MATHEMATICS 300 — FALL 1998

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 13. November 18, 1998

HOMEWORK ASSIGNMENT NO. 9, DUE ON MONDAY, NOVEMBER 23

1. Find integers a, b such that $37.a + 53.b = 1$.
2. Prove or disprove: there exist integers a, b such that $42.a + 91.b = 1$. If the numbers exist, find them.
3. Prove or disprove: there exist integers a, b such that $103.a + 107.b = 1$. If the numbers exist, find them.
4. Problems 2 and 3 in page 111 of the book.
5. How many 6-digit natural numbers are there having no repeated digits?
6. Write a formal proof of Theorem 5 of this handout. You **are** allowed to use Theorems 1, 2, 3, and 4.
7. Write an informal proof and a formal proof of Theorem 6 of this handout. You **are** allowed to use Theorems 1, 2, 3, 4, and 5. (Hint: pick $y = x/2$.)

MORE TYPOS IN HANDOUT NO. 11.

1. In page 13, step (15.&.&.&), the justification should be

   $$[\text{Rule 8, from (12) and (14)}]\,,$$

   rather than

   $$[\text{Rule 4, from (14)}]\,.$$

2. In page 14, step (5.&) of the proof of Theorem 4, the tautology should be $(\alpha \Leftrightarrow (\sim \alpha)) \Rightarrow \beta$ rather than $(\alpha \Rightarrow (\sim \alpha)) \Rightarrow \beta$.
3. In page 17, third line under the title "Axiomatic Set Theory" "NST.2" should be replaced by "NST.1".
4. In page 19, step (14.&.&.&.&) of the proof of Theorem 5, the justification should be

   $$[\text{Rule 4, from (11)}]\,,$$

   rather than

   $$[\text{Rule 4, from (13)}]\,.$$

THE AXIOMS OF REAL NUMBER ARITHMETIC AND OTHER NUMBER SYSTEMS

By now, you should be familiar with the following *number systems*:

1. The set $\mathbb{N}$ of *natural numbers*, also known as *positive integers* (this is the set of integers n such that $n \geq 1$).

2. The set $\mathbb{N}_{\geq 0}$ of *nonnegative integers* (so that $\mathbb{N}_{\geq 0} = \mathbb{N} \cup \{0\}$). Usually, a notation such as $\mathbb{Z}_+$ is used for this set.

3. The set $\mathbb{Z}$ of all *integers* (so that $\mathbb{Z} = \mathbb{N}_{\geq 0} \cup \{x \in \mathbb{R} : -x \in \mathbb{N}\}$).

4. The set $\mathbb{Z}_m$ of all *integers modulo m*. Here m is any natural number such that $m > 1$. By definition, $\mathbb{Z}_m$ consists of 0 and all the natural numbers n such that $n < m$. So, for example,

$$
\begin{aligned}
\mathbb{Z}_2 &= \{0,1\}\,,\\
\mathbb{Z}_3 &= \{0,1,2\}\,,\\
\mathbb{Z}_4 &= \{0,1,2,3\}\,,\\
&\ \vdots\\
\mathbb{Z}_{23} &= \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22\}\,,\\
&\ \vdots
\end{aligned}
$$

and so on. **Addition** and **multiplication** in $\mathbb{Z}_m$ are defined in the usual way, except that you must "reduce the result modulo m," that is, subtract m repeatedly until you end up with a number in $\mathbb{Z}_m$. For example, if you want to add 4 and 5 in $\mathbb{Z}_7$, you first get 9, but this is not acceptable because it is not in $\mathbb{Z}_7$, so you reduce modulo 7 by subtracting 7 and get

$$4 + 5 = 2 \quad \text{in} \quad \mathbb{Z}_7\,.$$

Similarly, if you multiply 4 and 5 in $\mathbb{Z}_7$, you first get 20, but this is not acceptable because it is not in $\mathbb{Z}_7$, so you reduce modulo 7 by subtracting 7 twice, and end up getting

$$4.5 = 6 \quad \text{in} \quad \mathbb{Z}_7\,.$$

Other examples of sums and products in $\mathbb{Z}_m$ are:

