# MATHEMATICS 300 — SPRING 2005

*Introduction to Mathematical Reasoning*

*H. J. Sussmann*

## INSTRUCTOR'S NOTES

*April 14, 2005*

## Contents



# 12 On homework, the second midterm, and the final exam

## 12.1 The second midterm and the final exam

**The second midterm exam will be on Thursday April 21. The final exam will be on Friday May 6, 12:00-3:00 pm.** NOTE: The midterm was originally scheduled for Tuesday April, but on Tuesday April 12 we decided to move it to APril 21.

## 12.2 Homework assignment no. 5, due on Thursday March 10:

1. Book, §2.1, pages 71 to 73, problems 1(b)(d)(f); 4 (all non-starred items), 5 (all non-starred items), 8, 19 (all non-starred items)

**2.** Book, §2.2, pages 77 to 80, problems 10(b)(d)(f), 11(a)(d), 17 (c)(f)(g)(h).

**3.** Prove: if $A$, $B$, $C$ are sets, and $A \subseteq B \cup C$, then $A \subseteq B \vee A \subseteq C$.

## 12.3 Homework assignment no. 6, due on Thursday March 24:

**1.** Redo Problems 4, 5, and 7 (part 2) of the midterm exam. In problem 4, make sure you give proofs clearly structured in numbered steps, and indicating for each step exactly which rule iyou are using to justify it. (And if you want to argue that a general statement is not true, give a specific counterexample.) In problem 5, make sure you answer **all** the questions that were asked, especially (a) when a proof did not get an "A", indicate why it is wrong. (Note: saying that "a proof is wrong because the conclusion is false" will not do. If a proof is wrong, then there must be a mistake somewhere. I want you to tell me what the mistake (or mistakes) is.

**2.** Book, §2.2, pages 77 to 80, problems 12, 15 and 16.

**3.** Book, §2.3, pages 87 to 90, problems 1(j)(k)(l)(m)(n), 4, 6(b), 7(b).

## 12.4 Homework assignment no. 7, due on Thursday March 31:

**1.** Book, §2.4, pages 100 to 103, problems 1(a)(c)(e), 2(a)(c)(d), 3, 4, 5(a)(c), 6(d)(e), 7(b), 8(a),(c),(e),(i),(l),(m), (13), 15(c)(d)(f).

**2.** In this problem, you are asked to prove that something cannot be proved using certain axioms. Specifically, you are asked to *prove that the formula "$1 \cdot 1 = 1$" cannot be proved from the book's axioms for natural numbers*, that is, from the 18 properties listed on Page 91, plus the Principle of Mathematical Induction stated on Page 92. Here is what you can do to prove this.

a. Create a new "multiplication" operation called $*$, defined as follows: if $x$ and $y$ are natural numbers then $x * y = 2 \cdot x \cdot y$.

b. Prove that, if you substitute this new operation for the ordinary multiplication (that is, if you consider the system of natural numbers but with the multiplication operation being $*$ instead of the ordinary multiplication $\cdot$, then all the book's axioms for natural numbers are still satisfied, but the assertion that "1 times 1 equals 1" is not, because $1 * 1$ is not equal to 1.

c. Conclude that "$1 * 1 = 1$" cannot be proved from the book's axioms for natural numbers. (Note: this is very similar to the "borogoves and mimsy things" problem in the first midterm. In that problem, you had to prove that, for example, the formula

$$\Big((\exists x)(x \text{ is a borogove}) \wedge (\exists x)(x \text{ is mimsy})\Big)$$
$$\Longrightarrow (\exists x)(x \text{ is a borogove} \wedge x \text{ is mimsy})$$

cannot be proved, and the way to prove that was to point out that, for example, "borogove" might mean "Republican" and "mimsy" might mean "a Democrat," and with these meanings of "borogove" and "mimsy" the statement isn't true. Here, I am asking you to show that if "times" meant "the operation $*$" instead of the usual multiplication, then all the axioms would be true but the formula "1 times 1=1" would not be true, so the formula cannot be proved from the axioms.

## 12.5 Homework assignment no. 8, due on Thu. April 7:

*NOTE: In the course, we skipped the PCI (Principle of Complete Induction). All the problems where you are asked to use the PCI can be, and should be, done using the WOP (Well-ordering principle). This applies to Homework No. 9 as well.*

**1.** Book, §2.4, pages 100 to 103, problem 14.

**2.** Book, §2.5, pages 109 to 111, problems 2, 3, 5(a)(b)(c), 6, 7, 8, 15(a)(c)(d).

**3.** Prove that

$$(\forall n \in \mathbb{N})\left(\sum_{k=1}^{n} k^3 = \Big(\frac{n^2+n}{2}\Big)^2\right).$$

**4.** **a.** Find a formula for $\sum_{k=1}^{n} k^4$, and prove it. (Hint: first make the guess that

$$\sum_{k=1}^{n} k^4 = An^5 + Bn^4 + Cn^3 + Dn^2 + En\,,$$

where $A, B, C, D, E$ are five natural numbers to be determined. Then find $A, B, C, D, E$. Then prove the formula you got by induction.)

**b.** Let $a \in \mathbb{R}$, $a > 0$. Let $S_N(a)$ be the Riemann sum for the integral $\int_0^a x^4\,dx$, corresponding to a subdivision of the interval $[0, a]$ into $N$ equal subintervals of length $\frac{a}{N}$, and to the choice, for each interval, of its rightmost point as a sample point. (This means that the intervals of the subdivision are $\left[0, \frac{a}{N}\right]$, $\left[\frac{a}{N}, \frac{2a}{N}\right]$, $\left[\frac{2a}{N}, \frac{3a}{N}\right]$, $\cdots$, $\left[\frac{(N-1)a}{N}, a\right]$, and then $S_N(a) = \frac{a}{N}\sum_{j=1}^{N}\left(\frac{ja}{N}\right)^4$.) Compute $S_N(a)$ using the formula you got in Part **a**.

**c.** Compute the integral $\int_0^a x^4\,dx$ by taking the limit of $S_N(a)$ as $N \to \infty$.

### 12.6 Homework assignment no. 9, due on Thu. April 14:

*NOTE: This homework assignment was written, by mistake, when I did not have a copy of Homework No. 8 in front of me, and I made the mistake of including some problems that were already there in Homework No. 8. You do not have to these problems twice. Just once, in Homework No. 8 or in No. 9, is enough.*

**1.** Book, §2.5, pages 109-111, problems 2, 3(a), 4 (the Fibonacci numbers $f_n$ are defined in the book on page 106), 5(a),(b),(c), 6(a),(b),(c), 11, 12, 13.

