are made out of letters.) Sometimes we admit as symbols certain groups of words. One can use words to create strings of words such as

0) “for all not Socrates man if”

The above string is considered “syntactically incorrect”. The sentences in the English language are the strings of symbols that are “syntactically correct” (in a sense to be made precise later). Here are some examples of sentences in this language:

1) “if Socrates is a wise man then Socrates is a man.”
2) “Socrates is not a mason and Socrates’ father is a mason”
3) “for all things either the thing is not a man or the thing is mortal.”
4) “there exists somebody who is Plato’s teacher”
5) “for all things the thing is Socrates if and only if the thing is Plato’s teacher”

In order to separate sentences from a surrounding text we put them between quotation marks (and sometimes we write them in italics). So quotation marks do not belong to the language but rather they lie outside the language. Checking syntax presupposes a partitioning of $L_{Eng}$ into various categories of words; no word should appear in principle in two different categories, but this requirement is often violated in practice (which may lead to different readings of the same text). Here are the categories:

- variables: “thing, somebody,...”
- constants: “Socrates, Plato, the Wise, the Mason,...”
- functional symbols: “the father of, the teacher of,...”
- relational predicates: “is (belongs to), is a man, is mortal,...”
- connectives: “and, or, not, if...then, if and only if”
- quantifiers: “for all, there exists”
- equality: “is, equals”
- separators: parantheses “(,)” and comma “,”
The above categories are referred to as **logical categories**. (They are quite different from, although related to, the **grammatical categories** of nouns, verbs, etc. See Remark 1.14 below for a more in depth discussion of grammatical categories; here we will only allude to them.) In general objects are named by constants or variables. (So constants and variables roughly correspond to nouns.) Constants are names for specific objects while variables are names for non-specific (generic) objects. Relational predicates say/affirm something about one or several objects; if they say/affirm something about one, two, three objects etc., they are unary, binary, ternary, etc. (So roughly unary relational predicates correspond to intransitive verbs; binary relational predicates correspond to transitive verbs.) Functional symbols have objects as arguments but do not say/affirm anything about them; all they do is refer to (or name, or specify, or point towards) something that could itself be an object. (Functional symbols are sometimes referred to as functional predicates but we will not refer to them as predicates here; this avoids confusion with relational predicates.) Again they can be unary, binary, ternary, etc., depending on the number of arguments. Connectives connect/combine sentences into longer sentences; they can be unary (if they are added to one sentence changing it into another sentence, binary if they combine two sentences into one longer sentence, ternary, etc.) Quantifiers specify quantity and are always followed by variables. Separators separate various parts of the text from various other parts.

In order to analyze a sentence using the logical categories above one first looks for the connectives and one splits the sentence into simpler sentences; alternatively sentences may start with quantifiers followed by variables followed by simpler sentences. In any case, once one identifies simpler sentences, one proceeds by identifying, in each of them, the constants, variables, and functional symbols applied to them (these are the objects that one is talking about), and finally one identifies the functional symbols (which say something about the objects). The above type of analysis (called **logical analysis**) is quite different from the **grammatical analysis** based on the grammatical categories of nouns, verbs, etc. (Cf. Remark 1.14 below.)

In our examples of sentences 1-5 logical analysis proceeds as follows.

In 1 “if...then” are connectives connecting the simpler sentences “Socrates is a wise man” and “Socrates is a man”. Let us look at the sentence “Socrates is a wise man”. The word “Socrates” here is viewed as a constant; the group of words “wise man” is viewed as a constant; “is” is a binary relational predicate (it says/affirms something about 2 objects: “Socrates” and “the wise men”; it says that the first object belongs to the second object). Let us look now at the sentence “Socrates is a man”. We could read this second sentence the way we read the first one but let us read it as follows: we may still view “Socrates” as a constant but we will view “is a man” as a unary relational predicate (that says/affirms something about only one object, Socrates).

A concise way of understanding the logical analysis of English sentences as above is to create another language $L_{For}$ (let us call it Formal) consisting of the following symbols:

- variables: “x, y, ...”
- constants: “s, p, w, m”
- functional symbols: “f, □”
- relational predicates: “∈, ρ, ‖”
- connectives: “∧, ∨, ¬, →, ↔”
1. LANGUAGES

- quantifiers: “∀, ∃”
- equality: “=”
- separators: parantheses “(,)” and comma “,”

Furthermore let us introduce a rule (called translation) that attaches to each symbol in Formal a symbol in English as follows:

“x, y” are translated as “thing, somebody”
“s, p, w, m” are translated as “Socrates, Plato, the Wise, the Mason”,
“f, □” are translated as “the father of, the teacher of”
“∈, ρ, †” are translated as “belongs to, is a man, is mortal”
“∧, ∨, ¬, →, ↔” are translated as “and, or, not, if...then, if and only if”
“∀, ∃” are translated as “for all, there exists”
“=” is translated as “is”

Then the English sentence 1 is the translation of the following Formal sentence:

1’) “(s ∈ w) → (ρ(s))”

Conversely we say that 1’ is a formalization of 1.

Let us continue, in the spirit above, the analysis of the sentences 2,...,5 above.

In 2 “and” and “not” are connectives (binary and unary respectively): they are used to assemble our sentence 2 from two simpler sentences: “Socrates is a mason” and “Socrates’ father is a mason”. In both these simpler sentences “Socrates” and “mason” are constants; “the father of” is a unary functional symbols (it refers to Socrates and points towards/names his father but it does not say anything about Socrates); “is” is translated as “is a man, is mortal”

Here is a formalization of 2:

2’) “¬(s ∈ m) ∧ (f(s) ∈ m)”

Sentence 3 starts with a quantifier “for all” followed by a variable “things” followed by a simpler sentence. That simpler sentence is made out of 2 even simpler sentences “the thing is a man” and “the thing is mortal” assembled via connectives “and” and “or”. Finally “is a man, is mortal” are unary relational predicates. Here is a formalization of 3:

3’) “∀x((¬ρ(x)) ∨ †(x))”

Sentence 4 starts with a quantifier “there exists” followed by a variable “someone” followed by a simpler sentence that needs to be read as “that somebody is Plato’s teacher”. In the latter “teacher of” is a unary functional symbols while “is” is equality. Here is a formalization of 4:

4’) “∃y(y = □(p))”

Sentence 5 starts with a quantifier “for all” followed by a variable “things” followed by a simpler sentence. The simpler sentence is assembled from two even simpler sentences: “the thing is Socrates” and “the thing is Plato’s teacher” connected by the connective “if and only if”. Finally in these latter sentences “Socrates, Plato” are constants while “teacher of” is a unary functional symbol, and “is” is equality. Here is a formalization of 5:
We note that "or" in English is disjunctive: "this or that" is used in place of "this or that or both".

Also remark the use of "is" in 3 instances: as a binary relational predicate indicating belonging, as part of a unary relational predicate, and as equality.

Remark also that we view the variables "thing" and "somebody" on an equal footing, so we ignore the fact that the first suggests an inanimate entity whereas the second suggests a living entity.

Also note that all verbs in 1-5 are in the present tense. English allows other tenses, of course. But later in mathematics all predicates need to be viewed as tense indifferent: mathematics is atemporal. This is an instance of the fact that natural languages like English have more expressive power than mathematics.

Finally remark that the word "exists" which could be viewed as a relational predicate is treated instead as part of a quantifier. Sentences like "philosophers exist" and "philosophers are human" have a totally different logical structure. Indeed "philosophers exist" should be read as "there exists somebody who is a philosopher" while "philosophers are human" should be read as "for all things if the thing is a philosopher then the thing is a human". The fact that "exist" should not be viewed as a predicate was recognized already by Kant in his criticism of the "ontological argument".

**Remark 1.2.** (Syntax/semantics/reference/inference/truth of languages)

Syntax deals with rules of formation of "correct" sentences. We will examine these rules in detail in a subsequent chapter.

Semantics deals with meaning. At this stage we do not know what "meaning" is so the sentences 1,...,5 above should be viewed as meaningless; and they ARE meaningless for a person who does not know the English language. For such a person establishing meaning requires relating these sentences to sentences in another language (e.g. translating them into French, German, a "picture language", sign language, Braille, etc., or using a correspondence to "deeper" languages); the more translations available the more definite the meaning. On the other hand the meaning of 1',...,5' is taken to be given by the sentences 1,...,5 (where one assumes one knows English).

Words in English may refer to the physical or imaginary worlds (including symbols in languages which are also viewed as physical entities); the English word "Socrates" refers to the physical "man Socrates"; the English word "word" refers to symbols used in speech, writing, etc. Symbols in Formal can be attached their own reference.

As explained in the Introduction inference is a process by which we accept declarative sentences that have a meaning (rather than rejecting them) based on other declarative sentences that are already accepted; see the comments below on declarative sentences.

We could also ask if the sentences 1,...,5, 1',...,5' are "true" or "false". As explained in the Introduction we will not define truth/falsehood for sentences in any of our languages.

**Remark 1.3.** (Declarative/imperative/interrogative sentences) All sentences considered so far were declarative (they declare their content). Natural languages have other types of sentences: imperative (giving a command like: "Lift this
weight!') and interrogative (asking a question such as: “Is the electron in this portion of space-time?”). In principle, from now on, we will only consider declarative sentences in our languages. An exception to this will later be the use of imperative forms in a language called Argot; Argot will be a language in which we will write most of our proofs and imperative forms to be used in it will be, for instance: “consider”, “assume”, “let...be”, “let us...”, etc.)

Remark 1.4. (Definitions) A language may be enlarged by definitions. More precisely one can add new predicates or constants to a language by, at the same time, recording certain sentences, called definitions. As an example for the introduction of a new relational predicate in English we can add to English the relational predicate is an astrochicken by recording the following sentence:

Definition 1.5. Something is an astrochicken if and only if it is a chicken and also a space ship.

Here are alternative ways to give this definition:

Definition 1.6. An astrochicken is something which is a chicken and also a space ship.

Definition 1.7. Something is called (or referred to as) astrochicken if it is a chicken and also a space ship.

Similarly, if in Formal we have a binary relational predicate $\in$ and two constants $c$ and $s$ then one could introduce a new relational predicate $\epsilon$ into Formal and record the definition:

Definition 1.8. $\forall x(\epsilon(x) \leftrightarrow ((x \in c) \land (x \in s)))$

The two definitions are related by translating $\in$, $c$, $s$, and $\epsilon$ as “belongs to”, “chicken”, “space ships”, and “is an astrochicken” respectively. The word astrochicken is taken from an essay by Freeman Dyson on “Science and science fiction”.

In a similar way one can introduce new functional symbols or new constants.

Remark 1.9. (Naming) It is useful to give names to sentences. For instance if we want to give the name $P$ to the English sentence “Socrates is a man” we write $P$ equals “Socrates is a man”.

The latter is not a sentence in English: neither $P$ nor the quotation marks belong to what we declared to be English; and the word is outside the quotation marks should be viewed as different from the word “is” inside the quotation marks. Later we will see that these words outside the quotation marks belong to what we shall call metalanguage. One can give various different names to the same sentence. In a similar way one can give names to sentences in Formal:

$Q$ equals “$\rho(s)$”

In the above discussion we encountered 2 examples of languages: English and Formal. Later we will introduce other languages. We would like to “define” languages in general; we cannot do it in the sense of Remark 1.4 because definitions in that sense require a language to begin with. All we can do is describe in English what the definition of a language would look like. So the remark below is NOT a definition in the sense of Remark 1.4.
Remark 1.10. (Description in English of the concept of language) A first order language (or simply a language) is a collection of symbols with the following properties. Assume \( L \) is language. Then the symbols in \( L \) are divided into 8 categories called logical categories. They are: variables, constants, functional symbol, relational predicates, logical connectives, quantifiers, equality, and separators. Some of these may be missing. (Functional symbol and equality can always be “eliminated” in an obvious sense.) Also we assume that the list of the variables never ends (is “infinite” in the intuitive sense). The list of constants may or may not end. Finally we assume that the only allowed separators are parentheses (,) and commas; we especially ban quotation marks “...” from the separators allowed in a language (because we want to use them in what we shall call later metalanguage). Given a language \( L \) one can consider the collection \( L^* \) of all strings of symbols. We will later define what one means by a string in \( L^* \) to be a sentence. The collection of sentences in \( L^* \) is denoted by \( L_s \). (We sometimes say “sentence in \( L \)” instead of sentence in \( L^* \).) As in the examples above we can give names \( P, ... \) to the sentences in \( L \); these names \( P, ... \) do NOT belong to the language. A translation of a language \( L \) into another language \( L' \) is a rule that attaches to any symbol in \( L \) a symbol in \( L' \); we assume constants are attached to constants, variables to variables, etc. Due to syntactical correctness (to be discussed later) such a translation attaches to sentences \( P \) in \( L \) sentences \( P' \) in \( L' \). The analysis of translations is part of semantics and will be discussed later in more detail. Actually the above concept of translation should be called word for word translation (or symbol for symbol) and it is way too rigid to be useful. In most examples translations should be allowed to transform sentences into sentences according to rules that are more complicated than the symbol for symbol rule.

Example 1.11. (Infinitely many constants) English and Formal are examples of languages. Incidentally in these languages the list of constants ends (there are only “finitely many” constants; here we use “finitely many” in an intuitive sense: their list “ends”.) But it is important to not impose that restriction for languages. If instead of English we consider a variant of English in which we have words involving arbitrary many letters (e.g. words like “man, superman, supersuperman,...” etc.) then we have an example of a language with an “infinite” number of constants. There is an easy trick allowing one to reduce the case of “infinitely many” symbols to the case of “finitely many” symbols; one needs to slightly alter the syntax by introducing one more logical category, an operator denoted, say, by ‘; then one can form constants \( c', c'', c''', ... \) starting from a constant \( c \); one can form variables \( x', x'', x''', ... \) from a variable \( x \); and one can do the same with functional symbols, predicates, etc.; we will not pursue this in what follows.

Example 1.12. (Alternative translations) We already gave an example of translation of Formal into English; cf. Example 1.1. (Strictly speaking that example of translation was not really a word for word translation.) The translation given there for connectives, quantifiers, and equality is called the standard translation. But there are alternative translations as follows.

Alternative translations of \( \to \) into English are “implies”, or “by...it follows that”, or “since...we get”, etc.. An alternative translation of \( \leftrightarrow \) into English is “is equivalent to”.

Alternative translations of \( \forall \) into English are “for any”, or “for every”.

Alternative translations of \( \exists \) into English are “for some” or “there is an/a”.
English has many other connectives (such as “before”, "after", “but”, “in spite of the fact that”, etc.). Some of these we will ignore; others will be viewed as interchangeable with others; e.g. “but” will be viewed as interchangeable with “and” (although the resulting meaning is definitely altered). Also English has other quantifiers (such as “many”, “most”, “quite a few”, “half”, “for at least three”, etc.); we will ignore these other quantifiers.

Remark 1.13. (Texts) Let us consider the following types of objects:
1) symbols (e.g. \(x, y, a, b, f, \square, ..., \in, \rho, ..., \land, \lor, \neg, \to, \leftrightarrow, \forall, \exists, =, (, )\));
2) collections of symbols (e.g. the collection of symbols above, denoted by \(L\));
2′) strings of symbols (e.g. \(\exists x \forall y (x \in y)\));
3) collections of strings of symbols (e.g. \(L^*, L^s\) encountered above or theories \(T\) to be encountered later);
3′) strings of strings of symbols (such as the proofs to be encountered later).

In the above collections are unordered while strings are ordered. The above types of objects will be referred to as texts; they are precursors of (or rather concrete models for) what later will be referred to as sets. Texts should be though of as concrete (physical) objects, like symbols written on a piece of paper or papyrus, words that can be uttered, images in a book or in our minds, etc. We assume we know what we mean by saying that a symbol belongs to (or is in) a given collection/string of symbols; or that a string of symbols belongs to (or is in) a given collection/string of strings of symbols. We will not need to iterate these concepts. (Later, with sets, we will assume we can indefinitely iterate concepts like these.) We will also assume we know what we mean by performing some simple operations on such objects like: concatenation of strings, deleting symbols from strings, substituting symbols in strings with other symbols, “pairing” strings with other strings, etc. These will be encountered and explained later. Texts will be crucial in introducing our concepts of logic. Note that it might look like we are already assuming some kind of logic when we are dealing with texts; so our introduction to logic might seem circular. But actually the “logic” of texts that we are assuming is much more elementary than the logic we want to introduce later; so what we are doing is not circular.

Remark 1.14. (Grammatical analysis) Earlier we said that logical analysis of sentences in English is quite different from grammatical analysis. Let us take a quick look at the latter in the following simple example. Consider the following sentence in English:

“The father of Socrates is a mason”

The grammatical (as opposed to logical) categories here are:
- nouns: Socrates, father, mason
- verbs: is
- determinators: a, the

The sentence (S) above is constructed from a noun phrase (NP) “the father of Socrates” followed by a verb phrase (VP) “is a mason”. The noun phrase “the father of Socrates” is constructed from the noun phrase “the father” and the prepositional phrase (PP) “of Socrates”. The noun phrase “the father” is constructed from a determinator (D) “the” and a noun phrase which itself consists of a noun (N) “father”. The prepositional phrase “of Socrates” is constructed from a preposition...
“of” and a noun phrase which itself consists of a noun, “Socrates”. The verb phrase “is a mason” is constructed from a verb (V) “is”, and a noun phrase “a mason”. The latter is constructed from a determinator (D) “a”, and a noun (N) “mason”. One can represent the above grammatical analysis as an array:

\[
S \\
NP \\
NP \\
D N P N V D N
\]

the father of Socrates is a mason

The above may be referred to as a grammatical sentence formation; such a formation is something quite different from the (logical) formula/sentence formations to be introduced later based on logical analysis. One can add edges to the array above as follows: each entry \( X \) in a given row is linked by an edge to the closest entry \( Y \) in the previous row that is above or to the left of \( X \). In this way we get an inverted tree. Such inverted trees are the basis for Chomsky’s generative grammar [3]. Alternatively one can store in the information contained in a grammatical sentence formation as follows. One enriches English by adding separators \( S \) and \( S \) for sentences, \( NP \) and \( NP \) for noun phrases, etc., and one stores the above sentence formation as a string of words in this enriched English:

\[
\]

This enriched English is what Chomsky calls deep structure English. Grammatical sentence formations are obtained by applying substitution rules symbolically written, for instance, as

\[
S \rightarrow NP \ VP \\
NP \rightarrow NP \ PP \\
VP \rightarrow V \ NP \\
NP \rightarrow D \ NP \\
NP \rightarrow N \\
PP \rightarrow P \ NP \\
N \rightarrow \text{father} \\
N \rightarrow \text{Socrates} \\
etc.
\]

More complicated rules are, of course, present in English. On the other hand very simple “superrules” that generate these complicated rules in virtually all languages have been discovered by Chomsky. The symbols of deep structure English are the same as the symbols of what Chomsky calls surface structure English; but the latter has a syntax different from deep structure English and there are are well defined ways to pass from deep structure to surface structure via operations on the corresponding trees (ellipses, permutations, etc). This way of looking at natural languages such as English has deep consequences in psychology and the philosophy of mind; however this approach does not seem appropriate for the study of languages such as Formal or other languages of interest to science and mathematics. Mathematics will require logical (rather than grammatical) analysis. So we will not pursue grammatical analysis beyond this point.
CHAPTER 2

Reference

In the previous discussion we introduced languages and translations between them. Translations are an example of correspondence between languages. *Linguistic reference* is another example of correspondence between languages as we will explain below.

Indeed, more generally, one can talk about the reference of a language: it is “whatever there is in the physical or imaginary worlds that the language is talking about”. There are two kinds of reference: linguistic and non-linguistic.

Here is an example of a non-linguistic reference: the English sentence “Napoleon is dead” makes a non-linguistic reference to the physical “man Napoleon” (rather than to the “word Napoleon”). Another example is the sentence “Hamlet killed Polonius”. If two sentences are obtained from each other by translation they have, essentially, the same non-linguistic reference; e.g. “My dog loves me” and “Mon chien m’adore” have the same non-linguistic reference, namely the physical “animal I call “my dog””. We will have very little to say about non-linguistic reference in what follows because we chose, in this course, to essentially ignore everything in the physical world except languages themselves. Rather we will concentrate now on linguistic reference.

Linguistic reference is a correspondence between two languages in which the first language $\hat{L}$ “talks about/refers to” the second language $L$ as a language (i.e. it “talks about/refers to” the syntax, semantics, etc. of $L$). Once we have fixed $L$ and $\hat{L}$ we shall call $L$ the *object language* and $\hat{L}$ the *metalanguage*. (The term *metalanguage* was introduced by Tarski in his theory of truth; but our metalanguage differs from his in certain respects, cf. Remark 2.4 below. Also this kind of correspondence between $\hat{L}$ and $L$ is reminiscent of Russell’s theory of types of which, however, we will say nothing here.)

Metalanguages and object languages are similar structures (they are both languages!) but we shall keep them separate and we shall hold them to different standards. In particular syntax of object languages will be described by metalanguage; and metalanguage will explain (in a self-referential way) its own syntax. Meaning and reference will be ignored in the object language but will NOT be ignored in metalanguage; the reference of metalanguage is always linguistic and is the object language itself. Inference in the object language will be called *proof* and will be discussed later; the rules governing proofs are expressed in metalanguage. Inference in metalanguage will be called *metaproof* and will be explained (in a self-referential way) in metalanguage itself. See more on metaproof below. Truth will be banned from both the object language and the metalanguage.

Sentences in metalanguage are called *metasentences*. If we treat English and Formal as object languages then all our discussion of English and Formal consists of metasentences. The rest of the course will actually consist of metasentences.
“talking about” various languages that are treated as object languages. Let’s have a closer look at this concept. First some examples.

**Example 2.1.** Assume we have fixed an object language $L$ such as English or Formal (or several object languages $L, L', ...$). In what follows we introduce a metalanguage $\hat{L}$. Here are some examples of metasentences in $\hat{L}$. First some examples of metasentences of the type we already encountered (where the object language $L$ is either English or Formal):

1) $x$ is a variable in the sentence “$\forall x (x \in a)$”.
2) $P$ equals “Socrates is a man”.

Later we will encounter other examples of metasentences such as:

3) $P(b)$ is obtained from $P(x)$ by replacing $x$ with $b$
4) Under the translation of $L$ into $L'$ the translation of $P$ is $P'$
5) By the table

<table>
<thead>
<tr>
<th>$P$</th>
<th>$\neg P$</th>
<th>$P \vee \neg P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

the sentence $P \vee \neg P$ is a tautology.
6) $c_P$ is an existential witness for $P$
7) The string of sentences $P, Q, R, ...$, $U$ is a proof of $U$
8) $U$ is a theorem in $T$
9) The theory $T$ is consistent
10) A term is a string of symbols $u$ for which there is a term formation which ends with $u$.

The metasentences 1, 3, 6 are explanations of syntax in $L$ (see later); 2 is a definition (referred to as a notation or naming); 4 is an explanation of semantics (see later); 5 is part of a metaproof; and 7, 8, 9 are claims about inference (see later). 10 is a definition in metalanguage.

Here are the symbols in $\hat{L}$:

- variables: symbol, string, language, term, sentence, theorem, $P, Q, R, ...$, $c_P, c_P', ...$
- constants: “Socrates”, “Socrates is a man”, “$\land$”, “$=$”, “$\forall$”, $T, F, L, L^*, L^s, T, F, ...$
- functional symbols: the variables in, the translation of, $\land, \lor, \neg, \leftrightarrow, \exists x, \forall x$;
- relational predicates: is translated as, occurs in, is obtained from...by replacing...with..., is a tautology, is a proof, is consistent,..., follows from, by ... it follows that..., by ... one gets that...
- connectives: and, or, not, if...then, if and only if, because,...
- quantifiers: for all, there exists
- equality: is, equals
- separators: parantheses (,), comma ,, frames of tables

**Remark 2.2.** Note that names of sentences in the object language become variables (although sometimes also constants) in metalanguage. The sentences of the object language become constants in metalanguage. The connectives of the object language become functional symbols in metalanguage. The symbols “$\land, ...$” used as constants, the symbols $\land, ...$ used as functional symbols, and the symbols
and,... viewed as connectives should be viewed as different symbols (normally one should use different notation for them). Etc.

**Remark 2.3.** The above metalanguage can be viewed as a *MetaEnglish* because it is based on English. One can construct a *MetaFormal* metalanguage by replacing the English words with symbols including:

- connectives: & (for and), ⇒ (for if...then), ⇔ (for if and only if).
- equality: ≡ (for is, equals)

We will not precede this way, i.e. we will always use MetaEnglish as our metalanguage.

**Remark 2.4.** What Tarski called metalanguage is close to what we call metalanguage but not quite identical. The difference is that Tarski allows metalanguage to contain the symbols of original object language written *without* quotation marks. So for him (but not for us), if the language is Formal, then the following is a metasentence:

\[ \forall x \exists y \text{ys}(x, y) \]

Allowing the above to be a metasentence helped Tarski define *truth in a language* (the famous Tarski *T* scheme); we will not do this here.

**Remark 2.5.** (Syntax/semantics/reference/inference/truth of metalanguage)

Metalanguage has a syntax of its own which we keep less precise than that of languages so that we avoid the necessity of introducing a metametalanguage which regulates it; that would prompt introducing a metametametalanguage that regulates the metametalanguage, etc. The hope is that metalanguage, kept sufficiently loose from a syntactic viewpoint, can sufficiently well explain its own syntax without leading to contradictions. The very text you are reading now is, in effect, metalanguage explaining its own syntactic problems. The syntactically correct texts in metalanguage are referred to as metasentences. Definitions in metalanguage are called metadefinitions. It is crucial to distinguish between words in sentences and words in metasentences which are outside the quotation marks; even if they look the same they should be regarded as different words. In order to sustain the distinctions between sentences and metasentences that we have put forward, metasentences are never viewed themselves as sentences; one syntactical way to guarantee this is to ban quotation marks (or letters like P,Q,...) from sentences. Also we will never name metasentences by letters like P,Q,...; the latter letters will be reserved for naming sentences.

In terms of semantics metasentences have, in their turn, a metameaning derived from their own correspondences with, e.g. translation into, other metalanguages or from correspondences with other metalanguages; but we shall ignore this issue and assume we understand their metameaning (as it is rather simpler than the meaning of sentences). Also metasentences have a reference: they always refer to sentences in the object language. Further, metasentences are assumed to have no truth value (it does not make sense to say they are true or false).

For instance the metasentences

a. The word “elephants” occurs in the sentence “elephants are blue”

b. The word “crocodiles” occurs in the sentence “elephants are grey”

can be translated in the “metalanguage of letter searches” (describing how to search a word in a sentence, say). Both metasentences have a meaning. Intuitively we are
tempted to say that (a) is true and (b) is false. As already mentioned we do not want to introduce the concepts of true and false in this course. Instead we infer sentences respectively metasentences; inference of sentences will be called proof; inference of metasentences will be called metaproof. The rules regulating proofs and metaproofs will be explained as we go.

As a general rule metaproofs must be finitistic, by which we mean that they are not allowed to involve quantifiers in the metalanguage; in particular no metasentence involving quantifiers “over infinite domains” can be metaproved. Metaproving can also be called showing.

As examples note that (a) above can be metaproved; also the negation of (b) can be metaproved. Metaproof is usually based on a translation into a “computer language”: for instance to metaprove (a) take the words of the sentence “elephants are blue” one by one starting from the right (say) and ask if the word is “elephants”; the third time you ask the answer is yes, which ends the metaproof of (a). A similar discussion applies to some other types of metasentences; e.g. to the metasentences (1)-(7) in Example 2.1. The metaproof of (5) in Example 2.1 involves, for instance, “showing tables” whose correctness can be checked by inspection by a machine. (This will be explained later.) The situation with the metasentences (8) and (9) in Example 2.1 is quite different: there is no “finitistic” method (program) that can decide if there is a metaproof for (8); neither is there a “finitistic” method that can find a metaproof for (8) in case there is one; same for (9). But if one already has a proof of $U$ in (8) then checking that the alleged proof is a proof can be done finitistically and this provides a metaproof for (8). Finally (10) is a definition in metalanguage (a metadefinition); definitions will be accepted without metaproofs; in fact most metaproofs consist in checking that a definition applies to a given metasentence. The rules governing the latter would be spelled out in metametalanguage; we will not do this here.

Remark 2.6. Since $P, Q$ are variables (sometimes constants) in metalanguage and $\&, \lor, ...$ $\exists x$ are functional symbols in metalanguage one can form syntactically correct strings $P \& Q,..., \exists x P$ in metalanguage, etc. If

$$P \text{ equals } “p...”$$

$$Q \text{ equals } “q...”$$

where $p,...,q,...$ are symbols in the object language then:

$$P \& Q \text{ equals } “(p...) \& (q...)”$$

The above should be viewed as one of the rules allowed in metaproofs. Similar obvious rules can be given for $\lor, \exists$, etc. Note that the parentheses are many times necessary; indeed without them the string $P \lor Q \& R$ would be ambiguous. We will drop parentheses however each time there is no ambiguity. For instance we will never write $(P \lor Q) \& R$ as $P \lor Q \& R$. Note that according to these conventions $(P \lor Q) \lor R$ and $P \lor (Q \lor R)$ are still considered distinct.

Remark 2.7. Assume we are given a metadefinition:

$$P \text{ equals } “p...”$$

Then we say $P$ is a name for the sentence “p...”. We impose the following rule for this type of metadefinitions: if two sentences have the same name they are identical (as strings of symbols in the object language; identity means exactly the
same symbols in the same order and it is a physical concept). Note on the other hand that the same sentence in the object language can have different names.

In the same spirit if

\[ P(x) \text{ equals } "p...x..." \]

is a metadefinition in metalanguage then we will add to the object language a new predicate (still denoted by \( P \)) by adding, to the definitions of the object language, the following definition:

\[ \forall x(P(x) \leftrightarrow (p...x...)) \]

So the symbol \( P \) appears once as a constant in metalanguage and as a predicate in the object language. (We could have used two different letters instead of just \( P \) but it is more suggestive to let \( P \) play two roles.) This creates what one can call a correspondence between part of the metalanguage and part of the language. This correspondence, which we refer to as linguistics reference, is not like a translation between languages because constants in metalanguage do not correspond to constants in the object language but to sentences (or to new predicates) in the object language. In some sense this linguistic reference is a “vertical” correspondence between languages of “different scope” whereas translation is a “horizontal” correspondence between languages with “equal scope”. The words “vertical” and “horizontal” should be taken as metaphors rather than precise terms.

**Remark 2.8.** (Disquotation) There is an operation (called disquotation or deleting quotation marks) that attaches to certain metasentences in metalanguage a sentence in the object language. Consider for instance the metasentence in MetaEnglish

1. From “Socrates is a man” and “all men are mortal” it follows that “Socrates is mortal”

   Its disquotation is the following sentence in (object) English:

   2. “Since Socrates is a man and all men are mortal it follows that Socrates is mortal”

   Note that 1 refers to some sentences in English whereas 2 refers to something (somebody) called Socrates. So the references of 1 and 2 are different; and so are their meaning (if we choose to care about the meaning of 2 which we usually don’t).

   If \( P \) equals “Socrates is a man”, \( Q \) equals “all men are mortal”, and \( R \) equals “Socrates is mortal” then 2 above is also viewed as the disquotation of:

   1’. From \( P \) and \( Q \) it follows that \( R \).

   Disquotation is not always performable: if one tries to apply disquotation to the metasentence

   1. \( x \) is a free variable in “for all \( x \), \( x \) is an elephant”

   one obtains

   2. “\( x \) is a free variable in for all \( x \), \( x \) is an elephant”

   which is not syntactically correct.

   Disquotation is a concept involved in some of the classical theories of truth, e.g. in Tarski’s famous:

   “Snow is white” if and only if snow is white
Since we are not concerned with truth in this course we will not discuss this connection further.

We will often apply disquotation without any warning if there is no danger of confusion.

**Remark 2.9.** (Declarative/imperative/interrogative) All metasentences considered so far were declarative (they declare their content). There are other types of metasentences: imperative (giving a command like: “Prove this theorem!”, “Replace $x$ by $b$ in $P$”, “Search for $x$ in $P$”, etc.) and interrogative (asking a question such as: “What is the value of the function $f$ at 5?”, “Does $x$ occur in $P$?”, etc.).

The syntax of metasentences discussed above only applies to declarative metasentences. We will only use imperative/interrogative metasentences in the exercises or some metaproofs (the latter sharing a lot with computer programs); these other types of metasentences require additional syntactic rules which are clear and we will not make explicit here.

**Exercise 2.10.** Consider the following utterances and explain how they can be viewed as metasentences; explain the syntactic structure and semantics of those metasentences.

1) To be or not to be, that is the question.
2) I do not make hypotheses.
3) The sentence labelled 3 is false.

1 is, of course, from Shakespeare. 2 is from Newton. 3 is, of course, the liar’s “paradox”.

**FROM NOW ON WE MAKE THE FOLLOWING CONVENTION:** IN ANY DISCUSSION ABOUT LANGUAGES WE ASSUME WE HAVE FIXED AN OBJECT LANGUAGE AND A METALANGUAGE; THE OBJECT LANGUAGE WILL SIMPLY BE REFERRED TO AS A “LANGUAGE” (SO THE WORD “OBJECT” WILL SYSTEMATICALLY BE DROPPED).
CHAPTER 3

Syntax

We already superficially mentioned syntax. In this chapter we discuss, in some detail, the syntax of languages. (The syntax of metalanguages will be not explicitly addressed but should be viewed as similar.) All the explanations below are, of course, written in metalanguage.

As we saw a language is a collection $L$ of symbols. Given $L$ we considered the collection $L^*$ of all strings of symbols in $L$. In this chapter we explain the definition of sentences (which will be certain special strings in $L^*$). Being a sentence will involve, in particular, a certain concept of “syntactic correctness”. The kind of syntactic correctness discussed below makes $L$ a first order language. There are other types of languages whose syntax is different (e.g. second order languages, in which one is allowed to say, for instance, “for any relational predicate etc....”); or languages whose syntax is based on grammatical categories rather than logical categories; or computer languages, not discussed in this course at all). First order languages are the most natural (and are entirely sufficient) for developing mathematics.

In what follows we let $L$ be a collection of symbols consisting of variables $x, y, ...$, constants, functional symbols, relational predicates, connectives $\land, \lor, \neg, \rightarrow, \leftrightarrow$ (where $\neg$ is unary and the rest are binary), quantifiers $\forall, \exists$, equality $=$, and, as separators, parentheses $(, )$, and commas. (For simplicity we considered 5 “standard” connectives, 2 “standard” quantifiers, and a “standard” symbol for equality; this is because most examples will be like that. However any number of connectives and quantifiers, and any symbols for them would do. In particular some of these categories of symbols may be missing.) According to our conventions recall that we will also fix a metalanguage $\hat{L}$ in which we can “talk about” $L$.

Example 3.1. If $L$ has constants $a, b, ...$, a functional symbol $f$, and a relational predicate $\Box$ then here are examples of strings in $L^*$:

1) $(x\forall\exists aby(\rightarrow$
2) $f(f(a))$
3) $\exists y((a\Box x) \rightarrow (a\Box y))$
4) $\forall x(\exists y((a\Box x) \rightarrow (a\Box y)))$

In what follows we will define terms, formulas and sentences; 1 above will not be a term, a formula, or a sentence; 2 will be a term; 3 will be a formula but not a sentence; 4 will be a sentence.

The metadefinition below introduces the new words term formation into metalanguage.

Metadefinition 3.2. A term formation is a string $t$
...  
\[ s \]  
...  
\[ u \]
of strings in \( L^* \) such that for any string \( s \) of symbols in the string of strings above (including \( t \) and \( u \)) one of the following holds:

1) \( s \) is a constant or a variable;
2) \( s \) is preceded by \( s', s'' \), ... such that \( s \) equals \( f(s', s'', ...) \) where \( f \) is a functional symbol.

**Metadefinition 3.3.** A term is a string \( u \) for which there is a term formation ending with \( u \).

**Remark 3.4.** Functional symbols may be unary \( f(t) \), binary \( f(t, s) \), ternary \( f(t, s, u) \), etc. When we write \( f(t, s) \) we simply mean a string of 5 symbols:

\[ "f", \"(\", \"t\", \",\", \"s\", \")" \]

**Example 3.5.** If \( a, b, ... \) are constants, \( x, y, ... \) are variables, \( f \) is a unary functional symbol and \( g \) is a a binary functional symbol, all of them in \( L \), then

\[ f(g(f(b), g(x, g(x, y)))) \]
is a term; a term formation for it is

\[ b \]
\[ x \]
\[ y \]
\[ f(b) \]
\[ g(x, y) \]
\[ g(x, g(x, y)) \]
\[ g(f(b), g(x, g(x, y))) \]
\[ f(g(f(b), g(x, g(x, y)))) \]

The latter should be simply viewed, again, as a string of symbols; there is no “substitution” involved here. Substitution will play a role later, though; cf. 3.16.

**Remark 3.6.** If \( t, s, \ldots \) are terms and \( f \) is a functional symbol then \( f(t, s, \ldots) \) is a term. The latter is a metasentence; if it is viewed as involving quantifiers applied to variables \( t, s, \ldots \) then this metasentence cannot be metaproved. If however one views \( t, s, \ldots \) as constants in the metalanguage then a metaproof that \( f(t, s, \ldots) \) is a term can be done by “showing” as follows. If \( t, s, \ldots \) are terms then we have term formations

\[ t' \]
\[ t'' \]
...  
\[ t \]

and

\[ s' \]
\[ s'' \]
...  
\[ s \]
Hence we can write a term formation
\[ t' \]
\[ t'' \]
\[ ... \]
\[ t \]
\[ s' \]
\[ s'' \]
\[ ... \]
\[ s \]
\[ f(t, s, ...) \]

Hence \( f(t, s, ...) \) is a term.

**Metadefinition 3.7.** A formula formation is a string
\[ P \]
\[ ... \]
\[ Q \]
\[ ... \]
\[ R \]
of strings in \( L^* \) such that for any string of symbols \( Q \) in the string of strings above (including \( P \) and \( R \)) one of the following holds:
1) \( Q \) equals \( t = s \) where \( t, s \) are terms;
2) \( Q \) equals \( \rho(t, s, ...) \) where \( t, s, ... \) are terms and \( \rho \) is a relational predicate.
3) \( Q \) is preceded by \( Q', Q'' \) and \( Q \) equals \( Q' \land Q'', Q' \lor Q'', \neg Q', Q' \rightarrow Q'', Q' \leftrightarrow Q'' \).
4) \( Q \) equals \( \forall x Q' \) or \( \exists x Q' \) where \( Q' \) precedes \( Q \).

Recall our convention that if we have a different number of symbols (written differently) we make similar metadefinitions for them; in particular some of the symbols may be missing altogether. E.g. if quantifiers are missing from \( L \) then we ignore 4. If equality is missing from \( L \) we ignore 1.

**Metadefinition 3.8.** A string \( R \) in \( L^* \) is called a formula if there is a formula formation that ends with \( R \). We denote by \( L_f \) the collection of all formulas in \( L^* \).

**Remark 3.9.** Relational predicates can be unary \( \rho(t) \), binary \( \rho(t, s) \), ternary \( \rho(t, s, u) \), etc. Again, \( \rho(t, s) \) simply means a string of 5 symbols \( \rho, (, t, s, ) \) and nothing else. Sometimes one uses another syntax for relational predicates: instead of \( \rho(t, s) \) one writes \( tps \) or \( pts \); instead of \( \rho(t, s, u) \) one may write \( ptsu \), etc. All of this is in the language \( L \). On the other hand if some variables \( x, y, ... \) appear in a formula \( P \) we sometimes write in metalanguage \( P(x, y, ...) \) instead of \( P \). In particular if \( x \) appears in \( P \) (there may be other variables in \( P \) as well) we sometimes write \( P(x) \) instead of \( P \). Formulas of the form (i.e. which are equal to one of) \( \forall x P \), \( \forall x P(x) \) are referred to as universal formulas. Formulas of the form \( \exists x P \), \( \exists x P(x) \) are referred to as existential formulas. Formulas of the form \( P \rightarrow Q \) are referred to as conditional formulas. Formulas of the form \( P \leftrightarrow Q \) are referred to as biconditional formulas.

**Exercise 3.10.** Give a metaproof of the following:
1) if \( P \) and \( Q \) are formulas then \( P \land Q, P \lor Q, \neg P, P \rightarrow Q, P \leftrightarrow Q \) are formulas.
2) if \( P \) is a formula then \( \forall x P \) and \( \exists x P \) are formulas.
(In the above metasentences $P,Q$ are thought of constants in metalanguage; if the above metasentences were viewed as involving quantifiers then they could not be metaproofed.)

**Example 3.11.** Assume $L$ contains a constant $c$, a unary relational predicate $\rho$, and a unary functional symbol $f$. Then the following is a formula:

$$\forall x(f(x) = c) \rightarrow (\rho(f(x)))$$

A formula formation for it is:

$$f(x) = c$$
$$\rho(f(x))$$
$$\forall x(f(x) = c)$$
$$\forall x(f(x) = c) \rightarrow (\rho(f(x)))$$

**Metadefinition 3.12.** We define the free occurrences of a variable $x$ in a formula by the following conditions:

1) The free occurrences of $x$ in a formula of the form $t = s$ are all the occurrences of $x$ in $t$ together with all the occurrences of $x$ in $s$;

2) The free occurrences of $x$ in a formula $\rho(t,s,...)$ are all the occurrences of $x$ in $t$, together with all the occurrences of $x$ in $s$, etc.