$$
\begin{aligned}
2+2 &= 0 \quad \text{in} \quad \mathbb{Z}_4\,,\\
2+2 &= 4 \quad \text{in} \quad \mathbb{Z}_5\,,\\
2+2 &= 4 \quad \text{in} \quad \mathbb{Z}_{11}\,,\\
2+3 &= 1 \quad \text{in} \quad \mathbb{Z}_4\,,\\
2+3 &= 0 \quad \text{in} \quad \mathbb{Z}_5\,,\\
2+3 &= 5 \quad \text{in} \quad \mathbb{Z}_{11}\,,\\
8+7 &= 2 \quad \text{in} \quad \mathbb{Z}_{13}\,,\\
8+7 &= 15 \quad \text{in} \quad \mathbb{Z}_{23}\,,\\
8+7 &= 15 \quad \text{in} \quad \mathbb{Z}_{93}\,,\\
2.2 &= 0 \quad \text{in} \quad \mathbb{Z}_4\,,\\
2.2 &= 4 \quad \text{in} \quad \mathbb{Z}_5\,,\\
2.2 &= 4 \quad \text{in} \quad \mathbb{Z}_{11}\,,
\end{aligned}
$$

$$\begin{aligned}
2.3 &= 2 \text{ in } \mathbb{Z}_4\,,\\
2.3 &= 1 \text{ in } \mathbb{Z}_5\,,\\
2.3 &= 6 \text{ in } \mathbb{Z}_{11}\,,\\
8.7 &= 4 \text{ in } \mathbb{Z}_{13}\,,\\
8.7 &= 10 \text{ in } \mathbb{Z}_{23}\,,\\
8.7 &= 56 \text{ in } \mathbb{Z}_{93}\,.
\end{aligned}$$

5. The set $\mathbb{Q}$ of all *rational numbers*. By definition,

$$\mathbb{Q} = \{x \in \mathbb{R} : (\exists n)(\exists m)((n \in \mathbb{Z} \wedge m \in \mathbb{Z}) \wedge (n \neq 0 \wedge n.x = m))\}\,.$$

   In other words, a rational number is a number that is a quotient of two integers. ("Ratio" is an old word for "quotient.")

6. The set $\mathbb{R}$ of all *real numbers.*

7. The set $\mathbb{C}$ of all *complex numbers.* By definition, a *complex number* is an ordered pair of real numbers, so the set $\mathbb{C}$ is just $\mathbb{R} \times \mathbb{R}$. Complex numbers are added and multiplied as follows: if $a, b, c, d \in \mathbb{R}$, then

$$(a,b) + (c,d) = (a+c, b+d) \qquad \text{and} \qquad (a,b).(c,d) = (ac - bd, ad + bc)\,.$$

   Also, complex numbers can be multiplied by real numbers:

$$a.(b,c) = (a.b, a.c)\,.$$

   The complex numbers $(1,0)$ and $(0,1)$ are called 1 and i, respectively. Then, if a, b are arbitrary real numbers, we have

$$(a,b) = a.1 + b.i\,.$$

   We will simply write $a + bi$ instead of (a,b) or $a.1 + b.i$. Notice that, according to our definition of multiplication of complex numbers, $i.i = -1$.

REMARK. The above list consists of *infinitely many* number systems. Why do I say "infinitely many" and not just "seven"? That's because Item 4 in our list is not just *one* system, but a collection of infinitely many such systems, since there is one system $\mathbb{Z}_m$ for each m.

Now we would like to be able to prove various properties of these number systems. We will do this by starting with some *axioms* or *postulates*, and then using them to prove lots of other things.

First, let us write down some basic properties that we know are true for the *real* numbers. In the following list, you should think of the universe of discourse as being $\mathbb{R}$, the set of real numbers. However, notice that $\mathbb{R}$ itself is never mentioned in these statements, so we can ask whether they are valid over the other number systems that we have listed above.

These properties will be used as *axioms* for the real number system. They involve

1. two primitive constants, namely, "0" and "1,"

2. six primitive binary predicates, namely, "$=$", "$\neq$", "$<$", "$\leq$", "$>$", and "$\geq$", and

3. four primitive two-variable function symbols, namely, "+" , "−" , "." , and "/" . (Sometimes, we will write $\frac{a}{b}$ rather than a/b.

4. one primitive 1-variable function symbol, namely, "−".

REMARK. You should not confuse the two-variable function symbol "−" (as in "$7-3=4$") with the one-variable function symbol "−" (as in "$(-3).(-3)=9$"). Sometimes, both symbols are used in the same formula, e.g. if we write

$$8-13=-5\,,$$

in which case the leftmost "−" is the 2-variable "−" and the rightmost "−" is the 1-variable "−". ♢

REMARK. In principle, in the axioms we will write below, the universe of discourse will be $\mathbb{R}$, so when we write an expression such as $(\forall x)$ this is meant to be exacty equivalent to $(\forall x\in\mathbb{R})$. This, however, is only temporary. Most of the axioms make perfect sense in other number systems as well, and the question whether any of them—and if so which ones—are valid in other systems will keep us busy for a while later on. ♢

There will be **24 axioms**. They will be displayed in the next page.