**2.** Book, §2.5, pages 109 to 111, problem 7. Note: the important thing here is that, when we proved that $\sqrt{2}$ is irrational, at one point in the proof we used one of those "... and so on ... until the process stops" arguments that are of dubious validity; specifically, at some point we said something like "if $m$ and $n$ are both even, then factor out 2 from both of them, if the results are still both even, factor out a 2 again, and keep doing this util the process stops, at which point you will end up with $m$ and $n$ not both even." Now I am asking you to write a complete proof that $\sqrt{2}$ is irrational **without** using this "... and so on ... until the process stops" argument, and using the WOP instead. Hint: look at the set of all natural numbers $n$ such that $(\exists m \in \mathbb{N})(m^2 = 2n^2)$; prove that this set has a smallest element, and then use this fact.)

**3.** Using the same method as in the previous problem, prove that $\sqrt{3}$ is irrational.

**4.** Using the same method as in the two previous problems, try to prove that $\sqrt{4}$ is irrational. and indicate exactly where the proof breaks down. (Please, do not just tell me that "you cannot prove this because it isn't true." What I want to know is *why* the same proof technique that works perfectly for 2 and 3 fails to work for 4.)

**5.** Given $a = 234$, $b = 275$, findg the GCD $g$ of $a$ and $b$ and find integers $m, n$ such that $g = m \cdot a + n \cdot b$.

**6.** Book, §2.5, pages 109 to 111, problem 8. NOTE: We already proved the theorem of the division algorithm in class, for natural numbers. (And it is also proved in the book, on page 108.) In Part (b) of this problem, I actually want to do two different things:

(b.1) Prove that the theorem on the Division Algorithm for integers follows from the theorem on the Division Algorithm for $\mathbb{N}$. (That is, using Theorem 2.15 of the book—or, if you prefer, the theorem I gave in class, which is slightly stronger—deduce the theorem on the Division Algorithm for integers.)

(b.2) Independently, prove the theorem on the Division Algorithm for integers directly, without going through the theorem for $\mathbb{N}$.

## 12.7 Some review questions for the second midterm

1. Define "subset."

2. Define "union" of two sets.

3. Define "intersection" of two sets.

4. Define "union" of a family of sets.

5. Define "intersection" of a family of sets.

6. Define "power set."

7. Define "even integer."

8. Define "odd integer."

9. Define "rational number."

10. Define "irrational number."

11. Define the predicate "divides."

12. Define the concept of "prime number."

13. Define "absolute value." (To refresh your memory: if $a$ is a real number, the **absolute value** of $a$ is the number $|a|$ given by $|a| = a$ if $a \geq 0$ and $|a| = -a$ if $a < 0$.

14. Define "greatest common divisor."

15. State the Principle of Mathematical Induction.

16. State and prove the Well Ordering Principle.

17. State and prove the theorem on the division algorithm. (Here is the statement, so you will not forget it: If $a, b$ are integers and $b \neq 0$, then there exist integers $q, r$ such that $a = q \cdot b + r$, $0 \leq r$, and $r < |b|$.)

18. State and prove the theorem on the greatest common divisor being an integer linear combination. (Here is the statement, so you will not forget it: If $a, b$ are integers and $g$ is a natural number, then $g$ is the greatest common divisor of $a$ and $b$ if and only if the following is true:

$$(g|a \wedge g|b) \wedge (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(g = m \cdot a + n \cdot b)\,.$$

    Recall that "$x|y$" means "$x$ divides $y$," that is, "$y$ is divisible by $x$." )

19. Prove the following: if $a, b, p$ are integers, $p$ is prime, and $p|a\cdot b$, then $p|a$ or $p|b$. (Here is the proof: suppose $\sim p|a$. We want to prove that $p|b$. Since $\sim p|a$, the GCD of $a$ and $p$ is 1, because $1|a$, $1|p$, and if $h \in \mathbb{N}$ is such that $h|a$ and $h|p$, then $h$ must be 1 or $p$, because $p$ is prime, and $h$ cannot be $p$, because $h$ divides $a$ but $p$ does not. So $h = 1$, and then $h \leq 1$, showing that $1 = GCD(a, p)$. Then the theorem on the GCD tells us that we can pick integers $m$, $n$ such that $1 = m \cdot a + n \cdot p$. Mutiplying boith sides by $b$, we get $b = m \cdot a \cdot b + n \cdot b \cdot p$. We are assuming that $p|a \cdot b$, so we can pick an integer $k$ for which $a \cdot b = k \cdot p$. But then

$$b = m \cdot a \cdot b + n \cdot b \cdot p = m \cdot (k \cdot p) + n \cdot b \cdot p = (m \cdot k + n \cdot b) \cdot p\,,$$

so $p$ divides $b$.)

# 13 Some more logic

## 13.1 The basic logical vocabulary

L1. The **right and left parentheses:** ( and )

L2. The **logical connectives:**

- L2.P. The **propositional connectives:**
  - L2.P.a. the *negation symbol* ("$\sim$ ...", read as "not ...", or "it is not the case that ..."),
  - L2.P.b. the *conjunction symbol* ("... $\wedge$ ...", read as "... and ..."),
  - L2.P.c. the *disjunction symbol* ("... $\vee$ ...", read as "... or ..."),
  - L2.P.d. the *implication symbol* ("... $\Longrightarrow$ ...", read as "if ... then ..."),
  - L2.P.e. the *biconditional symbol*("... $\Leftrightarrow$ ...", read as "... if and only if ...").
- L2.Q. The **quantifiers:** $\exists$ (the existential quantifier; we read "$(\exists A)B$" as "there exists $A$ such that $B$.") and $\forall$ (the universal quantifier; we read "$(\forall A)B$" as "for every $A$, $B$").
- L2.V. The **letter variables:** $a$, $b$, ..., $f$, $g$, ..., $i$, $j$, $k$, ..., $m$, $n$, $p$, $q$, $r$, $s$, $t$, $u$, ..., $x$, $y$, $z$,..., $A$, $B$, ..., $F$, $G$, ..., $I$, $J$, $K$, ..., $M$, $N$, $P$, $Q$, $R$, $S$, $T$, $U$, ..., $X$, $Y$, $Z$, ....
- L2.S. **Special symbols** such as $+$, $\cdot$, $\in$.

## 13.2 On variables

What, exactly, is a "variable"? The answer is, anything you want to use as a variable. For example, in a court of justice the phrases "the defendant", "the prosecutor" and "the judge" are variables, because the precise person that each of these phrases stands for changes (i.e., ***varies***) from trial to trial. (In one trial the variable "the defendant" may stand for "Michael Jackson," while in another trial it stood for "Scott Peterson.")

In a newspaper or magazine or book, the words (pronouns) "he" and "she" will stand for different people in different articles or chapters, or even within the same article or chapter. (For example, you may find in a newspaper article the sentence

> Mr. Hector Sussmann, of Piscataway, NJ, was bitten by a dog yesterday as he was picking up his mail. He filed a complaint against the dog's owner. The owner, however, denied that he was at fault.

Notice that the first and second "he" (and the "his" of "his mail") refer to "Mr. Hector Sussmann", but the third one clearly one refers to "the dog's owner." The change in the reference of "he" is achieved in this case by the following procedure: every time a new person is introduced, then, as long as this person is male, "he' ceases to refer to whomever it referred to before, and instead starts referring to the newly introduced person.

