MATHEMATICS 300 — SPRING 1997

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 13. April 3, 1997

READING ASSIGNMENTS SO FAR

- For the week of January 28 and 30, you have to read *all of Chapter 1.* Plus, of course, the first handout.
- For the week of February 4 and 6, you have to read *Sections 1, 2 and 3 of Chapter 2.*
- For the week of February 11 and 13, you have to read *Sections 2.4, 3.1 and 3.2.*
- For the week of February 18 and 20, you have to read *Sections 3.3 and 3.4.*
- No new reading assignment for the week of February 25 and 27.
- For the weeks of March 4-6 and 11-13, you have to read *Sections 3.4 and 3.5.*
- For the week of March 25-27, you have to read *Handout No. 10* (very carefully) and the article by P. R. Halmos (Handout No. 12).
- For the week of April 8-10, you have to read this handout (No. 13), very carefully.

HOMEWORK ASSIGNMENTS SO FAR

(1) *Originally due on Tuesday, January 28. The deadline was subsequently extended to February 4.* Page 14, Problem 4; Page 15, Problem 7; Page 26, Problem 10; Page 27, Problem 11; Page 37, Problems 2 and 8.

(2) *Due Tuesday, February 4.* Page 14, Problem 5; Page 47, Problems 1 (parts (a), (j), (q)), 2, and 3; Page 48, Problems 5 (parts (a), (c)) and 7; Page 49, Problems 11 and 12.

(3) *Due Tuesday, February 11.* See Handout No. 3.

(4) *Due Tuesday, February 18.* Page 70, problems 4, 6, 8, 9. Page 72, problem 14. Page 73, problem 16. Page 76, problems 6 and 9.

(5) **Optional homework assignments**, *due Tuesday, February 25.* See handout No.7 for details.

(6) *Due Thursday, March 6.* Page 90, Problems 6, 9, 10. Page 99, Problems 1, 2. Page 100, Problems 5, 6. Page 121, Problems 8, 9.

(7) *Due Thursday, March 13.* Pages 122-123, Problems 11, 12, 16, 17, 18, 21, 22.

(8) *Due Tuesday, April 1.* See Handout 11.

(9) *Due Thursday, April 10.* In this problem, the universe of discourse is **R**, the set of real numbers, and the axioms are those of real arithmetic, given in Handout 10.

Each of the following seven statements is true or false. If it is true, give a proof, using just the axioms and rules of inference, and nothing else. If it is false, give a proof of its negation, using just the axioms and rules of inference, the theorems of this handout (i.e. Theorems T1 through T6), and nothing else.

I $(\forall x)(\forall y)(x.y = 0 \rightarrow (x = 0 \vee y = 0))$.
II $(\forall x)(\forall y)(\forall z)((x + y = x + z \rightarrow y = z)$.
III $(\forall x)(\forall y)(\forall z)((x.y = x.z \rightarrow y = z)$.
IV $(\forall x)(\exists y)(y + y = x)$.
V $(\forall x)(\forall y)(x + y \in \mathcal{P} \rightarrow (x \in \mathcal{P} \wedge y \in \mathcal{P}))$.
VI $1 + 1 \neq 0$ (that is, $\sim 1 + 1 = 0$)
VII $(\forall x)(x + x \in \mathcal{P} \rightarrow x \in \mathcal{P})$.

EXAMPLES OF PROOFS

Here is an example of a proof done *completely from first principles*, using only our axioms and the eight rules, and *nothing else.*

The lines that are not numbered are not really part of the proof, and could be omitted. They are *comments*, put there to help a reader understand what is going on.

THEOREM 1P. $1 \in \mathcal{P}$.

This theorem says that 1 is positive. Your obvious objection is going to be "but I know that already." Sure, you do. But what we are trying to do here is organize and systematize all our "knowledge." The way we do that is by giving a set of axioms and rules of inference, and replacing the vague notion of "things we know to be true" by the much more precise notion of "things we can prove from the axioms using the rules." So the reason for wanting to prove this theorem is not that we want to find out if it is true. Of course **we know it is true**. But *we want to find out if we can prove it from our axioms using our rules.* If we weren't able to prove it, then we would need more axioms, because we *know* that $1 \in \mathcal{P}$ is true. To show that we *don't* need more axioms (at least, not at this point) we must prove our theorem.