COMMENTS ON THE AXIOMS: The first eight axioms (except for Axiom A2) are essentially "axiom-definitions," telling us how the symbols $\neq$, $\geq$, $<$, $\leq$, $-$ (the binary function sysmbol), $/$, and $-$ (the 1-variable function symbol) can be expressed in terms of the other symbols. One could equally well adopt the point of view that these symbols are not "primitive," and Axioms A1, A3, A4, A5, A6, A7 and A8 "define what theese symbols mean." If on takes this point of view, then these axioms should be thought of as definitions rather than real axioms. Naturally, when we want to prove theorems it makes no difference which point of view we espouse. Axiom A2 is also—in a sense—a kind of definition, because it tells us how the predicate $>$ can be defined in terms of the more basic notion of "positive number," i.e. "number x such that $x>0$."

Axioms A9, A13 and A14 say that addition, subtraction, and multiplication are binary operations *defined on the whole universe of numbers.* To understand the importance of this, can compare with the operation of division. Axiom A19 does **not** say that the quotient x/y exists for all x, y. It only tells us that the quotient exists **if** $y\neq 0$.

Axioms A10 and A11 are the usual **commutative law** and **associative law** of addition. Axioms A16 and A17 are the commutative law and associative law of multiplication. Axiom A17 is the **distributive law** of multiplication with respect to addition. Axioms A12 and A18 describe the basic properties of 0 and 1. (The appropriate mathematical jargon is "0 is an additive identity" and "1 is a multiplicative identity.")

Axioms A21, A22 and A23 describe the basic properties of the "$>$" relation: A21 says that the sum of two positive numbers is positive, A22 says that the product of two psitive numbers is positive, and A23 says, roughly, that every number is either positive, zero, or negative.

Axiom A20 may look weird to you. Of course you know that one is not equal to zero!!! So what is the point? The point is, simply, that precisely because we "know" that $1\neq 0$, it is quite reasonable to put this as an axiom. (After all, axioms are things that we take for granted, things that we aceept without discussion.) The only possible objection to this axiom might be that perhaps it is not needed. Actually, **Axiom A20 is indispensable.** Without this axiom, it would not be possible to prove that the are any real numbers at all other than zero.

RECOMMENDED EXERCISE. Prove that, if we take a number system consisting of just one number—called 0—and define addition, subtraction and multiplication in the only possible way—namely, $0+0=0$, $0-0=0$, $0.0=0$—and then define 1 to be 0, and take the set of "positive" numbers to be the empty set (so that $x > y$ is always false for x and y in our system, that is, for $x = y = 0$) then **all the axioms are true except for A20.** Conclude that **it is not possible to deduce A20 from the other axioms.**

THE 24 BASIC AXIOMS FOR THE REAL NUMBER SYSTEM

A1. $(\forall x)(\forall y)(x \neq y \Leftrightarrow (\sim x = y))$.

A2. $(\forall x)(\forall y)\Big(x > y \Leftrightarrow x - y > 0)$.

A3. $(\forall x)(\forall y)(x \geq y \Leftrightarrow (x = y \vee x > y))$.

A4. $(\forall x)(\forall y)(x < y \Leftrightarrow y > x)$.

A5. $(\forall x)(\forall y)(x \leq y \Leftrightarrow (x = y \vee x < y))$.

A6. $(\forall x)(\forall y)(\forall z)(x - y = z \Leftrightarrow x = y + z)$.

A7. $(\forall x)(\forall y)(\forall z)(z = x/y \Leftrightarrow (y \neq 0 \wedge z.y = x))$

A8. $(\forall x)(-x = 0 - x)$.

A9. $(\forall x)(\forall y)(\exists z)(x + y = z)$.

A10. $(\forall x)(\forall y)(x + y = y + x)$.

A11. $(\forall x)(\forall y)(\forall z)\Big((x + y) + z = x + (y + z)\Big)$.

A12. $(\forall x)(0 + x = x)$.

A13. $(\forall x)(\forall y)(\exists z)(x - y = z)$.

A14. $(\forall x)(\forall y)(\exists z)(x.y = z)$.

A15. $(\forall x)(\forall y)(x.y = y.x)$.

A16. $(\forall x)(\forall y)(\forall z)\Big((x.y).z = x.(y.z)\Big)$.

A17. $(\forall x)(\forall y)(\forall z)\Big((x + y).z = x.z + y.z\Big)$.

A18. $(\forall x)(1.x = x)$.

A19. $(\forall x)(\forall y)(y \neq 0 \Rightarrow (\exists z)(z = x/y)\Big)$.

A20. $1 \neq 0$.

A21. $(\forall x)(\forall y)\Big((x > 0 \wedge y > 0) \Rightarrow x + y > 0\Big)$.

A22. $(\forall x)(\forall y)\Big((x > 0 \wedge y > 0) \Rightarrow x.y > 0\Big)$.