So, a ***variable*** is a symbol or string of symbols whose meaning can change. For example, when you buy a house, your lawyer will have you sign a contract in which there is mention of "the buyer" and "the seller." The phrases "the buyer" and "the seller" are variables, because what they stand for changes from contract to contract: when you are done with your transaction and leave your lawyer's office, another buyer and seller will go in, and then the lawyer will use another contract in which the phrases "the buyer" and "the seller" refer to the new buyer and the new seller. Since the meaning of these phrases can change from contract to contract, every time you start a new contract the meaning has to be *declared*. (In a contract, typically, there will be a statement at the beginning saying something like that "John W. Doe, henceforth referred to as 'the buyer', and Alice H. Smith, henceforth referred to as 'the seller' '.

In general, a variable will refer to whatever you make it refer to. If you are going to use a variable, then you are the one who has to ***declare*** a value for it. And if you do not, then I don't know what you are talking about.

In Mathematics, letter variables function exactly as I have just explained. If I write "$x < 5$", just like that, then you do not know what this is really saying, and you cannot tell if it is true or not, because you don't know what "$x$" stands for. If, on the other hand, I write

$$\text{Let } x = 1. \text{ Then } x < 5.$$

then everything is clear.

Letter variables can only be used if they have a declared value. After a value has been declared, e.g., by saying "let $x = 5$" or "let $x$ be arbitrary", then the variable has that value (that is, it becomes a "constant") until the declaration ceases to be valid, at which point we can declare a new value. (This is exactly as in our examples: outside the article about Mr.Sussmann andthe dog, the pronoun "he" is available for use with a different value.)

Sometimes several sentences, starting with the declaration of a value of a variable, and going until the declaration ceases to be valid, are written as a single sentence. For example, you should think of the sentence

$$(\forall x)(x \in \mathbb{R} \Longrightarrow x^2 \geq 0)$$

as being, really, a way to write in one sentence, the following:

Let $x$ be arbitrary.
Then if $x \in \mathbb{R}$ then $x^2 > 0$.

In the sentence $(\forall x)(x \in \mathbb{R} \Longrightarrow x^2 \geq 0)$, the part $(x \in \mathbb{R} \Longrightarrow x^2 \geq 0)$ is the ***scope*** of the quantifier $(\forall x)$. The left parenthesis indicates where the validity of the declaration starts, and the right parenthesis tells you where it ends. So after the right parenthesis, if you write another sentence, then $x$ has no delcared value, unless you declare one. So, for example, it does not make sense to write

$(\forall x)(x \in \mathbb{R} \Longrightarrow x^2 \geq 0)$
$x \in \mathbb{R}$

but it is perfectly meaningful to write

$(\forall x)(x \in \mathbb{R} \Longrightarrow x^2 \geq 0)$
$(\forall x)(x \in \mathbb{Z} \Longrightarrow (x \text{ is even} \wedge x \text{ is odd}))$

A similar situation occurs with the existential quantifier. Suppose you write

$$(\exists x)(x \in \mathbb{Z} \wedge x^2 = 36)$$

Then you are asserting that it is possible to pick a number which is an integer and whose square is 36. But ***you haven't picked it yet!*** You are only saying that *it is possible* to pick it. So, if you wrote

$$(\exists x)(x \in \mathbb{Z} \wedge x^2 = 36)$$
$$x = 6\,,$$

this would be unacceptable, because after the first sentenece is finished there is no value assigned to $x$, so in the second sentence, you cannot talk about "$x$" as if we new what it is. (If you want to *introduce* $x$ by saying that you want to declare the value of $x$ to be 6, then you should do exactly that, and write "let $x = 6$.")

Recall that one of our rules tells us exactly how to go about "picking an $x$" once you know that it is possible. Rule $\exists_{out}$ says that, for example, if you have $(\exists x)(x \in \mathbb{Z} \wedge x^2 = 36)$, then you can pick one as follows:

$(\exists x)(x \in \mathbb{Z} \wedge x^2 = 36)$
Pick an $x \in \mathbb{Z}$ such that $x^2 = 36$ and call it $\bar{x}$.
Then $\bar{x} \in \mathbb{Z}$ and $\bar{x}^2 = 36$.

Why do I insist on *not* using $x$ to call this thing that you picked? The reason is that very often the same variable $x$ may appear again in another sentence later, and if you already have a constant named $x$ then you will be in trouble. You might end up with atrocities such as

$$\begin{array}{l} (\exists x)(x \in \mathbb{Z} \wedge x^2 = 36) \\ \text{Pick an } x \in \mathbb{Z} \text{ such that } x^2 = 36 \text{ and call it } x\,. \\ \text{Then } x \in \mathbb{Z} \text{ and } x^2 = 36\,. \\ (\exists x)(x \in \mathbb{Z} \wedge x^2 = 25)\,, \end{array}$$

or, even worse,

$$\begin{array}{l} (\exists x)(x \in \mathbb{Z} \wedge x^2 = 36) \\ \text{Pick an } x \in \mathbb{Z} \text{ such that } x^2 = 36 \text{ and call it } x\,. \\ \text{Then } x \in \mathbb{Z} \text{ and } x^2 = 36\,. \\ (\exists x)(x \in \mathbb{Z} \wedge x^2 = 25)\,. \\ \text{Pick an } x \in \mathbb{Z} \text{ such that } x^2 = 25 \text{ and call it } x\,. \\ \text{Then } x \in \mathbb{Z} \text{ and } x^2 = 25\,. \\ \text{Since } x^2 = 36 \text{ and } x^2 = 25, \text{ we have proved that } 36 = 25. \end{array}$$

## 13.3 Restricted quantifiers

The quantifiers we have seen so far are "unrestricted," that is, such that the variable that occurs in them can take all possible values.

For example, if you say

$$(\forall x)((x \text{ is a Republican} \vee x \text{ is a Democrat}) \vee x \text{ is an Independent})$$

this really says that "every entity $x$ in the universe is a Republican or a Democrat or an independent." For this to be true you would have to check that the assertion

$$(x \text{ is a Republican} \vee x \text{ is a Democrat}) \vee x \text{ is an Independent}$$

is true for every $x$, that is, for all U.S. people, and all foreigners, and all animals, and all trees and rocks and planets and books and numbers.

That is not the kind of thing one ever wants to say. What usually happens is that you have some very restricted set $A$ of entities or objects, and you want to say that something is true *for all $x$ that belong to $A$*. The way to say that is with the ***restricted universal quantifier*** $(\forall x \in A)$, which is read as "for all $x$ belonging to $A$." The sentence

$$(\forall x \in A)(\text{something about } x)$$

is read as "for all $x$ belonging to $A$ something about $x$," and is really an abbreviation of

$$(\forall x)(x \in A \Longrightarrow \text{something about } x)\,.$$

For example, suppose $\mathbb{N}$ is the set of all natural numbers. Then

$$(\forall x \in \mathbb{N})(x = 1 \vee x > 1)$$

is an abbreviation of

$$(\forall x)(x \in \mathbb{N} \Longrightarrow (x = 1 \vee x > 1))\,,$$

and says "every natural number is either equal to 1 or greater than 1."