3) The free occurrences of $x$ in $P \land Q, P \lor Q, P \rightarrow Q, P \leftrightarrow Q$ are the free occurrences of $x$ in $P$ together with the free occurrences of $x$ in $Q$. The free occurrences of $x$ in $\neg P$ are the free occurrences of $x$ in $P$.

4) No occurrence of $x$ in $\forall x P$ or $\exists x P$ is free.

**Example 3.13.** A variable $x$ is free in a formula $P$ if it has at least one free occurrence in $P$.

**Example 3.14.**

1) $x$ is not free in $\forall y \exists x(\rho(x,y))$.

2) $x$ is free in $(\exists x(\beta(x))) \lor \rho(x,a)$. ($x$ has a “free occurrence” in $\rho(x,a)$; the “occurrence” of $x$ in $\exists x(\beta(x))$ is not “free”.)

3) $x$ is not free in $\forall x((\exists x(\beta(x))) \lor \rho(x,a))$.

4) The free variables in $(\forall x \exists y(\alpha(x,y,z))) \land \forall u(\beta(u,y))$ are $z,y$.

**Metadefinition 3.15.** A string in $L^*$ is called a sentence if it is a formula (i.e. is in $L^\uparrow$) and has no free variables. Note that

1) $L^*$ is contained in $L^\uparrow$;

2) $L^\uparrow$ is contained in $L^*$;

3) all terms are in $L^*$; no term is in $L^\uparrow$.

**Metadefinition 3.16.** If $x$ is a free variable in a formula $P$ one can replace all its free occurrences with a term $t$ to get a formula which can be denoted by $P^t_x$. More generally if $x,y,...$ are variables and $t,s,...$ are terms we may replace all free occurrences of these variables by $t,s,...$ to get a formula $P^t_s_{xy...}$. A more suggestive (but less precise) notation is as follows. We write $P(x)$ instead of $P^x_x$. More generally we write $P(t,s,...)$ instead of $P^t_s_{xy...}$. We will constantly use this $P(t), P(t,s,...)$, etc. notation from now on.

Similarly if $u$ is a term containing $x$ and $t$ is another term then one may replace all occurrences of $x$ in $u$ by $t$ to get a term which we may denote by $u^t_x$; if we write $u(x)$ instead of $u$ then we can write $u(t)$ instead of $u^t_x$. And similarly we may replace two variables $x,y$ in a term $u$ by two terms $t,s$ to get a term $u^t_s_{xy}$, etc. We will not make use of this latter type of substitution in what follows.
EXAMPLE 3.17. If \( P \) equals “\( x \) is a man” then \( x \) is a free variable in \( P \). If \( a \) equals “Socrates” then \( P(a) \) equals “Socrates is a man”.

EXAMPLE 3.18. If \( P \) equals “\( x \) is a man and for all \( x \), \( x \) is mortal” then \( x \) is a free variable in \( P \). If \( a \) equals “Socrates” then \( P(a) \) equals “Socrates is a man and for all \( x \), \( x \) is mortal”.

EXERCISE 3.19. Is \( x \) a free variable in the following formulas?

1) \( (\forall y \exists x(x^2 = y^3)) \land (x \text{ is a man}) \)
2) \( (\forall y(x^2 = y^3)) \)

Here the upper indexes 2 and 3 are unary functional symbols.

EXERCISE 3.20. Compute \( P(t) \) if:

1) \( P(x) \) equals “\( \exists y(y^2 = x) \)” and \( t \) equals “\( x^4 \)”.
2) \( P(x) \) equals “\( \exists y(y \text{ poisoned } x) \)” and \( t \) equals “Plato’s teacher”.

The following metadefinition makes the concept of definition in \( L \) more precise:

METADEFINITION 3.21. A definition in \( L \) is a sentence of one of the following types:

1) \( c = t \) where \( c \) is a constant and \( t \) is a term without variables.
2) \( \forall x(\epsilon(x) \leftrightarrow E(x)) \)” where \( \epsilon \) is a unary relational predicate and \( E \) is a formula with one free variable. More generally for several variables, \( \forall x \forall y(\epsilon(x,y) \leftrightarrow E(x,y)) \)” is a definition, etc.
3) \( \forall x \forall y(y = f(x)) \leftrightarrow F(x,y)) \)” where \( f \) is a unary functional predicate and \( F \) is a formula with 2 free variables; more generally one allows several variables.

If any type of symbols is missing from the language we disallow, of course, the corresponding definitions.

A language together with a collection of definitions is referred to as a language with definitions.

A definition as in 1 should be viewed as either a definition of \( c \) (in which case it is called notation) or a definition of \( t \). A definition as in 2 should be viewed as a definition of \( \epsilon \). A definition as in 3 should be viewed as a definition of \( f \).

REMARK 3.22. Given a language \( L \) with definitions and a term \( t \) without variables one can add to the language a new constant \( c \) and one can add to the definitions the definition \( c = t \). We will say that \( c \) is (a new constant) defined by \( c = t \).

Similarly given a language \( L \) with definitions and a formula \( E(x) \) in \( L \) with one free variable \( x \) one can add to the relational predicates of \( L \) a new unary relational predicate \( \epsilon \) and one can add to the definitions the definition \( \forall x(\epsilon(x) \leftrightarrow E(x)) \). We will say that \( \epsilon \) is (a new relational predicate) defined by \( \forall x(\epsilon(x) \leftrightarrow E(x)) \).

One may introduce new functional symbols \( f \) by adding a symbol \( f \) and definitions of type 3 or of type 1 (such as \( c = f(a,b,...) \), for various constants \( a,b,c,... \)).

REMARK 3.23. In Remark 1.14 we discussed grammatical (as opposed to logical) categories/analysis of sentences in natural languages such as English. There is a syntax associated to that point of view as well. (If we call logical syntax the syntax discussed before this point in this chapter then what follows in this remark could be referred to as grammatical syntax.) Grammatical syntax proceeds as follows. One introduces grammatical categories such as: nouns (N), verbs (V), adjectives (A), prepositions (P), determinators (D), etc., and lists of words in each
grammatical category. Then one defines a noun phrase (NP) as a noun possibly preceded by adjectives and a determinator and possibly followed by a prepositional phrase (PP); one defines propositional phrases, verb phrases, etc. in a similar way. This scheme can be formalized (and needs to be appropriately modified using the so-called bar construction, etc.) What results is a very general theory (due to Chomsky) applicable to virtually all natural languages, not only to English. This kind of grammatical syntax differs from the logical syntax explained before this remark and is not appropriate for introducing mathematics; therefore we will not pursue this grammatical syntax further.
We already superficially mentioned semantics. In this chapter we discuss, in some detail, the semantics of languages. Semantics is the analysis of meaning and meaning comes, for us, mainly from translation. Recall:

**Metadefinition 4.1.** Let $L$ and $L'$ be two languages. By a translation of $L$ in $L'$ we understand a rule that attaches to any symbol $X$ in $L$ a symbol $X'$ in $L'$. We say that in our translation $X$ is translated as $X'$ or that $X$ is mapped into $X'$. We assume the rule “respects” the 8 types of symbols i.e. attaches variables to variables, constants to constants, functional symbols to functional symbols, etc.

**Remark 4.2.** By syntactic correctness it is intuitively clear that for any formula $P$ in $L$ if one replaces the symbols $X$ in $P$ by the symbols $X'$ one obtains a formula $P'$ in $L'$. And the same with sentences in place of formulas. We cannot prove this (because we would need induction to prove it but again we do not even know what proofs are at this point). We say that $P$ is translated (or mapped) into $P'$ or that $P'$ is the translation of $P$.

One sometimes needs more flexible notions of translation of formulas. Here is such a more flexible notion. (This concept will not play a role until near the end of the course.)

**Metadefinition 4.3.** Assume $D(x)$ is a formula in $L'$ with one free variable $x$ (which we refer as a “domain”). Assume we are given a translation of $L$ into $L'$. Replacing all constants and functional symbols $X$ in $L$ by the corresponding symbols $X'$ in $L'$ we get a way to attach to any term $t$ in $L$ a term $t'$ in $L'$. We define $D$-translation of formulas in $L$ into formulas in $L'$ by the following rules:

1) The translation $(t = s)'$ of $t = s$ is $t' = s'$;
2) The translation $(\rho(t, s, ...))'$ of $\rho(t, s, ...)$ is $\rho'(t', s', ...)$.
3) If $P', Q'$ are translations of formulae $P, Q$ in $L$ then the translation of $P \land Q$, $P \lor Q$, $\neg P$, $P \rightarrow Q$, $P \leftrightarrow Q$ are $P' \land Q'$, $P' \lor Q'$, $\neg P'$, $P' \rightarrow Q'$, $P' \leftrightarrow Q'$.
4) If $P(x)$ is a formula in $L$ with one free variable $x$ with translation $P'(x)$ then the translation $(\forall x P(x))'$ of $\forall x P(x)$ is $\forall x (D(x) \rightarrow P'(x))$ and the translation $(\exists x P(x))'$ of $\exists x P(x)$ is $\exists x (D(x) \land P'(x))$.

This $D$-translation intuitively asks that the translated sentences “always refer” to things that have “property” (or “domain”) $D$.

**Remark 4.4.** There are even more flexible notions of translations. Some of these are obtained by going from one given language “down to a deeper” language via a “vertical” correspondence and then “up to” a third language via yet another “vertical” correspondence, such that the resulting “composition” is a “horizontal” correspondence. One such example occurs when one uses natural languages: one...
goes from a surface structure English to a deep structure English which may essentially coincide with a deep structure French, and one then goes back from the latter to a surface structure French. Such a translation is far from being a word for word translation. Another example will occur later when we discuss proofs; we will then use a “vertical” conversion of text from an object language $L$ into a text in a metalanguage $\hat{L}$ followed by another “vertical” conversion (called disquotation) of the text in $\hat{L}$ back into a different object language $L_{\text{argot}}$; this will produce a “horizontal” correspondence (still referred to as translation) from $L$ into $L_{\text{argot}}$: we don’t need to explain this at this point.

Remark 4.5. Translations as above are precursors of the maps to be encountered later in set theory. But we do not view them as maps. Translations as above can be called metamaps; they should be thought of as concrete objects like dictionaries, tables, or picture books designed to teach foreign languages. Or as (infinite!) tables such as

<table>
<thead>
<tr>
<th>$P$</th>
<th>$P'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q$</td>
<td>$Q'$</td>
</tr>
</tbody>
</table>
| ... | ...

Remark 4.6. If $L$ is any language with connectives $\land, \lor, \neg, \to, \leftrightarrow$, quantifiers $\forall, \exists$, and equality $=$ then the “standard translation” of $L$ into the English language is the one specified in Example 1.1; e.g. $\forall, \exists$ is translated as “for all, there exists” etc. Sometimes, if we translate a language $L$ in English and we want the translation to say that all variables in $L$ refer to something specific in English (say to crocodiles) we use a translation where

- $\forall$ is translated as “for all crocodiles”,
- $\exists$ is translated as “there exists a crocodile”.

Later we will use “sets, rings”, etc. instead of “crocodiles”.

Example 4.7. If $L'$ and $L$ are English and Formal (cf. Example 1.1) then, as explained in that Example, there is a translation of $L$ into $L'$ such that the sentences 1, ..., 5 in $L$ are mapped into the sentences 1, ..., 5 in $L'$ respectively.

Exercise 4.8. Assume

- $P$ equals “$\forall x ((x > 0) \to (\exists y \exists z \exists u \exists v (x = y^2 + z^2 + u^2 + v^2))$”
- $P'$ equals “any positive integer is a sum of four squares”

Find languages $L$ and $L'$ for the sentences $P$ and $P'$ above and find a translation of $L$ into $L'$ such that $P$ is mapped into $P'$. Hint: We do not need to know at this point what integers are so we need a constant to denote the collection of integers and a predicate that stands for “belongs”. By the way this sentence turns out to be a theorem of Lagrange.

Exercise 4.9. Assume

- $P$ equals “($K(O) \land (\forall x (K(x) \to (x = O)))$”
- $P'$ equals “Oswald shot Kennedy and was the only person who shot Kennedy”

Find languages $L$ and $L'$ for the sentences $P$ and $P'$ above and find a translation of $L$ into $L'$ such that $P$ is sent into $P'$.

Metadefinition 4.10. Let $L'$ be the English language and $P'$ be a sentence in English. By a formalization of $P'$ we mean a sentence $P$ in a language $L$ and
a translation of $L$ into $L'$ such that $P$ is mapped into $P'$, the variables, constants, and predicates of $L$ are denoted by single marks on paper, and the connectives, quantifiers, and equality of $L$ are $\land, \lor, \neg, \to, \leftrightarrow, \forall, \exists, =$.

**Example 4.11.** In Example 1.1 the sentences $1',...,5'$ are formalizations of the sentences $1,...,5$.

**Exercise 4.12.** Find formalizations of the following English sentences:
2. “There is no hope for those who enter this realm.”
3. “There is nobody there.”
4. “There were exactly two people in that garden.”

**Exercise 4.13.** Find formalizations of the following English sentences:
1) “The movement of celestial bodies is not produced by angels pushing the bodies in the direction of the movement but by angels pushing the bodies in a direction perpendicular to the movement”
2) “I think therefore I am”
3) “Since existence is a quality and since a perfect being would not be perfect if it lacked one quality it follows that a perfect being must exists.”
4) “Since some things move and everything that moves is moved by a mover and an infinite regress of movers is impossible it follows that there is an unmoved mover”

Hints: “but” should be thought of as “and”; “therefore” should be thought of “implies” and hence as “if...then”; “since...it follows” should be thought of, again, as “implies”.

**Remark 4.14.** The sentence 1 above paraphrases a statement in one of Feynman’s lectures on gravity. The sentence 2 is, of course Decartes’ “cogito ergo sum”. The sentence 3 is a version of the “ontological argument” (cf. Anselm, Descartes, Leibniz, Gödel for versions of this; also cf. Aquinas and Kant for refutations of this). The sentence 4 is a version of the “cosmological argument” (cf. Aquinas).
CHAPTER 5

Witnesses

Let $L$ be a language possessing quantifiers $\forall, \exists$ (but not necessarily connectives or equality).

**Metadefinition 5.1.** A witness assignment on $L$ is a rule that attaches to any formula $P$ with exactly one free variable $x$ two constants $c_P$ and $c'_P$. The constant $c_P$ is called the witness for the sentence $\forall x P(x)$; $c'_P$ is called the witness for the sentence $\exists x P(x)$. If a witness assignment was fixed in $L$ we also say $L$ is a language with witnesses.

**Example 5.2.** The symbols $c_P$, $c'_P$ are, of course, constants (or variables) in metalanguage. Symbols such as $c_{x=a}, c_{x\square a}, c_{\forall y((y=b)\lor(y\square x))}$ are constants in a language if the language contains $x, y, =, \square, a, b$.

**Remark 5.3.** The witness terminology (and usefulness) will become clear later. But it is worth keeping in mind the following illustration of this concept. Assume that $\forall, \exists$ are translated in English as "for all elephants" and "there exists an elephant" and assume that $P(x)$ is translated as "$x$ is blue". Then $c_P$ should be translated as "the least blue elephant"; $c'_P$ should be translated as "the most blue elephant". We will see later how this works in proof theory.

**Metadefinition 5.4.** Given a language $L_0$ there is a canonical way to construct a language with witnesses, $L$, starting from $L_0$. Indeed one first adds to $L_0$ two new constants $c_P$ and $c'_P$ for each formula $P$ in $L_0'$ with exactly one free variable. (Each $c_P$ is viewed as a new symbol; and the same with $c'_P$.) Call $L_1$ the enlarged collection of symbols. (Note that in case $L_0$ is a language with definitions we DO NOT add to the definitions of $L_0$ any new definitions for the new constants!) Then repeat this construction with $L_1$ in place of $L_0$; we get a new set of symbols $L_2$. We continue this "indefinitely". Then we set $L$ the collection of all symbols in $L_0, L_1, L_2, ...$. Then clearly $L$ has a natural witness assignment. We call $L$ the witness closure of $L_0$.

**Example 5.5.** Let $L_0$ be the language with variables $x, y, z, ...$, no constants, no functional symbols, one binary relational predicate $\in$, connectives $\land, \lor, \neg, \rightarrow, \leftrightarrow$, quantifiers $\forall, \exists$, equality $=$, and typographical symbols $(, )$. Let $L$ be the witness closure of $L_0$. (This will play a role later when we introduce set theory.) Here are examples of constants in $L$:

- $c_{\exists y(x\in y)}$, $c_{\exists y(x\in y)}$
- $c_{x\in c_{\exists y(x\in y)}}$, $c_{x\in c_{\exists y(x\in y)}}$

The first row belongs to $L_1$, the second to $L_2$, etc.
Exercise 5.6. Write examples of sets belonging to $L_3$ and $L_4$.

Metadefinition 5.7. Let $P(x,y)$ be a formula with free variables $x,y$ and let $Q(x)$ equal $\forall y P(x,y)$. If $c'$ is the witness for $\exists x Q(x)$ and $c''$ is the witness for $\forall y P(c',y)$ then we say that $c', c''$ are the witnesses for $\exists x \forall y P(x,y)$. One gives a similar redefinition for witnesses $c', c'', c''', ...$ for sentences $\exists x \exists y \forall z(...)$, etc.

Example 5.8. Explicitly if $P(x,y)$ is a formula with free variables $x,y$ the witnesses $c', c''$ for $\exists x \forall y P(x,y)$ are given by:

$\forall y P(x,y)$, $c' P(x,y)$

Remark 5.9. If we deal with languages with witnesses we will always tacitly assume that all translations are compatible (in the obvious sense) with the witness assignments. Compatibility can be typically achieved as follows: if one is given a translation of a language $L_0$ into a language $L'_0$ then this translation can be extended uniquely to a translation, compatible with witness assignments, of the witness closure $L$ of $L_0$ into the witness closure $L'$ of $L'_0$.

Remark 5.10. There is a chapter of philosophy that deals with existence; it is called ontology. The philosophical analysis of existence is a highly difficult task; when we say in philosophy that something exists one immediately asks: where does this exist? in the physical world? in our imagination? in the realm of possibilities? how can one ascertain existence? etc. The concept of witness will later give a sweeping trivial answer to existence that is completely syntactical: we have created (or postulated) in the discussion above a constant $c^P$ for each possible formula $P(x)$ with exactly one free variable $x$; this constant will be viewed later as the “answer to the existence problem for objects with property $P$”. For instance the various sets of mathematics (such as unions, products, power sets, etc.) will be later defined as witnesses for various corresponding sentences. We will not have to ask (with Cantor’s critics) where do these sets exist. These sets will simply be constants indexed by formulas, hence they will exist as symbols written on paper. Ontology will be entirely replaced by syntax.
CHAPTER 6

Tautologies

We start now the analysis of inference within a given language (which is also referred to as deduction or proof). In order to introduce the general notion of proof we need to first introduce tautologies; in their turn tautologies are introduced via certain planar symbols in metalanguage called tables.

**Metadefinition 6.1.** Recall that $T$ and $F$ are two symbols in metalanguage. Recall also that we have separators in metalanguage that are frames of tables. Using the above plus arbitrary constants (or variables) $P$ and $Q$ in metalanguage we introduce the following strings of symbols in metalanguage (which are actually planar configurations rather than linear configurations but which can obviously be rearranged in the form of strings). They are referred to as the truth tables of the 5 standard connectives.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \land Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \lor Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \rightarrow Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \leftrightarrow Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$\neg P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

**Remark 6.2.** If in the tables above $P$ is the sentence “$p...$” and $Q$ is the sentence “$q...$” we allow ourselves, as usual, to identify the symbols $P, Q, P \land Q$, etc. with the corresponding sentences “$p...$$, “q...$$, “(p...\land(q...$$, etc. Also: the letters $T$ and $F$ evoke “truth” and “falsehood”; but they should be viewed as devoid of any meaning.

Fix in what follows a language $L$ that has the 5 standard connectives $\land, \lor, \neg, \rightarrow, \leftrightarrow$ (but does not necessarily have quantifiers or equality).

**Metadefinition 6.3.** Let $P, Q, ..., R$ be sentences in $L$. By a Boolean string generated by $P, Q, ..., R$ we mean a string of sentences

$P$
$Q$

...  
$R$
$U$

...
such that for any sentence $V$ among $U,...,W$ we have that $V$ is preceded by $V', V''$ (with $V', V''$ among $P,...,W$) and $V$ equals one of the following:

$$V' \land V'', V' \lor V'', \neg V', V' \rightarrow V'', V' \leftrightarrow V''$$

**Example 6.4.** The following is a Boolean string generated by $P, Q, R$:

- $P$
- $Q$
- $R$
- $\neg R$
- $Q \lor \neg R$
- $P \rightarrow (Q \lor \neg R)$
- $P \land R$
- $(P \land R) \leftrightarrow (P \rightarrow (Q \lor \neg R))$

**Example 6.5.** The following is a Boolean string generated by $P \rightarrow (Q \lor \neg R)$ and $P \land R$:

- $P \rightarrow (Q \lor \neg R)$
- $P \land R$
- $(P \land R) \leftrightarrow (P \rightarrow (Q \lor \neg R))$

**Remark 6.6.** The same sentence may appear as the last sentence in two different Boolean strings; cf. the last 2 examples.

**Metadefinition 6.7.** Assume we are given a Boolean string generated by $P, Q, ..., R$. For simplicity assume it is generated by $P, Q, R$. (When more or less than 3 generators the metadefinition is similar.) The truth table attached to this Boolean string and to the fixed system of generators $P, Q, R$ is the following string of symbols (or rather plane configuration of symbols thought of as reduced to a string of symbols):

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$R$</th>
<th>$U$</th>
<th>$V$</th>
<th>$W$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Note that the 3 columns of the generators consist of all 8 possible combinations of $T$ and $F$. The dotted columns correspond to the sentences other than the generators and are computed by the following rule. Assume $V$ is not one of the generators $P, Q, R$ and assume that all columns to the left of the column of $V$ were computed; also assume that $V$ is obtained from $V'$ and $V''$ via some connective $\land, \lor, ...$. Then the column of $V$ is obtained from the columns of $V'$ and $V''$ using the tables of the corresponding connective $\land, \lor, ...$ respectively.
The above rule should be viewed as a syntactic rule for metalanguage; we did not introduce the syntax of metalanguage systematically but the above is one instance when we are quite precise about it.

**Example 6.8.** Consider the following Boolean string generated by \( P \) and \( Q \):

\[
P \\
Q \\
\neg P \\
\neg P \land Q
\]

Its truth table is:

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( \neg P )</th>
<th>( \neg P \land Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Note that the generators \( P \) and \( Q \) are morally considered “independent” (in the sense that all 4 possible combinations of \( T \) and \( F \) are being considered for them); this is in spite of the fact that actually \( P \) and \( Q \) maybe, for instance \( a = b \) and \( \neg (a = b) \) respectively.

**Metadefinition 6.9.** A sentence \( S \) is a tautology if one can find a Boolean string generated by some sentences \( P, Q, ..., R \) such that

1) The last sentence in the string is \( S \)
2) The truth table attached to the string and the generators \( P, Q, ..., R \) has only \( T \)s in the \( S \) column.

**Remark 6.10.** We do not ask, in the metadefinition above, that for any Boolean string ending in \( S \) and for any generators the last column of the truth table have only \( T \)s; we only ask this to hold for one Boolean string and one system of generators.

**Example 6.11.** \( P \lor \neg P \) is a tautology. To metaprove this consider the Boolean string generated by \( P \),

\[
P \\
\neg P \\
P \lor \neg P
\]

Its truth table is (check!):

<table>
<thead>
<tr>
<th>( P )</th>
<th>( \neg P )</th>
<th>( P \lor \neg P )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

This ends out metaproof of the metasentence \( P \lor \neg P \) is a tautology.

Remark that if we view the same Boolean string

\[
P \\
\neg P \\
P \lor \neg P
\]

as a Boolean string generated by \( P \) and \( \neg P \) the corresponding truth table is
and the last column in the latter table does not consist of $T$s only. This does not change the fact that $P \lor \neg P$ is a tautology. Morally, in this latter computation we had to treat $P$ and $\neg P$ as “independent”; this is not a mistake but rather a poor choice in trying to prove that $P \lor \neg P$ is a tautology.

Example 6.12. $(P \land (P \to Q)) \to Q$ is a tautology; it is called *modus ponens*. To metaprove this consider the following Boolean string generated by $P, Q, R$:

- $P$
- $Q$
- $P \to Q$
- $P \land (P \to Q)$
- $(P \land (P \to Q)) \to Q$

Its truth table is:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \to Q$</th>
<th>$P \land (P \to Q)$</th>
<th>$T$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Exercise 6.13. Explain how the table above was computed.

Exercise 6.14. Give a metaproof of the fact that each of the sentences below is a tautology:
1) $(P \to Q) \leftrightarrow (\neg P \lor Q)$
2) $(P \leftrightarrow Q) \leftrightarrow ((P \to Q) \land (Q \to P))$

Exercise 6.15. Give a metaproof of the fact that each of the sentences below is a tautology:
1) $(P \land Q) \to P$
2) $P \to (P \lor Q)$
3) $((P \land Q) \land R) \leftrightarrow (P \land (Q \land R))$
4) $(P \land Q) \leftrightarrow (Q \land P)$
5) $(P \land (Q \lor R)) \leftrightarrow ((P \land Q) \lor (P \land R))$
6) $(P \lor (Q \land R)) \leftrightarrow ((P \lor Q) \land (P \lor R))$

Metadefinition 6.16.
1) $Q \to P$ is called the converse of $P \to Q$
2) $\neg Q \to \neg P$ is called the contrapositive of $P \to Q$

Exercise 6.17. Give a metaproof of the fact that each of the sentences below is a tautology:
1) $((P \lor Q) \land (\neg P)) \to Q$ (modus ponens, variant)
2) $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ (contrapositive argument)
3) $(\neg(P \land Q)) \leftrightarrow (\neg P \lor \neg Q)$ (de Morgan law)
4) $(\neg(P \lor Q)) \leftrightarrow (\neg P \land \neg Q)$ (de Morgan law)
5) \(((P \rightarrow R) \land (Q \rightarrow R)) \rightarrow ((P \lor Q) \rightarrow R)\) (case by case argument).
6) \((\neg(P \rightarrow Q)) \iff (P \land \neg Q)\) (negation of an implication)
7) \((\neg(P \leftrightarrow Q)) \iff ((P \land \neg Q) \lor (Q \land \neg P))\) (negation of an equivalence)

REMARK 6.18. 2) in Exercise 6.17 says that the contrapositive of an implication is equivalent to the original implication.

EXERCISE 6.19. (VERY IMPORTANT) Give a metaproof of the fact that the sentence

\[(P \rightarrow Q) \iff (Q \rightarrow P)\]

is not a tautology. In other words the converse of an implication is not equivalent to the original implication. “If c a human then c mortal” is not equivalent to “If c is mortal then c is a human”.

METARDEFINITION 6.20. A sentence \(P\) is a contradiction if \(\neg P\) is a tautology.

EXERCISE 6.21. Give a metaproof of the fact that for any \(P\) the sentence \(P \lor \neg P\) is a tautology and the sentence \(P \land \neg P\) is a contradiction.

EXERCISE 6.22. Formalize the following English sentences, negate their formalization, and give the English translation of these formalized negations:
1) If Plato eats this nut then Plato is a bird.
2) Plato is a bird if and only if he eats this nut.
CHAPTER 7

Theories

Recall that for a language $L$ equipped with the 5 standard connectives we defined a collection of sentences in $L$ called tautologies; cf. 6.9. In what follows (essentially throughout the course) we assume that $L$ is a language equipped with the 5 standard connectives $\land, \lor, \neg, \to, \leftrightarrow$, quantifiers $\forall, \exists$, and equality $=$ and we assume $L$ has definitions and witnesses.

**Metadefinition 7.1.** A quantifier axiom is a sentence of one of the following forms. In what follows $P$ runs through all the formulas $P(x)$ with a free variable $x$ and $t$ runs through the terms without variables.

\[
\begin{align*}
    P(c_P) & \to (\forall x P(x)) \\
    (\forall x P(x)) & \to P(t) \\
    P(t) & \to (\exists x P(x)) \\
    (\exists x P(x)) & \to P(c_P) \\
\end{align*}
\]

One can write the above sentences in the form:

\[
\begin{align*}
    P(c_P) & \to (\forall x P(x)) \to P(t) \to (\exists x P(x)) \to P(c_P)
\end{align*}
\]

**Remark 7.2.** To understand the intuitive content of the quantifier axioms involving witnesses let us look again at an example considered earlier. So assume that $\forall, \exists$ are translated in English as “for all elephants” and “there exists an elephant” and assume that $P(x)$ is translated as “$x$ is blue”. Let $c_P$ be translated as “the least blue elephant” and let $c_P$ be translated as “the most blue elephant”. Then the axiom $P(c_P) \to (\forall x P(x))$ is translated as “if the least blue elephant is blue then all elephants are blue”. Also the axiom $\exists x P(x) \to P(c_P)$ is translated as “if there exists a blue elephant then the most blue elephant is blue”. These translations are reasonable and could be kept in the back of our minds when dealing with witnesses; but the correct way to think about witnesses is to completely forget about their translation into natural languages.

**Metadefinition 7.3.** An equality axiom is a sentence of one of the following forms. In what follows $t, s, u$ run through all $(n$-tuples of) without variables, $f$ runs through all $n$-ary functional symbols, and $P(x)$ runs through all formulas with free $(n$-tuples of) variables $x$.

\[
\begin{align*}
    t & = t \\
    (t = s) & \leftrightarrow (s = t) \\
    ((t = s) \land (s = u)) & \to (t = u) \\
    (t = s) & \to (f(t) = f(s)) \\
    (t = s) & \to (P(t) \leftrightarrow P(s)) \\
\end{align*}
\]

It is convenient to collect some of the mdefinitions above into one mdefinition:
Metadefinition 7.4. Let $L$ be a language with definitions and witnesses. By a background axiom we understand a sentence which is either a tautology, or a definition, or a quantifier axiom, or an equality axiom.

Metadefinition 7.5. A collection $T$ of sentences in $L$ is a theory if and only if it satisfies the following conditions:

1) $T$ contains all background axioms;
2') (Closure under conjunction) If $P, Q$ are in $T$ then $P \land Q$ is in $T$;
2") (Closure under modus ponens) If $P$ and $P \rightarrow Q$ are in $T$ then $Q$ is in $T$.

The sentences in a theory are called theorems (in that theory).

Remark 7.6. A proposition is a theorem which is less “important” in the theory. A lemma is a theorem which “helps prove” another theorem. One usually reserves the word theorem for the most important sentences that belong to a theory. For a while we will not make any distinction between theorems, propositions, and lemmas. But later, in mathematics, we will start making this distinction.

Metadefinition 7.7. If we fix a collection of sentences $A, B, ...$ and we refer to them as specific axioms then by an axiom we will understand either a background axiom or a specific axiom.

Metadefinition 7.8. Fix a collection of specific axioms $A, B, ...$. Let $U$ be a sentence. By a proof (or a derivation) of $U$ from $A, B, ...$ we understand a string of sentences

\[ P \]
\[ Q \]
\[ R \]
\[ ... \]
\[ ... \]
\[ U \]

with the following property. Let $S$ be one of $P, Q, R, ...$. Then one of the following holds:

1) $S$ is an axiom.
2) $S$ is preceded in the list by sentences $S'$ and $S''$ such that $S$ is $S' \land S''$.
3) $S$ is preceded in the proof by sentences $S'$ and $S' \rightarrow S$.

Exercise 7.9. Fix a collection of specific axioms $A, B, ...$. Give a metaproof of the fact that a sentence $U$ has a proof from $A, B, ...$ if and only if there is a string of sentences

\[ P \]
\[ Q \]
\[ R \]
\[ ... \]
\[ ... \]
\[ U \]

with the following property. Let $S$ be one of $P, Q, R, ...$. Then one of the following holds:

1) $S$ is an axiom.
2) $S$ is preceded in the list by (not necessarily different) sentences $S'$ and $S''$ such that $(S' \land S'') \rightarrow S$ is an axiom. (We then say $S$ is inferred from $S'$ and $S''$ or that $S$ follows from $S'$ and $S''$.)

Strings as above will still be referred to as proofs.

**Metadefinition** 7.10. Fix again specific axioms $A, B, \ldots$. The collection of all sentences $U$ for which there is a proof of $U$ from $A, B, \ldots$ is a theory (see the Exercise below) and is called the theory with (or generated by the) specific axioms $A, B, \ldots$ and is denoted by $T(A, B, \ldots)$.

**Exercise** 7.11. Metaprove that $T(A, B, \ldots)$ is indeed a theory.

**Exercise** 7.12. Metaprove that any theory is of the form $T(A, B, \ldots)$.

**Remark** 7.13. If one removes the background axioms from a system of specific axioms the theory does not change. So we may (and will) assume our systems of specific axioms do not contain background axioms.

**Remark** 7.14. Two different systems of specific axioms $A, B, \ldots$ and $A', B', \ldots$ can generate the same theory: i.e. $T(A, B, \ldots)$ may coincide with $T(A', B', \ldots)$.

**Exercise** 7.15. Let $T$ be a theory in $L$ with specific axioms $A, B, \ldots$. Explain why any background axiom and any specific axiom is a theorem.

**Exercise** 7.16. Assume we have a theory $T(A, B, \ldots)$ and a sentence $U$. Metaprove that $U$ is a theorem in $T(A, B, \ldots)$ if and only if we have a string of sentences

\[ P \]
\[ Q \]
\[ R \]
\[ \ldots \]
\[ \ldots \]
\[ U \]

with the following property. Let $S$ be one of $P, Q, R, \ldots$. Then one of the following holds:

1) $S$ is a theorem in $T(A, B, \ldots)$;

2) $S$ is preceded in the list by (not necessarily different) sentences $S'$ and $S''$ such that $(S' \land S'') \rightarrow S$ is a theorem in $T(A, B, \ldots)$.

Strings as above will still be referred to as proofs. In particular this says that we can use previously proved theorems to prove new theorems.

**Remark** 7.17. If the theory has, among its theorems (in particular among its axioms), the sentence $\exists x P(x)$ then note that the sentence $P(c^P)$ is a theorem. We refer to $c^P$ as the witness for the theorem $\exists x P(x)$. More generally if $c', c'', c''', \ldots$ are the witnesses for the sentence $\exists x \exists y \exists z \ldots P(x, y, z, \ldots)$ and the latter sentence is a theorem then $P(c', c'', c''', \ldots)$ is a theorem.

**Exercise** 7.18. Metaprove the latter assertion.

**Remark** 7.19. (Important) If the language $L$ is the witness closure of a language $L_0$ then the only theorems in $L^*$ that we are morally interested in are the ones that already belong to $L_0^*$. So, in some sense, one views $L$ as an artificial language created by introducing artificial witnesses. The role of $L$ is to allow one to define the notion of theory/theorem; but what one is really interested in are the theorems that do not contain the artificially introduced witnesses.
Exercise 7.20. Metaprove the above.

Exercise 7.21. Explain why if one erases the last sentence in a proof one obtains a proof of the next to the last sentence in the original proof.

Exercise 7.22. Explain why if two of the sentences in a proof have the form $S' \rightarrow S''$ and $S'' \rightarrow S'''$ respectively adding $S' \rightarrow S'''$ to the proof yields a proof.

Hint: $((S' \rightarrow S'') \land (S'' \rightarrow S''')) \rightarrow (S' \rightarrow S''')$ is a tautology in $S', S'', S'''$.

Exercise 7.23. Explain why if the sentences $S', S''$ appear in a proof then adding $S' \land S''$ to the proof yields a proof.

Exercise 7.24. Explain why if $S'$ appears in a proof and $S' \rightarrow S$ is a tautology then adding $S$ to the proof yields a proof. (Use modus ponens.)

Exercise 7.25. Explain why if $S'$ and $S' \rightarrow S$ appear in the proof then adding $S$ to the proof yields a proof. (Use case by case argument.)

Metadefinition 7.27. A theory $T$ is complete if for any sentence $P$ either $P$ is in $T$ or $\neg P$ is in $T$.

Metadefinition 7.28. A theory is inconsistent if there is sentence $P$ such that both $P$ and $\neg P$ are theorems. A theory is consistent if it is not inconsistent; i.e. if for any sentence $P$ either $P$ is not a theorem or $\neg P$ is not a theorem.

Remark 7.29. Strictly speaking, since the metadefinitions above involve quantifiers one cannot metaprove that a given theory is consistent or complete. (Meta proofs are not allowed to involve quantifiers.) Dealing with completeness/consistency requires reformulating the problem within mathematics (i.e. in mathematical logic) where more tools are available that can deal with quantifiers. See the last part of the course.

Remark 7.30. Let $T$ be a theory in a language $L$. So $T$ is contained in $L^x$. Let $F$ be the collection of all sentences $P$ in $L^x$ such that $\neg P$ is in $T$. Finally let $N$ be the collection of all sentences that are neither in $T$ nor in $F$. There are 3 possible cases:

1) $T$ is inconsistent (and in particular complete). In this case both $T$ and $F$ coincide with $L^x$ and $N$ contains no sentence.

2) $T$ is consistent and incomplete. In this case any sentence is exactly in one of $T, F, N$ and $N$ contains at least one sentence.

3) $T$ is consistent and complete. In this case any sentence is exactly in one of $T, F$ hence $N$ contains no sentence.

In case 3 note that we may define truth/falsehood of sentences syntactically as follows: a sentence $P$ is true if it is in $T$; and it is false if it is in $F$. This is a metadefinition and implies that a sentence is either true or false and cannot be both true and false.

However one can prove a sentence in mathematics whose translation into English says that for most interesting theories if these theories are consistent then they are incomplete. So in these theories we have no reasonable metadefinition of truth/falsehood.

Due to the discussion above it is safer and simpler to NOT define truth/falsehood; this is the way we follow in this course.
Exercise 7.31. Let $T$ be a theory and let $F$ be the collection of all sentences $P$ such that $\neg P$ is in $T$. Show that if $P$ and $Q$ are in $T$ then $P \land Q$ is in $T$; and if at least one of $P$ or $Q$ is in $F$ then $P \land Q$ is in $F$. Also if exactly one of $P$ and $Q$ is in $N$ then $P \land Q$ is in $N$. And if both $P$ and $Q$ are in $N$ then $P \land Q$ is either in $F$ or in $N$. The preceding utterances are all metasentences and can be summarized in a $T/F/N$ “table” as follows:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \land Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$N$</td>
<td>$T$</td>
<td>$N$</td>
</tr>
<tr>
<td>$N$</td>
<td>$F$</td>
<td>$N$</td>
</tr>
<tr>
<td>$T$</td>
<td>$N$</td>
<td>$N$</td>
</tr>
<tr>
<td>$F$</td>
<td>$N$</td>
<td>$N$</td>
</tr>
<tr>
<td>$N$</td>
<td>$F$</td>
<td>$N$ or $F$</td>
</tr>
</tbody>
</table>

The top of this table is entirely analogous to the $T/F$ truth table of $\land$. Show that the $T/F$ truth tables of $\lor, \rightarrow, \leftrightarrow, \neg$ have similar analogous $T/F/N$ tables. Note the following difference of status between the $T/F$ truth tables and the $T/F/N$ tables: the $T/F$ tables are just some meaningless graphical symbols in metalanguage; they helped us define proofs and theories; the $T/F/N$ tables, being notation for metasentences, have a meaning.

Exercise 7.32. Assume neither $P$ nor $\neg P$ is in the theory $T(A, B, ...)$. Give a metaproof that both $T(P, A, B, ...)$ and $T(\neg P, A, B, ...)$ are consistent. (As usual we assume here that $A, B, ...$ are constants in the metalanguage and not variables!) Hint: Assume for instance that $T(P, A, B, ...)$ is inconsistent. Let

\[
\begin{align*}
Q \\
R \\
... \\
C \land \neg C
\end{align*}
\]

be a derivation of $C \land \neg C$ from $P, A, B, ...$. Then one notes that

\[
\begin{align*}
A \\
B \\
... \\
P \rightarrow Q \\
P \rightarrow R \\
... \\
P \rightarrow (C \land \neg C) \\
(C \lor \neg C) \rightarrow \neg P \\
C \lor \neg C \\
\neg P
\end{align*}
\]

is a derivation of $\neg P$ from $A, B, ...$ so $\neg P$ is in $T(A, B, ...)$, a contradiction.

Exercise 7.33. Metaprove that if a consistent theory $T$ is not complete then there exist at least two consistent theories containing $T$ and not coinciding with $T$. 
Metadefinition 7.34. A theory $T$ is maximal if it is consistent and if any consistent theory containing $T$ coincides with $T$.

Exercise 7.35. Metaprove that a consistent theory is complete if and only if it is maximal.

Remark 7.36. One can ask if any consistent theory is contained in a complete theory. The mirror of this in mathematical logic is a theorem (a consequence of what is called Zorn’s lemma).
CHAPTER 8

Proofs

Throughout this chapter we fix a language $L$ as in the previous chapter (i.e. equipped with the standard 5 connectives $\land, \lor, \neg, \rightarrow, \leftrightarrow$, quantifiers $\forall, \exists$, equality $=$, definitions, and witnesses) and we also fix a theory $T$ in $L$ with (specific) axioms $A, B, \ldots$. Recall the metadefinition of a proof 7.8. In this chapter we want to discuss this concept in some detail, and to give the first examples of proofs.