PROOF:

The basic strategy is to use Axiom A14, which tells us that if x is any number, then either x is positive, or $x = 0$, or $-x$ is positive. We specialize this to $x = 1$, and we know that either 1 is positive, or $1 = 0$, or -1 is positive. Now, $1 = 0$ is excluded by Axiom A16, so we are left with the other two possibilities, namely "1 is positive" and "-1 is positive." The first one poses no problem, because "1 is positive" is precisely what we want. The case that requires more work is when "-1 is positive." (Of course, this cannot happen, but at this point we don't know that yet. Our axioms do not tell us explicitly that -1 isn't positive. They *imply it*, but we would have to prove that they do, and we haven't done it yet[1] .)

Now, if -1 is positive, then $(-1).(-1)$ would be positive, because Axiom A13 tells us that the product of two positive numbers is positive.

But $(-1).(-1) = 1$, so in fact 1 is positive. In order words, *even in the "bad" case when -1 is positive, it still follows that 1 is positive.* So 1 is positive in all possible cases, and our proof is finished.

This is basically all there is to the proof, except that

- The axioms do not tell us that $(-1).(-1) = 1$, so if we want to use this fact we have to prove it first.

So we have to take care of this other problem first. How do we prove that $(-1)(-1) = 1$? How do we even *say it*, given that in our language we do not have the "$-$" symbol, and in our theory we do not have any axioms that talk about -1?

One possible answer to this would be to proceed as follows:

a. *define* -1 first,

b. then prove that $(-1).(-1) = 1$ as a separate theorem,

c. then use this theorem in our proof of Theorem 1P.

I will show you how to do it this way later, but first let us do everything directly to see how it can be done.

Since our axioms do not talk about an object called -1, we have to introduce such an object. The axiom that enables us to do this is A9, which tells us that every number has an additive inverse. Invoking this axiom, we can bring into our proof an additive inverse of 1, and call it a. (Rule 6 enables us to do that.)

This a is going to be our way of referring to -1 without really writing -1.

Now we have to prove that $a.a = 1$. How do we do that? The strategy here is to take the equality $1 + a = 0$ (which says that a is an additive inverse of 1), multiply both sides by a, and get $a.(1 + a) = a.0 = 0$, so $a + a.a = 0$. So $a + a.a + 1 = 1$, and, since $a + 1 = 0$, we get $a.a = 1$.

[1] We could include a proof that -1 is not positive as part of our proof of Theorem 1P, but we will not do it because we do not need it.

All this is fine, but we need to use $a.0 = 0$. How do we prove that?

Once again, we could prove another theorem before we embark upon our proof of Theorem 1P. This theorem would say that $(\forall x)(x.0 = 0)$. Then we would use this theorem here.

But we prefer to do the whole thing directly. The strategy to prove $a.0 = 0$ is to use $0 = 0 + 0$, so $a.0 = a.(0 + 0)$, i.e. $a.0 = a.0 + a.0$. Cancel $a.0$ from both sides and you get $0 = a.0$, as desired.

But, we are not there yet. Why can we "cancel $a.0$"? There is no "cancellation axiom" in our axiom list! Presumably, what we mean by the possibility of "cancelling" is a statement like

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

But this "cancellation law" is not one of our axioms, so if we want to use it then we have to prove it first. How do we prove it? Well, we take the additive inverse of x and add it to both sides.

Now, here is our proof of Theorem 1P.

In Steps 1, 2, 3 we will introduce a symbol a that will stand for -1, and in Steps 4 to 45 we will prove that $a.a = 1$.

(1)	$(\forall x)(\exists y)(x + y = 0)$	[A9]
(2)	$(\exists y)(1 + y = 0)$	[R4, spec. x to 1 in (1)]

We pick a such that

(3)	$1 + a = 0$	[R6, from (2)]

We now set out to prove that $a.a = 1$. As explained before, we will first prove that $0 = 0.a$. This is going to take us 22 steps, from Step 4 up to Step 25.

(4)	$(\exists y)((0 + 0).a + y = 0)$	[R4, spec. x to $(0 + 0).a$ in (1)]