There is also a ***restricted existential universal quantifier*** $(\exists x \in A)$, which is read as "there exists an $x$ belonging to $A$ such that." The sentence

$$(\exists x \in A)(\text{something about } x)$$

is read as "there exists an $x$ belonging to $A$ such that something about $x$," and is really an abbreviation of

$$(\exists x)(x \in A \wedge \text{something about } x)\,.$$

For example, suppose $\mathbb{N}$ is the set of all natural numbers. Then

$$(\exists x \in \mathbb{N})(x < 7 \wedge x \cdot x = 36)$$

is an abbreviation of

$$(\exists x)(x \in \mathbb{N} \wedge (x < 7 \wedge x \cdot x = 36))\,,$$

and says "there exists a natural number which is smaller than 7 and whose square is equal to 36," or "there exists a natural number $x$ such that $x$ is smaller than 7 and $x$ squared is equal to 36."

We have already seen the four logical rules for unrestricted quantifiers, namely, Rules $\forall_{out}$ and $\forall_{in}$, and Rules $\exists_{out}$ and $\exists_{in}$. For each of these rules, there is the corresponding restricted version, so we have the following four ***restricted quantifier rules***:

***The restricted Rule*** $\forall_{out}$***, a.k.a. the " restricted specialization rule."*** Suppose $A$ is a set, $p(x)$ is a formula where there is no quantifier involving $x$, $t$ is a constant term, and $p(x \to t)$ is what you get from $p(x)$ by substituting $t$ for $x$ in **all** the occurrences of $x$ in $p(x)$. Then, if you have $(\forall x \in A)p(x)$, and $t \in A$, you can go to $p(x \to t)$.

***The restricted Rule*** $\forall_{in}$***.*** Suppose $A$ is a set, $p(x)$ is a formula where there is no quantifier involving $x$, $a$ is a letter, and $p(x \to a)$ is what you get from $p(x)$ by substituting $a$ for $x$ in **all** the occurrences of $x$ in $p(x)$. ***Suppose the letter*** $a$ ***has not appeared before***. Then you can start a proof within a proof by saying "Let $a \in A$ be arbitrary," and in this proof you can use "$a \in A$." If in this proof within a proof you get to $p(x \to a)$, then you can go to $(\forall x \in A)p(x)$ in your main proof.

***The restricted Rule*** $\exists_{out}$. Suppose $A$ is a set, $p(x)$ is a formula where there is no quantifier involving $x$, $a$ is a letter, and $p(x \to a)$ is what you get from $p(x)$ by substituting $a$ for $x$ in **all** the occurrences of $x$ in $p(x)$. ***Suppose that the letter*** $a$ ***has NOT appeared before. Suppose you have proved*** $(\exists x \in A)p(x)$. Then you can start a proof within a proof by introducing a new object, calling it $a$, and stipulating that $p(x \to a)$ and $x \in A$. This effectively declares $a$ to be a constant, locally, within the "proof within a proof." If you ever get to something that does *not* contain $a$, then you can use it outside your proof within a proof, in the main proof.

***The restricted Rule*** $\exists_{in}$***, a.k.a. the restricted witness rule.*** Suppose $A$ is a set, $p(x)$ is a formula where there is no quantifier involving $x$, $t$ is a constant term, and $p(x \to t)$ is what you get from $p(x)$ by substituting $t$ for $x$ in **all** the occurrences of $x$ in $p(x)$. Then from $p(x \to t)$ and $t \in A$ you can go to $(\exists x \in A)p(x)$.

## 13.4 Justification of the restricted quantifier rules

The four "restricted quantifier rules" can be easily justified in terms of our unrestricted rules.

For example, let us justify the restricted Rule $\forall_{out}$. Suppose you have $(\forall x \in A)p(x)$ and $t \in A$. Then the restricted Rule $\forall_{out}$ would enable you to go to $p(x \to t)$. Let me show how you could achieve exactly the same thing without using the restricted rule. Here is what you could do.

| | | |
|---|---|---|
| (1) | $(\forall x \in A)p(x)$ | |
| (2) | $t \in A$ | |
| (3) | $(\forall x)(x \in A \Longrightarrow p(x))$ | [Rewriting of (1)] |
| (4) | $t \in A \Longrightarrow p(x \to t)$ | [Rule $\forall_{out}$, from (3)] |
| (5) | $p(x \to t)$ | [Rule $\Longrightarrow_{out}$ from (2) and (4)] |

So all that the restricted Rule $\forall_{out}$ does is enable you to do three steps in just one step, by writing

| | | |
|---|---|---|
| (1) | $(\forall x \in A)p(x)$ | |
| (2) | $t \in A$ | |
| (3) | $p(x \to t)$ | [ Restricted Rule $\forall_{out}$, from (1) and (2)] |

As a second example, let us justify the restricted Rule $\exists_{out}$. Suppose you have $(\exists x \in A)p(x)$ Then the restricted Rule $\exists_{out}$ would enable you to introduce an $a$ and stipulate that $a \in A$ and $p(x \to a)$. Again, let me show how you could achieve exactly the same thing without using the restricted rule. Here is what you could do.

| | | |
|---|---|---|
| (1) | $(\exists x \in A)p(x)$ | |
| (2) | $(\exists x)(x \in A \wedge p(x))$ | [Rewriting of (1)] |
| (3) | Pick $x$ as in (2) and call it $a$, so $a \in A \wedge p(x) \to a$. | [R. $\exists_{out}$, fr. (2)] |
| (4) | $a \in A$ | [Rule $\wedge_{out}$ from (3)] |

(5) $\quad p(x \to a)$ $\quad$ [Rule $\wedge_{out}$ from (2) and (4)]

So all that the restricted Rule $\exists_{out}$ does is enable you to shorten this a little bit, by writing

(1) $\quad (\exists x \in A)p(x)$
(2) $\quad$ Pick $x$ as in (1) and call it $a$, so $a \in A$ and $p(x \to a)$
[Restricted Rule $\exists_{out}$ from (1)]

EXERCISE: Write justifications for the other two restricted quantifier rules, $\forall_{in}$ and $\exists_{in}$.

## 13.5 The equality axioms and the substitution rule

Here are the three axioms governing the use of the = symbol:

EQ1. $\quad (\forall x)(x = x)$;

EQ2. $\quad (\forall x)(\forall y)(x = y \Longrightarrow y = x)$;

EQ3. $\quad (\forall x)(\forall y)(\forall z)((x = y \wedge y = z) \Longrightarrow x = z)$;

In addition, we have the following ***substitution rule***, saying that "equals can be substitued for equals."