In order to make proofs more intelligible one usually uses labels and for each line one indicates in parentheses how the line was derived and one uses the following format:

**Theorem 8.1.** $U$.

**Proof.**
1. $P$ (by...)
2. $Q$ (by...)
3. $R$ (by...)
...
...
635. $U$ (by...)

The above should be viewed as a combination between the metasentence: $U$ is a theorem with proof: $P, Q, R, \ldots, U$ and a metaproof of it (which consists of the explanations (by...), (by...), ...).

Here is an example of a theorem and a proof. It is a theorem in any theory. It is referred to as the quantified modus ponens. Let $P(x)$ and $Q(x)$ be formulas with one free variable $x$; for each such pair of formulas we have the following:

**Theorem 8.2.** $((\exists x P(x)) \land (\forall x (P(x) \rightarrow Q(x)))) \rightarrow (\exists x Q(x)).$

**Proof.**
1. $(\exists x P(x)) \rightarrow P(c^n)$ (quantifier axiom)
2. $(\forall x (P(x) \rightarrow Q(x))) \rightarrow (P(c^n) \rightarrow Q(c^n))$ (quantifier axiom)
3. $((\exists x P(x)) \land (\forall x (P(x) \rightarrow Q(x)))) \rightarrow (P(c^n) \land (P(c^n) \rightarrow Q(c^n)))$ (by 1 and 2)
4. $((P(c^n) \land (P(c^n) \rightarrow Q(c^n)))) \rightarrow Q(c^n)$ (tautology: modus ponens)
5. $Q(c^n) \rightarrow \exists x Q(x)$ (quantifier axiom)
6. $((\exists x P(x)) \land (\forall x (P(x) \rightarrow Q(x)))) \rightarrow (\exists x Q(x))$ (by 3, 4, 5)

**Exercise 8.3.** Explain each step in the above proof.
Example 8.4. Theorem 8.2 should be understood as an “infinite” collection of theorems: for each choice of language and each choice of \( P(x) \) and \( Q(x) \) one has a specific theorem (and a specific proof). For instance say that \( L \) contains a binary relational predicates \( \dagger, \square \) and \( c, b \) are constants. Then one has the following theorem:

\[ ((\exists x (x \dagger b)) \land (\forall x ((x \dagger b) \rightarrow (x \square c)))) \rightarrow (\exists x (x \square c)). \]

The proof of Theorem 8.2 becomes, in this setting:

1. \((\exists x (x \dagger b)) \rightarrow (c^{x \dagger b} \dagger b)\)
2. \((\forall x ((x \dagger b) \rightarrow (x \square c))) \rightarrow ((c^{x \dagger b} \dagger b) \rightarrow (c^{x \dagger b} \square c))\)

etc.

Here is another easy example of a theorem which is, again, a theorem in any theory. Let \( P(x) \) and \( Q(x) \) be formulas with one free variable \( x \); for each such formula we have the following:

**Theorem 8.5.** \((\forall x (P(x) \land Q(x))) \rightarrow (\forall x P(x))\)

**Proof.**
1. \((\forall x (P(x) \land Q(x))) \rightarrow (P(c_P) \land Q(c_P))\) (quantifier axiom)
2. \((P(c_P) \land Q(c_P)) \rightarrow P(c_P)\) (tautology)
3. \(P(c_P) \rightarrow (\forall x P(x))\) (quantifier axiom)
4. \((\forall x (P(x) \land Q(x))) \rightarrow (\forall x P(x))\) (by 1,2,3)

\(\square\)

**Exercise 8.6.** Explain each step in the above proof.

The following theorem is, again, a theorem in any theory. Let \( R(x, y) \) be a formula with two free variables \( x, y \); for each such formula we have the following:

**Theorem 8.7.** \((\exists x \forall y R(x, y)) \rightarrow (\forall y \exists x R(x, y))\)

**Proof.**
1. \((\exists x \forall y R(x, y)) \rightarrow (\forall y R(c^{\forall y R(x, y)}, y))\) (quantifier axiom)
2. \((\forall y R(c^{\forall y R(x, y)}, y)) \rightarrow R(c^{\forall y R(x, y)}, c^{\exists x R(x, y)})\) (quantifier axiom)
3. \(R(c^{\forall y R(x, y)}, c^{\exists x R(x, y)}) \rightarrow (\exists x R(x, c^{\exists x R(x, y)}))\) (quantifier axiom)
4. \((\exists x R(x, c^{\exists x R(x, y)})) \rightarrow (\forall y \exists x R(x, y))\) (quantifier axiom)
5. \((\exists x \forall y R(x, y)) \rightarrow (\forall y \exists x R(x, y))\) (tautology plus 1, 2, 3, 4)

\(\square\)

**Remark 8.8.** The converse of Theorem 8.7 is seldom a theorem (unless our theory is inconsistent). Here is an example in English that suggests this. Translate \( R(x, y) \) as “\( x \) is the father of \( y \)”. Then Theorem 8.7 is translated as “if there is a person who is the father of everybody then everybody has a father”. But the converse of Theorem 8.7 is translated as “if everybody has a father then there is a person who is everybody’s father”.

**Exercise 8.9.** Prove the following sentences:
1. \((\forall x \forall y R(x, y)) \leftrightarrow (\forall y \exists x R(x, y))\)
2. \((\exists x \exists y R(x, y)) \leftrightarrow (\exists y \exists x R(x, y))\)
3. \((\exists x P(x)) \rightarrow (\exists x P(x))\)

The following theorem is, again, a theorem in any theory. Let \( P(x) \) be a formula with one free variable \( x \); for each such formula we have the following:
Theorem 8.10. \((\neg(\forall x P(x))) \iff (\exists x (\neg P(x)))\).

Proof.
1. \((\forall x P(x)) \iff P(c_P)\) (quantifier axiom)
2. \((\neg(\forall x P(x))) \iff (\neg P(c_P))\) (by 1)
3. \((\exists x (\neg P(x))) \iff (\neg P(c_P))\) (quantifier axiom)
4. \(P(c_P) \rightarrow P(c_{P'})\) (quantifier axiom)
5. \((\neg P(c_{P'})) \rightarrow (\neg P(c_P))\) (by 4)
6. \((\neg P(c_P)) \rightarrow (\neg P(c_{P'}))\) (quantifier axiom)
7. \((\neg P(c_P)) \iff (\neg P(c_{P'}))\) (by 5 and 6)
8. \((\neg(\forall x P(x))) \iff (\exists x (\neg P(x)))\) (by 2, 3, 7)

\[\square\]

Exercise 8.11. Explain each of the steps of the proof above.

Exercise 8.12. Prove the following sentences:
1) \((\neg(\exists x P(x))) \iff (\forall x (\neg P(x)))\)
2) \((\neg(\forall x\exists y P(x, y))) \iff (\exists y(\forall x (\neg P(x, y))))\)

Remark 8.13. It should be clear what the rule is to negate sentences that start with more quantifiers: negation changes \(\forall\) into \(\exists\), changes \(\exists\) into \(\forall\) and changes \(P\) into \(\neg P\). E.g.
\[\neg(\forall x\exists y\forall u\exists v P(x, y, z, u, v)) \iff (\exists x\forall y\forall u\exists v(\neg P(x, y, z, u, v)))\]

Example 8.14. We have
\[\neg((\forall x\exists y P(x, y)) \rightarrow (\exists y\forall u\forall v R(z, u, v)))\]
\[\iff \neg((\neg(\forall x\exists y P(x, y)) \lor (\exists y\forall u\forall v R(z, u, v)))\]
\[\iff (\forall x\exists y P(x, y)) \land (\exists y\forall u\forall v R(z, u, v)))\]
\[\iff (\forall x\exists y P(x, y)) \land (\forall z\exists u\exists v(\neg R(z, u, v)))\]

Exercise 8.15. Explain all the steps in the above example.

Exercise 8.16. Prove the following sentences:
1) \((\forall x(P(x) \land Q(x))) \iff ((\forall x P(x)) \land (\forall x Q(x)))\)
2) \((\exists x(P(x) \lor Q(x))) \iff ((\exists x P(x)) \lor (\exists x Q(x)))\)

Exercise 8.17. Let \(f\) and \(g\) be two unary functional symbols. Prove the following sentences. These sentences correspond to what later in set theory will read: \textit{the composition of two surjections, respectively injections is a surjection, respectively an injection.}
1) \(((\forall z\exists y((f(x) = y)) \land (\forall y\exists x(g(x) = y))) \rightarrow (\forall z\exists x(f(g(x)) = z))\)
2) \(((\forall x\forall y((f(x) = f(y)) \rightarrow (x = y))) \land (\forall x\forall y((g(x) = g(y)) \rightarrow (x = y)))\rightarrow ((\forall x\forall y((f(g(x)) = f(g(y)) \rightarrow (x = y))))\)

Exercise 8.18. Prove the following sentence:
\((\neg(\exists x P(x))) \rightarrow (\forall x (P(x) \rightarrow Q(x)))\)
The sentence intuitively says that things that don’t exist have all the conceivable properties. E.g. \textit{since unicorn don’t exist any unicorn is 10 feet long.} Here \(P(x)\) stands for \(x\) is a unicorn and \(Q(x)\) stands for \(x\) is 10 feet long.

In the next theorem \(P\) is a sentence and \(Q(x)\) is a formula with free variable \(x\).

Theorem 8.19. \((\forall x (P \rightarrow Q(x))) \rightarrow (P \rightarrow (\forall x Q(x)))\)
Proof.
1. \((\forall x (P \rightarrow Q(x))) \rightarrow (P \rightarrow Q(c_P))\) (quantifier axiom)
2. \(Q(c_P) \leftrightarrow (\forall x Q(x))\) (quantifier axiom)
3. \((P \rightarrow Q(c_P)) \leftrightarrow (P \rightarrow (\forall x Q(x)))\) (by 2)
4. \((\forall x (P \rightarrow Q(x))) \rightarrow (P \rightarrow (\forall x Q(x)))\) (by 1 and 3) \(\square\)

Remark 8.20. Consider the following sentences:

A) \((\forall x P(x)) \rightarrow P(t) \rightarrow (\exists x P(x)) \rightarrow P(c_P)\)

B) \((\neg (\forall x P(x))) \leftrightarrow (\exists x (\neg P(x)))\).

C) \((\forall x (P \rightarrow Q(x))) \rightarrow (P \rightarrow (\forall x Q(x)))\)

A represents the quantifier axioms minus the one involving \(c_P\). B and C are Theorems 8.10 and 8.19 respectively. Conversely if one defines the witness assignment such that \(c_P\) is \(c_{\neg P}\) then the quantifier axioms follow from A and B. Note that the sentences A (with the axiom on \(c_P\) removed), B, and C are taken as the quantifier axioms in Manin’s book on Mathematical Logic; the moral of the discussion is that our quantifier axioms (in a language in which \(c_P\) coincides with \(c_{\neg P}\)) are equivalent to Manin’s quantifier axioms plus the axiom on \(c_P\). Roughly, modulo witnesses, the two systems are equivalent.

Exercise 8.21. Let \(P(x)\) be a formula with free variable \(x\) and let \(Q\) be a sentence. Prove the following sentence:

\((\forall x (P(x) \rightarrow Q)) \leftrightarrow ((\exists x P(x)) \rightarrow Q)\)

Remark 8.22. Let \(L\) be a language (with witnesses), \(T\) a theory with axioms \(A, B, \ldots\). For a sentence \(U\) consider the following statements:

1) \(\neg U\) is not a theorem.
2) \(U\) is a theorem; i.e. there is a proof of \(U\). Here we recall that the correctness of a proof can be checked by a machine.
3) There is an algorithm that guarantees that a given machine will decide (at some unspecified point in time) whether or not there is a proof for \(U\).
4) There is an algorithm that guarantees that a given machine will decide (at some unspecified point in time) whether or not there is a proof for \(U\) and will print that proof in case there is one.
5) There is an algorithm that guarantees that a given machine will decide (within a known interval of time) whether there is a proof for \(U\) and will print such a proof if there is one.

Assertion 2 implies 1 (under the assumption of consistency). Also 5 implies 4. Also 4 implies 3. Finally 1 and 3 imply 2. The above shows that there is a whole hierarchy of concepts related to proof: morally 1 is the weakest and 5 is the strongest. However 5 is essentially never the case, while 1 is essentially never checkable. Among the concepts above the universally accepted standard of “proof” is provided by 2 which we have therefore called proof.

Remark 8.23. Given a language \(L\) we recall that it does not make sense to say that a sentence in \(L\) is true (or false). However one sometimes abusively uses the word truth in relation to sentences of \(L\) as follows. If \(P\) is a sentence in \(L\) then by the metasentence

(We) prove that \(P\) is true

we mean

(We) prove that \(P\) is true
(We) prove \( P \)

Furthermore the metasentence

(We) prove that \( P \) is false

means

(We) prove \( \neg P \)

As a variant, the metasentence

(We) give an example of an \( x \) such that \( P(x) \) is false

means

(We) prove \( \exists x(\neg P(x)) \)

A.s.o.

Remark 8.24. If one is given a translation of \( L \) into \( L' \) (as usual, compatible with witness assignments) then any proof in \( L \) yields, in a natural way, a proof in \( L' \). In particular if \( U \) is a theorem in \( L \) then the corresponding sentence \( U' \) in \( L' \) is a theorem in \( L' \).

Exercise 8.25. Formalize the following English sentences, negate their formalization, and give the English translation of these formalized negations:

1) If Plato eats at least one nut then Plato is a bird.
2) Plato is a bird if and only if he eats at least one nut.
3) For any planet there is a sun such that the planet revolves around that sun.
4) There exists a sun with no planets revolving around it.
CHAPTER 9

Argot

Given a language $L$ and a translation of $L$ into the English language $L_{Eng}$ one may construct a new language $L_{argot}$, called argotic $L$ (or simply argot, or slang) by replacing some of the symbols in $L$ by their corresponding symbols in $L_{Eng}$. Then there is a natural translation of $L$ into $L_{argot}$. When we write proofs we use however a more flexible version of this translation which deserves, maybe, a different name but which for simplicity we call still call translation. In this more flexible translation sentences may change more dramatically than in usual translation; new sentences may actually appear; others may disappear. Everything is subject to rules but rather than spelling out these rules we learn argot and the more flexible translation by example. The above type of translation has two steps: the first (which we already performed in the previous chapter) is to convert proofs from a string of sentences in $L$ into a string of metasentences containing the sentences themselves plus an explanation of the inference process; the second step is to convert this string of metasentences back into a string of sentences in argotic $L$ via a process involving disquotation (removing quotation marks).

Let us see how this works. As before we fix a theory $T$ in $L$ with axioms $A, B, ...$.

Remark 9.1. Start with a proof:

\[ P \]
\[ Q \]
\[ R \]
\[ ... \]
\[ ... \]
\[ U \]

Such a proof can be viewed (via disquotation) as a text in the language $L$. (Recall that disquotation means replacing $P, Q, ...$ by the sentences in $L$ they stand for, with quotation marks deleted). Let us view above however as a text in metalanguage. As already noted such a proof can be made more intelligible by adding labels 1, 2, 3, ... and explanations in parentheses showing how each sentence follows from other sentences; the proof will be then a text in metalanguage that could look like:

1. $P$ (tautology)
2. $Q$ (by axiom $E$ and 1)
3. $R$ (by 1 and 2)
   ....
   ....
66. $U$ (by axiom $B$ and 3)

The above proof can be rewritten as a text in metalanguage:
Proof. From $E$ and since $P$ we get that $Q$. Since $P$ and since $Q$ it follows that $R$ ....... By axiom $B$ and since $R$ it follows that $U$. □

We now apply disquotation to the latter text, i.e. replace the symbols $E, P, Q, ...$ by the sentences in $L$ that they stand for without quotation marks; in addition one is allowed to further replace some (or even all) of the symbols appearing in $E, P, Q, ...$ by corresponding words in English; e.g. if $E$ equals \"$\forall x \exists y (x \heartsuit y)$\" then the proof above becomes a text in argotic $L$ which could look like:

Proof. By axiom [number or name of the axiom] for all $x$ there is a $y$ such that $x \heartsuit y$; and since .... and ... it follows that ...

The process described above should be viewed as a (generalized concept of) translation of a proof from $L$ into argotic $L$.

Remark 9.2. As explained in Remark 8.23 one sometimes abusively introduces in metasentences the empty words \textit{true}, \textit{false} in reference to sentences. This can be done in argot as well: one may replace the words \textit{“we get”} by \textit{“we get that ... is true”} or \textit{“we get that ... holds”}, etc. Then the translation of the above proof in argot reads:

Proof. From axiom $E$ and since $P$ we get that $Q$ is true. Since $P$ and since $Q$ is true it follows that $R$ holds........ By axiom $B$ and since $R$ holds it follows that $U$ is true.

We prefer not to do so but one encounters this abuse in mathematical texts quite often.

Example 9.3. The statement and proof of Theorem 8.2 can be translated into argot as follows:

Theorem 9.4. If there exists $x$ such that $P(x)$ and if we know that, for all $x$, $P(x)$ implies $Q(x)$ it follows that there exists an $x$ such that $Q(x)$.

Proof. We know there exists $c'$ such that $P(c')$. Also we know that for all constants $c$ we have $P(c) \rightarrow Q(c)$. In particular for our $c'$ we have $P(c') \rightarrow Q(c')$. Since $P(c')$ it follows that $Q(c')$. This ends the proof. □

Note that $c'$ in the above proof plays the role of $c^P$ in the original proof.

Example 9.5. The statement and proof of Theorem 8.5 can be translated into argot as follows:

Theorem 9.6. Assume that, for all $x$, $P(x) \land Q(x)$. Then for all $x$, $P(x)$.

Proof. Let $c$ be a constant. We know $P(c) \land Q(c)$. In particular $P(c)$. Since $c$ was arbitrary the conclusion follows. □

Note that unlike with $c^P$ (whose role was played in the previous example by a \textit{“specific”} constant $c'$) the role of $c_P$ is played by an \textit{“arbitrary”} constant $c$. The words \textit{“specific”} and \textit{“arbitrary”} are, of course, vague. Vagueness is inherent in argot.

Exercise 9.7. Translate the statement and proof of Theorem 8.10 into argot.
Remark 9.8. If $U$ is of the form $H \rightarrow C$ (in which case $H$ is called hypothesis and $C$ is called conclusion) then the sentence $U$ is translated into argot as *If $H$ then $C$* or *Assume $H$; then $C$*. So

**Theorem.** $H \rightarrow C$

is translated into argot as either of the following:

**Theorem.** *If $H$ then $C$*

**Theorem.** *Assume $H$; then $C$*

Similarly

**Theorem.** $H \leftrightarrow C$

is translated into argot as:

**Theorem.** *$H$ if and only if $C$*

Remark 9.9. As with theorems and their proofs, definitions too can be expressed in argot. We will do this on a regular basis.

Remark 9.10. Formally metalanguage and argot are similar: they both involve symbols from the original language plus English words. But metalanguage and argot should not be confused. Metalanguage has a meaning that we care about (coming from the fact that it is “about” the syntax, semantics, and proofs of sentences; most of the text in this course is written in metalanguage so we better recognize its meaning). On the contrary argot has a meaning that we ignore; intuitively argot seems to be “about” the constants and variables of the language but it is, in fact, “about nothing”. One way to distinguish formally between metalanguage and argot is to enforce the following rule: symbols in the original language appear BETWEEN quotation marks in metalanguage and WITHOUT quotation marks in argot.
CHAPTER 10

Strategies

We discuss a series of standard strategies to prove theorems.
As before we fix a theory $T$ in $L$ with specific axioms $A, B, \ldots$.

**Example 10.1.** There are two strategies to prove a theorem of the form $H \rightarrow C$: “direct proof” and “proof by contradiction”. A direct proof (in the form of string of sentences) may look like this:

1. $H \rightarrow P$ (by axiom $B$)
2. $Q$ (by axiom $A$ and 1)
3. $H \rightarrow R$ (by 1 and 2)

....

835. $H \rightarrow C$ (by axiom $S$ and 3)

One usually translates the above proof into argot as follows:

**Proof.** Assume $H$. By axiom $B$ we get $P$. By axiom $A$ it follows that $Q$. From the latter and by $P$ we get $R$.... By axiom $S$ and since $R$ it follows that $C$. □

A proof of $H \rightarrow C$ by contradiction may look like this:

1. $(\neg C \land H) \rightarrow P$ (by axiom $A$
2. $Q$ (by axiom $V$ and 1)
3. $(\neg C \land H) \rightarrow R$ (by 1 and 2)

....

691. $(\neg C \land H) \rightarrow (A \land \neg A)$ (by 357 and 76)
692. $(\neg (C \land H))$ (by 691)
693. $H \rightarrow C$ (by 692)

One usually translates a proof as above into argot as follows.

**Proof.** Assume $\neg C$ and $H$ and seek a contradiction. By axiom $S$ we get $P$. By axiom $V$ and $P$ it follows that $Q$ .... By [here one needs to explicitly state 357 and 76] we get $A \land \neg A$, a contradiction. This ends the proof. □

**Exercise 10.2.** Explain what was used in step 692 above.

**Example 10.3.** Direct proofs and proofs by contradiction can be given to sentences $U$ which are not necessarily of the form $H \rightarrow C$. A direct proof of $U$ is just a proof that ends with $U$. A proof of $U$ by contradiction could proceed as follows:

1. $\neg U \rightarrow P$ (by axiom $A$)
2. $P \rightarrow Q$ (tautology)

....

99. $\neg U \rightarrow D \land \neg D$ (by 1 and 98)
100. \((\neg D \lor D) \rightarrow U\) (by 99)
101. \(U\) (by 100 and 3)

In argot:

Proof. Assume \(\neg U\) and seek a contradiction. Then by axiom \(A\) we get \(P\). Hence \(Q\)....Hence \(D \land \neg D\), a contradiction. This ends the proof. □

Example 10.4. Here is a strategy to prove a theorem of the form \((H' \lor H'') \rightarrow C\); this is called a case by case proof. It may run as follows:

1. \(H' \rightarrow P\) (by axiom \(A\))
2. \(H'' \rightarrow Q\) (by axiom \(B\))
3. \(H' \lor H'' \rightarrow P \lor Q\) (by 1 and 2)
   ....
   ....
76. \(P \rightarrow C\) (by 55 and 56)
77. \(Q \rightarrow C\) (by 64)
78. \(P \lor Q \rightarrow C\) (by 76 and 77)
79. \(H' \lor H'' \rightarrow C\) (by 3 and 78)

One usually translates a proof as above into argot as follows; note that this translation of the proof completely changes the order of the various steps.

Proof. There are two cases: Case 1 is \(H'\); Case 2 is \(H''\). Assume first that \(H'\). Then by axiom \(A\) we get \(P\).... By [here one needs to explicitly state 55 and 56] and since \(P\) we get \(C\). Now assume that \(H''\). By axiom \(B\) it follows that \(Q\).... By [here one needs to explicitly state 64] and \(Q\) we get \(C\). So in either case we get \(C\). This ends the proof. □

Direct proofs, proofs by contradiction, and case by case proofs can be combined; we shall see this in examples. Here is a generic example:

Example 10.5. A proof of \(U\) by contradiction plus case by case may look as follows. (In the proof below \(A\) is an arbitrary sentence. Deciding what \(A\) to use is a matter of art rather than science!)

1. \((\neg U \land A) \rightarrow B\) (an axiom)
2. \(B \rightarrow C\) (by 1 and axiom...) 
   ...
33. \(S \rightarrow (Q \land \neg Q)\) (by Axiom ... and 4,32)
34. \((\neg U \land A) \rightarrow (Q \land \neg Q)\) (by 1,...,33)
35. \((\neg Q \land Q) \rightarrow (U \land \neg A)\) (by 34)
36. \(\neg Q \land Q\) (tautology)
37. \(U \land \neg A\) (by 35, 36)
38. \((\neg U \land \neg A) \rightarrow B'\) (an axiom)
39. \(B' \rightarrow C'\) (by ... and axiom...)
   ...
100. \(S' \rightarrow (Q' \land \neg Q')\) (by Axiom ... and ...) 
101. \((\neg U \land \neg A) \rightarrow (Q' \land \neg Q')\) (by 38,...,100)
102. \((\neg Q' \land Q') \rightarrow (U \land A)\) (by 101)
103. \(\neg Q' \land Q'\) (tautology)
104. \(U \land A\) (by 102, 103)
105. \((U \land \neg A) \land (U \land A)\) (by 37, 104)
106. U (by 105)

One usually translates a proof as above into argot as follows.

**Proof.** Assume \( \neg U \) and seek a contradiction. There are two cases: either \( A \) or \( \neg A \). Assume first \( A \). Then, since \( \neg U \) and \( A \), by..., we get \( B \). Hence by ... we get \( C \). Hence by ... we get \( S \). Hence \( Q \land (\neg Q) \), a contradiction. Now assume \( \neg A \). Then, since \( \neg U \) and \( \neg A \) we get \( B' \). Hence \( C' \). Hence \( S' \). Hence \( Q' \land (\neg Q') \) which is again a contradiction. This ends the proof. \( \square \)

**Exercise 10.6.** Explain each step in the above formal proof.

**Example 10.7.** In order to prove a theorem \( U \) of the form \( P \leftrightarrow Q \) one may precede as follows:

1. \( P \rightarrow S \) (by...)
2. \( S \rightarrow Q \) (by...)
3. \( P \rightarrow Q \) (by 1 and 2)
4. \( Q \rightarrow T \) (by...)
5. \( T \rightarrow P \) (by...)
6. \( Q \rightarrow P \) (by 4 and 5)
7. \( P \leftrightarrow Q \) (by 3 and 6)

Alternatively, in argot,

**Proof.** We need to prove two things: first that \( P \rightarrow Q \); and next that \( Q \rightarrow P \).

To prove \( P \rightarrow Q \) assume \( P \). By ... we get \( S \). By ... we get \( Q \). So \( P \rightarrow Q \) is proved.

To prove \( Q \rightarrow P \) assume \( Q \). By ... we get \( T \). By ... we get \( P \). So \( Q \rightarrow P \) is proved.

This ends the proof of the theorem. \( \square \)

**Example 10.8.** Sometimes a theorem \( U \) has the statement:

**The following conditions are equivalent:**

1) \( P \);
2) \( Q \);
3) \( R \).

What is being meant is that \( U \) is

\[(P \leftrightarrow Q) \land (P \leftrightarrow R) \land (Q \leftrightarrow R)\]

One proceeds “in a circle” as follows. (We just give the argot version of the proof).

**Proof.** It is enough to prove 3 things: first that \( P \rightarrow Q \); then that \( Q \rightarrow R \); then that \( R \rightarrow P \). To prove that \( P \rightarrow Q \) assume \( P \). By \( P \) we get ... hence we get .... hence we get \( Q \). To prove that \( Q \rightarrow R \) assume \( Q \). By \( Q \) we get ... hence we get ... hence we get \( R \). To prove that \( R \rightarrow P \) assume \( R \). By \( R \) we get ... hence we get .... hence we get \( P \). \( \square \)

**Exercise 10.9.** Explain why, in the last Remark, it is enough to prove \( P \rightarrow Q \), \( Q \rightarrow R \), and \( R \rightarrow P \) in order to conclude \( U \).

**Example 10.10.** In order to prove a theorem of the form \( P \land Q \) one usually proceeds as follows:

**Proof.** We first prove \( P \). By ... and ... it follows that ...; by ... and ... it follows that \( P \). Next we prove \( Q \). By ... and ... it follows that ...; by ... and ... it follows that \( Q \). This ends the proof. \( \square \)
Example 10.11. In order to prove a theorem of the form $P \lor Q$ one may proceed by contradiction as follows:

Proof. Assume $\neg P$ and $\neg Q$ and seek a contradiction. By ... and ... it follows that ...; by ... and ... it follows that $A \land \neg A$, a contradiction. This end the proof. □

Example 10.12. In order to prove a theorem of the form $\forall x P(x)$ one may proceed as follows:

Proof. Let $c$ be arbitrary. By ... it follows that ... and hence $P(c)$. □

Example 10.13. In order to prove a theorem of the form $\exists x P(x)$ one may proceed as follows; this is called a proof by example and it applies only to existential sentences $\exists x P(x)$ (NOT to universal sentences like $\forall x P(x)$).

Proof. By ... we know that there exists $c$ such that $Q(c)$. By ... and ... it follows that ... By ... and ... it follows that $P(c)$. □

In the above $c$ in NOT ARBITRARY but rather an EXAMPLE.
CHAPTER 11

Fallacies

A fallacy is a logical mistake. Here are some typical fallacies:

Example 11.1. Confusing an implication with its converse. Say we want to prove that $H \rightarrow C$. A typical mistaken proof would be: Assume $C$; then by ... we get that ... hence $H$. The error consists of having proved $Q \rightarrow P$ rather than $P \rightarrow Q$.

Example 11.2. Proving a universal sentence by example. Say we want to prove $\forall x P(x)$. A typical mistaken proof would be: By ... there exists $c$ such that ... hence ... hence $P(c)$. The error consists in having proved $\exists x P(x)$ rather than $\forall x P(x)$.

Example 11.3. Defining a constant twice. Say we want to prove that $\neg(\exists x P(x))$ by contradiction. A mistaken proof would be: Assume there exists $c$ such $P(c)$. Since we know that $\exists x Q(x)$ let $c$ be (or define $c$) such that $Q(c)$. By $P(c)$ and $Q(c)$ we get ... hence ..., a contradiction. The error consists in defining $c$ twice in two unrelated ways: first $c$ plays the role of the specific constant $c^P$; then $c$ plays the role of $c^Q$. But $c^P$ and $c^Q$ are not the same. We will see examples of this later; see Exercise 18.28.

Exercise 11.4. Give examples of wrong proofs of each of the above types. If you can’t now wait until we get to discuss the integers.

Remark 11.5. Later, when we discuss induction we will discuss another typical fallacy; cf. Example 19.7.
CHAPTER 12

Examples

We analyze in what follows a few toy examples of theories and proofs of theorems in these theories. Later we will present the main example of theory which is set theory (identified with mathematics itself). As usual the witness assignment in our languages will not be given explicitly.

Example 12.1. The first example is what later in mathematics will be referred to as the uniqueness of neutral elements. The language \( L \) of the theory has constants \( e, f, \ldots \), variables \( x, y, \ldots \), and a binary functional symbol \( \star \). We introduce the following definition in \( L \):

**Definition 12.2.** \( e \) is called a neutral element if
\[
\forall x ((e \star x = x) \land (x \star e = x)).
\]

So we added “is a neutral element” as a new relational predicate. We do not consider any specific axiom. We prove the following:

**Theorem 12.3.** If \( e \) and \( f \) are neutral elements then \( e = f \).

The sentence that needs to be proved is: “If \( H \) then \( C \).” Recall that in general for such a sentence \( H \) is called hypothesis and \( C \) is called conclusion. Here is a direct proof:

**Proof.** Assume \( e \) and \( f \) are neutral elements. Since \( e \) is a neutral element it follows that \( \forall x (e \star x = x) \). By the latter \( e \star f = f \). Since \( f \) is a neutral element we get \( \forall x (x \star f = x) \). So \( e \star f = e \). Hence we get \( e = e \star f \). Hence we get \( e = f \). □

**Remark 12.4.** Note that we skipped some of the “explanations” showing what sentences have been used at various stages of the proof; this is common practice.

**Exercise 12.5.** Convert the above argot proof into the original (non-argotic) language. Here by “convert” we understand finding a proof whose translation in argot is the given argot proof.

**Exercise 12.6.** Convert the above argot proof into the original (non-argotic) language.

Example 12.7. The next example is related to the famous Pascal wager. The structure of Pascal’s argument is as follows. If the reward exists and I believe it exists then I get the reward. If the reward exists and I do not believe it exists
then I do not get the reward. If the reward does not exist but I believe it exists I do not get the reward. Finally if the reward does not exist and I do not believe it exists then I do not get the reward. Pascal’s conclusion is that if he believed the reward exists then there would be a one chance in 2 that he get the reward whereas if he did not believe the reward exists then there would be a zero chance that he get the reward. So he should believe the reward exists. The next example is a variation of Pascal’s wager showing that if one requires “sincere” belief rather than just belief based on logic then Pascal will not get the reward. Indeed assume the specific axioms:

A1) If the reward exists and a person does not believe sincerely in its existence then that person will not get the reward.

A2) If the reward does not exist then nobody gets the reward.

A3) If a person believes the reward exists motivated only by Pascal’s wager then that person does not believe sincerely.

We want to prove the following

**Theorem 12.8.** If Pascal believes motivated only by his own wager then he will not get the reward.

All of the above is formulated in the English language $L'$. We consider a simpler language $L$ and a translation of $L$ into $L'$.

The new language $L$ contains among its constant $p$ (for Pascal) and contains 4 unary relational predicates $g, w, s, r$ whose translation in English is as follows:

- $g$ is translated as “*is the reward*”
- $w$ is translated as “*believes motivated only by Pascal’s wager*”
- $s$ is translated as “*believes sincerely*”
- $r$ is translated as “*gets the reward*”

The specific axioms are

A1) $\forall y(\exists xg(x) \land \neg s(y) \rightarrow \neg r(y))$

A2) $\forall y((\exists xg(x)) \rightarrow (\neg r(y)))$

A3) $\forall y(w(y) \rightarrow (\neg s(y)))$.

In this language Theorem 12.8 is the translation of the following:

**Theorem 12.9.** If $w(p)$ then $\neg r(p)$.

So to prove Theorem 12.8 in $L'$ it is enough to prove Theorem 12.9 in $L$. We will do this by using a combination of direct proof and case by case proof.

**Proof of Theorem 12.9.** Assume $w(p)$. There are two cases: the first case is $\exists xg(x)$; the second case is $\neg(\exists xg(x))$. Assume first that $\exists xg(x)$. Since $w(p)$, by axiom A3 it follows that $\neg s(p)$. By axiom A1 $(\exists xg(x)) \land (\neg s(p)) \rightarrow \neg r(p))$. Hence $\neg r(p)$. Assume now $\neg(\exists xg(x))$. By axiom A2 we then get again $\neg r(p)$. So in either case we get $\neg r(p)$ which ends the proof.

**Exercise 12.10.** Convert the above argot proof into the original (non-argotic) language.

**Example 12.11.** The next example is again a toy example and comes from physics. In order to present this example we do not need to introduce anything physical. But it would help to keep in mind the two slit experiment in quantum mechanics (for which I refer to Feynman’s course, say). Now there are two types of physical theories that can be referred to as *phenomenological* and *explanatory*. 
They are intertwined but very different in nature. Phenomenological theories are simply descriptions of phenomena/effects of (either actual or possible) experiments; examples of such theories are those of Ptolemy, Copernicus, or that of pre-quantum experimental physics of radiation. Explanatory theories are systems postulating transcendent causes that act from behind phenomena; examples of such theories are those of Newton, Einstein, or quantum theory. The theory below is a baby example of the phenomenological (pre-quantum) theory of radiation; our discussion is therefore not a discussion of quantum mechanics but rather it suggests the necessity of introducing quantum mechanics. The language $L'$ and definitions are those of experimental/phenomenological (rather than theoretical/explanatory) physics. We will not make them explicit. Later we will move to a simplified language $L$ and will not care about definitions.

Consider the following specific axioms (which are the translation in English of the phenomenological predictions of classical particle mechanics and classical wave mechanics respectively):

A1) If radiation in the 2 slit experiment consists of a beam of particles then the impact pattern on the photographic plate consists of a series of successive flashes and the pattern has 2 local maxima.

A2) If radiation in the 2 slit experiment is a wave then the impact pattern on the photographic plate is not a series of successive flashes and the pattern has more than 2 local maxima.

We want to prove the following

**Theorem 12.12.** If in the 2 slit experiment the impact consists of a series of successive flashes and the impact pattern has more than 2 local maxima then in this experiment radiation is neither a beam of particles nor a wave.

The sentence reflects one of the elementary puzzles that quantum phenomena exhibit: radiation is neither particles nor waves but something else! And that something else requires a new theory which is quantum mechanics. (A common fallacy would be to conclude that radiation is both particles and waves !!!) Rather than analyzing the language $L'$ of physics in which our axioms and sentence are stated (and the semantics that goes with it) let us introduce a simplified language $L$ as follows.

We consider the language $L$ with constants $a, b, ...$, variables $x, y, ...$, and unary relational predicates $p, w, f, m$. Then there is a translation of $L$ into $L'$ such that:

- $p$ is translated as “is a beam of particles”
- $w$ is translated as “is a wave”
- $f$ is translated as “produces a series of successive flashes”
- $m$ is translated as “produces a pattern with 2 local maxima”.

Then we consider the specific axioms

A1) $\forall x(p(x) \rightarrow (f(x) \land m(x)))$.

A2) $\forall x(w(x) \rightarrow (\neg f(x)) \land \neg m(x)))$.

Theorem 12.12 above is the translation of the following theorem in $L$:

**Theorem 12.13.** $\forall x((f(x) \land (\neg m(x)))) \rightarrow ((\neg p(x)) \land (\neg w(x))))$.

So it is enough to prove Theorem 12.13. The proof below is, as we shall see, a combination of proof by contradiction and case by case.
12. EXAMPLES

Proof. We proceed by contradiction. So assume there exists a such that \( f(a) \land (\neg m(a)) \) and seek a contradiction. Since \( \neg (\neg p(a) \land (\neg w(a))) \) we get \( p(a) \lor w(a) \). There are two cases. The first case is \( p(a); \) the second case is \( w(a) \). We will get a contradiction in each of these cases separately. Assume first \( p(a) \). Then by axiom A1 we get \( f(a) \land m(a) \), hence \( m(a) \). But we assumed \( f(a) \land (\neg m(a)) \), hence \( -m(a) \), so we get a contradiction. Assume now \( w(a) \). By axiom A2 we get \( (\neg f(a)) \land (\neg m(a)) \) hence \( -f(a) \). But we assumed \( f(a) \land (\neg m(a)) \), hence \( f(a) \), so we get again a contradiction. \( \square \).

EXERCISE 12.14. Convert the above argot proof into the original (non-argotic) language.

EXERCISE 12.15. Consider the specific axioms A1 and A2 above and also the specific axioms:

A3) \( \exists x (f(x) \land (\neg m(x))) \)

A4) \( \forall x (p(x) \lor w(x)) \).

Metaprove that the theory with specific axioms A1, A2, A3, A4 is inconsistent. A3 is translated as saying that in some experiments one sees a series of successive flashes and, at the same time, one has more than 2 maxima. Axiom A4 is translated as saying that any type of radiation is either particles or waves. The inconsistency of the theory says that classical (particle and wave) mechanics is not consistent with experiment. (So a new mechanics, quantum mechanics, is needed.) Note that none of the above discussion has anything to do with any concrete proposal for a quantum mechanical theory; all that the above suggests is the necessity of such a theory.

EXAMPLE 12.16. The next example is a logical puzzle from the Mahabharata. King Yudhishthira loses his kingdom at a game of dice against Sakuni; then he stakes himself and he loses himself; then he stakes his wife Draupadi and loses her too. She objects by saying that her husband could not have staked her because he did not own her anymore after losing himself. Here is a possible formalization of her argument.

We use a language with constants \( i, d, \ldots \), variables \( x, y, z, \ldots \), the relational binary predicate “owns”, quantifiers, and equality =. We define a predicate \( \neq \) by \( (x \neq y) \leftrightarrow (\neg (x = y)) \). Consider the following specific axioms:

A1) For all \( x, y, z \) if \( x \) owns \( y \) and \( y \) owns \( z \) then \( x \) owns \( z \).

A2) For all \( y \) there exists \( x \) such that \( x \) owns \( y \).

A3) For all \( x, y, z \) if \( y \) owns \( x \) and \( z \) owns \( x \) then \( y = z \).

We will prove the following

THEOREM 12.17. If \( i \) does not own himself then \( i \) does not own \( d \).

Proof. We proceed by contradiction. So we assume \( i \) does not own \( i \) and \( i \) owns \( d \) and seek a contradiction. There are two cases: first case is \( d \) owns \( i \); the second case is \( d \) does not own \( i \). We prove that in each case we get a contradiction. Assume first that \( d \) owns \( i \); since \( i \) owns \( d \), by axiom A1, \( i \) owns \( i \), a contradiction. Assume now \( d \) does not own \( i \). By axiom A2 we know that there exists \( j \) such that \( j \) owns \( i \). Since \( i \) does not own \( i \) it follows that \( j \neq i \). Since \( j \) owns \( i \) and \( i \) owns \( d \), by axiom A1, \( j \) owns \( d \). But \( i \) also owns \( d \). By axiom A3, \( i = j \), a contradiction. \( \square \).