We pick b such that

(5)	$(0 + 0).a + b = 0$	[R6, from (4)]
(6)	$(\forall x)(0 + x = x)$	[A8]
(7)	$0 + 0 = 0$	[R4, spec. x to 0 in (6)]
(8)	$0.a + b = 0$	[R8, from (5) and (7)]
(9)	$(\forall x)(\forall y)(\forall z)((x + y).z = x.z + y.z)$	[A7]
(10)	$(\forall y)(\forall z)((0 + y).z = 0.z + y.z)$	[R4, spec. x to 0 in (9)]
(11)	$(\forall z)((0 + 0).z = 0.z + 0.z)$	[R4, spec. y to 0 in (10)]
(12)	$(0 + 0).a = 0.a + 0.a$	[R4, spec. z to a in (11)]
(13)	$(0.a + 0.a) + b = 0$	[R8, from (5) and (12)]
(14)	$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$	[A5]
(15)	$(\forall y)(\forall z)((0.a + y) + z = 0.a + (y + z))$	[R4, spec. x to $0.a$ in (14)]
(16)	$(\forall z)((0.a + 0.a) + z = 0.a + (0.a + z))$	[R4, spec. y to $0.a$ in (15)]
(17)	$(0.a + 0.a) + b = 0.a + (0.a + b)$	[R4, spec. z to b in (16)]
(18)	$0.a + (0.a + b) = 0$	[R8, from (13) and (17)]
(19)	$(\forall x)(\forall y)(x + y = y + x)$	[A3]
(20)	$\forall y)(0.a + y = y + 0.a)$	[R4, spec. x to $0.a$ in (19)]
(21)	$0.a + 0 = 0 + 0.a$	[R4, spec. y to 0 in (20)]
(22)	$0.a + 0 = 0$	[R8, from (8) and (18)]
(23)	$0 + 0.a = 0$	[R8, from (21) and (22)]
(24)	$0 + 0.a = 0.a$	[R4, spec. x to $0.a$ in (6)]
(25)	$0 = 0.a$	[R8, from (23) and (24)]

We have now achieved our first goal, namely, to prove $0 = 0.a$.

We now need 20 more steps to get to $a.a = 1$.

(26)	$0+1=1$	[R4, spec. x to 1 in (6)]
(27)	$0.a+1=1$	[R8, from (25) and (26)]
(28)	$(1+a).a+1=1$	[R8, from (3) and (27)]
(29)	$(\forall y)((1+a).a+y=y+(1+a).a)$	[R4, spec. x to $(1+a).a$ in (19)]
(30)	$(1+a).a+1=1+(1+a).a)$	[R4, spec. y to 1 in (29)]
(31)	$1+(1+a).a=1$	[R8, from (28) and (30)]
(32)	$(\forall y)(\forall z)((1+y).z=1.z+y.z)$	[R4, spec. x to 1 in (9)]
(33)	$(\forall z)((1+a).z=1.z+a.z)$	[R4, spec. y to a in (32)]
(34)	$(1+a).a=1.a+a.a$	[R4, spec. z to a in (33)]
(35)	$1+(1.a+a.a)=1$	[R8, from (31) and (34)]
(36)	$(\forall x)(1.x=x)$	[A10]
(37)	$1.a=a$	[R4, spec. x to a in (36)]
(38)	$1+(a+a.a)=1$	[R8, from (35) and (37)]
(39)	$(\forall y)(\forall z)((1+y)+z=1+(y+z))$	[R4, spec. of x to 1 in (14)]
(40)	$(\forall z)((1+a)+z=1+(a+z))$	[R4, spec. of y to a in (39)]
(41)	$(1+a)+a.a=1+(a+a.a)$	[R4, spec. of z to $a.a$ in (40)]
(42)	$0+a.a=1+(a+a.a)$	[R8, from (3) and (41)]
(43)	$0+a.a=a.a$	[R4, spec. of x to $a.a$ in (3)]
(44)	$a.a=1+(a+a.a)$	[R8, from (42) and (43)]
(45)	$a.a=1$	[R8, from (38) and (44)]

Now we got $a.a = 1$, as we wanted. We are now ready to go back to our main proof and finish it. We will essentially use a "proof by contradiction." Since we want to prove that $1 \in \mathcal{P}$, we assume that $\sim 1 \in \mathcal{P}$ and try to get a contradiction. To do this using our rules *and nothing else*, what we will do in fact is prove that $(\sim 1 \in \mathcal{P}) \to (1 \in \mathcal{P})$. (Intuitively, we will prove that "even if 1 isn't in $\mathcal{P}$ it still follows that 1 is in $\mathcal{P}$," which of course means that 1 *must* be in $\mathcal{P}$.)

(46)	$(\forall x)(x \in \mathcal{P} \vee x=0 \vee (\forall y)(x+y=0 \to y \in \mathcal{P}))$	[A14]
(47)	$1 \in \mathcal{P} \vee 1=0 \vee (\forall y)(1+y=0 \to y \in \mathcal{P})$	[R4, spec. x to 1 in (46)]
(48)	$\sim 1=0$	[A16]

So our next goal is to show that $(\sim 1 \in \mathcal{P}) \to (1 \in \mathcal{P})$. To do this, we will use Rule 3: we assume $\sim 1 \in \mathcal{P}$ and try to prove $1 \in \mathcal{P}$.