EQSUB. Suppose $p(x)$ is a formula with no quantifiers involving the variable $x$. Suppose $t_1$ and $t_2$ are constant terms. Let $p(x \to t_1)$, $p(x \to t_2)$, be the formulas obtained by substituting $t_1$ for $x$ and $t_2$ for $x$. Then,

EQSUB.a if you have if you have $t_1 = t_2$ and $p(x \to t_1)$, you can go to $p(x \to t_2)$,

EQSUB.b if you have if you have $t_1 = t_2$ and $p(x \to t_2)$, you can go to $p(x \to t_1)$.

EXAMPLE: Suppose you have
$$2.1 = 2$$
and
$$2 = 1 + 1\,,$$
and you want to go to
$$(1 + 1).1 = 2\,.$$
Here is how you could do it using the equality axioms and Rule EQSUB.

(1) $\quad 2.1 = 2$ $\quad$ [Given]
(2) $\quad 2 = 1 + 1$ $\quad$ [Given]
(3) $\quad (1 + 1) \cdot 1 = 1$ $\quad$ [ EQSUB from (1) and (2), with "$x.1 = 2$" as $p(x)$, 2 as $t_1$ and $1 + 1$ as $t_2$]

# 14 The arithmetic of natural numbers and integers

We are going to give a version of the axiom system for the natural numbers in which the natural numbers are part of a larger world where there lots of other things, and in particular sets.

Therefore, every time we want something to be a natural number, we have to say it, because in principle it could be something else. So we have to use restricted quantifiers. We cannot, for example, state the associative law of addition as follows:

$$(\forall x)(\forall y)(\forall)((x+y)+z=x+(y+z)),$$

because that would say that the equality $(x+y)+z=x+(y+z)$ holds for all triples $x, y, z$ of objects in the universe, so that, for example,

$$\text{Dame Edna}+\text{the planet Mars}=\text{Olivia the giraffe}.$$

This, of course, is quite ridiculous, because we don't know what it means to take the sum of Dame Edna and the planet Mars. So what we have to do is restrict the quantifiers to natural numbers, and write the associative law this way:

$$(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})((x+y)+z=x+(y+z)).$$

Before we actually state the axioms, we specify the basic vocabulary of natural number arithmetic. Since we want to work with natural numbers within a larger world in which there are sets, we will also need to have among our basic symbols the symbols of set theory:

**THE BASIC VOCABULARY OF SET THEORY**

$\sim \quad \wedge \quad \vee \quad \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad ( \quad ) \quad = \quad \in$

$\{ \quad \} \quad :$ and the variables.

And now we are ready to go to natural number arithmetic.

## 14.1 The basic vocabulary of natural number arithmetic

The vocabulary of natural number arithmetic will be the same as that of set theory, with the addition of some special **arithmetical symbols.**

The arithmetical symbols for the theory of natural numbers are

a. the *constant* "1" ("one"),

b. the *symbols for the arithmetical operations*: "+" ("plus") and "." ("times", sometimes written "×", and sometimes omitted, as in the expression "$xy$", which really means "$x \cdot y$".)

d. the *predicates:* "<" ("is less than", or "is smaller than"), "≤" ("is less than or equal to", or "is not greater than"),

e. The symbol "ℕ" for "the set of all natural numbers".

**THE BASIC VOCABULARY OF NATURAL NUMBER ARITHMETIC**

$$\sim \quad \wedge \quad \vee \quad \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad ( \quad ) \quad = \quad \in \quad \{ \quad \} \quad :$$

$1 \quad < \quad \leq \quad + \quad \cdot \quad \mathbb{N}$ and the variables.

## 14.2 The axioms of natural number and integer arithmetic

We now start developing the theory of the natural number system. We will start by giving a set of ***axioms***. These axioms are properties that we can use any time we want. On the other hand,

1. ***objects and predicates that do not appear in the list (such as, for example, the number* 2*, and the predicates* >*,* ≥*, "is prime," "is even," "is odd," "divides,") have to be defined.***

2. ***if you want to assert and/or use any statement which is not an axiom or a definition, then the statement has to be proved.***

We will also present ***integer arithmetic.*** The basic vocabulary of integer arithmetic will be the same as that of natural number arithmetic, with the addition of three more special symbols: 0, −, and ℤ.

**THE BASIC VOCABULARY OF INTEGER ARITHMETIC**

$$\sim \quad \wedge \quad \vee \quad \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad ( \quad ) \quad = \quad \in \quad \{ \quad \} \quad :$$

$0 \quad 1 \quad < \quad \leq \quad + \quad - \quad \cdot \quad \mathbb{N} \quad \mathbb{Z}$ and the variables.

## THE AXIOMS OF NATURAL NUMBER ARITHMETIC

### SUCCESSOR PROPERTIES

NNA1. $1 \in \mathbb{N}$

NNA2. $\sim (\exists x \in \mathbb{N})(x + 1 = 1)$.

### CLOSURE PROPERTIES

NNA3. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(x + y \in \mathbb{N})$.

NNA4. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(x \cdot y \in \mathbb{N})$.

### ASSOCIATIVITY PROPERTIES

NNA5. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})((x + y) + z = x + (y + z))$.

NNA6. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})((x.y).z = x.(y.z))$.

### COMMUTATIVITY PROPERTIES

NNA7. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(x + y = y + x)$.

NNA8. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(x \cdot y = y \cdot x)$.

### DISTRIBUTIVE PROPERTIES

NNA9. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x \cdot (y + z) = x \cdot y + x \cdot z)$.

NNA10. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})((y + z) \cdot x = y \cdot x + z \cdot x)$.

### CANCELLATION PROPERTIES

NNA11. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x + z = y + z \Longrightarrow x = y)$

NNA12. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x \cdot z = y \cdot z \Longrightarrow x = y)$

### MULTIPLICATIVE IDENTITY PROPERTY

NNA13. $(\forall x \in \mathbb{N})(x \cdot 1 = x)$.

### ORDER PROPERTIES

NNA14. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(x < y \Longleftrightarrow (\exists w \in \mathbb{N})(x + w = y))$

NNA15. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y \Longleftrightarrow (x < y \vee x = y))$

NNA16. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})((x < y \wedge y < z) \Longrightarrow x < z)$

NNA17. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})((x \leq y \wedge y \leq x) \Longrightarrow x = y)$

NNA18. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x < y \Longrightarrow x + z < y + z)$

NNA19. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x < y \Longrightarrow x \cdot z < y \cdot z)$

NNA20. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})((x < y \vee y < x) \vee x = y)$

### THE PRINCIPLE OF MATHEMATICAL INDUCTION

NNA21. $(\forall S)\left(\Big(S \subseteq \mathbb{N} \wedge (1 \in S \wedge (\forall u \in \mathbb{N})(u \in S \Longrightarrow u + 1 \in S))\Big) \Longrightarrow S = \mathbb{N}\right)$

**THE AXIOMS OF INTEGER ARITHMETIC**

**ZERO AND ONE PROPERTIES**

IA1. $0 \in \mathbb{Z}$
IA2. $1 \in \mathbb{Z}$

**CLOSURE PROPERTIES**

IA3.1 $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y \in \mathbb{Z})$.
IA3.2 $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x - y \in \mathbb{Z})$.
IA4. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x \cdot y \in \mathbb{Z})$.