A23. $(\forall x)((x > 0 \vee x = 0) \vee x > 0)$.

A24. $\sim 0 > 0$.

In addition, we will always assume the validity of the three axioms about equality, already presented in handout No. 2:

Eq1. $(\forall x)(x = x)$.

Eq2. $(\forall x)(\forall y)(x = y \Rightarrow y = x)$.

Eq3. $(\forall x)(\forall y)(\forall z)((x = y \wedge y = z) \Rightarrow x = z)$.

SOME EXAMPLES OF PROOFS

Here are some examples of proofs, using the axioms of real arithmetic plus the axioms on equality.

First, let us define the numbers 2, 3 and 4.

DEFINITION: $2 = 1 + 1$.

DEFINITION: $3 = 2 + 1$.

DEFINITION: $4 = 3 + 1$.

Now we can prove our first theorem. I am sure this result is not new to you, but before you laugh at the triviality of our theorem, remember that

> **At this point our objective is not to discover new mathematical truths.**
>
> **What we are trying to do is**
>
> **a. to test our rules by making sure that they enable us to prove what we want to be able to prove,**
>
> **and**
>
> **b. learn how to play the game of proving things by strictly obeying the rules.**

THEOREM 1: $\boxed{4 = 2 + 2}$.

INFORMAL PROOF: By definition, $4 = 3 + 1$, and $3 = 2 + 1$, so $4 = (2 + 1) + 1$. By the associative law, $(2 + 1) + 1 = 2 + (1 + 1)$. So $4 = 2 + (1 + 1)$. By the definition of 2, $1 + 1 = 2$. So $4 = 2 + 2$. **QED**

FORMAL PROOF:

(1)	$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$.	[Axiom A11]
(2)	$(\forall y)(\forall z)((2 + y) + z = 2 + (y + z))$.	[Rule 4, from (1)]
(3)	$(\forall z)((2 + 1) + z = 2 + (1 + z))$.	[Rule 4, from (2)]
(4)	$(2 + 1) + 1 = 2 + (1 + 1)$.	[Rule 4, from (3)]
(5)	$4 = 3 + 1$.	[Definition of "4"]
(6)	$3 = 2 + 1$.	[Definition of "3"]
(7)	$2 = 1 + 1$.	[Definition of "2"]
(8)	$4 = (2 + 1) + 1$.	[Rule 8, from (5) and (6)]
(9)	$4 = 2 + (1 + 1)$.	[Rule 8, from (4) and (7)]
(10)	$4 = 2 + 2$.	[Rule 8, from (6) and (8)]

QED

THEOREM 2: $1 > 0$.

INFORMAL PROOF: Axiom A23 says that either $1 > 0$ or $1 = 0$ or $0 > 1$. The possibility that $1 = 0$ is excluded by Axiom A20. So $1 > 0$ or $0 > 1$.

Assume that $0 > 1$. Then Axiom A2 tells us that $0 - 1 > 0$, and Axiom A8 says that $0 - 1 = -1$. So $-1 > 0$. We would like to conclude from this that $1 > 0$. The reason is that, since $-1 > 0$, Axiom A22 says that $(-1).(-1) > 0$. So we would get the conclusion we want if we could prove that $(-1).(-1) = 1$.

To prove that $(-1).(-1) = 1$, we write

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

This gives us what we want, provided we show that $(-1).0 = 0$. Let us show that $x.0 = 0$ for all x. Let a be arbitary. Then

$$a.0 = a.(0 + 0) = a.0 + a.0\,.$$

Let $b = 0 - a.0$, so $b + a.0 = 0$. Then

$$0 = b + a.0 = b + a.(0 + 0) = b + (a.0 + a.0) = (b + a.0) + a.0 = 0 + a.0 = a.0\,.$$

So $a.0 = 0$. Since a was arbitrary, we have $(\forall x)(x.0 = 0)$.
Therefore $(-1).0 = 0$. Since $(-1).(-1) = (-1).0 + 1$, we have $(-1).(-1) = 0 + 1 = 1$. So $(-1).(-1) = 1$, as desired.
We now go back to our main proof. We have shown that $(-1).(-1) = 1$. Since we are assuming that $0 > 1$, and we know that this implies $-1 > 0$, Axiom A22 enables us to conclude that $1 > 0$. Summarizing: we have shown that if $0 > 1$ then $1 > 0$. Also, we know that either $1 > 0$ or $0 > 1$. We have thus shown that there are only two possible cases, and in both cases $1 > 0$. So $1 > 0$.
QED

FORMAL PROOF:

COMMENT: In the first 12 steps we establish that $1 > 0 \vee 0 > 1$, *using Axioms A23 and A20. Since A20 uses "$\neq$", we also need Axiom A1 to know what "$\neq$" means.*

(1)	$(\forall x)((x > 0 \vee x = 0) \vee 0 > x)\,.$	[Axiom A23]
(2)	$(1 > 0 \vee 1 = 0) \vee 0 > 1\,.$	[Rule 4, from (1)]
(3)	$1 \neq 0\,.$	[Axiom A20]
(4)	$(\forall x)(\forall y)(x \neq y \Leftrightarrow (\sim x = y))\,.$	[Axiom A1]
(5)	$(\forall y)(1 \neq y \Leftrightarrow (\sim 1 = y))\,.$	[Rule 4, from (4)]
(6)	$1 \neq 0 \Leftrightarrow (\sim 1 = 0)\,.$	[Rule 4, from (5)]
(7)	$1 \neq 0 \Rightarrow ((1 \neq 0 \Leftrightarrow (\sim 1 = 0)) \Rightarrow (\sim 1 = 0))\,.$	[Tautology $\alpha \Rightarrow ((\alpha \Leftrightarrow \beta) \Rightarrow \alpha)$]
(8)	$(1 \neq 0 \Leftrightarrow (\sim 1 = 0)) \Rightarrow (\sim 1 = 0)\,.$	[Modus Ponens from (3) and (7)]
(9)	$\sim 1 = 0\,.$	[Modus Ponens from (6) and (8)]
(10)	$((1 > 0 \vee 1 = 0) \vee 0 > 1) \Rightarrow ((\sim 1 = 0) \Rightarrow (1 > 0 \vee 0 > 1))\,.$	[Tautology $((\alpha \vee \beta) \vee \gamma) \Rightarrow ((\sim \beta) \Rightarrow (\alpha \vee \gamma))$]
(11)	$(\sim 1 = 0) \Rightarrow (1 > 0 \vee 0 > 1)\,.$	[Modus Ponens from (2) and (10)]
(12)	$1 > 0 \vee 0 > 1\,.$	[Modus Ponens from (9) and (11)]

COMMENT: We now set out to prove that $0 = 0.x$ *for every* x. *This is going to take us 41 steps. We first bring in various axioms that will be needed in the proof.*

(13)	$(\forall x)(0 + x = x)\,.$	[Axiom A12]
(14)	$0 + 0 = 0\,.$	[Rule 4, from (13)]
(15)	$(\forall x)(\forall y)(\forall z)((x + y).z = x.z + y.z)\,.$	[Axiom A17]
(16)	$(\forall y)(\forall z)((0 + y).z = 0.z + y.z)\,.$	[Rule 4, from (15)]
(17)	$(\forall z)((0 + 0).z = 0.z + 0.z)\,.$	[Rule 4, from (16)]
(18)	$(\forall z)(0.z = 0.z + 0.z)\,.$	[Rule 8, from (14) and (17)]
(19)	$(\forall x)(\forall y)(\exists z)(x.y = z)\,.$	[Axiom A14]
(20)	$(\forall y)(\exists z)(0.y = z)\,.$	[Rule 4, from (19)]
(21)	$(\forall x)(\forall y)(\exists z)(x - y = z)\,.$	[Axiom A13]
(22)	$(\forall x)(\forall y)(\forall z)(x - y = z \Leftrightarrow x = y + z)\,.$	[Axiom A6]
(23)	$(\forall y)(\exists z)(0 - y = z)\,.$	[Rule 4, from (21)]
(24)	$(\forall x)(\forall y)(x + y = y + x)\,.$	[Axiom A10]
(25)	$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))\,.$	[Axiom A11]
(26.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(27.&)	$0.a = 0.a + 0.a\,.$	[Rule 4, from (18)]
(28.&)	$(\exists z)(0.a = z)\,.$	[Rule 4, from (20)]
(29.&.&)	Let b be such that $0.a = b\,.$	[Preparation to apply Rule 6]
(30.&.&)	$b = b + b\,.$	[Rule 8, from (27) and (29)]
(31.&.&)	$(\exists z)(0 - b = z)\,.$	[Rule 4, from (23)]