EXERCISE 12.18. Convert the above argot proof into the original (non-argotic) language.
EXAMPLE 12.19. This example illustrates the logical structure of the Newtonian theory of gravitation that unified Galileo’s phenomenological theory of falling bodies (the physics on Earth) with Kepler’s phenomenological theory of planetary motion (the physics of “Heaven”); Newton’s theory counts as an explanatory theory because its axioms, being truly general, go beyond experiment. The language \( L \) in which we are going to work has variables \( x, y, ... \), constants \( S, E, M \) (translated in English as “Sun, Earth, Moon”), a constant \( R \) (translated as “the radius of the Earth”), constants \( 1, \pi, r \) (where \( r \) is translated as a particular rock), relational predicates \( p, c, n \) (translated in English as “is a planet, is a cannon ball, is a number”), a binary relational predicate \( \circ \) (whose syntax is \( x \circ y \) and whose translation in English is “\( x \) revolves around the fixed body \( y \)”), a binary relational predicate \( f \) (where \( f(x, y) \) is translated as “\( x \) falls freely under the influence of \( y \)”), a binary functional symbol \( d \) (“distance between the centers of”), a unary functional symbol \( a \) (“acceleration”), a unary functional symbol \( T \) (where \( T(x, y) \) translated as “the period of revolution of \( x \) around \( y \)”), binary functional symbols \( :, \times \) (“division, multiplication”), and all the standard connectives, quantifiers, and parentheses. Note that we have no predicates for mass and force; this is remarkable because it shows that the Newtonian revolution has a purely geometric content. Now we introduce a theory \( T \) in \( L \) via its special axioms. The special axioms are as follows. First one asks that distances are numbers:

\[
\forall x \forall y (n(d(x, y)))
\]

and the same for accelerations, and times of revolution. (Note that we view all physical quantities as measured in centimeters and seconds.) For numbers we ask that multiplication and division of numbers are numbers:

\[
(n(x) \land n(y)) \to (n(x : y) \land n(x \times y))
\]

and that the usual laws relating \( : \) and \( \times \) hold. Here are two:

\[
\forall x(x : x = 1) \\
\forall x \forall y \forall z \forall u ((x : y = z : u) \leftrightarrow (x \times u = z \times y))
\]

Exercise: write down the all these laws. We sometimes write \( \frac{x}{y}, 1/x, xy, x^2, x^3, ... \) in the usual sense. The above is a “baby mathematics” and this is all mathematics we need. Next we introduce an axiom whose justification is in mathematics, indeed in calculus; here we ignore the justification and just take this as an axiom. The axiom gives a formula for the acceleration of a body revolving in a circle around a fixed body. (See the exercise after this example.) Here is the axiom:

\[
A) \forall x \forall y \left( (x \circ y) \to (a(x, y) = \frac{4\pi^2d(x, y)}{T^2(x, y)}) \right)
\]

To this one adds the following “obvious” axioms

\[
\begin{align*}
\text{O1)} & \forall x (c(x) \to d(x, E) = R) \\
\text{O2)} & M \circ E \\
\text{R)} & c(r) \\
\text{K1)} & \forall x (p(x) \to (x \circ S))
\end{align*}
\]

saying that the distance between cannon balls and the center of the Earth is the radius of the Earth; that the Moon revolves around the Earth; that the rock \( r \) is a cannon ball; and that all planets revolve around the Sun. (The latter is Kepler’s
first law in an approximate form; the full Kepler’s first law specifies the shape of orbits as ellipses, etc.) Now we consider the following sentences (NOT AXIOMS!):

G) $\forall x \forall y ((c(x) \land c(y)) \rightarrow (a(x, E) = a(y, E))$

K3) $\forall x \forall y (p(x) \land p(y)) \rightarrow \left( \frac{d^3(x, S)}{T^2(x, S)} = \frac{d^3(y, S)}{T^2(y, S)} \right)$

N) $\forall x \forall y \forall z \left( (f(x, z) \land f(y, z)) \rightarrow \left( \frac{a(x, z)}{1/d^2(x, z)} = \frac{a(y, z)}{1/d^2(y, z)} \right) \right)$

$G$ represents Galileo’s great empirical discovery that all cannon balls (by which we mean here terrestrial airborne objects with no self-propulsion) have the same acceleration towards the Earth. $K3$ is Kepler’s third law which is his empirical great discovery that the cubes of distances of planets to the Sun are in the same proportion as the squares of their periods of revolution. Kepler’s second law about equal areas being swept in equal times is somewhat hidden in axiom $A$ above.

$N$ is Newton’s law of gravitation saying that the accelerations of any two bodies moving freely towards a fixed body are in the same proportion as the inverses of the squares of the respective distances to the (center of the) fixed body. Newton’s great invention is the creation of a binary predicate $f$ (where $f(x, y)$ is translated in English as “$x$ is in free fall with respect to $y$”) equipped with the following axioms

F1) $\forall x (c(x) \rightarrow f(x, E))$

F2) $f(M, E)$

F3) $\forall x (p(x) \rightarrow f(x, S))$

expressing the idea that cannon balls and the Moon moving relative to the Earth and planets moving relative to the Sun are instances of a the more general predicate expressing “free falling”. Finally let us consider the definition

$g = a(r, E)$

and the following sentence:

X) $g = \frac{4\pi^2d^3(M, E)}{T^2(M, E)}$

The main results are the following theorems in $T$:

**Theorem 12.20.** $N \rightarrow X$

*Proof.* See the exercise after this example.

**Theorem 12.21.** $N \rightarrow G$

*Proof.* See the exercise after this example.

**Theorem 12.22.** $N \rightarrow K3$

*Proof.* See the exercise after this example.

So if one accepts Newton’s $N$ then Galileo’s $G$ and Kepler’s $K3$ follow, that is to say that $N$ “unifies” terrestrial physics with the physics of Heaven. The beautiful thing is however that $N$ not only unifies known paradigms but “predicts” new “facts”, e.g. $X$. Indeed one can verify $X$ using experimental (astronomical and terrestrial physics) data: if one enlarges our language to include numerals and numerical computations and if one introduces axioms as below (justified by measurements) then $X$ becomes a theorem. Here are the additional axioms:

$g = 981$ (the number of centimeters per second squared representing $g$)

$\pi = \frac{314}{100}$ (approximate value)
\[ R = \text{number of centimeters representing the radius of the Earth (measured for the first time by Eratosthenes using shadows at two points on Earth)} \]
\[ d(M, E) = \text{number of centimeters representing the distance from Earth to Moon (measured using parallaxes)} \]
\[ T(M, E) = \text{number of seconds representing the time of revolution of the Moon (the equivalent of 28 days)} \]

The fact that \( X \) is verified with the above data is the miraculous computation done by Newton that convinced him of the validity of his theory; see the exercise after this example.

**Remark 12.23.** This part of Newton’s early work had a series of defects: it was based on the circular (as opposed to elliptical) orbits, it assumed the center of the Earth (rather than all the mass of the Earth) as responsible for the effect on the cannon balls, it addressed only revolution around a fixed body (which is not realistic in the case of the Moon, since, for instance, the Earth itself is moving), and did not explain the difference between the \( d^3/T^2 \) of planets around the Sun and the corresponding quantity for the Moon and cannon balls relative to the Earth. Straightening these and many other problems is part of the reason why Newton postponed publication of his early discoveries. The final theory of Newton involves the introduction of absolute space and time, mass, and forces. The natural to develop it is within mathematics, as mathematical physics; this is essentially the way Newton himself presented his theory in published form. However the above example suggests that the real breakthrough was not mathematical but at the level of (pre-mathematical) logic.

**Exercise 12.24.**
1) Justify Axiom \( A \) above using calculus or even Euclidean geometry plus the definition of acceleration in an introductory physics course.
2) Prove Theorems 12.20, 12.21, and 12.22.
3) Verify that with the numerical data for \( g, \pi, R, d(M, E), T(M, E) \) available from astronomy (find the numbers in astronomy books) the sentence \( X \) becomes a theorem. This is Newton’s famous computation.
Part 2

Mathematics
Mathematics is a particular theory $T_{set}$ (called set theory) in a particular language $L_{set}$ (called the language of set theory) with specific axioms called the ZFC axioms. So $T_{set}$ will be $T(ZFC)$. We will introduce all of this presently.

**Metadefinition 13.1.** The language $L_{set}$ of set theory is the language with variables $x, y, z, \ldots$, constants $a, b, c, \ldots, A, B, C, \ldots$, $\alpha, \beta, \gamma, \ldots$, no functional symbol, a binary relational predicate $\in$, connectives $\lor, \land, \neg, \to, \leftrightarrow$, quantifiers $\forall, \exists$, equality $=$, and typographical symbols (,),. We also assume a witness assignment on $L_{set}$ and definitions in $L_{set}$ are given. We take the liberty to add, whenever it is convenient, new constants and new predicates to $L_{set}$ together with definitions for each of these new symbols. The constants of $L_{set}$ will be called sets.

**Remark 13.2.** In the above metadefinition the witness assignment and the definitions were left unspecified. If one wants to pin down this concept further one can start with the language $L_0$ that has variables $x, y, z, \ldots$, no constants, no functional symbol, a binary relational predicate $\in$, connectives $\lor, \land, \neg, \to, \leftrightarrow$, quantifiers $\forall, \exists$, equality $=$, and separators (parentheses (,) and comma); one assumes no definition in $L_0$. Then one can take $L'$ to be the witness closure of $L_0$. Next we let $L$ be obtained from $L'$ by adding new constants $a, b, \ldots$, together with definitions for them, and also adding new relational predicates $\neq, \notin, \subset, \not\subset$ defined by

\[
\forall x \forall y ((x \neq y) \leftrightarrow \neg(x = y))
\]
\[
\forall x \forall y ((x \notin y) \leftrightarrow \neg(x \in y))
\]
\[
\forall x \forall y ((x \subset y) \leftrightarrow \forall z ((z \in x) \to (z \in y)))
\]
\[
\forall x \forall y ((x \not\subset y) \leftrightarrow \neg(x \subset y))
\]

This $L$ is the prototypical example we have in mind for $L_{set}$. Even with other examples of $L_{set}$ we will maintain the above definitions of $\neq, \notin, \subset, \not\subset$.

**Remark 13.3.** We recall the fact that $L_{set}$ being a language it does not make sense to say that a sentence in it (such as, for instance, $a \in b$) is true or false.

**Remark 13.4.** Note that the collection of sets is “metacountable” in the sense that it can be arranged in an (unending) string of symbols with commas in between. Later we will introduce the concept of “countable” set and we will show that not all sets are countable. This seems to be a paradox (referred to as the Skolem paradox.) Of course this is not going to be a paradox: “metacountable” and “countable” will be two different concepts. The words “metacountable” belong to the metalanguage and can be translated in English in terms of arranging symbols on a piece of paper; whereas “$b$ is countable” is a definition in set theory; we define “$b$ is countable $\iff C(b)$” where $C(x)$ is a certain formula with free variable $x$ in the language of set theory.
Remark 13.5. There is a standard translation of the language $L_{\text{set}}$ of set theory into the English language as follows:

- $a, b, \ldots$ are translated as "the set $a$", "the set $b$",...
- $\in$ is translated as "belongs to the set" or as "is an element of the set"
- $=$ is translated as "equals"
- $\subseteq$ is translated as "is a subset"
- $\forall$ is translated as "for all sets"
- $\exists$ is translated as "there exists a set"

while the connectives are translated in the standard way.

Remark 13.6. Once we have a translation of $L_{\text{set}}$ into English we can speak of argot and translation of $L_{\text{set}}$ into argot; this simplifies comprehension of mathematical texts considerably.

Remark 13.7. The standard translation of the language of set theory into English (in the remark above) is standard only by convention. A perfectly good different translation is, for instance, the one in which

- $a, b, \ldots$ are translated as "crocodile $a"", "crocodile $b",,,,
- $\in$ is translated as "is dreamt by the crocodile"
- $=$ is translated as "has the same taste"
- $\forall$ is translated as "for all crocodiles"
- $\exists$ is translated as "there exists a crocodile"

One could read mathematical texts in this translation; admittedly the English text that would result from this translation would be somewhat strange.

Remark 13.8. Note that mathematics uses other symbols as well such as

\[ \leq, o, +, \times, \sum a_n, Z, Q, R, C, \equiv, \lim, \int f(x)dx, \frac{df}{dx}, \ldots \]

These symbols will originally be all sets (hence constants) and will be introduced through appropriate definitions (like the earlier definition of an elephant); they will all be defined through the predicate $\in$. In particular in the language of sets + or $\times$ are NOT originally functional symbols; and $\leq$ is NOT originally a relational predicate. However we will later tacitly enlarge the language of set theory by adding predicates (usually still denoted by) + or $\leq$ via appropriate definitions.

We next introduce the (specific) axioms of set theory.

Axiom 13.9. (Singleton axiom)

\[ \forall x \exists y ((x \in y) \land (\forall z ((z \in y) \rightarrow (z = x))) \]

The translation in argot is that for any set $x$ there is a set $y$ whose only element is $x$.

Axiom 13.10. (Unordered pair axiom)

\[ \forall x \forall x' \exists y ((x \in y) \land (x' \in y) \land ((z \in y) \rightarrow ((z = x) \lor (z = x')))) \]

In argot the translation is that for any two sets $x, x'$ there is a set that only has them as elements.

Axiom 13.11. (Separation axioms) For any formula $P(x)$ in the language of sets, having a free variable $x$, we introduce an axiom

\[ \forall y \exists z \forall x ((x \in z) \leftrightarrow ((x \in y) \land (P(x))) \]
The translation in argot is that for any set \( y \) there is a set \( z \) whose elements are all the elements \( x \) of \( y \) such that \( P(x) \).

**Axiom 13.12.** (Extensionality axiom)

\[
\forall u \forall v ((u = v) \leftrightarrow \forall x ((x \in u) \leftrightarrow (x \in v)))
\]

The translation in argot is that two sets \( u \) and \( v \) are equal if and only if they have the same elements.

**Axiom 13.13.** (Union axiom)

\[
\forall w \exists u \forall x ((x \in u) \leftrightarrow \exists t (((t \in w) \land (x \in t))))
\]

The translation in argot is that for any set \( w \) there exists a set \( u \) such that for any \( x \) we have that \( x \) is an element of \( u \) if and only if \( x \) is an element of one of the elements of \( w \).

**Axiom 13.14.** (Empty set axiom)

\[
\exists x \forall y (y \not\in x)
\]

The translation in argot is that there exists a set that has no elements.

**Axiom 13.15.** (Power set axiom)

\[
\forall y \exists z \forall x ((x \in z) \leftrightarrow (\forall u ((u \in x) \rightarrow (u \in y))))
\]

The translation in argot is that for any set \( y \) there is a set \( z \) such that a set \( x \) is an element of \( z \) if and only if all elements of \( x \) are elements of \( y \).

For simplicity the rest of the axis will be formulated in argot only.

**Axiom 13.16.** (Axiom of choice). For any set \( w \) whose elements are pairwise disjoint sets there is a set that has exactly one element in common with each of the sets in \( w \). (Two sets are disjoint if they have no element in common. The elements of a set are pairwise disjoint if any two elements are disjoint.)

**Axiom 13.17.** (Axiom of infinity). There exists a set \( x \) such that \( x \) contains some element \( u \) and such that for any \( y \in x \) there exists \( z \in x \) with the property that \( y \) is the only element of \( z \). Intuitively this axiom guarantees the existence of “infinite” sets.

**Axiom 13.18.** (Axiom of foundation). For any set \( x \) there exists \( y \in x \) such that \( x \) and \( y \) are disjoint.

One finally adds a technical list of axioms (indexed by formulas \( P(x,y,z) \)) about the “images of maps with parameters \( z \)”; we shall not state it precisely and we shall not use it in the sequel.

**Axiom 13.19.** (Axiom of replacement). If for any \( z \) and any \( u \) we have that \( P(x,y,z) \) “defines \( y \) as a function of \( x \in u \)” (i.e. for any \( x \in u \) there exists a unique \( y \) such that \( P(x,y,z) \)) then for all \( z \) there is a set \( v \) which is the “image of this map” (i.e. \( v \) consists of all \( y \)’s with the property that there is an \( x \in u \) such that \( P(x,y,z) \)). Here \( x, z \) may be tuples of variables.

**Exercise 13.20.** Write the axioms of choice, infinity, foundation, and replacement in the language of sets.
Metadefinition 13.21. All of the above axioms form the ZFC system of axioms (Zermelo-Fraenkel+Choice). Set theory $T_{set}$ is the theory $T(ZFC)$ in $L_{set}$ generated by the ZFC axioms. Unless otherwise specified all theorems in the rest of the course are understood to be theorems in $T_{set}$.

Remark 13.22. If set theory is to have a meaning at all one needs to be able to give a metaproof of the metasentence:

Set theory is consistent

But the above metasentence involves quantifiers so no metaproof for it can be given. The only argument in favor of using set theory seems to be the fact that nobody could prove so far a statement of the form $P \land \neg P$ in this theory. Once mathematics is introduced and mathematical logic is developed one can introduce something which we will call formalized set theory; we will be able then to consider a sentence $C$ in set theory whose translation in English will be:

Formalized set theory is formally consistent

(See the last part of the course dedicated to mathematical logic for an explanation of this sentence.) Gödel proved that the sentence $C$ viewed as a sentence in formalized theory is not “formally provable” (in a sense that, again, will be explained in the last part of the course).

Remark 13.23. Note the important fact that the axioms did not involve constants. In the next chapter we investigate the constants, i.e. the sets.
CHAPTER 14

Sets

We finally start discussing/proving facts about set theory.

FROM THIS MOMENT ON ALL PROOFS IN THIS COURSE WILL BE WRITTEN IN ARGOT; ALSO, UNLESS OTHERWISE STATED, ALL PROOFS REQUIRED TO BE GIVEN IN THE EXERCISES MUST BE WRITTEN IN ARGOT.

Recall that we introduced mathematics/set theory as being a specific theory \( T(ZFC) \) in the language \( L_{set} \), which we called \( T_{set} \), where \( ZFC \) is a list of axioms that was described in the last chapter.

Recall the following:

**Metadefinition 14.1.** A set is a constant in the language of set theory.

**Notation 14.2.** Sets will be denoted by \( a, b, ..., A, B, ..., \alpha, \beta, \gamma, ... \).

**Notation 14.3.** We define a new constant \( \emptyset \) as being equal to the witness for the axiom \( \exists x \forall y (y \not\in x) \); in other words \( \emptyset \) is defined by

\[
\emptyset = c \forall y (y \not\in x)
\]

We usually say that \( \emptyset \) denotes the witness above.

**Notation 14.4.** If \( a \) is a set we introduce a new constant \( \{ a \} \) defined to be the witness for the sentence \( \exists y P \) where

\[ P \] equals \( "(a \in y) \land (\forall z ((z \in y) \rightarrow (z = a)))" \)

In other words \( \{ a \} \) is defined by

\[
\{ a \} = c^P = c^{(a \in y) \land (\forall z ((z \in y) \rightarrow (z = a)))}
\]

The sentence \( \exists y P \) is a theorem (use the singleton axiom) so the following is a theorem:

\[
(a \in \{ a \}) \land (\forall z ((z \in \{ a \}) \rightarrow (z = a)))
\]

We can say (and we will usually say, by abuse of terminology) that \( \{ a \} \) is “the unique” set containing \( a \) only among its elements; we will often use this kind of abuse of terminology.

**Notation 14.5.** In particular \( \{ \{ a \} \} \) denotes the set whose only element is the set \( \{ a \} \), etc.

**Notation 14.6.** For any two sets \( a, b \) with \( a \neq b \) denote by \( \{ a, b \} \) the set that only has \( a \) and \( b \) as elements; the set \( \{ a, b \} \) exists by the unordered pair axiom. Also whenever we write \( \{ a, b \} \) we implicitly understand that \( a \neq b \).
Notation 14.7. For any set \( A \) and any formula \( P(x) \) in the language of sets, having one free variable \( x \) we denote by \( A(P) \) or \( \{ a \in A; P(a) \} \) the set whose elements are the elements \( a \in A \) such that \( P(a) \); the set \( A(P) \) equals by definition the witness for the separation axiom that corresponds to \( A \) and \( P \).

Exercise 14.8. Explain the last claim.

Lemma 14.9. If \( A = \{ a \} \) and \( B = \{ b, c \} \) then \( A \neq B \).

Proof. We proceed by contradiction. So assume \( A = \{ a \}, B = \{ b, c \} \) and \( A = B \) and seek a contradiction. Indeed since \( a \in A \) and \( A = B \), by the extensionality axiom we get \( a \in B \). Hence \( a = b \) or \( a = c \). Assume \( a = b \) and seek a contradiction. (In the same way we get a contradiction by assuming \( a = c \).) Since \( a = b \) we get \( B = \{ a, c \} \). Since \( c \in B \) and \( A = B \), by the extensionality axiom we get \( c \in A \). So \( c = a \). Since \( a = b \) we get \( b = c \). But by our notation for sets (elements listed are distinct) we have \( b \neq c \), a contradiction.

Exercise 14.10. Prove that:
1) If \( \{ a \} = \{ b \} \) then \( a = b \).
2) \( \{ a, b \} = \{ b, a \} \).
3) \( \{ a \} = \{ x \in \{ a, b \}; x \neq b \} \).
4) There is a set \( b \) whose only elements are \( \{ a \} \) and \( \{ a, \{ a \} \} \) such that \( b = \{ \{ a \}, \{ a, \{ a \} \} \} \).

Exercise 14.11. Prove that:
1) \( A(P \land Q) = A(P) \land A(Q) \).
2) \( A(P \lor Q) = A(P) \lor A(Q) \).
3) \( A(\neg P) = A \setminus A(P) \).

Notation 14.12. For any two sets \( A \) and \( B \) we define the set \( A \cup B \) (called the union of \( A \) and \( B \)) as the set such that for all \( c, c \in A \cup B \) if and only if \( c \in A \) or \( c \in B \); the set \( A \cup B \) is a witness for the union axiom.

We introduce the following definition in set theory:

Definition 14.13. The intersection of two sets \( A \) and \( B \) is the set
\[ A \cap B = \{ c \in A; c \in B \} . \]
The difference is the set
\[ A \setminus B = \{ c \in A; c \notin B \} . \]

Exercise 14.14. Prove that if \( a, b, c \) are such that \( (a \neq b) \land (b \neq c) \land (a \neq c) \) then there is a set denoted by \( \{ a, b, c \} \) whose only elements are \( a, b, c \); in other words prove the following sentence:
\[ \forall x \forall x' \forall x'' \exists y ((x \in y) \land (x' \in y) \land (x'' \in y) \land (z \in y)) \rightarrow ((z = x) \lor (z = x') \lor (z = x'')) \]
Hint: use the singleton axiom, the unordered pair axiom, and the union axiom, applied to the set \( \{ \{ a \}, \{ b, c \} \} \).

Notation 14.15. Similarly one defines sets \( \{ a, b, c, d \} \), etc. Whenever we write \( \{ a, b, c \} \) or \( \{ a, b, c, d \} \), etc, we imply that the elements in each set are pairwise unequal (pairwise distinct). Also denote by
\[ \{ a, b, c, ... \} \]
any set \( d \) such that
\[ (a \in d) \land (b \in d) \land (c \in d) \]
So the dots indicate that there may (or may not) be other elements in \( d \) other than \( a, b, c \); also note that when we write \( \{a, b, c, \ldots\} \) we implicitly imply that \( a, b, c \) are pairwise distinct.

**Definition 14.16.** Two sets \( a \) and \( b \) are disjoint if \( a \cap b = \emptyset \).

**Exercise 14.17.**
1) Prove that \( \{\emptyset\} \neq \emptyset \).
2) Prove that \( \{\{\emptyset\}\} \neq \emptyset \).

**Remark 14.18.** By the definition of the predicate \( \subseteq \) if \( A \) and \( B \) are sets then \( A \) is a subset of \( B \) if and only if for all \( c \), if \( c \in A \) then \( c \in B \); we write \( A \subseteq B \).

**Remark 14.19.** \( A = B \) if and only if \( A \subseteq B \) and \( B \subseteq A \).

**Exercise 14.20.** Prove that:
1) \( \{a, b, c\} = \{b, c, a\} \).
2) \( \{a, b\} \neq \{a, b, c\} \); Hint: use \( c \neq a, c \neq b \).
3) \( \{a, b, c\} = \{a, b, d\} \) if and only if \( c = d \).

**Exercise 14.21.** Let \( A = \{a, b, c\} \) and \( B = \{c, d\} \). Prove that
1) \( A \cup B = \{a, b, c, d\} \),
2) \( A \cap B = \{c\} \), \( A \setminus B = \{a, b\} \).

**Exercise 14.22.** Let \( A = \{a, b, c, d, e, f, g, h\} \), \( B = \{d, e, f, g, h\} \). Compute
1) \( A \cap B \),
2) \( A \cup B \),
3) \( A \setminus B \),
4) \( B \setminus A \),
5) \( (A \setminus B) \cup (B \setminus A) \).

**Exercise 14.23.** Prove the following:
1) \( A \cup B \subseteq A \),
2) \( A \subseteq A \cup B \),
3) \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \),
4) \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \),
5) \( (A \setminus B) \cap (B \setminus A) = \emptyset \).

**Notation 14.24.** For any set \( A \) we define the set \( \mathcal{P}(A) \) as the set whose elements are the subsets of \( A \); we call \( \mathcal{P}(A) \) the power set of \( A \); \( \mathcal{P}(A) \) is a witness for (a theorem obtained from) the power set axiom.

**Example 14.25.** If \( A = \{a, b, c\} \) then
\[
\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.
\]

**Exercise 14.26.** Let \( A = \{a, b, c, d\} \). Write down the set \( \mathcal{P}(A) \).

**Exercise 14.27.** Let \( A = \{a, b\} \). Write down the set \( \mathcal{P}(\mathcal{P}(A)) \).

**Definition 14.28.** (Ordered pairs) Let \( A \) and \( B \) be sets and let \( a \in A, b \in B \). If \( a \neq b \) the ordered pair \( (a, b) \) is the set \( \{\{a\}, \{a, b\}\} \). We sometimes say “pair” instead of “ordered pair”. If \( a = b \) the pair \( (a, b) = (a, a) \) is the set \( \{\{a\}\} \). Note that \( (a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \).
Notation 14.29. For any sets $A$ and $B$ we define the set $A \times B$ as the set (called the product of $A$ and $B$)
\[ \{ c \in \mathcal{P}(A \cup B); \exists x \exists y((x \in A) \land (y \in B) \land (c = (a, b))) \}\]
whose elements are exactly the pairs $(a, b)$ with $a \in A$ and $b \in B; A \times B$ is a witness for a theorem following from the separation axioms and the existence of ordered pairs.

Proposition 14.30. $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Proof. We need to prove that
1) If $a = c$ and $b = d$ then $(a, b) = (c, d)$ and
2) If $(a, b) = (c, d)$ then $a = c$ and $b = d$.

Now 1) is obvious. To prove 2) assume $(a, b) = (c, d)$.

Assume first $a \neq b$ and $c \neq d$. Then by the definition of pairs we know that
\[ \{ \{a\}, \{a, b\} \} = \{ \{c\}, \{c, d\} \}. \]
Since $\{a\} \in \{ \{a\}, \{a, b\} \}$ it follows (by the extensionality axiom) that $\{a\} \in \{ \{c\}, \{c, d\} \}$. Hence either $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$. But as seen before $\{a\} \neq \{c, d\}$. So $\{a\} = \{c\}$. Since $a \in \{a\}$ it follows that $a \in \{c\}$ hence $a = c$. Similarly since $\{a, b\} \in \{\{a\}, \{a, b\}\}$ we get $\{a, b\} \in \{\{c\}, \{c, d\}\}$. So either $\{a, b\} = \{c\}$ or $\{a, b\} = \{c, d\}$. Again as seen before $\{a, b\} \neq \{c\}$ so $\{a, b\} = \{c, d\}$. So $b \in \{c, d\}$.

So $b = c$ or $b = d$. Since $a \neq b$ and $a = c$ we get $b \neq c$. Hence $b = d$ and we are done in case $a \neq b$ and $c \neq d$.

Assume next $a = b$ and $c = d$. Then by the definition of pairs in this case we have $\{\{a\}\} = \{\{c\}\}$ and as before this implies $\{a\} = \{c\}$ hence $a = c$ so we are done in this case as well.

Finally assume $a = b$ and $c \neq d$. (The case $a \neq b$ and $c = d$ is treated similarly.) By the definition of pairs we get
\[ \{\{a\}\} = \{\{c\}, \{c, d\}\}. \]
We get $\{c, d\} \in \{\{a\}\}$. Hence $\{c, d\} \in \{a\}$ which is impossible, as seen before. This ends the proof. \hfill $\Box$

Exercise 14.31. If $A = \{a, b, c\}$ and $B = \{c, d\}$ then
\[ A \times B = \{(a, c), (a, d), (b, c), (b, d), (c, c), (c, d)\}. \]
Hint: by the above Proposition the pairs are distinct.

Exercise 14.32. Prove that
1) $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
2) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

Exercise 14.33. Prove that there does not exist a set $T$ such that for any set $A$ we have $A \in T$. (In other words there is no set of all sets.) Hint. Assume there is such a $T$ and derive a contradiction (which is called the Russell paradox; this is of course no paradox.) To derive a contradiction consider the set
\[ S = \{ A \in T; A \not\in A \}. \]
There are two possibilities. First $S \not\in S$ hence, by the definition of $S$, and since $S \in T$, we get that $S \in S$, a contradiction. The second possibility is that $S \in S$ hence, by the definition of $S$, and since $S \in T$, we get that $S \not\in S$, which is again a contradiction.
CHAPTER 15

Maps

Definition 15.1. A map of sets $F : A \to B$ (or a function) is a subset $F \subset A \times B$ such that for any $a \in A$ there is a unique $b \in B$ with $(a, b) \in F$.

Remark 15.2. We tacitly introduce the new predicate “is a map from ... to ...” by an appropriate definition in the language of sets. Also, if $F, A, B$ are sets (hence constants) such that “$F$ is a map from $A$ to $B$” is a theorem we may introduce a new functional symbol (still denoted by $F$) by

$$\forall x \forall y ((F(x) = y) \leftrightarrow ((x, y) \in F))$$

We sometimes write $a \mapsto F(a)$. Also we sometimes write $A \xrightarrow{F} B$.

Example 15.3. The set

$$(15.1) \quad F = \{(a, a), (b, c)\} \subset \{a, b\} \times \{a, b, c\}$$

is a map and $F(a) = a$, $F(b) = c$. On the other hand the subset

$F = \{(a, b), (a, c)\} \subset \{a, b\} \times \{a, b, c\}$

is not a map.

Definition 15.4. For any $A$ the identity map $I : A \to A$ is defined as $I(a) = a$, i.e.

$$I = I_A = \{(a, a); a \in A\} \subset A \times A.$$  

Definition 15.5. A map $F : A \to B$ is injective (or an injection, or one-to-one) if $F(a) = F(c)$ implies $a = c$.

Definition 15.6. A map $F : A \to B$ is surjective (or a surjection, or onto) if for any $b \in B$ there is a $a \in A$ such that $F(a) = b$.

Example 15.7. The map (15.1) is injective and not surjective.

Exercise 15.8. Give an example of a map which is surjective and not injective.

Exercise 15.9. If $F : A \to B$ and $G : B \to C$ are two maps then there exists a unique map $H : A \to C$ (denoted by $H = G \circ F$) such that $H(a) = G(F(a))$ for all $a$. Hint: we let $(a, c) \in H$ if and only if there exists $b \in B$ with $(a, b) \in F$, $(b, c) \in G$.

Exercise 15.10. Prove that if $F \circ G$ is surjective then $F$ is surjective. Prove that if $F \circ G$ is injective then $G$ is injective.

Notation 15.11. By a commutative diagram of sets

$$
\begin{array}{ccc}
A & \xrightarrow{F} & B \\
U & \downarrow & \downarrow V \\
C & \xrightarrow{G} & D
\end{array}
$$

93
we mean a collection of sets and maps as above with the property that \( G \circ U = V \circ F \).

**Exercise 15.12.** Prove that the composition of two injective maps is injective and the composition of two surjective maps is surjective.

**Definition 15.13.** A map is bijective (or a bijection) if it is injective and surjective.

Here is a fundamental theorem in set theory:

**Theorem 15.14.** *(Bernstein’s Theorem)* If \( A \) and \( B \) are sets and if there exist injective maps \( F : A \to B \) and \( G : B \to A \) then there exists a bijective map \( H : A \to B \).

The reader may attempt to prove this after he/she gets to the chapter on induction.

**Exercise 15.15.** Prove that if \( F : A \to B \) is bijective then there exists a unique bijective map denoted by \( F^{-1} : B \to A \) such that \( F \circ F^{-1} = I_B \) and \( F^{-1} \circ F = I_A \). \( F^{-1} \) is called the inverse of \( F \).

**Exercise 15.16.** Let \( F : \{a, b, c\} \to \{c, d, e\} \), \( F(a) = d \), \( F(b) = c \), \( F(c) = e \). Prove that \( F \) has an inverse and compute \( F^{-1} \).

**Exercise 15.17.** Prove that if \( A \) and \( B \) are sets then there exist maps \( F : A \times B \to A \) and \( G : A \times B \to B \) such that \( F(a, b) = a \) and \( G(a, b) = b \) for all \((a, b) \in A \times B \). (These are called the first and the second projection.) Hint: For \( G \) show that \( G = \{( (a, b), c) ; c = b \} \subset (A \times B) \times B \) is a map.

**Exercise 15.18.** Prove that \((A \times B) \times C \to A \times (B \times C)\), \( ((a, b), c) \mapsto (a, (b, c)) \) is a bijection.

**Notation 15.19.** Write \( A \times B \times C \) instead of \((A \times B) \times C \) and write \((a, b, c)\) instead of \(( (a, b), c) \). We call \((a, b, c)\) a triple. Write \( A^2 = A \times A \) and \( A^3 = A \times A \times A \). More generally adopt this notation for arbitrary number of factors. Elements like \((a, b), (a, b, c), (a, b, c, d), \ldots \) will be called tuples.

**Theorem 15.20.** If \( A \) is a set then there is no bijection between \( A \) and \( \mathcal{P}(A) \)

**Proof.** Assume there exists a bijection \( F : A \to \mathcal{P}(A) \) and seek a contradiction. Consider the set
\[
B = \{ a \in A ; a \notin F(a) \} \in \mathcal{P}(A)
\]
Since \( F \) is subjective there exists \( b \in A \) such that \( B = F(b) \). There are two cases: either \( b \in B \) or \( b \notin B \). If \( b \in B \) then \( b \in F(b) \) so \( b \notin B \), a contradiction. If \( b \notin B \) then \( b \notin F(b) \) so \( b \in B \), a contradiction, and we are done.

**Remark 15.21.** Note the similarity between the above argument and the argument showing that there is no set having all sets as elements (the “Russell paradox”).

**Definition 15.22.** Let \( S \) be a set of sets and \( I \) a set. A family of sets in \( S \) indexed by \( I \) is a map \( I \to S, i \mapsto A_i \). We sometimes drop the reference to \( S \). We also write \((A_i)_{i \in I}\) to denote this family. By the union axiom for any such family there is a set (denoted by \( \bigcup_{i \in I} A_i \), called their union) such that for all \( x \) we have that \( x \in \bigcup_{i \in I} A_i \) if and only if there exists \( i \in I \) such that \( x \in A_i \). Also a set (denoted by \( \bigcap_{i \in I} A_i \), called their intersection) exists such that for all \( x \) we have
that \( x \in \bigcap_{i \in I} A_i \) if and only if for all \( i \in I \) we have \( x \in A_i \). A family of elements in \((A_i)_{i \in I}\) is a map \( I \to \bigcup_{i \in I} A_i \), \( i \mapsto a_i \), such that for all \( i \in I \) we have \( a_i \in A_i \). Such a family of elements is denoted by \((a_i)_{i \in I}\). One defines the product \( \prod_{i \in I} A_i \) as the set \( \{ (a_i)_{i \in I} \mid a_i \in A_i \} \).

**Exercise 15.23.** Check that for \( I = \{ i, j \} \) the above definitions of \( \cup, \cap, \prod \) yield the usual definition of \( A_i \cap A_j, A_i \cap A_j \) and \( A_i \times A_j \).

**Definition 15.24.** Let \( F : A \to B \) be a map and \( X \subseteq A \). Define the image of \( X \) as the set

\[
F(X) = \{ F(x) \mid x \in X \} \subseteq B
\]

If \( Y \subseteq B \) define the inverse image of \( Y \) as the set

\[
F^{-1}(Y) = \{ x \in A \mid F(x) \in Y \} \subseteq A.
\]

For \( y \in B \) define

\[
F^{-1}(y) = \{ x \in A \mid F(x) = y \}
\]

(Note that \( F^{-1}(Y) \), \( F^{-1}(y) \) are defined even if the inverse map \( F^{-1} \) does not exist.)

**Exercise 15.25.** Let \( F : \{ a, b, c, d, e, f, g \} \to \{ c, d, e, h \} \), \( F(a) = d, F(b) = c, F(c) = c, F(d) = c, F(e) = d, F(f) = c, F(g) = c \). Let \( X = \{ a, b, c \}, Y = \{ c, h \} \). Compute \( F(X), F^{-1}(Y), F^{-1}(c), F^{-1}(h) \).

**Exercise 15.26.** Prove that if \( F : A \to B \) is a map and \( X \subseteq X' \subseteq A \) are subsets then \( F(X) \subseteq F(X') \).

**Exercise 15.27.** Prove that if \( F : A \to B \) is a map and \( (X_i)_{i \in I} \) is a family of subsets of \( A \) then

\[
F(\bigcup_{i \in I} X_i) = \bigcup_{i \in I} F(X_i),
\]

\[
F(\bigcap_{i \in I} X_i) = \bigcap_{i \in I} F(X_i).
\]

If in addition \( F \) is injective show that

\[
F(\bigcap_{i \in I} X_i) = \bigcap_{i \in I} F(X_i).
\]

Give an example showing that the latter may fail if \( F \) is not injective.

**Exercise 15.28.** Prove that if \( F : A \to B \) is a map and \( Y \subseteq Y' \subseteq B \) are subsets then \( F^{-1}(Y) \subseteq F^{-1}(Y') \).

**Exercise 15.29.** Prove that if \( F : A \to B \) is a map and \( (Y_i)_{i \in I} \) is a family of subsets of \( B \) then

\[
F^{-1}(\bigcup_{i \in I} Y_i) = \bigcup_{i \in I} F^{-1}(Y_i),
\]

\[
F^{-1}(\bigcap_{i \in I} Y_i) = \bigcap_{i \in I} F^{-1}(Y_i).
\]

(Here one does not need injectivity like in the case of unions.)

**Notation 15.30.** If \( A \) and \( B \) are sets we denote by \( B^A \subseteq \mathcal{P}(A \times B) \) the set of all maps \( F : A \to B \); sometimes one writes \( \text{Map}(A, B) = B^A \).

**Exercise 15.31.** Let \( 0, 1 \) be two elements. Prove that the map \( \{0, 1\}^A \to \mathcal{P}(A) \) sending \( F : A \to \{0, 1\} \) into the set \( \{ \{0, 1\} \subseteq \mathcal{P}(A) \) is a bijection.

**Exercise 15.32.** Find a bijection between \((C^B)^A\) and \( C^{A \times B} \). Hint: Send \( F \in (C^B)^A, F : A \to C^B \), into the set (map)

\[
\{(a, b, c) \in (A \times B) \times C \mid (a, c) \in F(b) \}.
\]
**Definition 15.33.** A topology on a set $X$ is a subset $\mathcal{T} \subset \mathcal{P}(X)$ of the power
with the following properties:
1) $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$;
2) If $U, V \in \mathcal{T}$ then $U \cap V \in \mathcal{T}$;
3) If $(U_i)_{i \in I}$ is a family of subsets $U_i \subset X$ and if for all $i \in I$ we have $U_i \in \mathcal{T}$
then $\bigcup_{i \in I} U_i \in \mathcal{T}$;

A subset $U \subset X$ is called open if $U \in \mathcal{T}$. A subset $Z \subset X$ is called closed if
$X \setminus Z$ is open.

**Example 15.34.** $\mathcal{T} = \mathcal{P}(X)$ is a topology on $X$.

**Example 15.35.** $\mathcal{T} = \{\emptyset, X\} \subset \mathcal{P}(X)$ is a topology on $X$.

**Exercise 15.36.** Prove that if $U, V \subset X$ then $\mathcal{T} = \{\emptyset, U, V, U \cup V, U \cap V, X\}$
is a topology. Find the closed sets of $X$.

**Exercise 15.37.** Prove that if $(\mathcal{T}_j)_{j \in J}$ is a family of topologies $\mathcal{T}_j \subset \mathcal{P}(X)$ on
$X$ then $\bigcap_{j \in J} \mathcal{T}_j$ is a topology on $X$.

**Definition 15.38.** If $\mathcal{T}_0 \subset \mathcal{P}(X)$ is a subset of the power set then the inter-
section $\mathcal{T} = \bigcup_{\mathcal{T}' \supset \mathcal{T}_0} \mathcal{T}'$
of all topologies $\mathcal{T}'$ containing $\mathcal{T}_0$ is called the topology generated by $\mathcal{T}_0$.

**Exercise 15.39.** Let $\mathcal{T}_0 = \{U, V, W\} \subset \mathcal{P}(X)$. Find explicitly the topology
generated by $\mathcal{T}_0$. Find all the closed sets in that topology.

**Definition 15.40.** A topological space is a pair $(X, \mathcal{T})$ consisting of a set $X$
and a topology $\mathcal{T} \subset \mathcal{P}(X)$ on $X$. Sometimes one writes $X$ instead of $(X, \mathcal{T})$ is $\mathcal{T}$ is
understood from context.

**Definition 15.41.** Let $(X, \mathcal{T})$ and $(X', \mathcal{T}')$ be two topological spaces. A map
$F : X \rightarrow X'$ is continuous if for all $V \in \mathcal{T}'$ we have $F^{-1}(V) \in \mathcal{T}$.