**ASSOCIATIVITY PROPERTIES**

IA5. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})((x + y) + z = x + (y + z))$.
IA6. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})((x.y).z = x.(y.z))$.

**COMMUTATIVITY PROPERTIES**

IA7. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = y + x)$.
IA8. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x \cdot y = y \cdot x)$.

**PROPERTIES RELATING THE THREE OPERATIONS**

IA9.1. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})(x \cdot (y + z) = x \cdot y + x \cdot z)$.
IA9.2. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})((y + z) \cdot x = y \cdot x + z \cdot x)$.
IA10. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x - y = z \Longleftrightarrow x = y + z)$.

**CANCELLATION PROPERTIES**

IA11. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})(x + z = y + z \Longrightarrow x = y)$
IA12. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})((\sim z = 0) \Rightarrow (x \cdot z = y \cdot z \Longrightarrow x = y))$

**ADDITIVE AND MULTIPLICATIVE IDENTITY PROPERTIES**

IA13.1. $(\forall x \in \mathbb{Z})(x + 0 = x)$.
IA13.2. $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y = 0)$.
IA13.2. $(\forall x \in \mathbb{Z})(x \cdot 1 = x)$.

**ORDER PROPERTIES**

IA14. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x < y \Longleftrightarrow (\exists w \in \mathbb{Z})(0 < w \wedge x + w = y))$
IA15. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x \leq y \Longleftrightarrow (x < y \vee x = y))$
IA16. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})((x < y \wedge y < z) \Longrightarrow x < z)$
IA17. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})((x \leq y \wedge y \leq x) \Longrightarrow x = y)$
IA18. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})(x < y \Longrightarrow x + z < y + z)$
IA19. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})((x < y \wedge 0 < z) \Longrightarrow x \cdot z < y \cdot z)$
IA20. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})((x < y \vee y < x) \vee x = y)$

**THE NATURAL NUMBERS AND**
**THE PRINCIPLE OF MATHEMATICAL INDUCTION**

IA21.1. $1 \in \mathbb{N}$
IA21.2. $(\forall x)(x \in \mathbb{N} \Rightarrow x + 1 \in \mathbb{N})$
IA21.3. $(\forall S)\Big(\Big(S \subseteq \mathbb{N} \wedge (1 \in S \wedge (\forall u \in \mathbb{N})(u \in S \Longrightarrow u + 1 \in S))\Big) \Longrightarrow S = \mathbb{N}\Big)$
IA21.4. $(\forall x)(x \in \mathbb{N} \Longleftrightarrow (x \in \mathbb{Z} \wedge 0 < x))$

## 14.3 Some definitions and very simple theorems

Now that we have the axioms, let us start proving some theorems.

**THEOREM T1.** $0 < 1$.

**PROOF.** $1 \in \mathbb{N}$ by IA21.1.

On the other hand, $1 \in \mathbb{N} \Longleftrightarrow (1 \in \mathbb{Z} \wedge 0 < 1)$, by specializing IA21.4 to $x = 1$ (i.e., applying Rule $\forall_{out}$ to IA21.4 with $x = 1$).

Therefore $1 \in \mathbb{Z} \wedge 0 < 1$, by Rule $\Longleftrightarrow_{out}$.

And then $0 < 1$ by Rule $\wedge_{out}$.

**THE END**

**DEFINITION D1.** $2 = 1 + 1$.

**DEFINITION D2.** $3 = 2 + 1$.

**DEFINITION D3.** $4 = 3 + 1$.

**THEOREM T2.** $2 + 2 = 4$.

**PROOF.**

| | |
|---|---|
| $2 + 2 = 2 + 2$ | EQ1 |
| $2 + 2 = 2 + (1 + 1)$ | D1+EQSUB |
| $= (2 + 1) + 1$ | IA5 |
| $= 3 + 1$ | D2+EQSUB |
| $= 4$ | D3+EQSUB |

**THE END**

**THEOREM T3.** $2.2 = 4$.

**PROOF.**

| | |
|---|---|
| $2.2 = 2.2$ | EQ1 |
| $2.2 = 2.(1 + 1)$ | D1 |
| $= 2.1 + 2.1$ | IA9.1 |
| $= 2 + 2$ | IA13.2 |
| $= 4$ | T2 |

**THE END**

**THEOREM T4.** $(\forall x \in \mathbb{Z})(x.0 = 0)$.

**PROOF.** Let $a \in \mathbb{Z}$ be arbitrary. Then

| | |
|---|---|
| $a.0 = a.0$ | |
| $0 + 0 = 0$ | |
| $a.(0 + 0) = a.0$ | |

$$\begin{aligned} a.0 + a.0 &= a.0 \\ a.0 + 0 &= a.0 \\ a.0 + a.0 &= a.0 + 0 \\ a.0 &= 0 \\ (\forall x \in \mathbb{Z})&(x.0 = 0) \end{aligned}$$

**THE END**

EXERCISE: *Fill in the justifications in the above proof.*

**DEFINITION D4.** $(\forall x \in \mathbb{Z})(-x = 0 - x)$.

**THEOREM T5.** $-0 = 0$.

**PROOF.**
IA10 tells us that $0 - 0 = 0$ if and only if $0 = 0 + 0$. But $0 + 0 = 0$ by IA13.1. So $0 - 0 = 0$. Finally, D4 says that $-0$ is precisely $0 - 0$, so $-0 = 0$. **THE END**

**THEOREM T6.** $(\forall x \in \mathbb{Z})(x + (-x) = 0)$.

**PROOF.**
Let $a \in \mathbb{Z}$ be arbitrary.
Then $0 - a = -a \Longleftrightarrow 0 = a + (-a)$.
But $0 - a = -a$ by D4.
So $0 = a + (-a)$,
and then $a + (-a) = 0$.
Since $a \in \mathbb{Z}$ was arbitrary, $(\forall x \in \mathbb{Z})(x + (-x) = 0)$.

**THE END**

**THEOREM T7.** $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x - y = x + (-y))$.

**PROOF.**
Let $a \in \mathbb{Z}, b \in \mathbb{Z}$ be arbitrary.
Then $a - b = a + (-b) \Longleftrightarrow a = b + (a + (-b))$.
But $b+(a+(-b)) = (b+a)+(-b) = (a+b)+(-b) = a+(b+(-b)) = a+0 = a$.
So $a = b + (a + (-b))$, and then $a - b = a + (-b)$.
Since $a \in \mathbb{Z}, b \in \mathbb{Z}$ were arbitrary, $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x - y = x + (-y))$.