So we assume:

(*49)	$\sim 1 \in \mathcal{P}$	[Assumption]

From now on, the statements that we prove using this assumption will be marked with a *. We do this to indicate that whatever we prove now is not something we have really proved under no conditions whatsoever. What we prove now, until further notice, is only *valid under the assumption (*49)*.

Since we don't want to write formulas that are too long, we introduce —temporarily— some abbreviations. We use α to stand for $1 \in \mathcal{P}$, β to stand for $1=0$, and γ to stand for $(\forall y)(1+y=0 \to y \in \mathcal{P})$. So (47) just says $\alpha \vee \beta \vee \gamma$, (48) says $\sim \beta$, and (*49) says that we are assuming $\sim \alpha$.

(*50)	$\sim \alpha \to (\sim \beta \to ((\alpha \vee \beta \vee \gamma) \to \gamma))$	[R1]

If you don't believe that the statement of (*50) is a tautology, you can check it using truth tables. But there is no need, really, bcause it is a matter of trivial common sense that this statement is a tautology: it says that "if we know that α doesn't happen then, if we know in addition that β doesn't happen either, then we can conclude, if we know that either α or β or γ happens, that γ happens." This is clearly true.

(*51)	$\sim \beta \to ((\alpha \vee \beta \vee \gamma) \to \gamma)$	[R2, from (*49) and (*50)]
(*52)	$(\alpha \vee \beta \vee \gamma) \to \gamma$	[R2, from (48) and (*51)]
(*53)	γ	[R2, from (47) and (*52)]

Recall that γ is just an abbreviation of $(\forall y)(1+y=0 \to y \in \mathcal{P})$.

(*54)	$1 + a = 0 \to a \in \mathcal{P}$	[R4, spec. y to a in (*53)]
(*55)	$a \in \mathcal{P}$	[R2, from (3) and (*54)]
(56)	$(\forall x)(\forall y)((x \in \mathcal{P} \wedge y \in \mathcal{P}) \to x.y \in \mathcal{P})$	[A13]
(*57)	$(\forall y)((a \in \mathcal{P} \wedge y \in \mathcal{P}) \to a.y \in \mathcal{P})$	[R4, spec. x to a in (56)]
(*58)	$(a \in \mathcal{P} \wedge a \in \mathcal{P}) \to a.a \in \mathcal{P}$	[R4, spec. y to a in (*57)]
(*59)	$(a \in \mathcal{P} \wedge a \in \mathcal{P}) \to 1 \in \mathcal{P}$	[R8, from (45) and (*58)]
(*60)	$a \in \mathcal{P} \to (a \in \mathcal{P} \wedge a \in \mathcal{P})$	[R1, tautology $p \to (p \wedge p)$]
(*61)	$a \in \mathcal{P} \wedge a \in \mathcal{P}$	[R2, from (*55) and (*60)]
(*62)	$1 \in \mathcal{P}$	[R2, from (*59) and (*61)]

Now you may think that we are finished, because we have "proved" $1 \in \mathcal{P}$. But *we haven't proved this yet!* We have only proved it under the assumption (*49).

However, we can now apply Rule 3, and get

(63) $(\sim 1 \in \mathcal{P}) \to 1 \in \mathcal{P}$ [R3, from (*49) and (*62)]

Now we need one more tautology to deliver the final blow:

(64) $((\sim 1 \in \mathcal{P}) \to 1 \in \mathcal{P}) \to 1 \in \mathcal{P}$ [R1, tautology $(\sim p \to p) \to p$]

Once again, if you don't believe this is a tautology, check it with truth tables. But you shouldn't really have to do that: $(\sim p \to p) \to p$ just says that "if you know that p must be true even when it isn't, then p must be true." This is quite obvious, isn't it?

(65) $1 \in \mathcal{P}$ [R2, from (63) and (64)]

END OF PROOF

HOW WE CAN BUILD THINGS UP STEP BY STEP

It is not possible to prove every theorem from first principles. So what one does is build things up. You prove certain facts, and then you can use them later and you don't have to prove them again. For example, the fact that $0.x = 0$ for all x is quite useful, as we have seen in the proof of Theorem 1P. It would be a terrible waste of effort if we had to prove that again every time we need it. So we prove this once and for all as a theorem, and then we just use it whenever we need to.

Similarly, it would be rather annoying if every time we need to talk about -1 we had to do it as we did in the proof of Theorem 1P. It's clear that the number -1 is quite useful, so we might as well introduce it, give it a name (for example, call it "-1") and then use it later.