**Exercise 15.42.** If $\mathcal{T}$ is a topology on $X$ and $\mathcal{T}'$ is the topology on $X'$ defined
by $\mathcal{T}' = \{\emptyset, Y\}$ then any map $F : X \rightarrow X'$ is continuous.

**Exercise 15.43.** If $\mathcal{T}$ is the topology $\mathcal{T} = \mathcal{P}(X)$ on $X$ and $\mathcal{T}'$ is any topology
on $X'$ then any map $F : X \rightarrow X'$ is continuous.

**Exercise 15.44.** Prove that if $(X, \mathcal{T}), (X', \mathcal{T}'), (X'', \mathcal{T}'')$ are topological spaces
and $G : X \rightarrow X'$, $F : X' \rightarrow X''$ are continuous maps then the composition
$F \circ G : X \rightarrow X''$ is continuous.

**Exercise 15.45.** Give an example of two topological spaces $(X, \mathcal{T})$ and $(X', \mathcal{T}')$
and of a bijection $F : X \rightarrow X'$ such that $F$ is continuous but $F^{-1}$ is not continuous.
CHAPTER 16

Relations

DEFINITION 16.1. If \( A \) is a set then a relation on \( A \) is a subset \( R \subseteq A \times A \). If \((a, b) \in R\) we write \( aRb \).

REMARK 16.2. We tacitly introduce the new predicate “is a relation on ...” by an appropriate definition in the language of sets. Also, if \( R, A \) are sets (hence constants) such that “\( R \) is a relation on \( A \)” is a theorem we may introduce a new relational predicate (still denoted by \( R \)) by

\[
\forall x \forall y((xRy) \leftrightarrow ((x, y) \in R))
\]

DEFINITION 16.3. A relation \( R \) is called an order if (writing \( a \leq b \) instead of \( aRb \)) we have, for all \( a, b, c \in A \), that

1) \( a \leq a \) (reflexivity),
2) \( a \leq b \) and \( b \leq c \) imply \( a \leq c \) (transitivity),
3) \( a \leq b \) and \( b \leq a \) imply \( a = b \) (antisymmetry).

NOTATION 16.4. One writes \( a < b \) if \( a \leq b \) and \( a \neq b \).

REMARK 16.5. One may introduce a new predicate “is an order relation” in the obvious way. The same can be done with other concepts to be introduced later.

DEFINITION 16.6. An order relation is called total if for any \( a, b \in A \) either \( a \leq b \) or \( b \leq a \). Alternatively we say \( A \) is totally ordered (by \( \leq \)).

EXAMPLE 16.7. For instance if \( A = \{a, b, c, d\} \) then

\[
R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c)\}
\]

is an order but not a total order.

EXERCISE 16.8. Let \( R_0 \subset A \times A \) be a relation and assume \( R_0 \) is contained in an order relation \( R_1 \subset A \times A \). Let

\[
R = \bigcap_{R' \supseteq R_0} R'
\]

be the intersection of all order relations \( R' \) containing \( R_0 \). Prove that \( R \) is an order relation and it is the smallest order relation containing \( R_0 \) in the sense that it is contained in any order relation that contains \( R_0 \).

EXERCISE 16.9. Let \( A = \{a, b, c, d, e\} \) and \( R_0 = \{(a, b), (b, c), (c, d), (c, e)\} \). Find an order relation containing \( R_0 \). Find the smallest order relation \( R \) containing \( R_0 \). Show that \( R \) is not a total order.

EXERCISE 16.10. Let \( A \) be a set. For any subsets \( X \subseteq A \) and \( Y \subseteq A \) write \( X \leq Y \) if and only if \( X \subseteq Y \). This defines a relation on the set \( \mathcal{P}(A) \). Prove that this is an order relation. Give an example showing that this is not in general a total order.
16. RELATIONS

**Definition 16.11.** An ordered set is a pair \((A, \leq)\) where \(A\) is a set and \(\leq\) is an order relation on \(A\).

**Definition 16.12.** Let \((A, \leq)\) and \((A', \leq')\) be ordered sets. A map \(F : A \to A'\) is called increasing if for any \(a, b \in A\) with \(a \leq b\) we have \(F(a) \leq' F(b)\).

**Exercise 16.13.** Prove that if \((A, \leq), (A', \leq'), (A'', \leq'')\) are ordered sets and \(G : A \to A', F : A' \to A''\) are increasing then \(F \circ G : A \to A''\) is increasing.

**Definition 16.14.** Let \(A\) be a set with an order \(\leq\). We say \(\alpha \in A\) is a minimal element of \(A\) if for all \(\alpha \leq a\) we must have \(a = \alpha\).

**Definition 16.15.** Let \(A\) be a set with an order \(\leq\). We say \(\beta \in A\) is a maximal element of \(A\) if for all \(\beta \leq b\) we must have \(\beta = b\).

**Definition 16.16.** Let \(A\) be a set with an order \(\leq\) and let \(B \subseteq A\). We say \(m \in B\) is a minimum element of \(B\) if for all \(b \in B\) we have \(m \leq b\). If a minimum element exists it is unique (check!) and we denote it by \(\min B\). Note that \(\min B\) if it exists, then by definition it belongs to \(B\).

**Definition 16.17.** Let \(A\) be a set with an order \(\leq\) and \(B \subseteq A\). We say \(M \in B\) is a maximum element of \(B\) if for all \(b \in B\) we have \(b \leq M\). If a maximum element exists it is unique and we denote it by \(\max B\). Again, if \(\max B\) exists then by definition it belongs to \(B\).

**Definition 16.18.** Let \(A\) be set with an order \(\leq\) and let \(B \subseteq A\). An element \(u \in A\) is called an upper bound for \(B\) if \(b \leq u\) for all \(b \in B\). We also say that \(B\) is bounded from above by \(u\). An element \(l \in A\) is called a lower bound for \(B\) if \(l \leq b\) for all \(b \in B\); we also say \(B\) is bounded from below by \(l\). If the set of upper bounds of \(B\) has a minimum element we call it the supremum of \(B\) and we denote it by \(\sup B\); if the set of lower bounds of \(B\) has a maximum element we call it the infimum of \(B\) and we denote it by \(\inf B\). (Note that if one of \(\sup B\) and \(\inf B\) exists that element is by definition in \(A\) but does not necessarily belong to \(B\).) We say \(B\) is bounded if it has both an upper bound and a lower bound.

**Exercise 16.19.** Consider the set \(A\) and the order \(\leq\) defined by the relation \(R\) in Exercise 16.9. Does \(A\) have a maximum element? Does \(A\) have a minimum element? Are there maximal elements in \(A\)? Are there minimal elements in \(A\)? List all these elements in case they exist. Let \(B = \{b, c\}\). Is \(B\) bounded? List all the upper bounds of \(B\). List all the lower bounds of \(B\). Does the supremum of \(B\) exist? If yes does it belong to \(B\)? Does the infimum of \(B\) exist? Does it belong to \(B\)?

**Definition 16.20.** A well ordered set is an ordered set \((A, \leq)\) such that any non-empty subset \(B \subseteq A\) has a minimum element.

**Exercise 16.21.** Prove that any well ordered set is totally ordered.

**Remark 16.22.** Later, when we will have introduced the ordered set of integers and the ordered set of rational numbers we will see that the non-negative integers are well ordered but the non-negative rationals are not well ordered.

The following theorems can be proved (but their proof is behind the scope of these notes):
Theorem 16.23. (Zorn’s lemma) Assume \((A, \leq)\) is an ordered set. Assume that any non-empty totally ordered subset \(B \subset A\) has an upper bound in \(A\). Then \(A\) has a maximal element.

Theorem 16.24. (Well ordering principle) Let \(A\) be a set. Then there exists an order relation \(\leq\) on \(A\) such that \((A, \leq)\) is well ordered.

Remark 16.25. It can be proved that if one removes from the axioms of set theory the axiom of choice then the axiom of choice, Zorn’s lemma, and the well ordering principle are all equivalent.

Exercise 16.26. Let \((A, \leq)\) and \((B, \leq)\) be totally ordered sets. Define a relation \(\leq\) on \(A \times B\) by

\[
((a, b) \leq (a', b')) \iff ((a \leq a') \lor (a = a') \land (b \leq b'))
\]

Prove that \(\leq\) is an order on \(A \times B\) (it is called the lexicographic order) and that \((A \times B, \leq)\) is totally ordered. (Explain how this order is being used to order words in a dictionary).

Definition 16.27. A relation \(R\) is called an equivalence relation if (writing \(a \sim b\) instead of \(aRb\)) we have, for all \(a, b, c \in A\), that

1) \(a \sim a\) (reflexivity),
2) \(a \sim b\) and \(b \sim c\) imply \(a \sim c\) (transitivity),
3) \(a \sim b\) implies \(b \sim a\) (symmetry);
we also say that \(\sim\) is an equivalence relation.

Exercise 16.28. Prove that if \(R'\) and \(R''\) are equivalence relations on \(A\) then \(R' \cap R''\) is an equivalence relation.

Exercise 16.29. Let \(R_0 \subset A \times A\) be a relation and let

\[ R = \bigcap_{R' \supset R_0} R' \]

be the intersection of all equivalence relations \(R'\) containing \(R_0\). Prove that \(R\) is an equivalence relation and it is the smallest equivalence relation containing \(R_0\) in the sense that it is contained in any other equivalence relation that contains \(R_0\).

Definition 16.30. Given an equivalence relation \(\sim\) as above for any \(a \in A\) we may consider the set \(\hat{a} := \{c \in A; c \sim a\}\) called the equivalence class of \(a\).

Notation 16.31. Sometimes, instead of \(\hat{a}\), one writes \(\overline{a}\) or \([a]\).

Exercise 16.32. Prove that \(\hat{a} = \hat{b}\) if and only if \(a \sim b\).

Exercise 16.33. Prove that:

1) if \(\hat{a} \cap \hat{b} \neq \emptyset\) then \(\hat{a} = \hat{b}\);
2) \(A = \bigcup_{a \in A} \hat{a}\).

Definition 16.34. If \(A\) is a set a partition of \(A\) is a family \((A_i)_{i \in I}\) if subsets \(A_i \subset A\) such that:

1) if \(i \neq j\) then \(A_i \cap A_j = \emptyset\)
2) \(A = \bigcup_{i \in I} A_i\).
EXERCISE 16.35. Let $A$ be a set and $\sim$ an equivalence relation on it. Prove that:

1) There exists a subset $B \subset A$ which contains exactly one element of each equivalence class (such a set is called a system of representatives; hint: use the axiom of choice).

2) The family $(\hat{b})_{b \in B}$ is a partition of $A$.

EXERCISE 16.36. Let $A$ be a set and $(A_i)_{i \in I}$ a partition of $A$. Define a relation $R$ on $A$ as follows:

$$R = \{(a, b) \in A \times A; \exists i ((i \in I) \land (a \in A_i) \land (b \in A_i))\}$$

Prove that $R$ is an equivalence relation.

EXERCISE 16.37. Let $A$ be a set. Prove that there is a bijection between the set of equivalence relations on $A$ and the set of partitions of $A$. Hint: use the above two exercises.

DEFINITION 16.38. The set of equivalence classes

$$\{\alpha \in \mathcal{P}(A); \exists a ((a \in A) \land (a = \hat{a}))\}$$

is denoted by $A/\sim$ and is called the quotient of $A$ by the relation $\sim$.

EXAMPLE 16.39. For instance if $A = \{a, b, c\}$ and

$$R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

then $R$ is an equivalence relation, $\hat{a} = \hat{b} = \{a, b\}$, $\hat{c} = \{c\}$, and $A/\sim = \{\{a, b\}, \{c\}\}$.

EXERCISE 16.40. Let $A = \{a, b, c, d, e, f\}$ and $R_0 = \{(a, b), (b, c), (d, e)\}$. Find the smallest equivalence relation $R$ containing $R_0$. Call it $\sim$. Write down the equivalence classes $\hat{a}, \hat{b}, \hat{c}, \hat{d}, \hat{e}, \hat{f}$. Write down the set $A/\sim$.

EXERCISE 16.41. Let $S$ be a set of sets. For any sets $X, Y \in S$ write $X \sim Y$ if and only if there exists a bijection $F : X \to Y$. This defines a relation on $S$. Prove that this is an equivalence relation.

EXERCISE 16.42. Let $S = \{A, B, C, D\}$, $A = \{a, b\}$, $B = \{b, c\}$, $C = \{x, y\}$, $D = \emptyset$. Let $\sim$ be the equivalence relation on $S$ defined in the previous exercise. Write down the equivalence classes $\hat{A}, \hat{B}, \hat{C}, \hat{D}$ and write down the set $S/\sim$.

DEFINITION 16.43. An affine plane is a pair $(A, \mathcal{L})$ where $A$ is a set and $\mathcal{L} \subset \mathcal{P}(A)$ is a set of subsets of $A$ satisfying a series of axioms which we now explain. It is convenient to introduce some terminology as follows. $A$ is the called the affine plane. The elements of $A$ are called points. The elements $L$ of $\mathcal{L}$ are called lines; so each such $L \subset A$. We say a point $P$ lies on a line $L$ if $P \in L$; we also say that $L$ passes through $P$. We say that two lines intersect if they have a point in common; we say that two lines are parallel if they either coincide or they do not intersect. We say that 3 points are collinear if they lie on the same line. Here are the axioms that we impose:

1) There exist 3 points which are not collinear and any line has at least 2 points.
2) Any 2 distinct points lie on exactly one line.
3) If $L$ is a line and $P$ is a point not lying on $L$ there exists exactly one line through $P$ which parallel to $L$. 

Remark 16.44. Note that we have not defined 2 or 3 yet; this will be done later when we introduce integers. The meaning of these axioms is however clearly expressible in terms that were already defined. For instance axiom 2 says that for any points $P$ and $Q$ with $P \neq Q$ there exists a line through $P$ and $Q$; we do not need to define the symbol 2 to express this. The same holds for the use of the symbol 3.

Exercise 16.45. Prove that any two distinct non-parallel lines intersect in exactly one point.

Exercise 16.46. Let $A = \{a, b\} \times \{a, b\}$ and let $\mathcal{L} \subset \mathcal{P}(A)$ consist of all subsets of 2 elements; (there are 6 of them). Prove that $(A, \mathcal{L})$ is an affine plane. (Again one can reformulate everything without reference to the symbols 2 or 6; one simply uses 2 or 6 letters and writes that they are $\neq$.)

Exercise 16.47. Let $A = \{a, b, c\} \times \{a, b, c\}$. Find all subsets $\mathcal{L} \subset \mathcal{P}(A)$ such that $(A, \mathcal{L})$ is an affine plane. (This is tedious!)

Definition 16.48. A projective plane is a pair $(\overline{A}, \overline{\mathcal{L}})$ where $\overline{A}$ is a set and $\overline{\mathcal{L}} \subset \mathcal{P}(\overline{A})$ is a set of subsets of $\overline{A}$ satisfying a series of axioms which we now explain. Again it is convenient to introduce some terminology as follows. $\overline{A}$ is the called the projective plane. The elements of $\overline{A}$ are called points, $P$. The elements $\overline{\mathcal{L}}$ of $\overline{\mathcal{L}}$ are called lines; so each such $\overline{\mathcal{L}} \subset \overline{A}$. We say a point $P$ lies on a line $\overline{\mathcal{L}}$ if $P \in \overline{\mathcal{L}}$; we also say that $\overline{\mathcal{L}}$ passes through $P$. We say that two lines intersect if they have a point in common; we say that two lines are parallel if they either coincide or they do not intersect. We say that 3 points are collinear if they lie on the same line. Here are the axioms that we impose:

1) There exist 3 points which are not collinear and any line has at least 3 points.
2) Any 2 distinct points lie on exactly one line.
3) Any 2 distinct lines meet in exactly one point.

Example 16.49. One can attach to any affine plane $(A, \mathcal{L})$ a projective plane $(\overline{A}, \overline{\mathcal{L}})$ as follows. We introduce the relation $\parallel$ on $\mathcal{L}$ by letting $L \parallel L'$ is and only if $L$ and $L'$ are parallel. This is an equivalence relation (check!). Denote by $\hat{L}$ the equivalence class of $L$. Then we consider the set of equivalence classes, $\mathcal{L}_\infty = \mathcal{L}/\parallel$; call this set the line at infinity. We let $\overline{A} = A \cup \mathcal{L}_\infty$ (disjoint union). Define a line in $\overline{A}$ to be either $\mathcal{L}_\infty$ or set of the form $\overline{\mathcal{L}} = L \cup \{\hat{L}\}$. Finally define $\overline{\mathcal{L}}$ to be the set of all lines in $\overline{A}$.

Exercise 16.50. Check that $(\overline{A}, \overline{\mathcal{L}})$ is a projective plane.

Exercise 16.51. Describe the projective plane attached to the affine plane in Exercise 16.46; how many points does it have? How many lines?
CHAPTER 17

Operations

**Definition 17.1.** A binary operation $\star$ on a set $A$ is a map $\star: A \times A \to A$, $(a, b) \mapsto \star(a, b)$.

**Notation 17.2.** We usually write $a \star b$ instead of $\star(a, b)$.

**Example 17.3.** For instance, we write $(a \star b) \star c$ instead of $\star(\star(a, b), c)$. Instead of $\star$ we sometimes use notation like $+$, $\times$, $\circ$, ...

**Remark 17.4.** We tacitly introduce the new predicate “is a binary operation on ...” by an appropriate definition in the language of sets. Also, if $\star, A$ are sets (hence constants) such that “$\star$ is a binary operation on $A$” is a theorem we may introduce a new functional symbol (still denoted by $\star$) by

$$\forall x \forall y \forall z ((x \star y = z) \leftrightarrow (((x, y), z) \in \star))$$

**Definition 17.5.** A unary operation $'$ on a set $A$ is a map $': A \to A$, $a \mapsto 'a$.

**Notation 17.6.** We usually write $a'$ or $'a$ instead of $'(a)$. Instead of $'$ we sometimes use notation like $-$, $i$, ...

**Example 17.7.** Let $S = \{0, 1\}$ where 0, 1 are two symbols (with no meaning). Then there are 3 interesting binary operations on $S$ denoted by $\land, \lor, +$ (and called supremum, infimum, and addition) defined as follows:

- $0 \land 0 = 0, \quad 0 \land 1 = 0, \quad 1 \land 0 = 0, \quad 1 \land 1 = 1$;
- $0 \lor 0 = 0, \quad 0 \lor 1 = 1, \quad 1 \lor 0 = 1, \quad 1 \lor 1 = 1$;
- $0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0$.

The $\land$ is also denoted by $\times$ or $\cdot$ is referred to as multiplication. $+$ is also denoted by $\Delta$. Also there is a unary operation $\neg$ on $S$ defined by

$$\neg 1 = 0, \quad \neg 0 = 0.$$ 

Note that if we denote 0 and 1 by $F$ and $T$ then the operations $\land, \lor, \neg$ on $\{0, 1\}$ correspond exactly to the “logical operations” on $F$ and $T$ defined in the section on tautologies. This is not a coincidence!

**Exercise 17.8.** Compute $((0 \land 1) \lor 1) + (1 \land (0 \lor (1 + 1)))$.

**Definition 17.9.** A Boolean algebra is a tuple

$$(A, \lor, \land, \neg, 0, 1)$$

where $\land, \lor$ are binary operations, $\neg$ is a unary operation and 0, 1 $\in A$ such that for all $a, b, c \in A$ the following axioms are satisfied:

1. $a \land (b \land c) = (a \land b) \land c$, $a \lor (b \lor c) = (a \lor b) \lor c$,
2. $a \land b = b \land a$, $a \lor b = b \lor a$, 

Note that if we denote 0 and 1 by $F$ and $T$ then the operations $\land, \lor, \neg$ on $\{0, 1\}$ correspond exactly to the “logical operations” on $F$ and $T$ defined in the section on tautologies. This is not a coincidence!
3) \( a \land 1 = a \), \( a \lor 0 = a \),
4) \( a \land (b \lor c) = (a \land b) \lor (a \land c) \), \( a \lor (b \land c) = (a \lor b) \land (a \lor c) \),
5) \( a \land (\neg a) = 0 \), \( a \lor (\neg a) = 1 \).

**Definition 17.10.** A commutative unital ring (or simply a ring) is a tuple 
\[ (R, +, \times, - , 0, 1) \]
(sometimes referred to as simply as \( R \)) where \( R \) is a set, \( 0, 1 \in R \), \( +, \times \) are two binary operations (write \( a \times b = ab \)) and \( - \) is a unary operation on \( R \) such that for any \( a, b, c \in R \) the following hold:
1) \( a + (b + c) = (a + b) + c \), \( a + 0 = a \), \( a + (-a) = 0 \), \( a + b = b + a \);
2) \( a(bc) = (ab)c \), \( 1a = a \), \( ab = ba \);
3) \( a(b + c) = ab + ac \).

**Notation 17.11.** We write \( a + b + c \) instead of \( (a + b) + c \) and \( abc \) for \( (ab)c \). We write \( a - b \) instead of \( a + (-b) \).

**Definition 17.12.** An element \( a \) of a ring \( R \) is invertible if there exists \( a' \in R \) such that \( aa' = 1 \); this \( a' \) is then easily proved to be unique, it is called the inverse of \( a \), and is denoted by \( a^{-1} \). A ring \( R \) is called a field if \( 0 \neq 1 \) and for any non-zero element is invertible.

**Definition 17.13.** A Boolean ring is a commutative unital ring such that \( 1 \neq 0 \) and for all \( a \in A \) we have \( a^2 = a \).

**Exercise 17.14.** Prove that in a Boolean ring \( A \) we have \( a + a = 0 \) for all \( a \in A \).

**Exercise 17.15.** Prove that
1) \( \{0, 1\}, \lor, \land, \neg , 0, 1 \) is a Boolean algebra.
2) \( \{0, 1\}, +, \times, I , 0, 1 \) is a Boolean ring and a field (\( I \) is the identity map).

**Exercise 17.16.** Prove that if a Boolean ring \( A \) is a field then \( A = \{0, 1\} \).

**Definition 17.17.** Let \( A \) be a set and let \( S = \mathcal{P}(A) \) be the power set of \( A \). Define the following operations on \( S \):
\[
\begin{align*}
X \land Y &= X \cap Y \\
X \lor Y &= X \cup Y \\
X \Delta Y &= (X \cup Y) \setminus (X \cap Y) \\
\neg X &= \complement X = A \setminus X
\end{align*}
\]

**Exercise 17.18.** Prove that
1) \( \mathcal{P}(A), \lor, \land, \neg , \emptyset, A \) is a Boolean algebra;
2) \( \mathcal{P}(A), \Delta, \land, I , \emptyset, A \) is a Boolean ring (\( I \) is the identity map).

Hint: For any \( a \in A \) one can define a map \( \psi_a : \mathcal{P}(A) \to \{0, 1\} \) by setting \( \psi_a(X) = 1 \) if and only if \( a \in X \). Note that
1) \( \psi_a(X \land Y) = \psi_a(X) \land \psi_a(Y) \),
2) \( \psi_a(X \lor Y) = \psi_a(X) \lor \psi_a(Y) \),
3) \( \psi_a(X \Delta Y) = \psi_a(X) + \psi_a(Y) \),
4) \( \psi_a(\neg X) = \neg \psi_a(X) \).
Next note that \( X = Y \) if and only if \( \psi_a(X) = \psi_a(Y) \) for all \( a \in A \). Use these functions to reduce the present exercise to the previous exercise.
DEFINITION 17.19. Given a subset $X \subset A$ one can define the characteristic function $\chi_X : A \to \{0, 1\}$ by letting $\chi_X(a) = 1$ if and only if $a \in X$; in other words $\chi_X(a) = \psi_a(X)$.

EXERCISE 17.20. Prove that
1) $\chi_{X \cup Y}(a) = \chi_X(a) \lor \chi_Y(a)$,
2) $\chi_{X \cap Y}(a) = \chi_X(a) \land \chi_Y(a)$,
3) $\chi_{X \Delta Y}(a) = \chi_X(a) + \chi_Y(a)$,
4) $\chi_{\neg X}(a) = \neg \chi_X(a)$.

DEFINITION 17.21. An algebraic structure is a tuple $(A, \star, \cdot, \ldots, \neg, -, \ldots, 0, 1, \ldots)$ where $A$ is a set, $\star, \cdot, \ldots$ are binary operations, $\neg, -, \ldots$ are unary operations, and $1, 0, \ldots$ are given elements of $A$. (Some of these may be missing; for instance we could have only one binary operation, one given element, and no unary operations.) Assume we are given two algebraic structures

$(A, \star, \cdot, \ldots, \neg, -, \ldots, 0, 1, \ldots)$ and $(A', \star', \cdot', \ldots, \neg', -, \ldots, 0', 1', \ldots)$

(with the same number of corresponding operations). A map $F : A \to A'$ is called a homomorphism if for all $a, b \in A$ we have:
1) $F(a \cdot b) = F(a) \cdot F(b)$, $F(a \star b) = F(a) \star F(b)$,
2) $F(-a) = \neg' F(a)$, $F(-a) = \neg F(a)$,
3) $F(0) = 0'$, $F(1) = 1'$,

EXERCISE 17.22. A map $F : A \to A'$ between two commutative unital rings is a called a homomorphism (of commutative unital rings) if for all $a, b \in A$ we have:
1) $F(a + b) = F(a) + F(b)$ and $F(ab) = F(a)F(b)$,
2) $F(-a) = \neg F(a)$ (prove that this is automatic !),
3) $F(0) = 0$ (prove that this is automatic !) and $F(1) = 1$.

DEFINITION 17.23. A subset $\mathcal{A} \subset \mathcal{P}(A)$ is called a Boolean algebra of sets if the following hold:
1) $\emptyset \in \mathcal{A}$, $A \in \mathcal{A}$;
2) If $X, Y \in \mathcal{A}$ then $X \cap Y \in \mathcal{A}$, $X \cup Y \in \mathcal{A}$, $\complement X \in \mathcal{A}$.
(Hence $(\mathcal{A}, \cup, \cap, \complement, \emptyset, A)$ is a Boolean algebra.)

EXERCISE 17.24. Prove that if $\mathcal{A}$ is a Boolean algebra of sets then for any $X, Y \in \mathcal{A}$ we have $X \Delta Y \in \mathcal{A}$. Prove that $(\mathcal{A}, \Delta, \cap, I, \emptyset, A)$ is a Boolean ring.

DEFINITION 17.25. A subset $\mathcal{B} \subset \mathcal{P}(A)$ is called a Boolean ring of sets if the following properties hold:
1) $\emptyset \in \mathcal{B}$, $A \in \mathcal{B}$;
2) If $X, Y \in \mathcal{B}$ then $X \cap Y \in \mathcal{B}$, $X \Delta Y \in \mathcal{B}$.
(Hence $(\mathcal{A}, \Delta, \cup, I, \emptyset, A)$ is a Boolean ring.)

EXERCISE 17.26. Prove that any Boolean ring of sets $\mathcal{B}$ is a Boolean algebra of sets.

DEFINITION 17.27. A commutative unital ordered ring (or simply an ordered ring) is a tuple

$(R, +, \times, -, 0, 1, \leq)$

where

$(R, +, \times, -, 0, 1)$
is a ring, \( \leq \) is a total order on \( R \), and for all \( a, b, c \in R \) the following axioms are satisfied

1) If \( a < b \) then \( a + c < b + c \);
2) If \( a < b \) and \( c > 0 \) then \( ac < bc \).

**Exercise 17.28.** Prove that if \( R \) is a finite ring then it cannot have a structure of ordered ring. In particular the unique order on \( \{0, 1\} \) with \( 0 \leq 1 \) does not make the tuple \( (\{0, 1\}, +, \times, -, 0, 1, \leq) \) an ordered ring!

**Remark 17.29.** We cannot give examples yet of ordered rings; in fact we will later postulate the existence of the ordered ring of integers; all other ordered rings will be constructed from the integers.

**Definition 17.30.** Let \( R \) be an ordered ring and let \( R_+ = \{ a \in R; a \geq 0 \} \). A finite measure space is a triple \( (A, \mathcal{A}, \mu) \) where \( A \) is a set, \( \mathcal{A} \subset \mathcal{P}(A) \) is a Boolean algebra of sets, and \( \mu : \mathcal{A} \rightarrow R_+ \) satisfying the following property for any \( X, Y \in \mathcal{A} \) with \( X \cap Y = \emptyset \) we have

\[
\mu(X \cup Y) = \mu(X) + \mu(Y).
\]

If in addition \( \mu(A) = 1 \) we say \( (A, \mathcal{A}, \mu) \) is a finite probability measure. We say that \( X, Y \in \mathcal{A} \) are independent if \( \mu(X \cap Y) = \mu(X) \cdot \mu(Y) \).

**Exercise 17.31.** Prove that in a finite measure space \( \mu(\emptyset) = 0 \) and for any \( X, Y \in \mathcal{A} \) we have

\[
\mu(X \cup Y) = \mu(X) + \mu(Y) - \mu(X \cap Y).
\]

**Exercise 17.32.** Let \( (A, \lor, \land, \neg, 0, 1) \) be a Boolean algebra. For any \( a, b \in A \) set

\[
a + b = (a \lor b) \land \neg(a \land b).
\]

Prove that \( (A, +, \land, I, 0, 1) \) is a Boolean ring (\( I \) the identity map.)

**Exercise 17.33.** Let \( (A, +, \land, -, 0, 1) \) be a Boolean ring. For any \( a, b \in A \) let

\[
a \lor b = a + b - ab
\]
\[
a \land b = ab
\]
\[
\neg a = 1 - a.
\]

Prove that \( (A, \lor, \land, \neg, 0, 1) \) is a Boolean algebra.

**Exercise 17.34.** Let \( (X, \mathcal{J}) \) be a topological space and let \( A \subset \mathcal{P}(A) \) be the set of all \( X \in \mathcal{P}(A) \) such that \( X \in \mathcal{J} \) and \( \mathcal{C}X \in \mathcal{J} \). (I.e. \( A \) is the collection of all sets which are both open and closed.) Then \( A \) is a Boolean algebra of sets.
CHAPTER 18

Integers

Definition 18.1. A well ordered ring is an ordered ring \((R, +, \times, 0, 1, \leq)\) with \(1 \neq 0\) having the property that any non-empty subset of \(R\) which is bounded from below has a minimum element.

Remark 18.2. If \((R, +, \times, 0, 1, \leq)\) is a well ordered ring then \((R, \leq)\) is not well ordered. But if \(R_{>0} = \{a \in R; a > 0\}\) then \((R_{>0}, \leq)\) is a well ordered set.

We have the following remarkable theorem in set theory \(T_{set}\):

Theorem 18.3. There exists a well ordered ring.

Remark 18.4. The above theorem is formulated in argot; but it should be understood as being a sentence \(Z\) in \(L_{set}\) of the form

\[ \exists r \exists s \exists p \exists o \exists u \exists l (...) \]

where we take a variable \(r\) to stand for the ring, a variable \(s\) for the sum, \(p\) for the product, \(o\) for 0, \(u\) for 1, \(l\) for \(\leq\), and the dots stand for the corresponding conditions in the definition of a well ordered ring, written in the language of sets. The sentence \(Z\) is complicated so we preferred to give the theorem not a sentence in \(L_{set}\) but as a sentence in argot. This kind of abuse is very common.

Remark 18.5. We are not going to prove Theorem 18.3 but rather sketch the idea of the proof which is rather involved. For the reader who feels he/she cannot accept such a basic theorem without proof one can simply proceed as follows: add this theorem to the ZFC and replace \(T_{set}\) by the theory with axioms this enriched system of axioms. This is what all working mathematicians essentially do anyway.

Notation 18.6. We let \(Z, +, \times, 0, 1, \leq\) be the witnesses for the sentence \(Z\) above; we call \(Z\) the ring of integers. In particular the conditions in the definition of rings (associativity, commutativity, etc.) and order (transitivity, etc.) become theorems for \(Z\). We also set \(N = \{a \in Z; a > 0\}\) and we call \(N\) the set of natural numbers. Later we will prove the “essential uniqueness” of \(Z\).

Remark 18.7. The only predicate in the language \(L_{set}\) of sets is \(\in\) and the constants in this language are called sets. In particular when we consider the ordered ring of integers \((Z, +, \times, 0, 1, \leq)\) the symbols \(Z, +, \times, 0, 1, \leq, N\) are all constants (they are sets). In particular +, \times are not originally functional symbols and \(\leq\) is not originally a relational predicate. But, according to our conventions, we may introduce functional symbols (still denoted by +, \times) and a relational predicate (still denoted by \(\leq\)) via appropriate definitions. (This is because “the set + is a ninary operation on \(Z\)” is a theorem, etc.)

Exercise 18.8. Prove that \(1 \in N\). Hint: use \((-1) \times (-1) = 1\).
Exercise 18.9. Prove that if \( a, b \in \mathbb{Z} \) and \( ab = 0 \) then either \( a = 0 \) or \( b = 0 \). Give an example of a ring where this is not true. (For the latter consider the Boolean algebra \( \mathcal{P}(A) \).)

Exercise 18.10. Prove that if \( a \in \mathbb{Z} \) then the set \( \{ x \in \mathbb{Z} ; a - 1 < x < a \} \) is empty. Hint (actually a complete proof): It is enough to show that \( S = \{ x \in \mathbb{Z} ; 0 < x < 1 \} \) is empty. Assume \( S \) is non-empty and let \( m = \min S \). Then \( 0 < m^2 < m \), hence \( 0 < m^2 < 1 \) and \( m^2 < m \), a contradiction.

Exercise 18.11. Prove that if \( a \in \mathbb{N} \) then \( a = 1 \) or \( a - 1 \in \mathbb{N} \). Conclude that \( \min \mathbb{N} = 1 \). Hint: use previous exercise.

In what follows we sketch the main idea behind the proof of Theorem 18.3. We begin with the following:

Definition 18.12. Define a Peano triple to be a triple \((N, 1, \sigma)\) where \( N \) is a set, \( 1 \in N \), and \( \sigma : N \to N \) is a map such that

1) \( \sigma \) is injective;
2) \( \sigma(N) = N \setminus \{1\} \) and
3) for any subset \( S \subset N \) if \( 1 \in S \) and \( \sigma(S) \subset S \) then \( S = N \).

The conditions 1,2,3 are called “Peano’s axioms”.

Remark 18.13. Given a well ordered ring one can easily prove there exists a Peano triple; cf. Exercise 18.14 below. Conversely given a Peano triple one can prove there exists a well ordered ring; this is tedious and will be addressed in Exercise 18.15. The idea of proof of Theorem 18.3 is to prove in set theory (i.e. ZFC) that there exists a Peano triple; here the axiom of infinity is crucial. Then the existence of a well ordered ring follows.

Exercise 18.14. Prove that if there exists a well ordered ring \( \mathbb{Z} \) then \( \sigma : \mathbb{N} \to \mathbb{N} \) is \( \sigma(x) = x + 1 \) then \((N, 1, \sigma)\) is a Peano triple.

Exercise 18.15. This exercise gives some steps towards showing how to construct a well ordered ring from a given Peano triple. Assume \((N, 1, \sigma)\) is a Peano triple. For \( y \in N \) let

\[ A_y = \{ \tau \in N^N ; \tau(1) = \sigma(y), \forall x(\tau(\sigma(x)) = \sigma(\tau(x))) \} \]

1) Prove that \( A_y \) has at most one element. Hint: if \( \tau, \eta \in A_y \) and \( S = \{ x ; \tau(x) = \eta(x) \} \) then \( 1 \in S \) and \( \sigma(S) \subset S \); so \( S = N \).
2) Prove that for any \( y \), \( A_y \neq \emptyset \). Hint: If \( T = \{ y \in N ; A_y \neq \emptyset \} \) then \( 1 \in T \) and \( \sigma(T) \subset T \); so \( T = N \).
3) By 1 and 2 we may write \( A_y = \{ \tau_y \} \). Then define + on \( N \) by \( x + y = \tau_y(x) \).
4) Prove that \( x + y = y + x \) and \( (x + y) + z = x + (y + z) \) on \( N \).
5) Prove that if \( x, y \in N \), \( x \neq y \), then there exists \( z \in N \) such that either \( y = x + z \) or \( x = y + z \).
6) Define \( N' = \{ - \} \times N, Z = N' \cup \{ 0 \} \cup N \) where 0 and \( - \) are two symbols. Extend naturally + to \( Z \).
7) Define \( \times \) on \( N \) and then on \( Z \) in the same style as for +.
8) Define \( \leq \) on \( N \) and prove \((N, \leq)\) is well ordered. Extend this to \( Z \).
9) Prove that \((Z, +, \times, 0, 1, \leq)\) is a well ordered ring.

From now on we accept Theorem 18.3 (either as a theorem whose proof we summarily sketched or as an additional axiom for set theory).
18. INTEGERS

Definition 18.16. Define the natural numbers 2, 3, ..., 9 by

\[
\begin{align*}
2 &= 1 + 1 \\
3 &= 2 + 1 \\
&\vdots \\
9 &= 8 + 1
\end{align*}
\]

Define 10 = 2 \times 5. Define 10^2 = 10 \times 10, etc. Define symbols like 423 as being

\[4 \times 10^2 + 2 \times 10 + 3,\] etc. This is called a decimal representation. (We will later prove that any natural number has a decimal representation.)

Exercise 18.17. Prove that 12 = 9 + 3. Hint (actually a complete proof): we have:

\[
\begin{align*}
12 &= 10 + 2 \\
&= 2 \times 5 + 2 \\
&= (1 + 1) \times 5 + 2 \\
&= 1 \times 5 + 1 \times 5 + 2 = 5 + 5 + 2 \\
&= 5 + 5 + 1 + 1 = 5 + 6 + 1 = 5 + 7 = 4 + 1 + 7 \\
&= 4 + 8 = 3 + 1 + 8 = 3 + 9 = 9 + 3
\end{align*}
\]

Exercise 18.18. Prove that 18 + 17 = 35. Prove that 17 \times 3 = 51.

Remark 18.19. In Kant’s Critique of pure reason statements like the ones in the previous exercise were viewed as synthetic; in contemporary mathematics, hence in the approach we follow, all these statements are, on the contrary, analytic statements. (The definition of analytic/synthetic is taken here in the sense of Leibniz and Kant; there is another pair of notions, a priori/a posteriori, whose definition in Leibniz is different from the one of Kant; we did not discuss and will not discuss this latter pair of notions here.)

Exercise 18.20. Prove that 7 \leq 20.

Notation 18.21. For any integers \(a, b \in \mathbb{Z}\) the set \(\{x \in \mathbb{Z}; a \leq x \leq b\}\) will be denoted, for simplicity, by \(\{a, ..., b\}\). This set is clearly empty if \(a > b\). If other numbers in addition to \(a, b\) are specified then the meaning of our notation will be clear from the context; for instance \(\{0, 1, ..., n\}\) means \(\{0, ..., n\}\) whereas \(\{2, 4, 6, ..., 2n\}\) will mean \(\{2x; 1 \leq x \leq n\}\), etc. A similar convention applies if there are no numbers after the dots.

Example 18.22. \(\{-2, ..., 11\}\) = \{-2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.

Recall that a subset \(A \subseteq \mathbb{N}\) is bounded (equivalently bounded from above) if there exists \(b \in \mathbb{N}\) such that \(a \leq b\) for all \(a \in A\); we say that \(A\) is bounded by \(b\) from above.

Exercise 18.23. Prove that \(\mathbb{N}\) is not bounded.

Exercise 18.24. Prove that any subset of \(\mathbb{Z}\) bounded from above has a maximum. Hint: If \(A\) is bounded from above by \(b\) consider the set \(\{b - x; x \in A\}\).

Definition 18.25. An integer \(a\) is even if there exists an integer \(b\) such that \(a = 2b\). An integer is odd if it is not even.

Exercise 18.26. Prove that if \(a\) is odd then \(a - 1\) is even. Hint: consider the set \(\{b \in \mathbb{N}; 2b \geq a\}\), and let \(c\) be the minimum element of \(S\). Then show that \(2(c - 1) < a\). Finally show that this implies \(a = 2c - 1\).
Exercise 18.27. Prove that if $a$ and $b$ are odd then $ab$ is odd. Hint: write $a = 2c + 1$ and $b = 2d + 1$ (cf. the previous exercise) and compute $(2c+1)(2d+1)$.

Exercise 18.28. Consider the following sentence: There is no bijection between $\mathbb{N}$ and $\mathbb{Z}$. Explain the mistake in the following wrong proof:

Proof. Assume there is a bijection $f : \mathbb{N} \to \mathbb{Z}$. Define $f(x) = x$. Then $f$ is not surjective so it is not a bijection.

Exercise 18.29. Prove that there is a bijection between $\mathbb{N}$ and $\mathbb{Z}$. 
CHAPTER 19

Induction

Let $P(x)$ be a formula in the language $L_{set}$ of sets, with free variable $x$. For each such $P(x)$ we have:

**Proposition 19.1.** (Induction Principle) Assume

1) $P(1)$.
2) For all $n \in \mathbb{N}$ if $n \neq 1$ and $P(n - 1)$ then $P(n)$.

Then for all $n \in \mathbb{N}$ we have $P(n)$.

The above is expressed, as usual, in argot. The same expressed as a sentence in $L_{set}$ reads:

$$(P(1) \land (\forall x ((x \in \mathbb{N}) \land (x \neq 0) \land P(x - 1)) \rightarrow P(x))) \rightarrow (\forall x ((x \in \mathbb{N}) \rightarrow P(x)))$$

We refer to the above as induction on $n$. For each explicit $P(x)$ this is a genuine theorem. Note that the above Proposition does not say “for all $P$ something happens”; that would not be a sentence in the language of sets.