**THE END**

**THEOREM T8.** $(-1).(-1) = 1$.

**PROOF.**

$$\begin{aligned} (-1).(-1) &= (-1).(-1) + 0 \\ &= (-1).(-1) + (1 + (-1)) \\ &= (-1).(-1) + (1 + (-1).1) \\ &= (-1).(-1) + ((-1).1 + 1) \end{aligned}$$

$$
\begin{aligned}
&= ((-1).(-1) + (-1).1) + 1 \\
&= (-1).((-1) + 1) + 1 \\
&= (-1).(1 + (-1)) + 1 \\
&= (-1).0 + 1 \\
&= 0 + 1 \\
&= 1 + 0 \\
&= 1
\end{aligned}
$$

**THE END**

**THEOREM T9.** $(\forall x \in \mathbb{Z})((-1).x = -x)$.

**PROOF.** Let $a \in \mathbb{Z}$ be arbitrary. Then

$$
\begin{aligned}
(-1).a &= (-1).a + 0 \\
&= (-1).a + (a + (-a)) \\
&= ((-1).a + a) + (-a) \\
&= (a.(-1) + a) + (-a) \\
&= (a.(-1) + a.1) + (-a) \\
&= a.((-1) + 1) + (-a) \\
&= a.(1 + (-1)) + (-a) \\
&= a.0 + (-a) \\
&= 0 + (-a) \\
&= (-a) + 0 \\
&= -a\,.
\end{aligned}
$$

**THE END**

**THEOREM T10.** $(\forall x \in \mathbb{Z})(-(-x) = x)$.

**PROOF.** Let $a \in \mathbb{Z}$ be arbitrary. Then

$$
\begin{aligned}
-(-a) &= (-a).(-1) \\
&= (a.(-1)).(-1) \\
&= a.((-1).(-1)) \\
&= a.1 \\
&= a
\end{aligned}
$$

**THE END**

**DEFINITION D5.** $(\forall x \in \mathbb{Z})(x \text{ is even } \iff (\exists y \in \mathbb{Z})(x = 2.y))$.

**DEFINITION D6.** $(\forall x \in \mathbb{Z})((x \text{ is odd } \iff (\exists y \in \mathbb{Z})(x = 2.y + 1))$.

**THEOREM T11.** $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})((x \text{ is even } \wedge y \text{ is even }) \implies x{+}y \text{ is even })$

**PROOF.** Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ be arbitrary. Suppose $a$ and $b$ are even. Since $a$ is even, $(\exists u \in \mathbb{Z})(a = 2.u)$. Pick one such $u$ and call it $u_1$. Since $b$ is even,

$(\exists u \in \mathbb{Z})(b = 2.u)$. Pick one such $u$ and call it $u_2$. Then $a = 2.u_1$ and $b = 2.u_2$. So $a+b = 2.(u_1+u_2)$. So $(\exists u \in \mathbb{Z})(a+b = 2.u)$. So $a+b$ is even. **THE END**

**THEOREM T12.** $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})((x \text{ is even } \wedge y \text{ is odd }) \Longrightarrow x+y \text{ is odd })$

**PROOF.** Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ be arbitrary. Suppose $a$ is even and $b$ is odd. Since $a$ is even, $(\exists u \in \mathbb{Z})(a = 2.u)$. Pick one such $u$ and call it Bob. Since $b$ is odd, $(\exists u \in \mathbb{Z})(b = 2.u + 1)$. Pick one such $u$ and call it Betty. Then $a = 2 \cdot \text{Bob}$ and $b = 2.\text{Betty} + 1$. So $a + b = 2.(\text{Bob} + \text{Betty}) + 1$. So $(\exists u \in \mathbb{Z})(a + b = 2.u + 1)$. So $a + b$ is odd. **THE END**

**THEOREM T13.** $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})((x \text{ is odd } \wedge y \text{ is odd }) \Longrightarrow x+y \text{ is even })$

**PROOF.** Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ be arbitrary. Suppose $a$ and $b$ are odd. Since $a$ is odd, $(\exists u \in \mathbb{Z})(a = 2.u + 1$. Pick one such $u$ and call it $\alpha$. Since $b$ is odd, $(\exists u \in \mathbb{Z})(b = 2.u + 1)$. Pick one such $u$ and call it $\beta$. Then $a = 2\alpha + 1$ and $b = 2.\beta + 1$. So $a + b = (2.\alpha + 1) + (2.\beta + 1) = 2.(\alpha + \beta + 1)$. So $(\exists u \in \mathbb{Z})(a + b = 2.u)$. So $a + b$ is even. **THE END**

**THEOREM T14.** $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x \text{ is even} \Longrightarrow x.y \text{ is even })$

**PROOF.** Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ be arbitrary. Suppose $a$ is even. Then $(\exists u \in \mathbb{Z})(a = 2.u)$. Pick one such $u$ and call it $\bar{u}$. Then $a = 2.\bar{u}$. So $a.b = (2.\bar{u}).b = 2.(\bar{u}.b)$. So $(\exists u \in \mathbb{Z})(a.b = 2.u)$. So $a.b$ is even. **THE END**

**THEOREM T15.** $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})((x \text{ is odd } \wedge y \text{ is odd }) \Longrightarrow x.y \text{ is odd })$

**PROOF.** Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ be arbitrary. Suppose $a$ and $b$ are odd. Since $a$ is odd, $(\exists u \in \mathbb{Z})(a = 2.u + 1)$. Pick one such $u$ and call it $\mu$. Since $b$ is odd, $(\exists u \in \mathbb{Z})(b = 2.u + 1)$. Pick one such $u$ and call it $\nu$. Then $a = 2\mu + 1$ and $b = 2.\nu+1$. So $a.b = (2.\mu+1).(2.\nu+1) = 4.\mu.\nu+2.\mu+2.\nu+1 = 2(2.\mu.\nu+\mu+\nu)+1$. So $(\exists u \in \mathbb{Z})(a.b = 2.u + 1)$. So $a.b$ is odd. **THE END**

**THEOREM T16.** $(\forall x \in \mathbb{N})(1 \leq x)$.

**PROOF.** Let $S$ be the set of all $n \in \mathbb{N}$ such that $1 \leq n$. Then $1 \in S$, because $1 \in \mathbb{N}$ by IA21.1, and $1 \leq 1$ because of IA15 and the fact that $1 = 1$. Let us show that $(\forall u \in \mathbb{N})(u \in S \Longrightarrow u + 1 \in S)$. Let $u \in \mathbb{N}$ be arbitrary. Assume $u \in S$. Then $u \in \mathbb{N}$ and $1 \leq u$. So $1 = u \vee 1 < u$. On the other hand, $u < u+1$, because of IA14, since $0 < 1$, because $1 \in \mathbb{N}$. If $1 = u$, then $1 < u + 1$. If $1 < u$, thenIA16 tells us that $1 < u + 1$. So $1 < u + 1$ in all cases. Furthermore, $u + 1 \in \mathbb{N}$ because $u \in \mathbb{N}$. So $u + 1 \in S$. The PMI then tells us that $S = \mathbb{N}$. So every $x \in \mathbb{N}$ belongs to $S$, showing that every $x \in \mathbb{N}$ satisfies $1 \leq x$. **THE END**

**THEOREM T17.** $(\forall x \in \mathbb{Z})(0 < x \Longrightarrow 1 \leq x)$.

**PROOF.** Let $a \in \mathbb{Z}$ be arbitrary. Suppose $0 < a$. Then $a \in \mathbb{N}$ by I21.4. So $1 \leq a$ by T16. **THE END**

## 14.4 Some real theorems

Now we are going to state and prove a couple of less trivial theorems. First, the definition of absolute value:

**DEFINITION D6.** $(\forall x \in \mathbb{Z})((0 \leq x \Longrightarrow |x| = x) \wedge (x < 0 \Longrightarrow |x| = -x))$.