How do we introduce new things? Can we, for example, introduce a number, called "*boo*", such that $boo + boo = 0 \wedge boo.boo = 1$? No! Why not? Intuitively, it's because such a number does not exist. (If $boo + boo = 0$ then $boo = 0$, but then $boo.boo = 0.0 = 0$, so $1 = 0$, contradicting A16.)

Also, can we introduce a number, called "*moo*", characterized by $moo.moo = 2$? Again, it is clear that this cannot be done, if we insist that the condition $moo.moo = 2$ *defines* our new number. This is because there are *two numbers* x such that $x.x = 2$, namely, $\sqrt{2}$ and $-\sqrt{2}$. So we cannot say that the condition $moo.moo = 2$ uniquely determines what *moo* is.

To be able to introduce a new object characterized by some condition, we should require that this object exist and that there be only one such object.

So, we introduce the abbreviation $(\exists! x)p(x)$, to stand for

$$(\exists x)(p(x) \wedge (\forall y)(p(y) \to y = x)). \qquad (\#)$$

In plain English, $(\exists! x)p(x)$ says "there exists one and only one x such that $p(x)$." Notice that (#) says there is an x such that (a) $p(x)$ is true, and (b) if y is any object for which $p(y)$ is true, then y must be x. This is clearly what "there exists one and only one x such that $p(x)$" means.

Here is an example of a theorem involving $\exists!$.

THEOREM T1. $(\forall x)(\exists! y)(x+y=0)$.

PROOF:

(*1)	Let a be arbitrary.	[Preparation to apply R5]
(*2)	$(\forall x)(\exists y)(x+y=0)$	[A9]
(*3)	$(\exists y)(a+y=0)$	[R4, spec. of x to a in (*3)]

We now pick b such that

(*4)	$a+b=0$	[R6, from (*3)]
(**5)	Let c be arbitrary.	[Preparation to apply R5]
(***6)	Assume $a+c=0$.	[Preparation to apply R3]
(***7)	$(\forall x)(0+x=x)$	[A8]
(***8)	$0+b=b)$	[R4, spec. of x to b in (***7)]
(***9)	$(a+c)+b=b)$	[R8, from (***6) and (***8)]
(***10)	$(\forall x)(\forall y)(x+y=y+x)$	[A3]
(***11)	$(\forall y)(a+y=y+a)$	[R4, spec. of x to a in (***10)]
(***12)	$a+c=c+a)$	[R4, spec. of y to c in (***11)]
(***13)	$(c+a)+b=b$	[R8, from (***9) and (***12)]
(***14)	$(\forall x)(\forall y)(\forall z)((x+y)+z=x+(y+z))$	[A5]
(***15)	$(\forall y)(\forall z)((c+y)+z=c+(y+z))$	[R4, spec. of x to c in (***14)]
(***16)	$(\forall z)((c+a)+z=c+(a+z))$	[R4, spec. of y to a in (***15)]
(***17)	$(c+a)+b=c+(a+b)$	[R4, spec. of z to b in (***16)]
(***18)	$(c+a)+b=c+0$	[R8, from (*4) and (***17)]
(***19)	$c+0=b$	[R8, from (***13) and (***18)]
(***20)	$(\forall y)(c+y=y+c)$	[R4, spec. of x to c in (***10)]
(***21)	$c+0=0+c$	[R4, spec. of y to 0 in (***20)]
(***22)	$0+c=b$	[R8, from (***19) and (***21)]
(***23)	$0+c=c$	[R4, spec. of x to c in (***7)]
(***24)	$c=b$	[R8, from (***22) and (***23)]

We have proved $c=b$ assuming (in (***6)) that $a+c=0$. So we get

(**25)	$a+c=0 \rightarrow c=b$	[R3, from (***6) and (***24)]

We have proved $a+c=0 \rightarrow c=b$ assuming (in (**5)) that c was arbitrary. So we get

(*26)	$(\forall z)(a+z=0 \rightarrow z=b)$	[R5, from (**5) and (**25)]
(*27)	$a+b=0 \rightarrow ((\forall z)(a+z=0 \rightarrow z=b) \rightarrow (a+b=0 \wedge (\forall z)(a+z=0 \rightarrow z=b)))$	[Tautology $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))$]
(*28)	$(\forall z)(a+z=0 \rightarrow z=b) \rightarrow (a+b=0 \wedge (\forall z)(a+z=0 \rightarrow z=b))$	[R2, from (*4) and (*27)]
(*29)	$a+b=0 \wedge (\forall z)(a+z=0 \rightarrow z=b)$	[R2, from (*26)) and (*28)]
(*30)	$(\exists y)(a+y=0 \wedge (\forall z)(a+z=0 \rightarrow z=y)$	[R7, from (*29)]
(*30)	$(\exists! y)(a+y=0)$	[This is just an abbreviation]