**Proof.** Let $S = \{n \in \mathbb{N}; \neg P(n)\}$. Let $m$ be the minimum of $S$. By 1) $m \neq 1$. By Exercise 18.11 $m - 1 \in \mathbb{N}$. By minimality of $m$, we have $P(m - 1)$. By 2) we get $P(m)$, a contradiction.

**Exercise 19.2.** Define $n^2 = n \times n$ and $n^3 = n^2 \times n$ for any integer $n$. Prove that for any natural $n$ there exists an integer $m$ such that $n^3 - n = 3m$. (Later we will say that 3 divides $n^3 - n$.) Hint: proceed by induction on $n$ as follows. Let $P(n)$ be the sentence: for all natural $n$ there exists an integer $m$ such that $n^3 - n = 3m$. $P(1)$ is true because $1^3 - 1 = 3 \times 0$. Assume now that $P(n - 1)$ is true i.e. $(n - 1)^3 - (n - 1) = 3q$ for some integer $q$ and let us check that $P(n)$ is true i.e. that $n^3 - n = 3m$ for some integer $m$. The equality $(n - 1)^3 - (n - 1) = 3q$ reads $n^3 - 3n^2 + 3n - 1 - n + 1 = 3q$. Hence $n^3 - n = 3(n^2 - n)$ and we are done.

**Exercise 19.3.** Define $n^5 = n^3 \times n^2$. Prove that for any natural $n$ there exists an integer $m$ such that $n^5 - n = 5m$.

**Proposition 19.4.** If there exists a bijection $\{1, ..., n\} \rightarrow \{1, ..., m\}$ then $n = m$.

**Proof.** We proceed by induction on $n$. Let $P(n)$ be the statement of the Proposition. Clearly $P(1)$ is true; cf. the Exercise below. Assume now $P(n - 1)$ is true and let’s prove that $P(n)$ is true. So consider a bijection $F : \{1, ..., n\} \rightarrow \{1, ..., m\}$; we want to prove that $n = m$. Let $i = F(n)$ and define the map $G : \{1, ..., n - 1\} \rightarrow \{1, ..., m\} \setminus \{i\}$ by $G(j) = F(j)$ for all $1 \leq j \leq n - 1$. Then clearly $G$ is a bijection. Now consider the map $H : \{1, ..., m\} \setminus \{i\} \rightarrow \{1, ..., m - 1\}$ defined by $H(j) = j$ for $1 \leq j \leq i - 1$ and $H(j) = j - 1$ for $i + 1 \leq j \leq m$. (The
definition is correct because for any \(j \in \{1, \ldots, m\}\setminus \{i\}\) either \(j \leq i - 1\) or \(j \geq i + 1\); cf. Exercise 18.10.) Clearly \(H\) is a bijection. We get a bijection
\[
H \circ G : \{1, \ldots, n - 1\} \to \{1, \ldots, m - 1\}.
\]
Since \(P(n - 1)\) is true we get \(n - 1 = m - 1\). Hence \(n = m\) and we are done. \(\square\)

Exercise 19.5. Check that \(P(1)\) is true in the above Proposition.

Remark 19.6. Note the general strategy of proofs by inductions. Say \(P(n)\) is “about \(n\) objects”. There are two steps. The first step is the verification of \(P(1)\) i.e. one verifies the statement “for one object”. For the second step (called the induction step) one considers a situation with \(n\) objects; one “removes” from that situation “one object” to get a “situation with \(n - 1\) objects”; one uses the “induction hypothesis” \(P(n - 1)\) to conclude the claim for the “situation with \(n - 1\) objects”. Then one tries to “go back” and prove that the claim is true for the situation with \(n\) objects. So the second step is performed by “removing” one object from an arbitrary situation with \(n\) objects and NOT by adding one object to an arbitrary situation with \(n - 1\) objects. Below is an example of a fallacious reasoning by induction based on “adding” instead of “subtracting” an object.

Example 19.7. Here is a WRONG argument for the induction step in the proof of Proposition 19.4.

Let \(G : \{1, \ldots, n - 1\} \to \{1, \ldots, m - 1\}\) be any bijection and let \(F : \{1, \ldots, n\} \to \{1, \ldots, m\}\) be defined by \(F(i) = G(i)\) for \(i \leq n - 1\) and \(F(n) = m\). Clearly \(F\) is a bijection. Now by the induction hypothesis \(n - 1 = m - 1\). Hence \(n = m\). This ends the proof.

The mistake is that the above does not end the proof: the above argument only covers bijections \(F : \{1, \ldots, n\} \to \{1, \ldots, m\}\) constructed from bijections \(G : \{1, \ldots, n - 1\} \to \{1, \ldots, m - 1\}\) in the special way described above. In other words an arbitrary bijection \(F : \{1, \ldots, n\} \to \{1, \ldots, m\}\) does not always arise the way we defined \(F\) in the above “proof”. In some sense the mistake we just pointed out is that of defining the same constant twice (cf. Example 18.28): we were supposed to define the symbol \(F\) as being an arbitrary bijection but then we redefined \(F\) in a special way through an arbitrary \(G\). The point is that if \(G\) is arbitrary and \(F\) is defined as above in terms of \(G\) then \(F\) will not be arbitrary (because \(F\) will always send \(n\) into \(m\)). THIS KIND OF MISTAKE IS VERY COMMON WITH BEGINNERS IN MATHEMATICS.

Definition 19.8. A set \(A\) is finite if there exists an integer \(n \geq 0\) and a bijection \(F : \{1, \ldots, n\} \to A\). (\(n\) is then unique by Proposition 19.4.) We write \(|A| = n\) and we call this number the cardinality of \(A\) or the number of elements of \(A\). (Note that \(|\emptyset| = 0\).) If \(F(i) = a_i\) we write \(A = \{a_1, \ldots, a_n\}\). A set is infinite if it is not finite.

Exercise 19.9. Prove that \(|\{2, 4, -6, 9, -100\}| = 5\).

Exercise 19.10. For any finite sets \(A\) and \(B\) we have that \(A \cup B\) is finite and
\[|A \cup B| + |A \cap B| = |A| + |B|\]
Hint: Reduce to the case \(A \cap B = \emptyset\). Then if \(F : \{1, \ldots, a\} \to A\) and \(G : \{1, \ldots, b\} \to B\) are bijections prove that \(H : \{1, \ldots, a + b\} \to A \cup B\) defined by \(H(i) = F(i)\) for \(1 \leq i \leq a\) and \(H(i) = G(i - a)\) for \(a + 1 \leq i \leq a + b\) is a bijection.
Exercise 19.11. For any finite sets $A$ and $B$ we have that $A \times B$ is finite and 
\[ |A \times B| = |A| \times |B|. \]
Hint: Induction on $|A|$.

Exercise 19.12. Let $F : \{1, \ldots, n\} \to \mathbb{Z}$ be an injective map and write $F(i) = a_i$. We refer to such a map as a (finite) family of numbers. Prove that there exists a unique map $G : \{1, \ldots, n\} \to \mathbb{Z}$ such that $G(1) = a_1$ and $G(k) = G(k-1) + a_k$ for $2 \leq k \leq n$. Hint: induction on $n$.

Definition 19.13. In the notation of the above Exercise define the (finite) sum $\sum_{i=1}^{n} a_i$ as the number $G(n)$. We also write $a_1 + \ldots + a_n$ for this sum. If $a_1 = \ldots = a_n = a$ the sum $a_1 + \ldots + a_n$ is written as $a + \ldots + a$ ($n$ times).

Exercise 19.14. Prove that for any $a, b \in \mathbb{N}$ we have 
\[ a \times b = a + \ldots + a \, (b \text{ times}) = b + \ldots + b \, (a \text{ times}). \]

Exercise 19.15. Define in a similar way the (finite) product $\Pi_{i=1}^{n} a_i$ (which is also denoted by $a_1 \ldots a_n = a_1 \times \ldots \times a_n$). Prove the analogues of associativity and distributivity for sums and products of families of numbers. Define $a^b$ for $a, b \in \mathbb{N}$ and prove that $a^{b+c} = a^b \times a^c$ and $(a^b)^c = a^{bc}$.

Exercise 19.16. Prove that if $a$ is an integer and $n$ is a natural number then 
\[ a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \ldots + a + 1). \]
Hint: induction on $n$.

Exercise 19.17. Prove that if $a$ is an integer and $n$ is an integer then 
\[ a^{2n+1} + 1 = (a + 1)(a^{2n} - a^{2n-1} + a^{2n-2} - \ldots - a + 1). \]
Hint. Set $a = -b$.

Exercise 19.18. Prove that a subset $A \subset \mathbb{N}$ is bounded if and only if it is finite. Hint: To prove that bounded sets are finite assume this is false and let $b$ be the minimum natural number with the property that there is a set $A$ bounded from above by $b$ and infinite. If $b \notin A$ then $A$ is bounded from above by $b - 1$ (Exercise 18.10) and we are done. If $b \in A$ then, by minimality of $b$, that there is a bijection $A \setminus \{b\} \to \{1, \ldots, m\}$ and one constructs a bijection $A \to \{1, \ldots, m+1\}$ which is a contradiction. To prove that finite sets are bounded assume this is false and let $n$ be minimum natural number with the property that there is a finite subset $A \subset \mathbb{N}$ of cardinality $n$ which is not bounded. Let $F : \{1, \ldots, n\} \to A$ be a bijection, $a_i = F(i)$. Then $\{a_1, \ldots, a_{n-1}\}$ is bounded from above by some $b$ and conclude that $A$ is bounded from above by either $b$ or $a_n$.

Exercise 19.19. Prove that any subset of a finite set is finite. Hint: use the previous exercise.

Definition 19.20. Let $A$ be a set and $n \in \mathbb{N}$. Define the set $A^n$ to be the set $A^{(1,\ldots,n)}$ of all maps $\{1, \ldots, n\} \to A$. Call 
\[ A^* = \bigcup_{n=1}^{\infty} A^n \]
the set of words with letters in $A$. 
Notation 19.21. If \( f : \{1, \ldots, n\} \to A \) and \( f(i) = a_i \) we write \( f \) as a “tuple” \((a_1, \ldots, a_n)\) and sometimes as a “word” \(a_1 \ldots a_n\); in other words we add to the definitions of set theory the following definitions

\[
f = (a_1, \ldots, a_n) = a_1 \ldots a_n.
\]

Exercise 19.22. Show that the maps \( A^n \times A^m \to A^{n+m} \),

\[
((a_1, \ldots, a_n), (b_1, \ldots, b_m)) \mapsto (a_1, \ldots, a_n, b_1, \ldots, b_m)
\]

(called concatenations) are bijections. They induce a non-injective binary operation \( A^* \times A^* \to A^* \), \((u, v) \to uv\). Prove that \( u(vw) = (uv)w \).
CHAPTER 20

Rationals

Definition 20.1. For any \(a, b \in \mathbb{Z}\) with \(b \neq 0\) define the fraction \(\frac{a}{b}\) to be the set of all pairs \((c, d)\) with \(c, d \in \mathbb{Z}\), \(d \neq 0\) such that \(ad = bc\). Call \(a\) and \(b\) the numerator and the denominator of the fraction \(\frac{a}{b}\). Denote by \(\mathbb{Q}\) the set of all fractions. So

\[
\frac{a}{b} = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}; d \neq 0, ad = bc\},
\]

\[
\mathbb{Q} = \{\frac{a}{b}; a, b \in \mathbb{Z}, b \neq 0\}.
\]

Example 20.2.

\[
\frac{6}{10} = \{(6, 10), (-3, -5), (9, 15), \ldots\} \in \mathbb{Q}.
\]

Exercise 20.3. Prove that \(\frac{a}{b} = \frac{c}{d}\) if and only if \(ad = bc\). Hint: assume \(ad = bc\) and let us prove that \(\frac{a}{b} = \frac{c}{d}\). We need to show that \(\frac{a}{b} \subset \frac{c}{d}\) and that \(\frac{c}{d} \subset \frac{a}{b}\). Now if \((x, y) \in \frac{a}{b}\) then \(xb = ay\); hence \(xbd = ayd\). Since \(ad = bc\) we get \(xbd = bc\). Hence \(\frac{a}{b} \subset \frac{c}{d}\). The other inclusion is proved similarly. So the equality \(\frac{a}{b} = \frac{c}{d}\) is proved. Conversely if one assumes \(\frac{a}{b} = \frac{c}{d}\) one needs to prove \(ad = bc\); I leave this to the reader.

Exercise 20.4. On the set \(A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\) one can consider the relation: \((a, b) \sim (c, d)\) if and only if \(ad = bc\). Prove that \(\sim\) is an equivalence relation. Then observe that \(\frac{a}{b}\) is the equivalence class \(\hat{(a, b)}\) of \((a, b)\). Also observe that \(\mathbb{Q} = A/\sim\) is the quotient of \(A\) by the relation \(\sim\).

Notation 20.5. Write \(\frac{a}{b} = a;\) this identifies \(\mathbb{Z}\) with a subset of \(\mathbb{Q}\)

Definition 20.6. Define \(\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}\).

Exercise 20.7. Show that the above definition is correct (i.e. if \(\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}\) then \(\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}\) and similarly for the product.)

Exercise 20.8. Prove that \(\mathbb{Q}\) (with the operations + and \(\times\) defined above and with the elements 0, 1) is a field.

Definition 20.9. For \(\frac{a}{b}, \frac{c}{d}\) with \(b, d > 0\) write \(\frac{a}{b} \leq \frac{c}{d}\) if \(ad - bc \leq 0\). Also write \(\frac{a}{b} \leq \frac{c}{d}\) if \(\frac{a}{b} \leq \frac{c}{d}\) and \(\frac{a}{b} \neq \frac{c}{d}\).

Exercise 20.10. Prove that \(\mathbb{Q}\) equipped with \(\leq\) is an ordered ring but it is not a well ordered ring.
Exercise 20.11. Let $A$ be a finite set and define $\mu : \mathcal{P}(A) \to \mathbb{Q}$ by

$$\mu(X) = \frac{|X|}{|A|}.$$ 

1) $(A, \mathcal{P}(A), \mu)$ is a finite probability measure space.
2) Prove that if $X = Y \neq A$ then $X$ and $Y$ are not independent.
3) Prove that if $X \cap Y = \emptyset$ and $X \neq \emptyset$, $Y \neq \emptyset$ then $X$ and $Y$ are not independent.
4) Prove that if $A = B \times C$, $X = B' \times C$, $Y = B \times C'$, $B' \subset B$, $C' \subset C$, then $X$ and $Y$ are independent.

Exercise 20.12. Prove by induction the following equalities:

$$1 + 2 + \ldots + n = \frac{n(n + 1)}{2}.$$ 

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n + 1)(2n + 1)}{6}.$$ 

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n + 1)^2}{4}.$$
Definition 21.1. For \( n \in \mathbb{N} \) define the factorial of \( n \) (read \( n \) factorial) by
\[
 n! = 1 \times 2 \times \ldots \times n \in \mathbb{N}.
\]
Also set \( 0! = 1 \).

Definition 21.2. For \( 0 \leq k \leq n \) in \( \mathbb{N} \) define the binomial coefficient
\[
 \binom{n}{k} = \frac{n!}{k!(n-k)!} \in \mathbb{Q}.
\]
One also reads this “\( n \) choose \( k \)”.

Exercise 21.3. Prove that
\[
 \binom{n}{k} = \binom{n}{n-k}
\]
and
\[
 \binom{n}{0} = 1, \quad \binom{n}{1} = n.
\]

Exercise 21.4. Prove that
\[
 \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.
\]
Hint: direct computation with the definition.

Exercise 21.5. Prove that
\[
 \binom{n}{k} \in \mathbb{Z}.
\]
Hint: fix \( k \) and proceed by induction on \( n \); use Exercise 21.4.

Exercise 21.6. For any \( a, b \) in any ring we have
\[
 (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.
\]
Here if \( c \) is in a ring \( R \) and \( m \in \mathbb{N} \) then \( mc = c + \ldots + c \) (\( m \) times). Hint: Induction on \( n \) and use Exercise 21.4.

Exercise 21.7. (Subsets) Prove that if \( |A| = n \) then \( |\mathcal{P}(A)| = 2^n \). (A set with \( n \) elements has \( 2^n \) subsets.) Hint: induction on \( n \); if \( A = \{a_1, \ldots, a_{n+1}\} \) use
\[
 \mathcal{P}(A) = \{B \in \mathcal{P}(A); a_{n+1} \in B\} \cup \{B \in \mathcal{P}(A); a_{n+1} \notin B\}.
\]
Exercise 21.8. (Combinations) Let $A$ be a set with $|A| = n$, let $0 \leq k \leq n$ and set

$$\text{Comb}(k, A) = \{B \in \mathcal{P}(A); |B| = k\}$$

Prove that

$$|\{\text{Comb}(k, A)\}| = \binom{n}{k}.$$ 

I.e. a set of $n$ elements has exactly $\binom{n}{k}$ subsets with $k$ elements. A subset of $A$ having $k$ elements is called a combination of $k$ elements from the set $A$.

Hint: Fix $k$ and proceed by induction on $n$. If $A = \{a_1, ..., a_{n+1}\}$ use Exercise 21.4 plus the fact that $\text{Comb}(k, A)$ can be written as

$$\{B \in \mathcal{P}(A); |B| = k, a_{n+1} \in B\} \cup \{B \in \mathcal{P}(A); |B| = k, a_{n+1} \notin B\}.$$ 

Exercise 21.9. (Permutations) For a set $A$ let $\text{Perm}(A) \subset A^A$ be the set of all bijections $F : A \to A$. Prove that if $|A| = n$ then

$$|\text{Perm}(A)| = n!.$$ 

The elements of $\text{Perm}(A)$ are called permutations of $A$ so the exercise says that a set of $n$ elements has $n!$ permutations. Hint: Let $|A| = |B| = n$ and let $\text{Bij}(A, B)$ be the set of all bijections $F : A \to B$; it is enough to show that $|\text{Bij}(A, B)| = n!$. Proceed by induction on $n$; if $A = \{a_1, ..., a_{n+1}\}$, $B = \{b_1, ..., b_{n+1}\}$ then use the fact that

$$\text{Bij}(A, B) = \bigcup_{k=1}^{n+1} \{F \in \text{Bij}(A, B); F(a_1) = b_k\}.$$ 

For $d \in \mathbb{N}$ and $X$ a set write $X^d$ be the set of all maps $\{1, ..., d\} \to X$.

Exercise 21.10. (Combinations with repetition) Let

$$\text{Combrep}(n, d) = |\{(x_1, ..., x_d) \in \mathbb{Z}^d; x_i \geq 0, x_1 + \ldots + x_d = n\}|$$

Prove that

$$|\text{Combrep}(n, d)| = \binom{n + d - 1}{d - 1}.$$ 

Hint: Let $A = \{1, ..., n + d - 1\}$. Prove that there is a bijection

$$\text{Comb}(d - 1, A) \to \text{Combrep}(n, d)$$

The bijection is given by attaching to any subset

$$\{i_1, ..., i_{d-1}\} \subset \{1, ..., n + d - 1\}$$

(where $i_1 < ... < i_{d-1}$) the tuple $(x_1, ..., x_{d-1})$ where

1) $x_1 = |\{i \in \mathbb{Z}; 1 \leq i < i_1\}|$,
2) $x_k = |\{i \in \mathbb{Z}; i_k < i < i_{k+1}\}|$, for $2 \leq k \leq d - 1$, and
3) $x_d = |\{i \in \mathbb{Z}; i_{d-1} < i \leq n + d - 1\}|$. 

CHAPTER 22

Sequences

DEFINITION 22.1. A sequence in a set $A$ is a map $F : \mathbb{N} \to A$. If we write $F(n) = a_n$ we also say that $a_1, a_2, \ldots$ is a sequence in $A$.

THEOREM 22.2. (Recursion theorem) Let $A$ be a set, $a \in A$ an element, and let $F_1, F_2, \ldots$ be a sequence of maps $A \to A$. Then there is a unique map $G : \mathbb{N} \to A$ such that $F(1) = a$ and $G(n + 1) = F_n(G(n))$ for all $n \in \mathbb{N}$.

Sketch of proof. We construct $G$ as a subset of $\mathbb{N} \times A$. Let $Y$ be the set of all subsets $Y \subseteq \mathbb{N} \times A$ with the property that $(1, a) \in Y$ and $(n, x) \in Y \Rightarrow \forall n((n + 1, F_n(x)) \in Y)$ and we define

$$G = \bigcap_{Y \in Y} Y.$$ 

Then one proves by induction on $n$ that for any $n \in \mathbb{N}$ there exists unique $x \in A$ such that $(n, x) \in G$. So $G$ is a map. One then checks that $G$ has the desired property. □

Here are some applications of recursion.

Proposition 22.3. Let $(A, \leq)$ be an ordered set that has no maximal element. Then there is a sequence $F : \mathbb{N} \to A$ such that for all $n \in \mathbb{N}$ we have $F(n) < F(n + 1)$.

Proof. Let $B = \{(a, b) \in A \times A; a < b\}$ where $a < b$ means, of course, $a \leq b$ and $a \neq b$. By hypothesis the first projection $F : B \to A$, $(a, b) \mapsto a$ is surjective. By the axiom of choice there exists $G : A \to B$ such that $F \circ G = I_A$. Then $G(a) > a$ for all $a$. By the recursion theorem there exists $F : \mathbb{N} \to A$ such that $F(n + 1) = G(F(n))$ for all $n$ and we are done. □

Exercise 22.4. (Uniqueness of the ring of integers) Let $Z$ and $Z'$ be two ordered rings satisfying the well ordering axiom. Prove that there exists a unique ring homomorphism $F : Z \to Z'$; prove that this $F$ is bijective and increasing. Hint: Let $Z_+$ be the set of all elements in $Z$ which are $> 0$ and similarly for $Z'$. By recursion (which is, of course, valid in any ordered ring satisfying the well ordering axiom: explain!) there is a unique $F : Z_+ \to Z'_+$ satisfying $F(1) = 1$ and $F(n + 1) = F(n)$. Define $F$ on $Z$ by $F(-n) = F(n)$ for $-n \in Z_+$.

Definition 22.5. A set $A$ is countable if there exists a bijection $F : \mathbb{N} \to A$.

Example 22.6. The set of all squares $S = \{n^2; n \in \mathbb{N}\}$ is countable; indeed $F : \mathbb{N} \to S$, $F(n) = n^2$ is a bijection.
Exercise 22.7. Any subset of a countable set is countable. Hint: It is enough to show that any subset $A \subset \mathbb{N}$ is countable. Let $F \subset \mathbb{N} \times \mathbb{N}$ be the set

$$F = \{(x,y); y = \min(B \cap \{z \in \mathbb{N}; z > x\}\}$$

which is of course a map. By the recursion theorem there exists $G: \mathbb{N} \rightarrow \mathbb{N}$ such that $G(n + 1) = F(G(n))$. One checks that $G$ is injective and its image is $B$.

Exercise 22.8. Prove that $\mathbb{N} \times \mathbb{N}$ is countable. Hint: One can find injections $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$; e.g. $(m,n) \mapsto (m + n)^2 + m$.

Exercise 22.9. Prove that $\mathbb{Q}$ is countable.

Example 22.10. $\mathcal{P}(\mathbb{N})$ is not countable. Indeed this is a consequence of the more general theorem we proved that there is no bijection between a set $A$ and its power set $\mathcal{P}(A)$. However it is interesting to give a reformulation of the argument in this case (Cantor’s diagonal argument). Assume $\mathcal{P}(\mathbb{N})$ is countable and seek a contradiction. Since $\mathcal{P}(\mathbb{N})$ is in bijection with $\{0, 1\}^\mathbb{N}$ we get that there is a bijection $F: \mathbb{N} \rightarrow \{0, 1\}^\mathbb{N}$. Denote $F(n)$ by $F_n: \mathbb{N} \rightarrow \{0, 1\}$. Construct a map $G : \mathbb{N} \rightarrow \{0, 1\}$ by the formula

$$G(n) = \neg(F_n(n))$$

where $\neg : \{0, 1\} \rightarrow \{0, 1\}$, $\neg 0 = 1$, $\neg 1 = 0$. (The definition of $G$ does not need the recursion theorem; one can define $G$ as a “graph” directly (check!)). Since $F$ is surjective there exists $m$ such that $G = F_m$. In particular:

$$G(m) = F_m(m) = \neg G(m)$$

a contradiction.

Remark 22.11. Consider the following statement called the continuum hypothesis:

*For any set $A$ if there exists an injection $A \rightarrow \mathcal{P}(\mathbb{N})$ then either there exists an injection $A \rightarrow \mathbb{N}$ or there exists a bijection $A \rightarrow \mathcal{P}(\mathbb{N})$."

Answering this question (raised by Cantor) lead to important investigations in set theory. The answer (given by two theorems of Gödel and Cohen in the framework of mathematical logic rather than logic) turned out to be rather surprising; see the last part of this course.
CHAPTER 23

Reals

Definition 23.1. (Dedekind). A real number is a subset \( u \subset \mathbb{Q} \) of the set \( \mathbb{Q} \) of rational numbers with the following properties:
1) \( u \neq \emptyset \) and \( u \neq \mathbb{Q} \),
2) if \( x \in u, y \in \mathbb{Q} \), and \( x \leq y \) then \( y \in u \).
Denote by \( \mathbb{R} \) the set of real numbers.

Example 23.2.
1) Any rational number \( x \in \mathbb{Q} \) can be identified with the real number \( u_x = \{ y \in \mathbb{Q}; x \leq y \} \).
   It is clear that \( u_x = u_{x'} \) for \( x, x' \in \mathbb{Q} \) implies \( x = x' \). We identify any rational number \( x \) with \( u_x \). So we may view \( \mathbb{Q} \subset \mathbb{R} \).
2) One defines, for instance, for any \( n \in \mathbb{N} \), \( \sqrt{n} = \{ x \in \mathbb{Q}; x \geq 0, x^2 \geq n \} \).

Definition 23.3. If \( u \) and \( v \) are real numbers we write \( u \leq v \) if and only if \( v \subset u \). For \( u, v \geq 0 \) define
\[
    u + v = \{ x + y; x \in u, y \in v \}
\]
\[
    u \times v = uv = \{ xy; x \in u, y \in v \}.
\]
Note that this extends addition and multiplication on the non-negative rationals.

Exercise 23.4. Naturally extend the definition of addition + and multiplication \( \times \) of real numbers to the case when the numbers are not necessarily \( \geq 0 \). Prove that \( (\mathbb{R}, +, \times, -0, 1) \) is a field. Naturally extend the order \( \leq \) on \( \mathbb{Q} \) to an order on \( \mathbb{R} \) and prove that \( \mathbb{R} \) with \( \leq \) is an ordered ring.

Exercise 23.5. Define the sum and the product of a family of real (or complex) numbers indexed by a finite set. Hint: use the already defined concept for integers (and hence for the rationals).

Exercise 23.6. Prove that \((\sqrt{n})^2 = n\).

Exercise 23.7. Prove that for any \( r \in \mathbb{R} \) with \( r > 0 \) there exists a unique number \( \sqrt{r} \in \mathbb{R} \) such that \( \sqrt{r} > 0 \) and \((\sqrt{r})^2 = r\).

Exercise 23.8. Prove that \( \sqrt{2} \notin \mathbb{Q} \). Hint: assume there exists a rational number \( x \) such that \( x^2 = 2 \) and seek a contradiction. Let \( a \in \mathbb{N} \) be minimal with the property that \( x = \frac{a}{b} \) for some \( b \). Now \( \frac{a^2}{2} = 2 \) hence \( 2b^2 = a^2 \). Hence \( a^2 \) is even. Hence \( a \) is even (because if \( a \) were odd then \( a^2 \) would be odd.) Hence \( a = 2c \) for some integer \( c \). Hence \( 2b^2 = (2c)^2 = 4c^2 \). Hence \( b^2 = 2c^2 \). Hence \( b^2 \) is even. Hence \( b \) is even. Hence \( b = 2d \) for some integer \( d \). Hence \( x = \frac{2d}{2d} = \frac{1}{2} \) and \( c < a \). This contradicts the minimality of \( a \) which ends the proof.
Remark 23.9. The above proof is probably one of the “first” proofs by contra-
diction in the history of mathematics; this proof appears, for instance, in Aristotle
(4th century BC), and it is believed to have been discovered by the Pythagoreans.
The irrationality of $\sqrt{2}$ was translated by the Greeks as evidence that arithmetic is
insufficient to control geometry ($\sqrt{2}$ is the length of the diagonal of a square with
side 1) and arguably created the first crisis in the history of mathematics, leading
to a separation of algebra and geometry that lasted until Descartes (17th century).

Exercise 23.10. Prove that the set
\[ \{ r \in \mathbb{Q}; r > 0, r^2 < 2 \} \]
has no supremum in $\mathbb{Q}$.

Remark 23.11. Later we will prove that $\mathbb{R}$ is not countable.

Definition 23.12. For $a < b$ in $\mathbb{R}$ we define the open interval
\[ (a, b) = \{ c \in \mathbb{R}; a < c < b \} \subset \mathbb{R} \]
(Not to be confused with the pair $(a, b) \in \mathbb{R} \times \mathbb{R}$ which is denoted by the same
symbol.) A subset $U \subset \mathbb{R}$ is called open if for any $x \in U$ there exists an open
interval containing $x$ and contained in $U$: $x \in (a, b) \subset U$. Let $\mathcal{T} \subset \mathcal{P}(\mathbb{R})$ be the set
of all open sets of $\mathbb{R}$.

Exercise 23.13. Prove that $\mathcal{T}$ is a topology on $\mathbb{R}$; we call this the Euclidean
topology.
CHAPTER 24

Complexes

Once one has the notion of real number that of complex number is easy to introduce:

DEFINITION 24.1. A complex number is a pair \((a, b)\) where \(a, b \in \mathbb{R}\). We denote by \(\mathbb{C}\) the set of complex numbers. Hence \(\mathbb{C} = \mathbb{R} \times \mathbb{R}\). Define the sum and the product of two complex numbers by

\[
(a, b) + (c, d) = (a + c, b + d) \\
(a, b) \times (c, d) = (ac - bd, ad + bc).
\]

REMARK 24.2. Identify any real number \(a \in \mathbb{R}\) with the complex number \((a, 0) \in \mathbb{C}\); hence write \(a = (a, 0)\). In particular \(0 = (0, 0)\) and \(1 = (1, 0)\).

EXERCISE 24.3. Prove that \(\mathbb{C}\) equipped with 0, 1 above and with the operations +, \times above is a field. Also note that the operations + and \times on \(\mathbb{C}\) restricted to \(\mathbb{R}\) are the “old” operations + and \times on \(\mathbb{R}\).

NOTATION 24.4. We set \(i = (0, 1)\).

REMARK 24.5. \(i^2 = -1\). Indeed

\[
i^2 = (0, 1) \times (0, 1) = (0 \times 0 - 1 \times 1, 0 \times 1 + 1 \times 0) = (-1, 0) = -1.
\]

REMARK 24.6. For any complex number \((a, b) = a + bi\). Indeed

\[
(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi.
\]

DEFINITION 24.7. For any complex number \(z = a + bi\) we define its absolute value

\[
|z| = \sqrt{a^2 + b^2}.
\]

DEFINITION 24.8. For any complex number number \(z = a + bi \in \mathbb{C}\) and any real number \(r > 0\) we define the open disk with center \(z\) and radius \(r\),

\[
D(z, r) = \{w \in \mathbb{C}; |w - z| < r\} \subset \mathbb{C}
\]

A subset \(U \subset \mathbb{C}\) is called open if for any \(z \in U\) there exists an open disk centered at \(z\) and contained in \(U\). Let \(\mathcal{T} \subset \mathcal{P}(\mathbb{C})\) be the set of all open sets of \(\mathbb{C}\).

EXERCISE 24.9. Prove that \(\mathcal{T}\) is a topology on \(\mathbb{C}\); we call this the Euclidean topology.

EXERCISE 24.10. Prove that \(\mathbb{C}\) cannot be given the structure of an ordered ring.
CHAPTER 25

Residues

First we develop some “arithmetic” in \( \mathbb{Z} \).

**Definition 25.1.** For integers \( a \) and \( b \) we say \( a \) divides \( b \) if there exists an integer \( n \) such that \( b = an \). We write \( a|b \). We also say \( a \) is a divisor of \( b \). If \( a \) does not divide \( b \) write \( a \not{|} b \).

**Example 25.2.** \( 4|20; 6 \not{|} 20 \).

**Exercise 25.3.** Prove that
1) if \( a|b \) and \( b|c \) then \( a|c \);  
2) if \( a|b \) and \( a|c \) then \( a|b+c \);  
3) \( a|b \) defines an order relation on \( \mathbb{N} \) but not on \( \mathbb{Z} \).

**Theorem 25.4.** (Euclid division). For any \( a \in \mathbb{Z} \) and \( b \in \mathbb{N} \) there exist unique \( q, r \in \mathbb{Z} \) such that \( a = bq + r \) and \( 0 \leq r < b \).

**Proof.** We prove the existence of \( q, r \). The uniqueness is left to the reader. We may assume \( a \in \mathbb{N} \). We proceed by contradiction. So assume there exists \( b \) and \( a \in \mathbb{N} \) such that for all \( q, r \in \mathbb{Z} \) with \( 0 \leq r < b \) we have \( a \neq bq + r \). Fix such a \( b \). We may assume \( a \) is minimum with the above property. If \( a < b \) we can write \( a = 0 \times b + a \), a contradiction. If \( a = b \) we can write \( a = 1 \times a + 0 \), a contradiction. If \( a > b \) set \( a' = a - b \). Since \( a' < a \), there exist \( q', r \in \mathbb{Z} \) such that \( 0 \leq r < b \) and \( a' = q'b + r \). But then \( a = qb + r \), where \( q = q' + 1 \), a contradiction. \( \square \)

**Notation 25.5.** For \( a \in \mathbb{Z} \) denote \( \langle a \rangle \) the set \( \{na; n \in \mathbb{Z}\} \) of integers divisible by \( a \). For \( a, b \in \mathbb{Z} \) denote by \( \langle a, b \rangle \) the set \( \{ma + nb; m, n \in \mathbb{Z}\} \) of all numbers expressible as a multiple of \( a \) plus a multiple of \( b \).

**Proposition 25.6.** For any integers \( a, b \) there exists an integer \( c \) such that \( \langle a, b \rangle = \langle c \rangle \).

**Proof.** If \( a = b = 0 \) we can take \( c = 0 \). Assume \( a, b \) are not both 0. Then the set \( S = \langle a, b \rangle \cap \mathbb{N} \) is non-empty. Let \( c \) be the minimum of \( S \). Clearly \( \langle c \rangle \subset \langle a, b \rangle \). Let us prove that \( \langle a, b \rangle \subset \langle c \rangle \). Let \( u = ma + nb \) and let us prove that \( u \in \langle c \rangle \). By Euclidean division \( u = cq + r \) with \( 0 \leq r < c \). We want to show \( r = 0 \). Assume \( r \neq 0 \) and seek a contradiction. Write \( c = m'a + n'a \). Then \( r \in \mathbb{N} \) and also \( r = u - cq = (ma + nb) - (m'a + n'a)q = (m - m'q)a + (n - n'q)b \in \langle a, b \rangle \). Hence \( r \in S \). But \( r < c \). So \( c \) is not the minimum of \( S \), a contradiction. \( \square \)

**Proposition 25.7.** If \( a \) and \( b \) are integers and have no common divisor > 1 then there exist integers \( m \) and \( n \) such that \( ma + nb = 1 \).

**Proof.** By the above Proposition \( \langle a, b \rangle = \langle c \rangle \) for some \( c \geq 1 \). In particular \( c|a \) and \( c|b \). The hypothesis implies \( c = 1 \) hence \( 1 \in \langle a, b \rangle \). \( \square \)

One of the main definitions of number theory is
Definition 25.8. An integer \( p \) is prime if \( p > 1 \) and if its only positive divisors are 1 and \( p \).

Proposition 25.9. If \( p \) is a prime and \( a \) is an integer such that \( p \neq a \) then there exist integers \( m, n \) such that \( ma + np = 1 \).

Proof. \( a \) and \( p \) have no common divisor > 1 and we conclude by Proposition 25.7. \( \square \)

Proposition 25.10. (Euclid Lemma) If \( p \) is a prime and \( p \mid ab \) for integers \( a \) and \( b \) then either \( p \mid a \) or \( p \mid b \).

Proof. Assume \( p \nmid a, p \nmid b \), and seek a contradiction. By Proposition 25.9 \( ma + np = 1 \) for some integers \( m, n \) and \( m'b + n'p = 1 \) for some integers \( m', n' \). We get \[ 1 = (ma + np)(m'b + n'p) = mm'ab + p(nm' + n'm + nn'). \]
Since \( p \nmid ab \) we get \( p \mid 1 \), a contradiction. \( \square \)

Exercise 25.11. Prove that any integer \( n > 1 \) can be written uniquely as a product of primes. (This is the Fundamental Theorem of Arithmetic). Hint: prove existence of decomposition by contradiction by considering the smallest number which is not a product of primes. Prove uniqueness by contradiction by assuming \( n \) is the smallest integer such that \( p_1p_2\ldots = q_1q_2\ldots \) with \( p_i \) and \( q_j \) prime, \( p_1 \leq p_2 \leq \ldots \), \( q_1 \leq q_2 \leq \ldots \).

Definition 25.12. Fix an integer \( m \neq 0 \). Define a relation \( \equiv \) on \( \mathbb{Z} \) by \( a \equiv b \) if and only if \( m \mid a - b \). Say \( a \) congruent to \( b \mod m \); instead of \( a \equiv b \) one usually writes (following Gauss):
\[ a \equiv b \mod m. \]

Example 25.13. \( 3 \equiv 17 \mod 7 \).

Exercise 25.14. Prove that \( \equiv \) is an equivalence relation. Prove that the equivalence class \( \overline{a} \) of \( a \) consists of all the numbers of the form \( mb + a \) where \( m \in \mathbb{Z} \).

Example 25.15. If \( m = 7 \) then \( \overline{3} = \overline{10} = \{\ldots, -4, 3, 10, 17, \ldots \} \).

Definition 25.16. For the equivalence relation \( \equiv \) on \( \mathbb{Z} \) the set of equivalence classes \( \mathbb{Z}/\equiv \) is denoted by \( \mathbb{Z}/m\mathbb{Z} \). The elements of \( \mathbb{Z}/m\mathbb{Z} \) are called residue classes mod \( m \).

Exercise 25.17. Prove that \[ \mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}. \]
So the residue classes mod \( m \) are: \( \overline{0}, \overline{1}, \ldots, \overline{m-1} \). Hint: use Euclid division.

Definition 25.18. Define operations \( +, \times, - \) on \( \mathbb{Z}/m\mathbb{Z} \) by
\[ \overline{a} + \overline{b} = \overline{a + b} \]
\[ \overline{a} \times \overline{b} = \overline{ab} \]
\[ -\overline{a} = -\overline{a} \]
Exercise 25.19. Check that the above definitions are correct, in other words that if \( \overline{a} = \overline{c} \) and \( \overline{b} = \overline{d} \) then

\[
\begin{align*}
\overline{a + b} &= \overline{c + d} \\
\overline{ab} &= \overline{cd} \\
\overline{-a} &= \overline{-c}.
\end{align*}
\]

Furthermore check that \((\mathbb{Z}/m\mathbb{Z}, +, \times, 0, 1)\) is a ring.

Notation 25.20. If \( p \) is a prime we write \( \mathbb{F}_p \) in place of \( \mathbb{Z}/p\mathbb{Z} \).

Exercise 25.21. Prove that \( \mathbb{F}_p \) is a field. Hint: use Proposition 25.9.
**p-adics**

p-adic numbers were invented by Hensel at the turn of the 20th century. They are “alternative worlds” with respect to the reals and, in a precise sense, the “only alternative worlds”.

**Definition 26.1.** Let $p$ be a prime. Let $S$ be the set of all sequences $(a_n)$ of integers $a_n \in \mathbb{Z}$ such that for all $n$

$$a_n \equiv a_{n+1} \mod p^n.$$ 

Say that two sequences $(a_n)$ and $(b_n)$ as above are equivalent (write $(a_n) \sim_p (b_n)$) if for all $n$

$$a_n \equiv b_n \mod p^n.$$ 

Denote by $[a_n]$ the equivalence class of the sequence $(a_n)$. Denote by

$$\mathbb{Z}_p = S/\sim_p$$

the set of equivalence classes. Then $\mathbb{Z}_p$ is a ring with addition and multiplication defined by

$$[a_n] + [b_n] = [a_n + b_n]$$

$$[a_n][b_n] = [a_nb_n];$$

0 and 1 in this ring are the classes of the constant 0, respectively 1 sequences. $\mathbb{Z}_p$ is called the ring of p-adic integers. (N.B. $\mathbb{Z}_p$ is the standard notation for this object in number theory; however in many books $\mathbb{Z}_p$ is used to denote what we denoted by $\mathbb{F}_p$; one should be aware of this discrepancy between generally accepted notation.)

**Exercise 26.2.** Check that the ring axioms are satisfied.

**Exercise 26.3.** Consider a sequence $(b_n)$ and the sequence

$$a_n = b_1 + pb_2 + p^2b_3 + \ldots + p^{n-1}b_n.$$ 

Prove that $(a_n) \in S$. Also, any element in $S$ can be written like this.

**Remark 26.4.** There is a surjective natural homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$, $[a_n] \mapsto \overline{a_n}$. 