(32.&.&.&) Let c be such that $0-b=c$. [Preparation to apply Rule 6]
(33.&.&.&) $(\forall y)(\forall z)(0-y=z \Leftrightarrow 0=y+z)$. [Rule 4, from (22)]
(34.&.&.&) $(\forall z)(0-b=z \Leftrightarrow 0=b+z)$. [Rule 4, from (33)]
(35.&.&.&) $0-b=c \Leftrightarrow 0=b+c$. [Rule 4, from (34)]
(36.&.&.&) $(0-b=c \Leftrightarrow 0=b+c) \Rightarrow (0-b=c \Rightarrow 0=b+c)$. [Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\alpha \Rightarrow \beta)$]
(37.&.&.&) $0-b=c \Rightarrow 0=b+c$. [Modus Ponens from (35) and (36)]
(38.&.&.&) $0=b+c$. [Modus Ponens from (32) and (37)]
(39.&.&.&) $0+b=b$. [Rule 4, from (13)]
(40.&.&.&) $(\forall y)(b+y=y+b)$. [Rule 4, from (24)]
(41.&.&.&) $b+c=c+b$. [Rule 4, from (40)]
(42.&.&.&) $0=c+b$. [Rule 8, from (41)]
(43.&.&.&) $(c+b)+b=b$. [Rule 8, from (39) and (42)]
(44.&.&.&) $(\forall y)(\forall z)((c+y)+z=c+(y+z))$. [Rule 4, from (25)]
(45.&.&.&) $(\forall z)((c+b)+z=c+(b+z))$. [Rule 4, from (44)]
(46.&.&.&) $(c+b)+b=c+(b+b)$. [Rule 4, from (45)]
(47.&.&.&) $c+(b+b)=b$. [Rule 8, from (43) and (46)]
(48.&.&.&) $c+b=b$. [Rule 8, from (30) and (47)]
(49.&.&.&) $0=b$. [Rule 8, from (42) and (48)]
(50.&.&) $0=b$. [Rule 6, from (32) and (49)]
(51.&.&) $0=0.a$. [Rule 8, from (29) and (50)]
(52.&) $0=0.a$. [Rule 6, from (29) and (51)]
(53) $(\forall x)(0=0.x)$. [Rule 5, from (26) and (52)]

COMMENT: We have now proved that $0=0.x$ for all x. Next, we apply this to $x=-1$, and use the result to prove that $(-1).(-1)=0$. This is going to take us 41 steps.

(54) $(\forall x)(-x=0-x)$. [Axiom A8]
(55) $-1=0-1$.[Rule 4, from (14)]
(56) $(\forall y)(\exists z)(0-y=z)$. [Rule 4, from (21)]
(57) $(\exists z)(0-1=z)$. [Rule 4, from (56)]
(58.&) Let d be such that $0-1=d$. [From (57), preparation to apply Rule 6]
(59.&) $0=0.d$. [Rule 4, from (53)]
(60.&) $(\forall y)(\exists z)(d.y=z)$. [Rule 4, from (19)]
(61.&) $(\exists z)(d.d=z)$. [Rule 4, from (60)]
(62.&.&) Let m be such that $d.d=m$. [From (61), preparation to apply Rule 6]
(63.&.&) $0+m=m$. [Rule 4, from (13)]
(64.&.&) $(\forall y)(\forall z)(0-y=z \Leftrightarrow 0=y+z)$. [Rule 4, from (22)]
(65.&.&) $(\forall z)(0-1=z \Leftrightarrow 0=1+z)$. [Rule 4, from (64)]
(66.&.&) $0-1=d \Leftrightarrow 0=1+d$. [Rule 4, from (65)]
(67.&.&) $(0-1=d \Leftrightarrow 0=1+d) \Rightarrow (0-1=d \Rightarrow 0=1+d)$. [Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\alpha \Rightarrow \beta)$]
(68.&.&) $0-1=d \Rightarrow 0=1+d$. [Modus Ponens from (66) and (67)]
(69.&.&) $0=1+d$. [Modus Ponens from (58) and (68)]
(70.&.&) $(1+d)+m=m$. [Rule 8, from (63) and (69)]
(71.&.&) $(\forall y)(\forall z)((1+y)+z=1+(y+z))$. [Rule 4, from (25)]
(72.&.&) $(\forall z)((1+d)+z=1+(d+z))$. [Rule 4, from (71)]
(73.&.&) $(1+d)+m=1+(d+m)$. [Rule 4, from (72)]
(74.&.&) $1+(d+m)=m$. [Rule 8, from (70) and (73)]
(75.&.&) $(\forall y)(\forall z)((1+y).z=1.z+y.z)$. [Rule 4, from (15)]
(76.&.&) $(\forall z)((1+d).z=1.z+d.z)$. [Rule 4, from (75)]
(77.&.&) $(1+d).d=1.d+d.d$. [Rule 4, from (76)]
(78.&.&) $(1+d).d=1.d+m$. [Rule 8, from (62) and (77)]
(79.&.&) $0.d=1.d+m$. [Rule 8, from (69) and (78)]
(80.&.&) $0=1.d+m$. [Rule 8, from (59) and (79)]