We have proved $(\exists! y)(a+y=0)$ assuming (in (*1)) that a was arbitrary. So we get

(31)	$(\forall x)(\exists! y)(a+y=0)$	[R5, from (*1) and (*30)]

END OF PROOF

HOW TO DEFINE NEW THINGS

If you have proved

$$(\exists! x)p(x)$$

then you can introduce a new object, with a name that is a letter or word that has *not* been used before as a name of anything —say a— and *define* a to mean "the unique object x such that $p(x)$."

Formally, you would say:

DEFINITION. We let a denote the unique object x such that $p(x)$.

When you do this, you are entitled from that moment on to use

$$p(a)\,.$$

In other words, it is as if you had added a *new axiom* that says "$p(a)$."
For example, you can prove

THEOREM T2. $(\exists! y)(1 + y = 0)$.

PROOF:

(1)	$(\forall x)(\exists! y)(x + y = 0)$	[Theorem T1]
(2)	$(\exists! y)(1 + y = 0)$	[R4, spec. of x to 1 in (1)]

END OF PROOF

So now, thanks to Theorem T2, you are entitled to say:

DEFINITION. We let -1 denote the unique object y such that $1 + y = 0$.

From now on, you can use

$$1 + (-1) = 0$$

as if it was an axiom. (When you use it, you justify your step by saying "by the definition of -1.)

FOUR THEOREMS

Now we can prove

THEOREM T3. $(\forall x)(0 = 0.x)$.

THEOREM T4. $(-1)(-1) = 1$.

PROOF OF THEOREM T3:

(*1)	Let a be arbitrary	[Preparation to apply R5]
(*2)	$(\exists y)((0 + 0).a + y = 0)$	[R4, spec. x to $(0 + 0).a$ in (*1)]

We pick b such that

(*3)	$(0 + 0).a + b = 0$	[R6, from (*2)]
(4)	$(\forall x)(0 + x = x)$	[A8]
(*5)	$0 + 0 = 0$	[R4, spec. x to 0 in (4)]
(*6)	$0.a + b = 0$	[R8, from (*3) and (*5)]
(7)	$(\forall x)(\forall y)(\forall z)((x + y).z = x.z + y.z)$	[A7]
(8)	$(\forall y)(\forall z)((0 + y).z = 0.z + y.z)$	[R4, spec. x to 0 in (7)]
(9)	$(\forall z)((0 + 0).z = 0.z + 0.z)$	[R4, spec. y to 0 in (8)]
(*10)	$(0 + 0).a = 0.a + 0.a$	[R4, spec. z to a in (*9)]
(*11)	$(0.a + 0.a) + b = 0$	[R8, from (*3) and (*10)]
(12)	$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$	[A5]
(*13)	$(\forall y)(\forall z)((0.a + y) + z = 0.a + (y + z))$	[R4, spec. x to $0.a$ in (12)]

(*14)	$(\forall z)((0.a+0.a)+z=0.a+(0.a+z))$	[R4, spec. y to $0.a$ in (*13)]
(*15)	$(0.a+0.a)+b=0.a+(0.a+b)$	[R4, spec. z to b in (*14)]
(*16)	$0.a+(0.a+b)=0$	[R8, from (*11) and (*15)]
(17)	$(\forall x)(\forall y)(x+y=y+x)$	[A3]
(*18)	$\forall y)(0.a+y=y+0.a)$	[R4, spec. x to $0.a$ in (17)]
(*19)	$0.a+0=0+0.a$	[R4, spec. y to 0 in (*18)]
(*20)	$0.a+0=0$	[R8, from (*6) and (*16)]
(*21)	$0+0.a=0$	[R8, from (*19) and (*21)]
(*22)	$0+0.a=0.a$	[R4, spec. x to $0.a$ in (4)]
(*23)	$0=0.a$	[R8, from (*21) and (*22)]

We have proved $0 = 0.a$ assuming (in (*1)) that a was arbitrary. So we get

(24)	$(\forall x)(0=0.x)$	[R5, from (*1) and (*23)]

END OF PROOF

PROOF OF THEOREM T4:

(1)	$(\forall x)(0+x=x)$	[A8]
(2)	$0+1=1$	[R4, spec. x to 1 in (1)]
(3)	$(\forall x)(0=0.x)$	[Theorem T3]
(4)	$0=0.(-1)$	[R4, spec. of x to $0.(-1)$ in (3)]
(5)	$0.(-1)+1=1$	[R8, from (2) and (4)]
(6)	$1+(-1)=0$	[Definition of -1]
(7)	$(1+(-1)).(-1)+1=1$	[R8, from (5) and (6)]
(8)	$(\forall x)(\forall y)(\forall z)((x+y).z=x.z+y.z)$	[A7]
(9)	$(\forall y)(\forall z)((1+y).z=1.z+y.z)$	[R4, spec. x to 1 in (8)]
(10)	$(\forall z)((1+(-1)).z=1.z+(-1).z)$	[R4, spec. y to -1 in (9)]
(11)	$(1+(-1)).(-1)=1.(-1)+(-1).(-1)$	[R4, spec. z to -1 in (10)]
(12)	$(1.(-1)+(-1).(-1))+1=1$	[R8, from (7) and (11)]
(13)	$(\forall x)(1.x=x)$	[A10]
(14)	$1.(-1)=-1$	[R4, spec. of x to -1 in (13)]
(15)	$((-1)+(-1).(-1))+1=1$	[R8, from (12) and (14)]
(16)	$(\forall x)(\forall y)(x+y=y+x)$	[A3]
(17)	$(\forall y)((-1)+y=y+(-1))$	[R4, spec. x to -1 in (16)]
(18)	$(-1)+(-1).(-1)=(-1).(-1)+(-1)$	[R4, spec. y to $(-1).(-1)$ in (17)]
(19)	$((-1).(-1)+(-1))+1=1$	[R8, from (15) and (18)]
(20)	$(\forall x)(\forall y)(\forall z)((x+y)+z=x+(y+z))$	[A5]
(21)	$(\forall y)(\forall z)(((-1).(-1)+y)+z=(-1).(-1)+(y+z))$	[R4, spec. x to $(-1).(-1)$ in (20)]
(22)	$(\forall z)(((-1).(-1)+(-1))+z=(-1).(-1)+((-1)+z))$	[R4, spec. y to -1 in (21)]
(23)	$((-1).(-1)+(-1))+1=(-1).(-1)+((-1)+1))$	[R4, spec. z to 1 in (22)]
(24)	$(-1).(-1)+((-1)+1)=1$	[R8, from (19) and (23)]
(25)	$(-1)+1=1+(-1))$	[R4, spec. y to 1 in (17)]
(26)	$(-1).(-1)+(1+(-1))=1$	[R8, from (24) and (25)]
(26)	$(-1).(-1)+0=1$	[R8, from (6) and (26)]
(27)	$(\forall y)(0+y=y+0)$	[R4, spec. x to 0 in (16)]
(28)	$0+(-1).(-1)=(-1).(-1)+0)$	[R4, spec. y to $(-1).(-1)$ in (27)]
(29)	$0+(-1).(-1)=1$	[R8, from (26) and (28)]
(30)	$0+(-1).(-1)=(-1).(-1)$	[R4, spec. of x to $(-1).(-1)$ in (1)]
(31)	$(-1).(-1)=1$	[R8, from (29) and (30)]

END OF PROOF

THEOREM T5. $1 \in \mathcal{P}$.

PROOF:

(1) $(\forall x)(x \in \mathcal{P} \vee x = 0 \vee (\forall y)(x + y = 0 \rightarrow y \in \mathcal{P}))$ [A14]

(2) $1 \in \mathcal{P} \vee 1 = 0 \vee (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})$ [R4, spec. x to 1 in (1)]

(3) $\sim 1 = 0$ [A16]

Assume:

(*4) $\sim 1 \in \mathcal{P}$ [Assumption]

(*5) $\sim 1 \in \mathcal{P} \rightarrow (\sim 1 = 0 \rightarrow ((1 \in \mathcal{P} \vee 1 = 0 \vee (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})) \rightarrow (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})))$
[Tautology $\sim p \rightarrow (\sim q \rightarrow ((p \vee q \vee r) \rightarrow r))$]

(*6) $\sim 1 = 0 \rightarrow ((1 \in \mathcal{P} \vee 1 = 0 \vee (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})) \rightarrow (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P}))$
[R2, from (*4) and (*5)]

(*7) $(1 \in \mathcal{P} \vee 1 = 0 \vee (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})) \rightarrow (\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})$
[R2, from (3) and (*6)]