**Remark 26.5.** We summarize the main rings of numbers we have encountered so far; they are the main types of numbers in mathematics:
Exercise 26.6. Prove that there are no ring homomorphisms $\mathbb{C} \to \mathbb{F}_p$ and there are no ring homomorphisms $\mathbb{F}_p \to \mathbb{C}$. (Morally the worlds of $\mathbb{F}_p$ and $\mathbb{C}$ do not “communicate directly”, although they “communicate via $\mathbb{Z}$).

Remark 26.7. There exist (many) injective ring homomorphisms $\mathbb{Z}_p \to \mathbb{C}$ but they are not “natural” in any way.
Algebra

Algebra is the study of algebraic structures, i.e. sets with operations on them. We already introduced, and constructed, some elementary examples of algebraic structures such as rings and, in particular, fields. With rings/fields at our disposal one can study some other fundamental algebraic objects such as groups, matrices, vector spaces, polynomials, etc. In what follows we briefly survey some of these.

In some sense groups are more fundamental than rings and fields; but in order to be able to look at more interesting examples we found it convenient to postpone the discussion of groups until this point.

Definition 27.1. A group is a tuple \((G,\star,\prime,e)\) consisting of a set \(G\), a binary operation \(\star\) on \(G\), a unary operation \(\prime\) on \(G\) (write \(\prime(x) = x'\)), and an element \(e \in G\) (called the identity element) such that for any \(x,y,z \in G\) the following axioms are satisfied:

1) \(x \star (y \star z) = (x \star y) \star z\);
2) \(x \star e = e \star x = x\);
3) \(x \star x' = x' \star x = e\).

If in addition \(x \star y = y \star x\) for all \(x,y \in G\) we say \(G\) is commutative (or Abelian in honor of Abel).

Notation 27.2. Sometimes one writes \(e = 1\), \(x \star y = xy\), \(x' = x^{-1}\), \(x \star \ldots \star x = x^n\) (\(n \geq 1\) times). In the Abelian case one sometimes writes \(e = 0\), \(x \star y = x + y\), \(x' = -x\), \(x \star \ldots \star x = nx\) (\(n \geq 1\) times). These notations depend on the context and are justified by the following examples.

Example 27.3. If \(R\) is a ring then \(R\) is an Abelian group with \(e = 0\), \(x \star y = x + y\), \(x' = -x\). Hence \(\mathbb{Z},\mathbb{Z}/m\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\) are groups “with respect to addition”.

Example 27.4. If \(R\) is a field then \(R^\times = R \setminus \{0\}\) is an Abelian group with \(e = 1\), \(x \star y = xy\), \(x' = x^{-1}\). Hence \(\mathbb{Q}^\times,\mathbb{R}^\times,\mathbb{C}^\times,\mathbb{F}_p^\times\) are groups “with respect to multiplication”.

Example 27.5. The set \(S(X)\) of bijections \(\sigma : X \to X\) from a set \(X\) into itself is a (non-Abelian) group with \(e = 1_X\) (the identity map), \(\sigma \star \tau = \sigma \circ \tau\) (composition), \(\sigma^{-1}\) =inverse map. If \(X = \{1,\ldots,n\}\) then one writes \(S_n = S(X)\) and call this group the symmetric group. If \(\sigma(1) = i_1,\ldots,\sigma(n) = i_n\) one usually writes

\[
\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.
\]

Exercise 27.6. Compute

\[
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}.
\]
Also compute

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 \\
3 & 2 & 5 & 4 & 3
\end{pmatrix}^{-1}
\]

**Example 27.7.** A $2 \times 2$ matrix with coefficients in a field $R$ is an element $A = (a, b, c, d) \in R^4 = R \times R \times R \times R$. We usually write such an $A$ as

\[
A = \begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]

Define the sum and the product of two matrices by

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix} + \begin{pmatrix}
a' & b' \\
c' & d'
\end{pmatrix} = \begin{pmatrix}
a + a' & b + b' \\
c + c' & d + d'
\end{pmatrix}
\]

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix} \cdot \begin{pmatrix}
a' & b' \\
c' & d'
\end{pmatrix} = \begin{pmatrix}
a a' + b c' & a b' + b d' \\
c a' + d c' & c b' + d d'
\end{pmatrix}
\]

Define the product of an element $r \in R$ with a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by

\[
 r \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix}
\]

Say a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible if $\delta = ad - bc \neq 0$ and we define its inverse by

\[
A^{-1} = \delta^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}
\]

Define the identity matrix by

\[
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\]

and the zero matrix by

\[
O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\]

Let $M_2(R)$ be the set of all matrices and $GL_2(R)$ be the set of all invertible matrices. Then the following are true:

1) $M_2(R)$ is a group with respect to addition of matrices;
2) $GL_2(R)$ is a group with respect to multiplication of matrices;
3) $(A + B)C = AC + BC$ and $C(A + B) = CA + CB$ for any matrices $A, B, C$;
4) There exist matrices $A, B$ such that $AB \neq BA$.

**Exercise 27.8.** Prove 1), 2), 3), 4) above.

**Example 27.9.** Groups are examples of algebraic structures so there is a well defined notion of homomorphism of groups (or group homomorphism). According to the general definition a group homomorphism is a map between the two groups $F : G \to G'$ such that for all $a, b \in G$:

1) $F(a \ast b) = F(a) \ast F(b)$;
2) $F(a^{-1}) = F(a)^{-1}$ (this is automatic!);
3) $F(e) = e$ (this is, again, automatic!).

Here we used $\ast$ for both operations in $G$ and $G'$.

Next we discuss vector spaces.
DEFINITION 27.10. Let $R$ be a field. A vector space is an abelian group $(V, +, - , 0)$ together with a map $R \times V \rightarrow V$, $(a, v) \mapsto av$ satisfying the following conditions for all $a, b \in R$ and all $u, v \in V$:  
1) $(a + b)v = av + bv$  
2) $a(u + v) = au + av$  
3) $a(vu) = (a)v$  
4) $1v = v$

DEFINITION 27.11. The elements $u_1, \ldots, u_n \in V$ are linearly independent if whenever $a_1, \ldots, a_n \in R$ satisfies $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ it follows that $a_1u_1 + \ldots + a_nu_n \neq 0$.

DEFINITION 27.12. The elements $u_1, \ldots, u_n \in V$ generate $V$ if for any $u \in V$ there exist $a_1, \ldots, a_n \in R$ such that $u = a_1u_1 + \ldots + a_nu_n$.

DEFINITION 27.13. The elements $u_1, \ldots, u_n \in V$ are a basis of $V$ if they are linearly independent and generate $V$.

EXERCISE 27.14. If $V$ has a basis $u_1, \ldots, u_n$ elements then the map $R^n \rightarrow V$, $(a_1, \ldots, a_n) \mapsto a_1u_1 + \ldots + a_nu_n$ is bijective. Hint: directly from definitions.

EXERCISE 27.15. If $V$ is generated by $u_1, \ldots, u_n$ then $V$ has a basis consisting of at most $n$ elements. Hint: considering a subset of $\{u_1, \ldots, u_n\}$ minimal with the property that it generates $V$ we may assume that any subset obtained from $\{u_1, \ldots, u_n\}$ does not generate $V$. We claim that $u_1, \ldots, u_n$ are linearly independent. Assume not. Hence there exists $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ such that $a_1u_1 + \ldots + a_nu_n = 0$. We may assume $a_1 = 1$. Then one checks that $u_2, \ldots, u_n$ generate $V$, contradicting minimality.

EXERCISE 27.16. Assume $R = \mathbb{F}_p$ and $V$ has a basis with $n$ elements. Then $|V| = p^n$.

THEOREM 27.17. If $V$ has a basis $u_1, \ldots, u_n$ and a basis $v_1, \ldots, v_m$ then $n = m$.

Proof. We prove $m \leq n$; similarly one has $n \leq m$. Assume $m > n$ and seek a contradiction. Since $u_1, \ldots, u_n$ generate $V$ we may write $v_1 = a_1u_1 + \ldots + a_nu_n$ with not all $a_1, \ldots, a_n$ zero. Renumbering $u_1, \ldots, u_n$ we may assume $a_1 \neq 0$. Hence $v_1, v_2, \ldots, u_n$ generates $V$. Hence $v_2 = b_1v_1 + b_2u_2 + \ldots + b_nu_n$. But not all $b_2, \ldots, b_n$ can be zero because $v_1, v_2$ are linearly independent. So renumbering $u_2, \ldots, u_n$ we may assume $b_2 \neq 0$. So $v_1, v_2, u_3, \ldots, u_n$ generates $V$. Continuing (one needs induction) we get that $v_1, v_2, \ldots, v_n$ generates $V$. So $v_{n+1} = d_1v_n + \ldots + d_nv_n$. But this contradicts the fact that $v_1, \ldots, v_m$ are linearly independent.

EXERCISE 27.18. Give a quick proof of the above theorem in case $R = \mathbb{F}_p$. Hint: We have $p^n = p^m$ hence $n = m$.

EXERCISE 27.19. Give an example of a vector space which, for all $n$, does not have a basis with $n$ elements.

DEFINITION 27.20. Assume $V$ has a basis $u_1, \ldots, u_n$. Then we define the dimension of $V$ to be $n$; write $\dim V = n$. (The definition is correct due to the above Proposition.)

DEFINITION 27.21. If $V$ and $W$ are vector spaces a map $F: V \rightarrow W$ is called linear if for all $a \in K$, $u, v \in V$ we have:
1) $F(au) = aF(u)$,
2) $F(u + v) = F(u) + F(v)$.

**Exercise 27.22.** Prove that $F : V \rightarrow W$ is a linear map of vector spaces then $V' = F^{-1}(0)$ and $V'' = F(V)$ are vector spaces (with respect to the obvious operations) and
$$\dim V = \dim V' + \dim V''.$$ Hint: construct corresponding bases.

Here is the link with matrices:

**Remark 27.23.** If $F : V \rightarrow W$ is a linear map of vector spaces and $v_1, ..., v_n$ and $w_1, ..., w_m$ are bases of $V$ and $W$ respectively then one can write uniquely $F(v_i) = \sum_{j=1}^{m} a_{ij} w_j$; one obtains $nm$ numbers $a_{ij} \in R$ which completely characterize $F$.

Finally we mention polynomials and algebraic equations.

**Definition 27.24.** Let $R$ be a ring and $n \in \mathbb{Z}, n \geq 0$. A function $f : R \rightarrow R$ is called a polynomial function of degree $n$ if there exist elements $a_0, ..., a_n \in R$, $a_n \neq 0$, such that for all $b \in R$,
$$f(b) = a_n b^n + ... + a_1 b + a_0.$$ A function $R \rightarrow R$ is called a polynomial function if it is either the zero function (the function that sends $R$ into 0) or if it is a polynomial function of some degree. An element $c \in R$ is called a root of $f$ (or a zero of $f$) if $f(c) = 0$. (Sometimes we say “a root in $R$” instead of “a root”.)

The study of roots of polynomial functions is one of the main concerns of algebra. Here are two of the main basic theorems about roots; their proof is beyond the scope of this course.

**Theorem 27.25.** *(Lagrange)* If $R$ is a field then any polynomial function of degree $n \geq 1$ has at most $n$ roots in $R$.

**Theorem 27.26.** *(Gauss)* If $R = \mathbb{C}$ is the complex field then any polynomial function of degree $n \geq 1$ has at least one root in $\mathbb{C}$.

**Remark 27.27.** The main problems about roots are:
1) Find the number of roots; in case $R = \mathbb{F}_p$ this leads to some of the most subtle problems in number theory.
2) Find (if possible) formulae that compute roots (such as formulae involving radicals); this leads to Galois theory.
CHAPTER 28

Geometry

Geometry is the study of shapes such as lines and planes, or, more generally, curves and surfaces, etc. There are two paths towards this study: the synthetic one and the analytic (or algebraic) one. Synthetic geometry is geometry without algebra. Analytic geometry is geometry through algebra. Synthetic geometry originates with the Greek mathematics of antiquity (e.g. the treatise of Euclid). Analytic geometry was invented by Fermat and Descartes in the 17th century. We already encountered the synthetic approach in the discussion of the affine plane and the projective plane which were purely combinatorial objects. Here we introduce some of the most elementary structures of analytic geometry.

Definition 28.1. Let $R$ be a field. The affine plane $\mathbb{A}^2 = \mathbb{A}^2(R)$ over $R$ is the set $R^2 = R \times R$. A point $P = (x, y)$ in the plane is an element of $R \times R$. A subset $L \subset R \times R$ is called a line if there exist $a, b, c \in R$ such that $(a, b) \neq (0, 0)$ and

$$L = \{(x, y) \in R^2; ax + by + c = 0\}$$

We say a point $P$ lies on the line $L$ (or we say $L$ passes through $P$) if $P \in L$. Two lines are said to be parallel if they either coincide or their intersection is empty (in the last case we say they don’t meet). 3 points are collinear if they lie on the same line.

Notation 28.2. We sometimes write $L = L(R)$ if we want to stress that coordinates are in $R$.

Exercise 28.3. Prove that:

1) There exist 3 points which are not collinear.

2) For any two distinct points $P_1$ and $P_2$ there exists a unique line $L$ (called sometimes $P_1P_2$) passing through $P_1$ and $P_2$. Hint: If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and if

$$m = (y_2 - y_1)(x_2 - x_1)^{-1}$$

then the unique line through $P_1$ and $P_2$ is:

$$L = \{(x, y) \in R \times R; y - y_1 = m(x - x_1)\}.$$ 

In particular any two non-parallel distinct lines meet in exactly one point.

3) Given a line $L$ and a point $P$ there exists exactly one line $L'$ passing through $P$ and parallel to $L$. (This is called Euclid’s fifth postulate but in our exposition here this is not a postulate).

Hence $\mathbb{A}^2 = R^2 = R \times R$ together with the set $\mathcal{L}$ of all lines (in the sense above) is an affine plane in the sense of Definition 16.43.

Remark 28.4. Not all affine planes in the sense of Definition 16.43 are affine planes over a field in the sense above. Hilbert [5] proved that an affine plane is the
affine plane over some field if and only if the theorems of Desargues (Parts I and II) and Pappus hold. See below for the “only if direction”.

**Exercise 28.5.** Prove that any line in $\mathbb{F}_p \times \mathbb{F}_p$ has exactly $p$ points.

**Exercise 28.6.** How many lines are there in the plane $\mathbb{F}_p \times \mathbb{F}_p$?

**Exercise 28.7.** (Desargues’ Theorem, Part I) Let $A_1, A_2, A_3, A'_1, A'_2, A'_3$ be distinct points in the plane. Also for all $i \neq j$ assume $A_iA_j$ and $A'_iA'_j$ are not parallel and let $P_{ij}$ be their intersection. Assume the 3 lines $A_1A'_1, A_2A'_2, A_3A'_3$ have a point in common. Then prove that the points $L_{12}, L_{13}, L_{23}$ are collinear (i.e. line on some line). Hint: Consider the “space” $R \times R \times R$ and define planes and lines in this space. Prove that if two planes meet and don’t coincide then they meet in a line. Then prove that through any two points in space there is a unique line and through any 3 non-collinear points there is a unique plane. Now consider the projection $R \times R \times R \to R \times R, (x, y, z) \mapsto (x, y)$ and show that lines project onto lines. Next show that configuration of points $A_i, A'_i \in R \times R$ can be realized as the projection of a similar configuration of points $B_i, B'_i \in R \times R \times R$ not contained in a plane. (Identifying $R \times R$ with the set of points in space with zero third coordinate we take $B_i = A_i, B'_i = A'_i$ for $i = 1, 2, 3$, we let $B_3$ have a nonzero third coordinate and then we choose $B'_3$ such that the lines $B_1B'_1, B_2B'_2, B_3B'_3$ have a point in common.) Then prove Desargues in space (by noting that if $Q_{ij}$ is the intersection of $B_iB_j$ with $B'_iB'_j$ then $Q_{ij}$ is in the plane containing $B_1, B_2, B_3$ and also in the plane containing $B'_1, B'_2, B'_3$, hence $Q_{ij}$ is in the intersection of these planes which is a line.) Finally deduce the original plane Desargues by projection.

**Exercise 28.8.** (Desargues’ Theorem, Part II) Let $A_1, A_2, A_3, A'_1, A'_2, A'_3$ be distinct points in the plane. Assume the 3 lines $A_1A'_1, A_2A'_2, A_3A'_3$ have a point in common or they are parallel. Assume $A_1A_2$ is parallel to $A'_1A'_2$ and $A_1A_3$ is parallel to $A'_1A'_3$. Prove that $A_2A_3$ is parallel to $A'_2A'_3$. Hint: compute coordinates. There is an alternative proof that reduces Part II to Part I by using the “projective plane over our field”.

**Exercise 28.9.** (Pappus’ Theorem) Let $P_1, P_2, P_3$ be points on a line $L$ and let $Q_1, Q_2, Q_3$ be points on a line $M \neq L$. Let $A_1$ be the intersection of $P_2Q_3$ with $P_3Q_2$, and define $A_2, A_3$ similarly. (Assume the lines in question are not parallel.) Then prove that $A_1, A_2, A_3$ are collinear. Hint for the case $L$ and $M$ meet. Then one can assume $L = \{(x, 0); x \in R\}, M = \{(0, y); y \in R\}$ (explain why). Let the points $P_i = (x_i, 0)$, and $Q_i = (0, y_i)$ and compute the coordinates of $A_i$. Then check that the line through $A_1$ and $A_2$ passes through $A_3$.

**Remark 28.10.** One can identify the projective plane $(\overline{\mathbb{F}}^2, \mathcal{L})$ attached to the affine plane $(\mathbb{A}^2, \mathcal{L})$ with the pair $(\mathbb{F}^2, \overline{\mathbb{F}}^2)$ defined as follows. Let $\mathbb{F}^2 = R^3/\sim$ where $(x, y, z) \sim (x', y', z')$ if and only if there exists $0 \neq \lambda \in R$ such that $(x', y', z') = (\lambda x, \lambda y, \lambda z)$. Denote the equivalence class of $(x, y, z)$ by $(x : y : z)$. Identify a point $(x, y)$ in the affine plane $\mathbb{A}^2 = R^2 = R \times R$ with the point $(x : y : 1) \in \mathbb{F}^2$. Identify a point $(x_0 : y_0 : 0)$ in the complement $\mathbb{F}^2 \setminus \mathbb{A}^2$ with the class of lines in $\mathbb{A}^2$ parallel to the line $y_0x - x_0y = 0$. This allows one to identify the complement $\mathbb{F}^2 \setminus \mathbb{A}^2$ with the line at infinity $L_\infty$ of $\mathbb{A}^2$. Hence we get an identification of $\mathbb{F}^2$ with $\overline{\mathbb{F}}^2$. Finally define a line in $\mathbb{F}^2$ as a set of the form

$$\mathcal{L} = \{(x : y : z); ax + by + cz = 0\}$$
So under the above identifications,
\[ \mathcal{L} = \{(x : y : 1); ax + by + c = 0\} \cup \{(x : y : 0); ax + by = 0\} = L \cup \{\hat{L}\} \]
where \( L \) is the line in \( \mathbb{R}^2 \) defined by \( ax + by + c = 0 \). Then define \( \hat{L} \) to be the set of all lines \( \overline{\mathcal{L}} \) in \( \mathbb{P}^2 \). We get an identification of \( \hat{\mathbb{P}}^2 \) with \( \mathbb{F}^2 \).

So far we were concerned with points, lines, planes. Let us tackle “curved shapes”, e.g. “higher degree curves”.

**Definition 28.11.** The circle of center \((a, b) \in \mathbb{R} \times \mathbb{R}\) and radius \(r\) is the set
\[ C(R) = \{(x, y) \in \mathbb{R} \times \mathbb{R}; (x - a)^2 + (y - b)^2 = r^2\} \]

**Definition 28.12.** A line is tangent to a circle if it meets it in exactly one point. (We say that the line is tangent to the circle at that point). Two circles are tangent if they meet in exactly one point.

**Exercise 28.13.** Prove that for any circle and any point on it there is exactly one line tangent to the circle at that point.

**Exercise 28.14.** Prove that:
1) A circle and a line meet in at most 2 points.
2) Two circles meet in at most 2 points.

**Exercise 28.15.** How many points does a circle of radius 1 in \( \mathbb{F}_{13} \) have? Same problem for \( \mathbb{F}_{11} \).

**Exercise 28.16.** Prove that the circle \( C(R) \) with center \((0, 0)\) and radius 1 is an Abelian group with \( e = (1, 0), (x, y)' = (x, -y) \), and group operation
\[ (x_1, y_1) \ast (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \]

**Exercise 28.17.** Consider the circle \( C(\mathbb{F}_{17}) \). Show that \((3, \bar{3}), (\bar{1}, 0) \in C(\mathbb{F}_{17})\) and compute \((3, \bar{3}) \ast (\bar{1}, 0)\) and \(2(\bar{1}, 0)\) (where the latter is of course \((\bar{1}, 0) \ast (\bar{1}, 0)\)).

Circles are special cases of conics:

**Definition 28.18.** A conic is a subset \( Q \subset \mathbb{R} \times \mathbb{R} \) of the form
\[ Q = Q(R) = \{(x, y) \in \mathbb{R} \times \mathbb{R}; ax^2 + bxy + cy^2 + dx + ey + f = 0\} \]
for some \((a, b, c, d, e, f) \in \mathbb{R} \times \ldots \times \mathbb{R}\), where \((a, b, c) \neq (0, 0, 0)\).

We refer to \((a, b, c, d, e, f)\) as the equation of the quadric and if the corresponding quadric passes through a point we say that the equation of the quadric passes through the point. We sometimes say “quadric” instead of “equation of the quadric”.

**Exercise 28.19.** (Uses the concept of vector space and dimension). Prove that if 5 points are given in the plane such that no 4 of them are collinear then there exists a unique quadric passing through these given 5 points. Hint: consider the vector space of all (equations of) quadrics that pass through a given set \( S \) of points. Next note that if one adds a point to \( S \) the dimension of this space of quadrics either stays the same or drops by one. Since the space of all quadrics has dimension 6 it is enough to show that for \( r \leq 5 \) the quadrics passing through \( r \) points are fewer than those passing through \( r - 1 \) of the \( r \) points. For \( r = 4 \), for instance, this is done by taking a quadric that is a union of 2 lines.
DEFINITION 28.20. Let $R$ be a field in which $2 := 1 + 1 \neq 0$, $3 := 1 + 1 + 1 \neq 0$. A subset $Z = Z(R) \subset R \times R$ is called an affine elliptic curve if there exist $a, b \in R$ with $4a^3 + 27b^2 \neq 0$ such that

$$Z(R) = \{(x, y) \in R \times R; y^2 = x^3 + ax + b\}.$$ 

We call $Z(R)$ the elliptic curve over $R$ defined by the equation $y^2 = x^3 + ax + b$. Next we define the projective elliptic curve defined by the equation $y^2 = x^3 + ax + b$. as the set

$$E(R) = Z(R) \cup \{\infty\}$$

where $\infty$ is an element not belonging to $Z(R)$. (We usually drop the word “projective” and we call $\infty$ the point at infinity on $E(R)$.) If $(x, y) \in E(R)$ define $(x, y)' = (x, -y)$. Also define $\infty' = \infty$. Next we define a binary operation $+$ on $E(R)$ called the chord-tangent operation; we will see that $E(R)$ becomes a group with respect to this operation. First define $(x, y) + (x, -y) = \infty$, $\infty + (x, y) = (x, y)\infty = (x, y)$, and $\infty + \infty = \infty$. Also define $(x, 0) + (x, 0) = \infty$. Next assume $(x_1, y_1), (x_2, y_2) \in E(R)$ with $(x_2, y_2) \neq (x_1, -y_1)$. If $(x_1, y_1) \neq (x_2, y_2)$ we let $L_{12}$ to be the unique line passing through $(x_1, y_1)$ and $(x_2, y_2)$. Recall that explicitly

$$L_{12} = \{(x, y) \in R \times R; y - y_1 = m(x - x_1)\}$$

where

$$m = (y_2 - y_1)(x_2 - x_1)^{-1}.$$ 

If $(x_1, y_1) = (x_2, y_2)$ we let $L_{12}$ be the “line tangent to $Z(R)$ at $(x_1, y_1)$” which is by definition given by the same equation as before except now $m$ is defined to be

$$m = (3x_1^2 + a)(2y_1)^{-1}.$$ 

(This definition is inspired by the definition of slope in analytic geometry.) Finally one defines

$$(x_1, y_1) + (x_2, y_2) = (x_3, -y_3)$$

where $(x_3, y_3)$ is the “third point of intersection of $E(R)$ with $L_{12}$”; more precisely $(x_3, y_3)$ is defined by solving the system consisting of the equations defining $E(R)$ and $L_{12}$ as follows: replacing $y$ in $y^2 = x^3 + ax + b$ by $y_1 + m(x - x_1)$ we get a cubic equation in $x$:

$$(y_1 + m(x - x_1))^2 = x^3 + ax + b$$

which can be rewritten as

$$x^3 - m^2x^2 + \ldots = 0.$$ 

$x_1, x_2$ are known to be roots of this equation. We define $x_3$ to be the third root which is then

$$x_3 = m^2 - x_1 - x_2;$$ 

so we define

$$y_3 = y_1 + m(x_3 - x_1).$$

Summarizing, the definition of $(x_3, y_3)$ is

$$(x_3, y_3) = \left((y_2 - y_1)^2(x_2 - x_1)^{-2} - x_1 - x_2, y_1 + (y_2 - y_1)(x_2 - x_1)^{-1}(x_3 - x_1)\right)$$

if $(x_1, y_1) \neq (x_2, y_2)$, $(x_1, y_1) \neq (x_2, -y_2)$ and

$$(x_3, y_3) = \left((3x_1^2 + a)^2(2y_1)^{-2} - x_1 - x_2, y_1 + (3x_1^2 + a)(2y_1)^{-1}(x_3 - x_1)\right)$$

if $(x_1, y_1) = (x_2, y_2)$, $y_1 \neq 0$.

Then $E(R)$ with the above definitions is an Abelian group.
EXERCISE 28.21. Check the last statement. (N.B. Checking associativity is a
very laborious exercise.)

EXERCISE 28.22. Consider the group \( E(\mathbb{F}_{13}) \) defined by the equation \( y^2 = x^3 + 8 \). Show that \((1, 3), (2, 4) \in E(\mathbb{F}_{13})\) and compute \((1, 3) \ast (2, 4)\) and \(2(2, 4)\) (where the latter is of course \((2, 4) \ast (2, 4)\)).

Affine elliptic curves are special examples of cubics:

DEFINITION 28.23. A cubic is a subset \( X = X(R) \subset R \times R \) of the form
\[
X(R) = \{(x, y) \in R \times R; ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\}
\]
where \((a, b, c, ..., j) \in R \times ... \times R\), \((a, b, c, d) \neq (0, ..., 0)\).

As usual we refer to the tuple \((a, b, c, ..., j)\) as the equation of a cubic (or, by
abuse, simply a cubic).

EXERCISE 28.24. (Three cubics theorem) Prove that if two cubics meet in
exactly 9 points and if a third cubic passes through 8 of the 9 points then the
third cubic must pass through the 9th point. Hint: First show that if \( r \leq 8 \) and
\( r \) points are given then the set of cubics passing through them is strictly larger
than the set of cubics passing through \( r - 1 \) of the \( r \) points. (To show this show
first that no 4 of the 9 points are on a line. Then in order to find, for instance,
a cubic passing through \( P_1, ..., P_7 \) but not through \( P_8 \) one considers the cubics
\( C_i = Q_{1234i} + L_{jk}, \{i, j, k\} = \{5, 6, 7\}, \) where \( Q_{1234i} \) is the unique quadric passing
through \( P_1, P_2, P_3, P_4, P_i \) and \( L_{jk} \) is the unique line through \( P_j \) and \( P_k \). Assume
\( C_5, C_6, C_7 \) all pass through \( P_8 \) and derive a contradiction as follows. Note that \( P_8 \)
cannot lie on 2 of the 3 lines \( L_{jk} \) because this would force us to have 4 collinear
points. So we may assume \( P_8 \) does not lie on either of the lines \( L_{57}, L_{67} \). Hence
\( P_8 \) lies on both \( Q_{12345} \) and \( Q_{12346} \). So these quadrics have 5 points in common.
Form here one immediately gets a contradiction) Once this is proved let \( P_1, ..., P_9 \)
be the points of intersection of the cubics with equations \( F \) and \( G \). We know that
the space of cubics passing through \( P_1, ..., P_9 \) has dimension 2 and contains \( F \) and
\( G \). So any cubic in this space is a linear combination of \( F \) and \( G \), hence will pass
through the \( P_9 \).

EXERCISE 28.25. (Pascal’s Theorem) Let \( P_1, P_2, P_3, Q_1, Q_2, Q_3 \) be points on a
conic \( C \). Let \( A_1 \) be the intersection of \( P_2Q_3 \) with \( P_3Q_2 \) and define \( A_2, A_3 \) similarly.
(Assume the lines in question are not parallel.) Then prove that \( A_1, A_2, A_3 \) are
collinear. Hint: The cubics
\[
Q_1P_2 \cup Q_2P_3 \cup Q_3P_1 \quad \text{and} \quad P_1Q_2 \cup P_2Q_3 \cup P_3Q_1
\]
pass through all of the following 9 points:
\[
P_1, P_2, P_3, Q_1, Q_2, Q_3, A_1, A_2, A_3
\]
on the other hand the cubic \( C \cup A_2A_3 \) passes through all these points except
possibly \( A_1 \). Then by the Three cubics theorem \( C \cup A_2A_3 \) passes through \( A_1 \).
Hence \( A_2A_3 \) passes through \( A_1 \).


Remark 28.27. An extended version of the Three cubics theorem implies the
associativity of the chord-tangent operation on a cubic. (The extended version, to
be explained below follows from the usual version by passing through the “projective
The rough idea is as follows. Let $E$ be the elliptic curve and $Q, P, R$ points on it. Let

\[ PQ \cup E = \{P, Q, U\} \]
\[ \infty U \cup E = \{\infty, U, V\} \]
\[ VR \cup E = \{V, R, W\} \]
\[ PR \cap E = \{P, R, X\} \]
\[ \infty X \cap E = \{\infty, X, Y\}. \]

Here $\infty A$ is the vertical passing through a point $A$. Note that

\[ Q \star P = V, \quad V \star R = W', \quad P \star R = Y. \]

We want to show that

\[ (Q \star P) \star R = Q \star (P \star R) \]

This is equivalent to

\[ V \star R = Q \star Y \]

i.e. that

\[ W' = Q \star Y \]

i.e. that $Q, Y, W$ are collinear. Now the two cubics

\[ E \quad \text{and} \quad PQ \cup WR \cup YX \]

both pass through the 9 points

\[ P, Q, R, U, V, W, X, Y, \infty \]

On the other hand the cubic

\[ \Gamma = UV \cup PR \cup QY \]

passes through all 9 points except $W$. By the Three cubics theorem (applied to points which may be $\infty$) we get that $\Gamma$ passes through $W$ hence $QY$ passes through $W$. The above argument only applies to chords and not to tangents. When dealing with tangents one needs to repeat the argument and look at multiplicities. So making the argument rigorous becomes technical.
Analysis

Analysis is the study of “passing to the limit”. The key words are sequences, convergence, limits, and later differential and integral calculus. We survey here some of the most basic structures of analysis. For any \(a \in \mathbb{R}\) we let \(|a|\) be \(a\) or \(-a\) according as \(a \geq 0\) or \(a \leq 0\) respectively.

**Definition 29.1.** A sequence in \(\mathbb{R}\) is a map \(F : \mathbb{N} \to \mathbb{R}\); if \(F(n) = a_n\) we say \(a_1, a_2, \ldots\) is the sequence. Or \((a_n)\) is the sequence. We let \(F(\mathbb{N})\) be denoted by \(\{a_n; n \geq 1\}\); this is a subset of \(\mathbb{R}\).

**Definition 29.2.** A subsequence of a sequence \(F : \mathbb{N} \to \mathbb{R}\) is a sequence of the form \(F \circ G\) where \(G : \mathbb{N} \to \mathbb{N}\) is an increasing map. If \(a_1, a_2, a_3, \ldots\) is \(F\) then \(F \circ G\) is \(a_{k_1}, a_{k_2}, a_{k_3}, \ldots\) (or \((a_{k_n})\)) where \(G(n) = k_n\).

**Definition 29.3.** A sequence \((a_n)\) is convergent to \(a_0 \in \mathbb{R}\) if for any real number \(\epsilon > 0\) there exists an integer \(N\) such that for all \(n \geq N\) we have \(|a_n - a_0| < \epsilon\). We write \(a_n \to a_0\) and we say \(a_0\) is the limit of \((a_n)\).

**Definition 29.4.** A sequence is called convergent if there exists \(a \in \mathbb{R}\) such that the sequence converges to \(a\).

**Exercise 29.5.** Prove that \(a_n = \frac{1}{n}\) converges to 0.

**Exercise 29.6.** Prove that \(a_n = n\) is not convergent.

**Exercise 29.7.** Prove that \(a_n = (-1)^n\) is not convergent.

**Definition 29.8.** A sequence \((a_n)\) is convergent to \(a_0 \in \mathbb{R}\) if for any real number \(\epsilon > 0\) there exists an integer \(N\) such that for all \(n \geq N\) we have \(|a_n - a_0| < \epsilon\).

**Definition 29.9.** A sequence \(F\) is bounded if the set \(F(\mathbb{N}) \subset \mathbb{R}\) is bounded.

**Definition 29.10.** A sequence \((a_n)\) is Cauchy if for any real \(\epsilon > 0\) there exists an integer \(N\) such that for all integers \(m, n \geq N\) we have \(|a_n - a_m| < \epsilon\).

**Exercise 29.11.** Prove that any convergent sequence is Cauchy. Hint: easy.

**Exercise 29.12.** Prove the following statements in the prescribed order:
1) Any Cauchy sequence is bounded.
2) Any bounded sequence contains a sequence which is either increasing or decreasing.
3) Any bounded sequence which is either increasing or decreasing is convergent.
4) Any Cauchy sequence which contains a convergent subsequence is itself convergent.
5) Any Cauchy sequence is convergent.

Hints: For 1 let \(\epsilon = 1\), let \(N\) correspond to this \(\epsilon\) and get that \(|a_n - a_N| < 1\) for all \(n \geq N\); conclude from here. For 2 consider the sets \(A_n = \{a_m; m \geq n\}\). If at
least one of these sets has no maximal element we get an increasing subsequence by Proposition 22.3. If each $A_n$ has a maximal element $b_n$ then $b_n = a_{k_n}$ for some $k_n$ and the subsequence $a_{k_n}$ is decreasing. For 3 we view each $a_n \in \mathbb{R}$ as a Dedekind cut i.e. as a subset $a_n \subseteq \mathbb{Q}$; the limit will be either the union of the sets $a_n$ or the intersection. Statement 4 is easy. Statement 5 follows by combining the previous statements.

**Exercise 29.13.** Prove that any subset in $\mathbb{R}$ which is bounded from below has an infimum; and any subset in $\mathbb{R}$ which is bounded from above has a supremum.

**Definition 29.14.** A function $F : \mathbb{R} \to \mathbb{R}$ is continuous at a point $a_0 \in \mathbb{R}$ if for any sequence $(a_n)$ converging to $a_0$ we have that the sequence $(F(a_n))$ converges to $F(a_0)$.

**Exercise 29.15.** Prove that a map $F : \mathbb{R} \to \mathbb{R}$ is continuous (for the Euclidean topology on both the source and the target) if and only if it is continuous at any point of $\mathbb{R}$.

**Definition 29.16.** Let $(a_n)$ be a sequence and $s_n = \sum_{k=1}^{n} a_n$. If $(s_n)$ is convergent we say $\sum_{k=1}^{\infty} a_n$ is convergent and we also denote by $\sum_{k=1}^{\infty} a_n$ the limit.

**Exercise 29.17.** Prove that

1) $\sum_{n=1}^{\infty} \frac{1}{n}$ is not convergent.

2) $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is convergent.

**Exercise 29.18.** Let $S \subseteq \{0,1\}^\mathbb{N}$ be the set of all sequences $(a_n)$ such that there exist $N$ with $a_n = 1$ for all $n \geq N$. Prove that the map

$\{0,1\}^\mathbb{N} \setminus S \rightarrow \mathbb{R}, \quad (a_n) \mapsto \sum_{n=1}^{\infty} \frac{a_n}{2^n}$

is (well defined and) an injective. Conclude that $\mathbb{R}$ is not countable.

Real analysis (analysis of sequences, continuity, and other concepts of calculus like differentiation and integration of functions on $\mathbb{R}$) can be extended to complex analysis. A more surprising path is towards $p$-adic analysis (which is crucial to number theory). Recall the ring of $p$-adic numbers $\mathbb{Z}_p$ whose elements are denoted by $[a_n]$.

**Exercise 29.19.** Say that $p^e$ divides $\alpha = [a_n]$ if there exists $\beta = [b_n]$ such that $[a_n] = [p^e b_n]$; write $p^n|\alpha$.

**Definition 29.20.** For any $0 \neq \alpha = [a_n] \in \mathbb{Z}_p$ let $v = v(\alpha)$ be the unique integer such that $p^v a_n$ for $n \leq v$ and $p^{v+1} \not| a_{v+1}$. Then define the norm of $\alpha$ by the formula $|\alpha| = p^{-v(\alpha)}$. We also set $|0| = 0$.

**Exercise 29.21.** Prove that if $\alpha = [a_n]$ and $\beta = [b_n]$ then

$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$.

**Definition 29.22.** Consider a sequence $[a_{n1}], [a_{n2}], [a_{n3}], ...$ of elements in $\mathbb{Z}_p$ which for simplicity we denote by $\alpha_1, \alpha_2, \alpha_3, ...$

1) $\alpha_1, \alpha_2, \alpha_3, ...$ is called a Cauchy sequence if is called Cauchy if for any real (or, equivalently, rational) $\epsilon > 0$ there exists an integer $N$ such that for all $m, m' \geq N$ we have $|\alpha_m - \alpha_{m'}| \leq \epsilon$. 

2) We say that \( \alpha_1, \alpha_2, \alpha_3, \ldots \) converges to some \( \alpha_0 \in \mathbb{Z}_p \) if for any real (or, equivalently, rational) \( \epsilon > 0 \) there exists an integer \( N \) such that for all \( m \geq N \) we have \( |\alpha_m - \alpha_0| \leq \epsilon \). We say \( \alpha_0 \) is the limit of \( (\alpha_n) \) and we write \( \alpha_n \to \alpha_0 \).

**Exercise 29.23.** Prove that a sequence in \( \mathbb{Z}_p \) is convergent if and only if it is Cauchy.

The following is in deep contrast with the case of \( \mathbb{R} \):

**Exercise 29.24.** Prove that if \( (\alpha_n) \) is a sequence in \( \mathbb{Z}_p \) with \( \alpha_n \to 0 \) then the sequence

\[
s_n = \sum_{k=1}^{n} \alpha_k
\]

is convergent in \( \mathbb{Z}_p \); the limit of the latter is denoted by \( \sum_{n=1}^{\infty} \alpha_n \). In particular, for instance, \( \sum_{n=1}^{\infty} p^{n-1} \) is convergent. Prove that \( \sum_{n=1}^{\infty} p^{n-1} \) is the inverse of \( 1 - p \) in \( \mathbb{Z}_p \).

**Exercise 29.25.** Prove that if \( \alpha \in \mathbb{Z}_p \) has \( |\alpha| = 1 \) then \( \alpha \) is invertible in \( \mathbb{Z}_p \). Hint: Use the fact that if \( p \) does not divide an integer \( a \in \mathbb{Z} \) then there exist integers \( m, n \in \mathbb{Z} \) such that \( ma + np = 1 \); then use the previous exercise.
CHAPTER 30

Metamodels

In this chapter we briefly discuss the problem of translating various theories into set theory. One can give the following metadefinition which is not standard but expresses a standard idea about the interaction between mathematics and various fields of knowledge (including mathematics itself):

METADefinition 30.1. Let $T$ be a theory in a language $L$ with specific axioms $A, B, \ldots$. Assume in addition that one may be given a “domain” formula $D(x)$ in $L_{set}$ with one free variable $x$. (We allow that $D$ be not present.) By a mathematical model with domain $D$ (or simply a metamodel) for $T$ we mean data $\tilde{L}, \tilde{T}, \tilde{\varphi}$ consisting of

i) a language $\tilde{L}$ obtained from the language of set theory $L_{set}$ by adding various constants and predicates plus definitions for each of the predicates;

ii) a $D$-translation $\tilde{\varphi}$ of $L$ into the language $\tilde{L}$ and

iii) a theory $\tilde{T}$ in $\tilde{L}$ such that:

1) $\tilde{T}$ contains $T_{set}$;

2) $\tilde{T}$ contains the translations $\tilde{A}, \tilde{B}, \ldots$ of the specific axioms $A, B, \ldots$;

3) $\tilde{T}$ contains $D(t)$ for all terms $t$ in $L$ without free variables.

Remark 30.2. It is easy to check that the $D$-translations of all background axioms of $T$ are contained in $\tilde{T}$; therefore the $D$-translation of any theorem in $T$ will be a theorem in $\tilde{T}$.

Remak 30.3. If $D$ in the above mdefinition is not present then $D$-translations are simply translations, condition 3) can be dropped, etc.