**THEOREM T18.** (The division algorithm, a.k.a. "Euclidean algorithm," for dividing by a natural number.)

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(x = q.y + r \wedge 0 \leq r \wedge r < y)$$

**PROOF.** Let $a \in \mathbb{Z}, b \in \mathbb{N}$ be arbitrary. Let $S$ be the set of all $n \in \mathbb{N}$ such that $(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = q \cdot b + r \wedge (0 \leq r \wedge r < b))$. We want to prove that $S = \mathbb{N}$. If $b = 1$ this is trivial, because in that case, if $n \in \mathbb{N}$ then $n = n \cdot b + 0$, so $n \in S$, because we cantake $q = n$, $r = 0$ as witnesses. If $b > 1$, then we will prove that $S = \mathbb{N}$ by induction. First of all, $1 \in S$, because $1 = 0. \cdot b + 1$, and $1 < b$ (since $b > 1$), so we may take $q = 0$, $r = 1$ as witnesses. Next, suppose that $n \in S$. Let us prove that $n + 1 \in S$. Since $n \in S$, we can pick $\bar{q} \in \mathbb{Z}$, $\bar{r} \in \mathbb{Z}$, such that $n = \bar{q} \cdot b + \bar{r}$, and $0 \leq \bar{r} < b$. Distinguish two cases, according to whether $\bar{r} + 1 < b$ or $\bar{r} + 1 = b$. If $\bar{r} + 1 < b$, then $n + 1 = \bar{q} \cdot b + r$, where $r = \bar{r} + 1$, and $0 \leq r < b$, so $n+1 \in S$. If $\bar{r}+1 = b$, then $n+1 = \bar{q} \cdot b + \bar{r} + 1 = \bar{q} \cdot b + b = (\bar{q}+1) \cdot b$, so $n + 1 \in S$ because we may take $q = \bar{q} + 1$ and $r = 0$ as witnesses. In either case, $n + 1 \in S$. It follows from the PMI that $S = \mathbb{N}$.

Now that we know that $S = \mathbb{N}$, we prove that $a$ has the desired property by considering three cases. First, look at the case when $0 < a$. Then $a \in \mathbb{N}$, so $a \in S$, and this implies that

$$(\exists q \in \mathbb{Z})(r \in \mathbb{Z})(a = q \cdot b + r \wedge (0 \leq r \wedge r < b))\,. \tag{14.4.1}$$

Next, look at the case when $a = 0$. Then $a = 0 \cdot b + 0$, so (14.4.1) is also true, because we can take $q = 0$, $r = 0$. Finally, look at the case when $a < 0$. Then $-a > 0$, so $-a \in \mathbb{N}$, and then $-a \in S$, so we can pick integers $\bar{q}, \bar{r}$ for which $-a = \bar{q} \cdot b + \bar{r}$, and $0 \leq \bar{r} < b$. Therefore $a = (-\bar{q}) \cdot b + (-\bar{r})$. But then $a = (-\bar{q} - 1) \cdot b + (b - \bar{r})$. If $\bar{r} > 0$, then $0 < b - \bar{r} < b$, so (14.4.1) holds, since we can take $q = -\bar{q} - 1$ and $r = b - \bar{r}$ as witnesses. If $\bar{r} = 0$, then $a = (-\bar{q}) \cdot b + 0$, so (14.4.1) holds, since we can take $q = -\bar{q}$ and $r = 0$ as witnesses.

Hence (14.4.1) holds in all cases. Since $a$ and $b$ were arbitrary, we have

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{N})(\exists q \in \mathbb{Z})(r \in \mathbb{Z})(a = q \cdot b + r \wedge (0 \leq r \wedge r < b))\,, \tag{14.4.2}$$

as desired. **THE END**

**THEOREM T19.** (The division algorithm, a.k.a. "Euclidean algorithm," for dividing by a nonzero integer.)

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})\Big(\sim y = 0 \Longrightarrow (\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(x = q.y + r \wedge 0 \leq r \wedge r < |y|)\Big)$$

**PROOF.** Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ be arbitrary. Assume that $\sim b = 0$. We want to prove that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = q.b + r \wedge 0 \leq r \wedge r < |b|) \tag{14.4.3}$$

We consider two cases, namely, $b > 0$ and $b < 0$. If $b > 0$, then we can apply Theorem T18 and conclude that (14.4.3) holds.

Now suppose that $b < 0$. Then $-b > 0$, so we can apply Theorem T18 and conclude that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(-a = q.(-b) + r \wedge 0 \leq r \wedge r < |b|)\,. \tag{14.4.4}$$

Pick one such $q, r$,and call them $\bar{q}$, $\bar{r}$. Then $\bar{q} \in \mathbb{Z}$, $\bar{r} \in \mathbb{Z}$, $0 \leq \bar{r} < |b|$, and $-a = \bar{q} \cdot (-b) + \bar{r}$. It follows that

$$a = \bar{q} \cdot b - \bar{r}\,.$$

If $\bar{r} = 0$, then (14.4.3) holds, since we can take $q = \bar{q}$ and $r = 0$ as witnesses. If $\bar{r} > 0$, then

$$a = \bar{q} \cdot b - \bar{r} = (\bar{q} + 1) \cdot b + (-b - \bar{r})\,,$$

and $0 \leq -b - \bar{r} < |b|$ (because $0 < \bar{r} < |b|$ and $-b = |b|$, so that $-b - \bar{r} = |b| - \bar{r}$), so (14.4.3) holds, since we can take $q = \bar{q} + 1$ and $r = -b - \bar{r}$ as witnesses.

Hence (14.4.3) holds in all cases. **THE END**

**THEOREM T20.** Every integer is even or odd, that is,

$$(\forall x \in \mathbb{Z})\Big((\exists k \in \mathbb{Z})(x = 2 \cdot k) \vee (\exists k \in \mathbb{Z})(x = 2 \cdot k + 1)\Big)\,.$$

**PROOF.** Let $a \in \mathbb{Z}$ be arbitrary. Apply the Euclidean algorithm with $y = 2$, to conclude that we may pick $kin\mathbb{Z}, r \in \mathbb{Z}$ such that $a = 2\dot{k} + r$ with $0 \leq r < 2$. Then $r = 0$ or $r = 1$. If $r = 0$, then $a$ is even. If $r = 1$, then $a$ is odd. **THE END**