(*8) $(\forall y)(1 + y = 0 \rightarrow y \in \mathcal{P})$ [R2, from (2) and (*7)]

(*9) $1 + (-1) = 0 \rightarrow (-1) \in \mathcal{P}$ [R4, spec. y to -1 in (*8)]

(10) $1 + (-1) = 0$ [Definition of -1]

(*11) $(-1) \in \mathcal{P}$ [R2, from (*9) and (10)]

(12) $(\forall x)(\forall y)((x \in \mathcal{P} \wedge y \in \mathcal{P}) \rightarrow x.y \in \mathcal{P})$ [A13]

(13) $(\forall y)(((-1) \in \mathcal{P} \wedge y \in \mathcal{P}) \rightarrow (-1).y \in \mathcal{P})$ [R4, spec. x to -1 in (12)]

(14) $((-1) \in \mathcal{P} \wedge (-1) \in \mathcal{P}) \rightarrow (-1).(-1) \in \mathcal{P}$ [R4, spec. y to -1 in (13)]

(15) $(-1).(-1) = 1$ [Theorem T4]

(16) $((-1) \in \mathcal{P} \wedge (-1) \in \mathcal{P}) \rightarrow 1 \in \mathcal{P}$ [R8, from (14) and (15)]

(17) $-1 \in \mathcal{P} \rightarrow (-1 \in \mathcal{P} \wedge -1 \in \mathcal{P})$ [R1, tautology $p \rightarrow (p \wedge p)$]

(*18) $-1 \in \mathcal{P} \wedge -1 \in \mathcal{P}$ [R2, from (11) and (17)]

(*19) $1 \in \mathcal{P}$ [R2, from (16) and (*18)]

(20) $\sim 1 \in \mathcal{P} \rightarrow 1 \in \mathcal{P}$ [R3, from (*4) and (*19)]

(21) $(\sim 1 \in \mathcal{P} \rightarrow 1 \in \mathcal{P}) \rightarrow 1 \in \mathcal{P}$ [Tautology $(\sim p \rightarrow p) \rightarrow p$]

(22) $1 \in \mathcal{P}$ [R2, from (20) and (21)]

END OF PROOF

THEOREM T6. $\sim ((-1) \in \mathcal{P})$.

PROOF:

Assume:

(*1) $(-1) \in \mathcal{P}$ [Preparation to apply R3]

(2) $1 \in \mathcal{P}$ [Theorem T5]

(3) $(\forall x)(\forall y)((x \in \mathcal{P} \wedge y \in \mathcal{P}) \rightarrow x + y \in \mathcal{P})$ [A12]

(4) $(\forall y)((1 \in \mathcal{P} \wedge y \in \mathcal{P}) \rightarrow 1 + y \in \mathcal{P})$ [R4, spec. of x to 1 in (3)]

(5) $(1 \in \mathcal{P} \wedge (-1) \in \mathcal{P}) \rightarrow 1 + (-1) \in \mathcal{P}$ [R4, spec. of y to -1 in (4)]

(6) $1 \in \mathcal{P} \rightarrow ((-1) \in \mathcal{P} \rightarrow (1 \in \mathcal{P} \wedge (-1) \in \mathcal{P}))$ [Tautology $p \rightarrow (q \rightarrow (p \wedge q))$]

(7) $(-1) \in \mathcal{P} \rightarrow (1 \in \mathcal{P} \wedge (-1) \in \mathcal{P})$ [R2, from (2) and (6)]

(*8) $1 \in \mathcal{P} \wedge (-1) \in \mathcal{P}$ [R2, from (*1) and (7)]

(*9) $1 + (-1) \in \mathcal{P}$ [R2, from (3) and (*8)]

(10) $1 + (-1) = 0$ [Definition of -1]

(*11) $0 \in \mathcal{P}$ [R8, from (*9) and (a0)]

(12) $(-1) \in \mathcal{P} \rightarrow 0 \in \mathcal{P}$ [R3, from (*1) and (*11)]

(13) $\sim 0 \in \mathcal{P}$ [A15]

(14) $((-1) \in \mathcal{P} \rightarrow 0 \in \mathcal{P}) \rightarrow (\sim 0 \in \mathcal{P} \rightarrow \sim (-1) \in \mathcal{P})$
[Tautology $(p \rightarrow q) \rightarrow (\sim q \rightarrow \sim p)$]

(15) $\sim 0 \in \mathcal{P} \rightarrow \sim (-1) \in \mathcal{P}$ [R2, from (12) and (14)]

(16) $\sim (-1) \in \mathcal{P}$ [R2, from (13) and (15)]

END OF PROOF