Remark 30.4. The concept of metamodel introduced above is completely different from (but also an inspiration for) the concept of model to be introduced in the chapter on models. Metamodels consist of texts; models in the chapter on models are sets.

Example 30.5. We illustrate metamodels by considering the “toy” theory $T$ of gravitation in Example 12.19. This example we will not involve any “domain formula $D$”. Let $L$ be the language in Example 12.19; recall the it contains constants $S, E, M, R, 1, \pi, g$ relational predicates $p, c, n, \circlearrowleft, f$, functional symbols $d, a, T, \vdots, \times$. We need to first specify a language $\tilde{L}$. We let $\tilde{L}$ be the language obtained from $L_{set}$ by adding symbols $\tilde{S}, \ldots, \tilde{T}$ (all the symbols above with a tilde on top) The translation of $L$ into $\tilde{L}$ is then just “putting $\tilde{\varphi}$ on top of the symbols”. We let $\mathcal{F}$ be a fixed subset of the set of infinitely differentiable maps $\mathbb{R} \rightarrow \mathbb{R}^3$ in the sense of analysis; see a textbook in analysis. Then we consider definitions such as:

1) $\tilde{\pi} = 314 : 100, \tilde{g} = 981, \ldots$

2) $\forall x(\tilde{n}(x) \leftrightarrow ((x \in \mathbb{R})) \land (x > 0))$
3) $\forall x \forall y (\tilde{f}(x, y) \leftrightarrow ((x \in \mathcal{F}) \land (y \in \mathbb{R})))$

4) $\circ$ expresses movement in a circle (ized mathematically, i.e. there exists a center and a radius such that...).

5) $\tilde{a}(x)$ is the “absolute value of the second derivative of the map $x$” (in the sense of analysis; later one may want to drop the “absolute value”), etc.

Finally $\tilde{T}$ is the theory with specific axioms those of $T_{set}$ to which one adds the translations in $\tilde{L}$ of the axioms in $T$ in Example 12.19. The above yields a metamodel of $T$.

**Exercise 30.6.** Attempt to make the above more explicit and to complete the definitions above. Analyze what becomes of the theorems in Example 12.19 when translated in $\tilde{T}$. There will be inconsistencies related to the fact that the Earth is sometimes viewed as fixed (when the Moon and the cannon balls are looked at), sometimes viewed as moving (when viewed as a planet). Try to fix these inconsistencies, for instance by considering two different translations. There is a way out of these problems by replacing the purely kinematic theory $T$ with a dynamical theory. (Kinematic means geometric i.e. not invoking forces whereas dynamical means involving forces.)

**Remark 30.7.** Other physical theories can be given metamodels in a similar way. The logical content of this operation is never made explicit because it is too laborious, and often leads to contradictions if not done in minute detail. But it is important to understand how things work at least in principle. Problems such as these are not uncommon: set theory acts sometimes like a “straight jacket” for physical theories.

**Exercise 30.8.** (For those who took courses in physics)

1) Give a metamodel for Newton’s dynamical theory of gravitation (based on forces).
2) Give a metamodel for classical mechanics of particles traveling in a field.
3) Give a metamodel for relativistic mechanics of particles moving freely.
4) Give a metamodel for a simple situation in quantum theory.

Next we consider the example of Peano arithmetic. The Peano axiom is the sentence in $L_{set}$ that there exists a Peano triple. But if one tries to write this axiom in a language that only contains, say, a constant 0, binary functional symbols $+, \times$, and unary functional symbol $s$, together with equality $=$ then one is bound to fail because there is no way to say, in this language, that “for any subset something happens”. Nevertheless there is a Peano system of axioms in such a language which we are going to consider below, together with a metamodel of the associated theory.

**Example 30.9.** Consider the language $L_{ar}$ with constant 0, binary functional symbols $+, \times$, and unary functional symbol $s$, together with equality $=$ and the
standard connectives and separators. This is called the language of Peano arithmetic. We consider the following specific axioms:

\[ A_1 \] \( \forall x (s(x) \neq 0) \)

\[ A_2 \] \( \forall x ((x \neq 0) \rightarrow \exists y (s(y) = x)) \)

\[ A_3 \] \( \forall x (x + 0 = x) \)

\[ A_4 \] \( \forall x \forall y (x + (s(y)) = s(x + y)) \)

\[ A_5 \] \( \forall x (x \times 0 = 0) \)

\[ A_6 \] \( \forall x \forall y (x \times (s(y)) = (x \times y) + x) \)

\[ A_P \] \( \forall w ((P(0, w) \land \forall v (P(v, w)) \rightarrow P(s(v), w))) \rightarrow \forall x (P(x, w)) \)

where \( P \) runs through all formulas in \( L_{ar}^f \) with the appropriate number of free variables. So this is a metacountable set of axioms; the latter series of axioms stands for a weak form of induction.

Exercise 30.10. Let \( D(x) \) be the formula “\( x \in \mathbb{N} \cup \{0\} \)” in \( L_{set}^f \). Let \( T_{ar} \) be the theory in \( L_{ar} \) with specific axioms \( A_1, ..., A_6, A_P, ... \); we call this theory the Peano arithmetic theory. Show that the theory \( T_{ar} \) has a metamodel with domain \( D \) in which \( \tilde{L}, \tilde{T} \) coincide with \( L_{set}, T_{set} \).

Here is another example which is a variant of Grothendieck’s universes; this is one of the way out of the logical difficulties of category theory, to be discussed later.

Example 30.11. Fix a set \( \mathcal{U} \) (i.e. a constant in \( T_{set} \)) referred to in what follows as a universe and introduce a predicate still denoted by \( \mathcal{U} \) equipped with the definition

\[ \forall x (\mathcal{U}(x) \leftrightarrow (x \in \mathcal{U})) \]

Let \( \tilde{L} \) be obtained from \( L_{set} \) by adding the above predicate. Also let \( \tilde{\cdot} \) be the natural \( \mathcal{U} \)-translation of formulas from \( L_{set} \) into \( \tilde{L} \). Finally let \( \tilde{T} \) be the theory in the language \( \tilde{L} \) generated by the axioms in \( ZFC \), the collection \( ZFC^\mathcal{U} \) of their \( \mathcal{U} \)-translations, and all sentences of the form \( \mathcal{U}(c) \) where \( c \) is a constant in \( L_{set} \). The above define a metamodel for \( T_{set} \) with domain \( \mathcal{U} \). (So we are dealing here with a \( \mathcal{U} \)-translation of the language of set theory essentially into itself which is not the “identity”! See the exercise below. We will see a similar, but also very different, procedure when we discuss models of set theory in the chapter on models.) Intuitively \( \tilde{T} \) is obtained from the set theory \( T_{set} \) by adding axioms saying that “all operations with sets that belong to \( \mathcal{U} \) lead to sets that belong to \( \mathcal{U} \)” and axioms saying that “all named sets in set theory are in \( \mathcal{U} \).” Of course the consistency of \( \tilde{T} \) is even more problematic than the consistency of set theory \( T_{set} \).

Exercise 30.12. Write down the axioms in \( ZFC^\mathcal{U} \). Hint: if \( S \) is the singleton axiom

\[ \forall x \exists y ((x \in y) \land (\forall z ((z \in y) \rightarrow (z = x))) \]

then its \( \mathcal{U} \)-translation \( \tilde{S} \) is:

\[ \forall x ((x \in \mathcal{U}) \rightarrow (\exists y ((y \in \mathcal{U}) \land (x \in y) \land (\forall z ((z \in \mathcal{U}) \land (z \in y) \rightarrow (z = x))))) \]
CHAPTER 31

Categories

Categories are one of the most important unifying concepts of mathematics. In particular they allow to create bridges between various parts of mathematics. Here we will only explore their definition and we give some examples. We begin with the simpler concept of correspondence.

**Definition 31.1.** A correspondence on a set $X^{(0)}$ is a triple $(X^{(1)}, \sigma, \tau)$ where $\sigma, \tau : X^{(1)} \to X^{(0)}$ are maps called source and target.

**Example 31.2.** If $R \subseteq A \times A$ is a relation and $\sigma : R \to A$ and $\tau : R \to A$ are defined by $\sigma(a, b) = a$, $\tau(a, b) = b$ then $(R, \sigma, \tau)$ is a correspondence.

**Example 31.3.** Let $X^{(0)}$ the set of all sets (belonging to a given set $u$, referred to as the universe) and let $X^{(1)}$ be the set of all triples $(A, B, F)$ with $A, B \in X^{(0)}$ and $F : A \to B$ a map (where we assume that all maps from $A$ to $B$ belong to $u$). Let $\sigma(A, B, F) = A$ and $\tau(A, B, F) = B$. This data define a correspondence.

**Example 31.4.** If in the above example we insist that all $F$s are bijective, say, then we get another example of a correspondence.

**Definition 31.5.** Assume $(X^{(1)}, \sigma, \tau)$ is a correspondence on $X^{(0)}$. Then one can define sets

$$X^{(2)} = \{(a, b) \in X^2; \tau(b) = \sigma(a)\}$$

$$X^{(3)} = \{(a, b, c) \in X^3; \tau(c) = \sigma(b), \tau(b) = \sigma(a)\}$$

etc.

We have natural maps $p_1, p_2 : X^{(1)} \to X^{(0)}$, $p_1(a, b) = a$, $p_2(a, b) = b$.

**Definition 31.6.** A small category is a tuple $(X^{(0)}, X^{(1)}, \sigma, \tau, \mu, \epsilon)$ where $X^{(0)}$ is a set, $(X^{(1)}, \sigma, \tau)$ is a correspondence on $X^{(0)}$, and $\mu : X^{(2)} \to X^{(1)}$, $\epsilon : X^{(0)} \to X^{(1)}$ are maps. We postulate that $\sigma \circ \epsilon = \tau \circ \epsilon = I$, the identity of $X^{(0)}$. Also we postulate that the following diagrams are commutative:

$$
\begin{array}{ccc}
X^{(2)} & \xrightarrow{\mu} & X^{(1)} \\
p_1 \downarrow & & \downarrow \tau \\
X^{(1)} & \xrightarrow{\tau} & X^{(0)}
\end{array}
$$

$$
\begin{array}{ccc}
X^{(2)} & \xrightarrow{\mu} & X^{(1)} \\
p_2 \downarrow & & \downarrow \sigma \\
X^{(1)} & \xrightarrow{\sigma} & X^{(0)}
\end{array}
$$
31. CATEGORIES

\[ X^{(3)} \xrightarrow{\mu \times 1} X^{(2)} \]
\[ 1 \times \mu \downarrow \quad \downarrow \mu \]
\[ X^{(2)} \xrightarrow{\mu} X^{(0)} \]

Finally we postulate that the compositions

\[ X^{(1)} \xrightarrow{1 \times (\epsilon \circ \sigma)} X^{(2)} \xrightarrow{\mu} X^{(1)} \]

and

\[ X^{(1)} \xrightarrow{(\epsilon \circ \tau) \times 1} X^{(2)} \xrightarrow{\mu} X^{(1)} \]

are the identity of \( X^{(1)} \), where \((1 \times (\epsilon \circ \sigma))(a) = (a, \epsilon(\sigma(a)))\) and \(((\epsilon \circ \tau) \times 1)(a) = (\epsilon(\tau(a)), a)\).

The set \( X^{(0)} \) is called the set of objects of the category. The set \( X^{(1)} \) is called the set of arrows or morphisms. The map \( \mu \) is called composition and we write \( \mu(a, b) = a \ast b \). The maps \( \sigma \) and \( \tau \) are called the source and the target map respectively. The map \( \epsilon \) is called the identity. We set \( \epsilon(x) = 1_x \) for all \( x \). The first commutative diagram says that the target of \( a \ast b \) is the target of \( a \). The second diagram says that the source of \( a \ast b \) is the source of \( b \). In the third diagram (called associativity diagram) the map \( \mu \times 1 \) is defined as \((a, b, c) \mapsto (a \ast b, c)\) while the map \( 1 \times \mu \) is defined by \((a, b, c) \mapsto (a, b \ast c)\); the diagram then says that \((a \ast b) \ast c = a \ast (b \ast c)\).

For \( x, y \in X^{(0)} \) one denotes by \( \text{Hom}(x, y) \) the set of all morphisms \( a \in X^{(1)} \) with \( \sigma(a) = x \) and \( \tau(a) = y \). We say \( a \in \text{Hom}(x, y) \) is an isomorphism if there exists \( a' \in \text{Hom}(y, x) \) such that \( a \ast a' = 1_y \) and \( a' \ast a = 1_x \). (Then \( a' \) is unique.) A category is called a groupoid if all morphisms are isomorphisms.

In what follows we give some basic examples of categories. Some of the examples involve universes. For those examples we let \( \mathcal{U} \) be a fixed universe and fix the metamodel \( \tilde{L}, \tilde{T}, \tilde{\ast} \) of set theory \( T_{set} \) attached to \( \mathcal{U} \); cf. Example 30.11. (So \( \tilde{T} \) is obtained from \( T_{set} \) by adding the corresponding axioms related to the universe.) For the various examples below that involve universes the correctness of the definitions depend on certain claims (typically that certain sets are maps, etc.) Those claims cannot be proved a priori in set theory \( T_{set} \) but they are trivially proved in \( \tilde{T} \); this shows that the correctness of the definition of some of the categories below requires the axioms of \( \tilde{T} \) hence more axioms than ZFC! The question of consistency of \( \tilde{T} \) becomes then acute: one has to believe that \( \tilde{T} \) is consistent in order to believe that the categories below are all well defined.

**Example 31.7.** Define the category of sets (in a given universe \( \mathcal{U} \)) denoted by \{sets\} as follows:

- \( X^{(0)} = \mathcal{U} \),
- \( X^{(1)} = \{(A, B, F) \in \mathcal{U}^3; F \in B^A\} \)
- \( \sigma(A, B, F) = A, \quad \tau(A, B, F) = B. \)

The following is a (trivially proved) theorem in \( \tilde{T} \):

\((*)\) The set

\[ \mu = \{(B, C, F), (A, B, G), (A, C, H) \in X^{(2)} \times X^{(1)}; H = F \circ G\} \]

is a map \( X^{(2)} \to X^{(1)} \).
(see the Exercise below). Similarly we may define the map \( \epsilon : X^{(0)} \to X^{(1)} \), \( \epsilon(A) = I_A \) (identity of \( A \)). With above definitions we get a category. In the examples below we will encounter from time to time the same kind of phenomenon (where the correctness of definitions depends on theorems in \( \tilde{T} \)); we will not repeat the corresponding discussion but we will simply add everywhere the words “in a given universe”.

**Exercise 31.8.** Prove that the above sentence (*) is a theorem in \( \tilde{T} \). Hint: use the fact that the axioms in \( \tilde{T} \) imply that if \( F,G \in \mathcal{U} \) then \( F \circ G \in \mathcal{U} \).

**Example 31.9.** If in the example above we insist that all \( F \)s are bijections we get a category called \( \{ \text{sets + bijections} \} \). This category is a groupoid.

**Example 31.10.** Let \( A \) be a set and consider the category denoted by \( \{ \text{bijections of } A \} \) defined as follows. We let \( X^{(0)} = \{ x \} \) be a set with one point, we let \( X^{(1)} \) be the set of all bijections \( F : A \to A \), we let \( \sigma \) and \( \tau \) be the constant map \( F \mapsto x \), we let \( \mu \) be defined again by \( \mu(F,G) = F \circ G \) (compositions of functions), and we let \( \epsilon(F) = I_A \). This category is a groupoid.

**Example 31.11.** Define the category \( \{ \text{ordered sets} \} \) as follows. We take \( X^{(0)} \) the set of all ordered sets \((A, \leq)\) with \( A \) in a given universe, we take \( X^{(1)} \) to be the set of all triples \((((A, \leq), (A', \leq'), F) \) with \(( (A, \leq), (A', \leq') \in X^{(0)} \) and \( F : A \to A' \) increasing, we take \( \mu \) to be again, composition, and we take \( \epsilon(A, \leq) = I_A \).

**Example 31.12.** Let \( (A, \leq) \) be an ordered set. Define the category \( \{(A, \leq)\} \) as follows. We let \( X^{(0)} = A \), we let \( X^{(1)} \) be the set \( \leq \) viewed as a subset of \( A \times A \), we let \( \sigma(a,b) = a \), \( \tau(a,b) = b \), we let \( \mu((a,b),(b,c)) = (a,c) \), and we let \( \epsilon(a) = (a,a) \).

**Example 31.13.** Equivalence relations give rise to groupoids. Indeed let \( A \) be a set with an equivalence relation \( R \subset A \times A \) on it which we refer to as \( \sim \). Define the category \( \{(A, \sim)\} \) as follows. We let \( X^{(0)} = A \), we let \( X^{(1)} = R \), we let \( \sigma(a,b) = a \), \( \tau(a,b) = b \), we let \( \mu((a,b),(b,c)) = (a,c) \), and we let \( \epsilon(a) = (a,a) \). This category is a groupoid.

**Example 31.14.** We fix the type of algebraic structures below. (E.g. two binary operations, one unary operation, two given elements.) Define the category \( \{ \text{algebraic structures} \} \) as follows. \( X^{(0)} \) is the set of all algebraic structures \((A, \star, ..., \neg, ..., 1, ...)\) of the given type with \( A \) in a given universe, \( X^{(1)} \) is the set of all triples \(((A, \star, ..., \neg, ..., 1, ...), (A', \star', ..., \neg', ..., 1', ...), F)\) with \( F \) a homomorphism, \( \sigma \) and \( \tau \) are the usual source and target, and \( \epsilon \) is the usual identity.
Example 31.15. Here is a variation on the above example. Consider the category of rings:

\[ \{ \text{commutative unital rings} \} \]
as follows. The set of objects \( X^{(0)} \) is the set of all commutative unital rings \((A, +, \times, 0, 1)\) (usually referred to as \( A \)) in a given universe and the set of arrows \( X^{(1)} \) is the set of all triples \((A, B, F)\) where \( A, B \) are rings and \( F : A \to B \) is a ring homomorphism. Also the target, source and identity are the obvious ones; the composition map is the usual composition.

Example 31.16. Define the category

\[ \{ \text{topological spaces} \} \]
as follows. We let \( X^{(0)} \) be the set of all topological spaces \((X, T)\) where \( X \) is a set in a given universe; we take \( X^{(1)} \) to be the set of all triples \(((X, T), (X', T'), F)\) with \( F : X \to X' \) continuous, we let \( \mu \) be given by usual composition of maps, \( \sigma \) and \( \tau \) the usual source and target maps, and \( \epsilon \) the usual identity.

Example 31.17. Define the category of groups:

\[ \{ \text{groups} \} \]
defined as follows. The set \( X^{(0)} \) of objects is the set of all groups whose set is in a given universe, and the set \( X^{(1)} \) is the set of all the triples consisting of two groups \( G, H \) and a homomorphism between them. The source, target, and identity are the obvious ones.

Example 31.18. If in the above example we restrict ourselves to groups which are Abelian we get the category of Abelian groups

\[ \{ \text{Abelian groups} \} \].

Example 31.19. A fixed group can be viewed as a category as follows. Fix a group \((G, \ast', e)\). Then one can consider the small category

\[ \{ G \} \]
where \( X^{(0)} = \{ x \} \) is a set consisting of one element, \( X^{(1)} = G, \mu(a, b) = a \ast b \), the source and the target are the constant maps, and \( \epsilon(x) = e \).

Example 31.20. Define the category

\[ \{ \text{vector spaces} \} \]
as follows. The set of objects \( X^{(0)} \) is the set of all vector spaces in a given universe; the set \( X^{(1)} \) of morphisms consists of all triples \((V, W, F)\) with \( F : V \to W \) a linear map; source, target, and identity are defined in the obvious way.

Exercise 31.21. Check that, in all examples above, the axioms in the definition of a category are satisfied. (This is long and tedious but straightforward.)
Part 3

Mathematical logic
CHAPTER 32

Models

We briefly indicate here how one can create a “mirror” of logic within mathematics (indeed largely within algebra). What results is a subject called mathematical logic (also referred to as formal logic); cf. the Introduction to this course. A special place in mathematical logic is played by models/model theory which we shall explain below in some detail. In particular we will discuss models of ZFC itself (and hence of mathematics itself); this concept of model is entirely different from that of metamodels in the chapter on metamodels. In the discussion of models of ZFC we will introduce what one can call formalized set theory. We will discuss models of other (simpler) theories as well such that the theory of Peano arithmetic.

The mirror of logic in mathematics that we are considering here is not entirely accurate: there is no one to one correspondence between “metamathematical” logic and mathematical logic. But as a general principle if a concept (say crocodile) is present in logic its mirror in mathematical logic will acquire the adjective formal in front (e.g. will be called a formal crocodile). The dichotomy non-formal/formal indicates the difference between set theory and what we shall call formalized set theory. Within each levels one has the syntactic/semantic dichotomy; semantic means of course coming from translation whereas syntactic means independent of translation.

Let $T$ be a set. By a $T$-partitioned set we mean in what follows a set $S$ together with a map $S \to T$. We let $S_t$ the preimage of $t$ in $S$. In the definition below we take

$$T = \{c, f_1, f_2, f_3, ..., r_1, r_2, r_3, ...\}.$$

Also we consider a set

$$V = \{x_1, x_2, x_3, ...\}$$

called the set of variables, and a set

$$W = \{\lor, \land, \neg, \forall, \exists, =, (, )\}$$

called the set of logic symbols. We sometimes write $x, y, z, ...$ instead of $x_1, x_2, x_3, ...$. Needless to say in the above $c, f_i, r_i, x_i, \land, ...$ are sets; if one wants to be precise one can take $c = 0, f_i = (1, i), r_i = (2, i), x_i = (3, i), \land = 1, \lor = 2, ...$

All definitions below are definitions in set theory.

**Definition 32.1.** Let $S$ be a $T$-partitioned set; the elements of $S_c$ are called constant symbols; the elements of $S_{f_n}$ are called $n$-ary function symbols; the elements of $S_{r_n}$ are called $n$-ary relation symbols. For any such $S$ we consider the set

$$\Lambda_S = V \cup W \cup S.$$
(referred to as the formal language attached to \( S \)). Then one considers the set of words \( \Lambda_S \) with letters in \( \Lambda_S \). One defines (in an obvious way, imitating the metadefinitions in the chapters on “non-mathematical” logic) what it means for an element \( \varphi \in \Lambda_S^* \) to be an \( S \)-formula or an \( S \)-formula without free variables (the latter are referred to as sentences). One denotes by \( \Lambda_S^f \subset \Lambda_S^* \) the set of all \( S \)-formulas and by \( \Lambda_S^S \subset \Lambda_S^* \) the set of all \( S \)-sentences.

**Example 32.2.** Assume \( \rho \in S_{c^3} \), \( a \in S_c \), and \( x, z \in V \). Then

\[
\varphi = \forall x \exists z(\rho(x, z, a))
\]

is a formula. But \( \exists a \forall z(\rho(x, z, a)) \) is not a formula because constants cannot have quantifiers \( \forall, \exists \) in front of them. Also \( \forall x \exists z(\rho(x, a)) \) is not a formula because \( \rho \) is “supposed to have 3 arguments”. If \( \Box \in S_{f_3} \) and \( a, x, z \) are as above then

\[
\varphi = \forall x \exists z(\Box(z, a) = z)
\]

is a formula.

**Remark 32.3.** One can define binary operations \( \land^* \) and \( \lor^* \) on \( \Lambda_S^* \) and a unary operation \( \lnot^* \) on \( \Lambda_S^* \). E.g. \( \land^* : \Lambda_S^* \times \Lambda_S^* \to \Lambda_S^* \) is defined by \( \varphi \land^* \psi = (\varphi) \land (\psi) \). We have \( \varphi \land^* (\psi \land^* \eta) = (\varphi) \land ((\psi) \land (\eta)) \neq (\varphi \land^* \psi) \land^* \eta \). So \( \Lambda_S^* \) is not a Boolean algebra with respect to these operations. For simplicity we continue to write \( \land, \lor, \lnot \) in place of \( \land^*, \lor^*, \lnot^* \).

**Example 32.4.** Let \( M \) be a set. We let \( S_c(M) = M \). For \( n \in \mathbb{N} \) we set \( S_{r_n}(M) = \mathcal{P}(M^n) \), the set of \( n \)-ary relations on \( M \) and \( S_{f_n}(M) \subset \mathcal{P}(M^{n+1}) \) the set of maps \( M^n \to M \). We consider the \( T \)-partitioned set \( S(M) \), union of the above. Then we can consider the formal language \( \Lambda_{S(M)} \). An assignment in \( M \) is a map

\[
\mu : V = \{x_1, x_2, x_3, \ldots \} \to M
\]

For any assignment \( \mu \) there exists a unique map \( v_{M, \mu} : \Lambda_{S(M)}^f \to \{0, 1\} \) which is a homomorphism with respect to \( \lor, \land, \lnot \), is compatible (in an obvious sense) with \( \lor, \land \), satisfies obvious properties with respect to relational and functional symbols, and also with \( \mu \). If \( \varphi \) has no free variables we write \( v_M(\varphi) \) in place of \( v_{M, \mu}(\varphi) \).

**Definition 32.5.** Next one discusses semantics. By a translation of \( \Lambda_S \) into \( \Lambda_{S'} \) we understand a map

\[
\mathfrak{m} : S \to S'
\]

which is compatible with the partitions (in the sense that \( \mathfrak{m}(S_t) \subset S_t' \) for all \( t \in T \)). For any \( \varphi \in \Lambda_S^f \) one can form, in an obvious way, a formula \( \mathfrak{m}(\varphi) \in \Lambda_{S'}^f \) obtained from \( \varphi \) by replacing the constants and relational and functional symbols by their images under \( \mathfrak{m} \) respectively. So we get a map

\[
\mathfrak{m} : \Lambda_S^f \to \Lambda_{S'}^f
\]

which is a homomorphism with respect to \( \lor, \land, \lnot \), compatible with \( \forall, \exists \).

An \( S \)-structure (or simply a structure if \( S \) is understood) is a pair \( M = (M, \mathfrak{m}) \) where \( M \) is a set and \( \mathfrak{m} \) is a translation

\[
\mathfrak{m} : S \to S(M)
\]

So we get a map

\[
\mathfrak{m} : \Lambda_S^f \to \Lambda_{S(M)}^f
\]
which is a homomorphism with respect to $\lor, \land, \neg$, compatible with $\forall, \exists$. Fix an assignment $\mu$ and set $v_{M,\mu} = v_M$. We have a natural map 
\[ v_M : \Lambda^F_S(M) \to \{0, 1\} \]

which is again a homomorphism compatible with $\forall, \exists$. So we may consider the composition 
\[ v_M = v_M \circ m : \Lambda^F_S \to \{0, 1\}. \]

We say that a sentence $\varphi \in \Lambda^S_S$ is satisfied in the structure $M$ if $v_M(\varphi) = 1$. This concept is independent of $\mu$. This is essentially Tarski’s famous semantic definition of truth: one can define in set theory the predicate is true in $M$ by the definition:
\[ \forall x((x \text{ is true in } M) \iff ((x \in \Lambda^S_S) \land (v_M(x) = 1))) \]

(We will continue to NOT use the word true in what follows, though.) If $v_M(\varphi) = 1$ we also say that $M$ is a model of $\varphi$ and we write $M \models \varphi$. (So “is a model” and “$\models$” are predicates that are being added to $L_{set}$.) We say a set $\Phi \subset \Lambda^S_S$ of sentences is satisfied in a structure (write $M \models \Phi$) if all the formulas in $\Phi$ are satisfied in this structure. We say that a sentence $\varphi \in \Lambda^S_S$ is a semantic formal consequence of a set of sentences $\Phi \subset \Lambda^S_S$ (and we write $\Phi \models \varphi$) if $\varphi$ is satisfied in any structure in which $\Phi$ is satisfied. Here the word semantic is used because we are using translations; and the word formal is being used because we are in formal logic rather than in ordinary logic. A sentence $\varphi \in \Lambda^S_S$ is valid (or a formal tautology) if it is satisfied in any structure, i.e. if $\emptyset \models \varphi$. We say a sentence $\varphi$ is satisfiable if there is a structure in which it is satisfied. Two sentences $\varphi$ and $\psi$ are semantically formally equivalent if each of them is a semantic formal consequence of the other, i.e $\varphi \models \psi$ and $\psi \models \varphi$; write $\varphi \equiv \psi$. Note that the quotient $\Lambda^S_S/\equiv$ is a Boolean algebra in a natural way. Moreover each structure $M$ defines a homomorphism $v_M : \Lambda^S_S/\equiv \to \{0, 1\}$ of Boolean algebras.

**Example 32.6.** Algebraic structures can be viewed as models. Here is an example. Let 
\[ S = \{\star, \iota, e\} \]

with $e$ a constant symbol, $\star$ a binary function symbol, and $\iota$ a unary function symbol. Let $\Phi_{gr}$ be the set of $S$-formulas $\Phi_{gr} = \{\varphi_1, \varphi_2, \varphi_3\}$ where
\begin{align*}
\varphi_1 &= \forall x \forall y \forall z(x \star (y \star z) = (x \star y) \star z) \\
\varphi_2 &= \forall x(x \star e = e \star x = x) \\
\varphi_3 &= \forall x(x \star \iota(x) = \iota(x) \star x = x).
\end{align*}

Then a group is simply a model of $\Phi_{gr}$ above. We also say that $\Phi_{gr}$ is a set of axioms for the formalized theory of groups.

More generally

**Definition 32.7.** A formalized (or formal) system of axioms is a pair $(S, \Phi)$ where $S$ is a $T$-partitioned set and $\Phi$ is a subset of $\Lambda^S_S$; then define 
\[ \Theta = \Phi^F = \{ \varphi \in \Lambda^S_S; \Phi \models \varphi \}; \]

$\Theta$ is called the formal theory with (or generated by) the system $(S, \Phi)$. 
Remark 32.8. One thinks of $\Phi^=\vdash$ as semantically defined because its definition involves models and hence translations. One may define a “syntactic” version of this set namely the set
\[
\Phi^\vdash = \{ \varphi \in \Lambda^S; \Phi \vdash \varphi \};
\]
where $\vdash$ is the predicate added to $L_{set}$ meaning “$\varphi$ provable from $\Phi$” in an obvious sense that imitates the definition of proof in pre-mathematical logic. We will not make this precise here, neither will we use the following theorem of Gödel which is usually referred to as Gödel’s completeness theorem. This theorem intuitively says that syntactic and semantic provability coincide.

Theorem 32.9. $\Phi^\vdash = \Phi^\models$.

Exercise 32.10. Write down a set of symbols $S$ and a set of formulas $\Phi$ which is a set of axioms for the formalized theory of:
1) commutative unital rings;
2) fields;
3) ordered sets;
4) vector spaces over a given field;
5) Boolean algebras;
6) sets;
Can one find such a pair $S, \Phi$ in the following cases?
7) well ordered sets;
8) topological spaces;
9) the ring of integers.
Incompleteness

Our aim here is to state and explain Gödel’s “incompleteness theorems of set theory and arithmetic”.

**Definition 33.1.** Formalized (or formal) set theory is the formal theory $\Theta_{\text{set}}$ generated by $(S_{\text{set}}, \Phi_{\text{set}})$ where $S_{\text{set}} = \{\in\}$ and $\Phi_{\text{set}}$ consists of the ZFC axioms of set theory viewed as elements of $\Lambda_{\text{set}} = \Lambda_{\{\in\}}$.

**Remark 33.2.** Unlike the language $L_{\text{set}}$ of set theory, which has infinitely many constants (e.g. the witnesses), $\Lambda_{\text{set}}$ above has no constants! Also, of course, $L_{\text{set}}$ is a text (more precisely collection of symbols) whereas $\Lambda_{\text{set}}$ is a set. Similarly the theory $T_{\text{set}}$ is a text (more precisely a collection of strings of symbols) while the formal theory $\Theta_{\text{set}}$ is itself a set (hence one symbol). However any sentence $P$ in $L_{\text{set}}$ without constants gives rise in an obvious way to a sentence (which we still denote by $P$) in $\Lambda_{\text{set}}$ and vice versa. We will use this abuse of notation freely in what follows.

**Metadefinition 33.3.** We let $T'_{\text{set}}$ the theory generated by $T_{\text{set}}$ and all sentences in $L_{\text{set}}^*$ of the form

$$P \leftrightarrow (P \in \Theta_{\text{set}})$$

where $P$ in the left hand side is viewed in $L_{\text{set}}^*$ and $P$ in the right hand side is viewed in $\Lambda_{\text{set}}^*$.

**Remark 33.4.** By Theorem 32.9 the new axioms above have the form

(33.1) $$P \leftrightarrow (P \in \Phi^r_{\text{set}})$$

Both the left hand side and the right hand side of the sentences 33.1 have a syntactic nature; but they are very different in that the left hand involves $P$ as a text (more precisely a string of symbols) whereas the right hand side involves $P$ as a set (hence as a symbol). In this way these new axioms “postulate a short-circuit” between texts and sets. This is not the standard way to present Gödel’s theorems that follow because it is not standard to distinguish between texts and sets; since we chose to make this distinction we are forced to add these new axioms to $T_{\text{set}}$. The translation in English of these new axioms 33.1 is something like: “If there is a proof that $P$ is provable then there is a proof of $P$”. The latter is, of course, very misleading because the words in English are ambiguous.

**Definition 33.5.** A formal theory $\Theta$ (generated by a system of axioms $(S, \Phi)$) is called formally inconsistent if there exists a sentence $\varphi \in \Lambda_{\text{set}}^*$ such that $\varphi \in \Theta$ and $\neg \varphi \in \Theta$. The theory is called formally consistent if it is not formally inconsistent. The theory is called formally complete if for any sentence $\varphi \in \Lambda_{\text{set}}^*$ either $\varphi \in \Theta$ or $\neg \varphi \in \Theta$. A theory is called formally incomplete if it is not formally complete.
Let $P_{\text{con}}$ be the sentence in $L_{\text{set}}^*$ (in set theory) expressing (in an “obvious way” which will not be made precise here) the formal consistency of formal set theory $\Lambda_{\text{set}}$. Then one can consider $P_{\text{con}}$ as a sentence in $\Lambda_{\text{set}}^*$ and then one can consider “$P_{\text{con}} \notin \Theta_{\text{set}}$” as a sentence in $L_{\text{set}}$. Gödel proved that this is a theorem in $T'_{\text{set}}$.

**Theorem 33.6.** $P_{\text{con}} \notin \Theta_{\text{set}}$.

With regards to the continuum hypothesis we have the following results due to Gödel and Cohen respectively. Let $P_{\text{CH}}$ be the sentence in $L_{\text{set}}$ expressing the continuum hypothesis, and view $P_{\text{CH}}$ as a sentence in $\Lambda_{\text{set}}^*$. We have the following theorems in $T_{\text{set}}'$:

**Theorem 33.7.** $\neg P_{\text{CH}} \notin \Theta_{\text{set}}$

**Theorem 33.8.** $P_{\text{CH}} \notin \Theta_{\text{set}}$

**Corollary 33.9.** $\Theta_{\text{set}}$ is formally incomplete.

Next we want to analyze the integers in mathematical logic.

**Remark 33.10.** The Peano axiom in set theory is the sentence that there exists a Peano triple. One can view this as a sentence in $\Lambda_{\text{set}}^* = \Lambda_{\{\in\}}$ of formalized set theory; indeed the words “there exists a set $z$ such that for any subset $y$ ...” can be written as

$$\exists z \forall y((\forall x(x \in y) \to (x \in z)) \to ...)$$

But if one tries to write this axiom in the formal language $\Lambda_{\text{ar}} = \Lambda_{\{+, \times, s, 0\}}$ where $+, \times$ are binary functions, $s$ is a unary function, and 0 is a constant then one is bound to fail because there is no way to say, in this formal language, that for any subset something happens. (If one says $\forall x$ then in any $S$-structure $(M, m)$ the variable $x$ is translated as an element of $M$ and not as a subset of $M$.) Nevertheless there is a formal Peano system of axioms in the formal language $\Lambda_{\text{ar}}$ which we are going to consider below.

**Definition 33.11.** Consider the set $S = S_{\text{ar}} = \{+, \times, s, 0\}$ where $+, \times$ are binary functional symbols, $s$ is a unary functional symbol, and 0 is a constant. Let $\Phi_{\text{ar}}$ be the following sentences in $\Lambda_{\text{ar}} = \Lambda_{S_{\text{ar}}}$ (called the formal Peano axioms): $A_1, ..., A_6, A_P$ (obtained from the Peano axioms). So this is a metacountable set of axioms; the latter series of axioms stands for a weak form of induction. The formal system of axioms of Peano arithmetic is the pair $(S_{\text{ar}}, \Phi_{\text{ar}})$. The theory $\Theta_{\text{ar}}$ generated by $(S_{\text{ar}}, \Phi_{\text{ar}})$ is called the Peano arithmetic.

Here is the famous Gödel’s incompleteness theorem of arithmetic. It is a theorem in $T_{\text{set}}'$.

**Theorem 33.12.** $\Theta_{\text{ar}}$ is formally incomplete.

**Sketch of proof.** We follow the informal presentation in the first pages of Gödel’s original article [4] (in combination with facts proved later in that paper). We refer to loc. cit. for the details. Also for any sentence $P$ in $L_{\text{ar}}^*$ we continue to denote by $P$ its image in $\Lambda_{\text{ar}}^*$ and also its translation in $L_{\text{set}}^*$ and the image of that translation in $\Lambda_{\text{ar}}^*$. The first step is to “tag” formulae by integers. One know there is a bijection between the set of symbols $\Lambda_{\text{set}}$ and $\mathbb{N}$; fix such a bijection and, for convenience, write this informally as

$$\Lambda_{\text{set}} = \{s_1, s_2, s_3, ...\}$$
Let \( p : \mathbb{N} \to \mathbb{N} \) be the function defined by letting \( p(i) \) be the \( i \)th prime. Then define the “Gödel numbering function”
\[
G : \Lambda^*_{\text{set}} \to \mathbb{N}
\]
by the rule
\[
G(s_{i_1}s_{i_2}s_{i_3} \ldots) = p(1)^{p(i_1)}p(2)^{p(i_2)}p(3)^{p(i_3)} \ldots
\]
Clearly \( G \) is injective and “definable in \( L_{\text{ar}} \)” in the sense that its graph is given by an appropriate formula in \( L_{\text{ar}} \) in two variables. Let \( \Sigma = G(\Lambda^*_{\text{set}}) \) and \( \Sigma' \) be the image by \( G \) of the set of all formulae with exactly one free variable. Let \( F : \Sigma \to \Lambda^*_{\text{set}} \) be the inverse of \( G : \Lambda^*_{\text{set}} \to \Sigma \).

The second step is to prove that the predicate “belongs to \( \Theta_{\text{ar}} \)” is “definable” in \( L_{\text{ar}} \) in the sense that there is a formula \( B \) in \( L_{\text{ar}} \) with one free variable such that for all \( n \in \Sigma \),
\[
(F(n) \in \Theta_{\text{ar}}) \leftrightarrow B(n).
\]
This is the heart of the proof: it amounts to showing that “provability of a sentence is an arithmetic property of the tag of the sentence”.

The third step is to show that there is a formula \( S \) in \( L_{\text{ar}} \) in two variables defining the following “substitution” function \( S : \Sigma' \times \mathbb{N} \to \mathbb{N} \): \( S(a, b) = c \) if and only if \( F(c) \) is the formula obtained from the formula \( F(a) \) by replacing the unique free variable of \( F(a) \) by \( b \); in other words \( F(S(a, b)) = F(a)(b) \). Now for \( x \) a variable we consider the formula \( P \) in \( L_{\text{ar}} \) having the property that, viewed as a formula in \( \Lambda^*_{\text{ar}} \), it satisfies (together with \( B \) and \( S \) viewed as sets),
\[
P = \neg B(S(x, x)) \in \Lambda^*_{\text{ar}} \quad \text{(equality of sets)}
\]
Since \( P \) has exactly one free variable there exists \( m \in \Sigma \) such that \( P = F(m) \). The key sentence to be considered now is
\[
P(m) = \neg B(S(m, m))) \in \Lambda^*_{\text{ar}}
\]
Note that
\[
F(S(m, m)) = F(m)(m) = P(m)
\]
and hence
\[
S(m, m) = G(P(m))
\]
and hence
\[
(33.2) \quad \neg P(m) = \neg B(G(P(m))) \leftrightarrow B(G(P(m))) \leftrightarrow (P(m) \in \Theta_{\text{ar}}) \rightarrow P(m)
\]
The last step of the proof is to check the following:
\[
(33.3) \quad P(m) \notin \Theta_{\text{ar}}
\]
\[
(33.4) \quad \neg P(m) \notin \Theta_{\text{ar}}
\]
To check 33.3 assume \( P(m) \in \Theta_{\text{ar}} \) and seek a contradiction. By 33.2 we get both \( P(m) \) and \( \neg P(m) \) which is a contradiction.

To check 33.4 assume \( \neg P(m) \in \Theta_{\text{ar}} \) and seek a contradiction. Since
\[
(\neg P(m) \in \Theta_{\text{ar}}) \rightarrow (\neg P(m))
\]
we get \( \neg P(m) \). By 33.2 we get \( P(m) \). This is a contradiction.
Remark 33.13. Since Theorems 33.6, 33.8, 33.7 are sentences in $L^a_{set}$, they have, according to the conventions in the present course, no meaning and no truth value. In particular any interpretation of these theorems as saying something about mathematics itself transcends the paradigm of the present course.
Bibliography