(81.&.&)	$(\forall x)(1.x = x)$.	[Axiom A18]
(82.&.&)	$1.d = d$.	[Rule 4, from (81)]
(83.&.&)	$0 = d + m$.	[Rule 8, from (80) and (82)]
(84.&.&)	$1 + 0 = m$.	[Rule 8, from (74) and (83)]
(85.&.&)	$(\forall y)(1 + y = y + 1)$.	[Rule 4, from (24)]
(86.&.&)	$1 + 0 = 0 + 1$.	[Rule 4, from (85)]
(87.&.&)	$0 + 1 = m$.	[Rule 8, from (84) and (86)]
(88.&.&)	$0 + 1 = 1$.	[Rule 4, from (13)]
(89.&.&)	$1 = m$.	[Rule 8, from (87) and (88)]
(90.&.&)	$1 = d.d$.	[Rule 8, from (62) and (89)]
(91.&)	$1 = d.d$.	[Rule 6, from (62) and (90)]
(92.&)	$-1 = d$.	[Rule 8, from (55) and (58)]
(93.&)	$1 = (-1).(-1)$.	[Rule 8, from (91) and (92)]
(94)	$1 = (-1).(-1)$.	[Rule 6, from (58) and (93)]

COMMENT: We are now ready for the finish. Just a few more steps (23 of them) to prove that if $0 > 1$ *then* $1 > 0$.

(95.&)	Assume $0 > 1$.	[Preparation to apply Rule 33]
(96.&)	$(\forall x)(\forall y)(x > y \Leftrightarrow x - y > 0)$.	[Axiom A2]
(97.&)	$(\forall y)(0 > y \Leftrightarrow 0 - y > 0)$.	[Rule 4, from (96)]
(98.&)	$0 > 1 \Leftrightarrow 0 - 1 > 0$.	[Rule 4, from (97)]
(99.&)	$(0 > 1 \Leftrightarrow 0 - 1 > 0) \Rightarrow (0 > 1 \Rightarrow 0 - 1 > 0)$.	[Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\alpha \Rightarrow \beta)$]
(100.&)	$0 > 1 \Rightarrow 0 - 1 > 0$.	[Modus Ponens from (98) and (99)]
(101.&)	$0 - 1 > 0$.	[Modus Ponens from (95) and (100)]
(102.&.&)	Let n be such that $0 - 1 = n$.	[From (57), preparation to apply Rule 6]
(103.&.&)	$n > 0$.	[Rule 8, from (101) and (102)]
(104.&.&)	$(\forall x)(\forall y)((x > 0 \wedge y > 0) \Rightarrow x.y > 0)$.	[Axiom A22]
(105.&.&)	$(\forall y)((n > 0 \wedge y > 0) \Rightarrow n.y > 0)$.	[Rule 4, from (104)]
(106.&.&)	$(n > 0 \wedge n > 0) \Rightarrow n.n > 0$.	[Rule 4, from (105)]
(107.&.&)	$((n > 0 \wedge n > 0) \Rightarrow n.n > 0) \Rightarrow (n > 0 \Rightarrow n.n > 0)$.	[Tautology $((\alpha \wedge \alpha) \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \beta)$]
(108.&.&)	$n > 0 \Rightarrow n.n > 0$.	[Modus Ponens from (106) and (107)]
(109.&.&)	$n.n > 0$.	[Modus Ponens from (103) and (108)]
(110.&.&)	$(0 - 1).(0 - 1) > 0$.	[Rule 8 from (102) and (109)]
(111.&.&)	$(-1).(-1) > 0$.	[Rule 8 from (55) and (110)]
(112.&.&)	$1 > 0$.	[Rule 8 from (94) and (111)]
(113.&)	$1 > 0$.	[Rule 6 from (102) and (112)]
(114)	$0 > 1 \Rightarrow 1 > 0$.	[Rule 3 from (95) and (113)]
(115)	$(1 > 0 \vee 0 > 1) \Rightarrow ((0 > 1 \Rightarrow 1 > 0) \Rightarrow 1 > 0)$.	[Tautology $(\alpha \vee \beta) \Rightarrow ((\beta \Rightarrow \alpha) \Rightarrow \alpha)$]
(116)	$(0 > 1 \Rightarrow 1 > 0) \Rightarrow 1 > 0$.	[Modus Ponens from (12) and (115)]
(117)	$1 > 0$.	[Modus Ponens from (114) and (116)]

QED

THEOREM 3: $2 \neq 0$.

INFORMAL PROOF: We already know that $1 > 0$. Axiom A21 then implies that $1 + 1 > 0$. Since $2 = 1 + 1$, we have $2 > 0$. If 2 was equal to 0, then $2 > 0$ would imply $0 > 0$, contradicting Axiom A24. So $2 \neq 0$. **QED**

FORMAL PROOF: First insert here the proof that $1 > 0$. That's 117 steps. Then let us go on.

(118) $(\forall x)(\forall y)((x>0 \wedge y>0) \Rightarrow x+y>0)$. [Axiom A21]
(119) $(\forall y)((1>0 \wedge y>0) \Rightarrow 1+y>0)$. [Rule 4, from (118)]
(120) $(1>0 \wedge 1>0) \Rightarrow 1+1>0$. [Rule 4, from (119)]
(121) $((1>0 \wedge 1>0) \Rightarrow 1+1>0) \Rightarrow (1>0 \Rightarrow 1+1>0)$. [Tautology $((\alpha \wedge \alpha) \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \beta)$]
(122) $1>0 \Rightarrow 1+1>0$. [Modus Ponens from (120) and (121)]
(123) $1+1>0$. [Modus Ponens from (117) and (122)]
(124) $2=1+1$. [Definition of "2"]
(125) $2>0$. [Rule 8, from (123) and (124)]
(126.&) Assume $2=0$. [Preparation to apply Rule 3]
(127.&) $0>0$. [Rule 8, from (125) and (126)]
(128) $2=0 \Rightarrow 0>0$. [Rule 3, from (126) and (127)]
(129) $\sim 0>0$. [Axiom A24]
(130) $(2=0 \Rightarrow 0>0) \Rightarrow ((\sim 0>0) \Rightarrow (\sim 2=0))$. [Tautology $(\alpha \Rightarrow \beta) \Rightarrow ((\sim \beta) \Rightarrow (\sim \alpha))$]
(131) $(\sim 0>0) \Rightarrow (\sim 2=0)$. [Modus Ponens from (128) and (130)]
(132) $\sim 2=0$. [Modus Ponens from (129) and (131)]
(133) $(\forall x)(\forall y)(x \neq y \Leftrightarrow (\sim x=y))$. [Axiom A1]
(134) $(\forall y)(2 \neq y \Leftrightarrow (\sim 2=y))$. [Rule 4 from (133)]
(135) $2 \neq 0 \Leftrightarrow (\sim 2=0)$. [Rule 4 from (134)]
(136) $(2 \neq 0 \Leftrightarrow (\sim 2=0)) \Rightarrow ((\sim 2=0) \Rightarrow 2 \neq 0)$. [Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\beta \Rightarrow \alpha)$]
(137) $(\sim 2=0) \Rightarrow 2 \neq 0$. [Modus Ponens from (135) and (136)]
(138) $2 \neq 0$. [Modus Ponens from (132) and (137)]

QED

THEOREM 4: $(\exists x)(x=1/2)$.
INFORMAL PROOF: We already know that $2 \neq 0$. So axiom A19 tells us that $1/2$ exists. **QED**
FORMAL PROOF: First insert the proof that $2 \neq 0$. That's 138 steps. Then go on as follows.

(139) $(\forall x)(\forall y)(y \neq 0 \Rightarrow (\exists z)(z=x/y))$. [Axiom A19]
(140) $(\forall y)(y \neq 0 \Rightarrow (\exists z)(z=1/y))$. [Rule 4, from (139)]
(141) $2 \neq 0 \Rightarrow (\exists z)(z=1/2)$. [Rule 4, from (140)]
(142) $(\exists z)(z=1/2)$. [Modus Ponens, from (138) and (141)]
(143.&) Let a be such that $a=1/2$. [From (142), preparation to apply Rule 6]
(144.&) $(\exists x)(x=1/2)$. [Rule 7, from (143)]
(145) $(\exists x)(x=1/2)$. [Rule 6, from (143) and (144)]

QED

From now on, we allow the use of previous proved theorems in a proof.

THEOREM 5: $(\forall x)(\exists y)(y+y=x)$.

INFORMAL PROOF: We know that there exists x such that $x=1/2$. So let $a=1/2$. Let u be arbitrary. Then there exists z such that $a.u=z$, by Axiom A14. Pick a b such that $a.u=b$. Then $b+b=a.u+a.u=(a+a).u=(1.a+1.a).u=((1+1).a).u=(2.a).u$.

Now, Axiom A7 tells us that $a=1/2 \Leftrightarrow (2 \neq 0 \wedge 2.a=1)$. Since $a=1/2$, we can conclude that $2 \neq 0 \wedge 2.a=1$. So in particular $2.a=1$. Since $b+b=(2.a).u$, we find that $b+b=1.u$, so $b+b=u$. Therefore $(\exists y)(y+y=u)$. Since u was arbitrary, we have proved that $(\forall x)(\exists y)(y+y=u)$. **QED**

THEOREM 6: $(\forall x)(x>0 \Rightarrow (\exists y)(y>0 \wedge x>y))$.