MATHEMATICS 300 — FALL 1997

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 8. November 25, 1997

THE AXIOMS OF REAL NUMBER ARITHMETIC AND OTHER NUMBER SYSTEMS

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

1. The set $\mathbf{N}$ of *natural numbers*, also known as *positive integers* (this is the set of integers n such that $n \geq 1$).
2. The set $\mathbf{N}_{\geq 0}$ of *nonnegative integers* (so that $\mathbf{N}_{\geq 0} = \mathbf{N} \cup \{0\}$). Usually, a notation such as $\mathbf{Z}_{+}$ is used for this set.
3. The set $\mathbf{Z}$ of all *integers* (so that $\mathbf{Z} = \mathbf{N}_{\geq 0} \cup \{x \in \mathbf{R} : -x \in \mathbf{N}\}$).
4. The set $\mathbf{Z}_m$ of all *integers modulo* m, where m is a natural number such that $m > 1$ (so that $\mathbf{Z}_m$ is the set $\mathbf{Z}/\equiv_m$ of equivalence classes modulo the equivalence relation $\equiv_m$. By definition, we say that two integers x, y are *equivalent modulo* m, and write $x \equiv_m y$, if m divides $x - y$. If $x \in \mathbf{Z}$, we use $[x]_m$ to denote the class of x modulo $\equiv_m$, i.e. the set $[x]_m = \{y \in \mathbf{Z} : x \equiv_m y\}$. Then the set $\mathbf{Z}_m$ has exactly m members, namely, the classes $[0]_m, [1]_m, \ldots, [m-1]_m$. When it is clear that we are working in $\mathbf{Z}_m$, for some fixed m we will just write $0, 1, \ldots, m-1$ instead of $[0]_m, [1]_m, \ldots, [m-1]_m$. With this notation, if we take, for example, $m = 7$, then the members of $\mathbf{Z}_7$ are $0, 1, 2, 3, 4, 5, 6$, and addition and multiplication are done modulo 7. (This means that, for example, $2+3=5$, $4+6=3$, $3.2=6$, $5.3=1$, $6.3=4$, and so on.)
5. The set $\mathbf{Q}$ of all *rational numbers*. By definition,

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

   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 $\mathbf{R}$ of all *real numbers*.
7. The set $\mathbf{C}$ of all *complex numbers*. By definition, a *complex number* is an ordered pair of real numbers, so the set $\mathbf{C}$ is just $\mathbf{R} \times \mathbf{R}$. Complex numbers are added and multiplied as follows: if $a, b, c, d \in \mathbf{R}$, 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 $\mathbf{Z}_m$ 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 $\mathbf{R}$, the set of real numbers. However, notice that $\mathbf{R}$ 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. one primitive one-variable predicate, namely, "$\in \mathcal{P}$" (meaning "is strictly positive"),
3. two primitive 2-variable function symbols, namely, "$+$" and "$.$",
4. one primitive 2-variable predicate, namely, "$=$".

In addition, we use "$S \neq T$" —if S, T are terms[1]— as an abbreviation of "$\sim S = T$", and "$S \notin \mathcal{P}$" —if S is a term— as an abbreviation of "$\sim S \in \mathcal{P}$".

Because the universe of discourse is $\mathbf{R}$, an expression such as $(\forall x)$ is exacty equivalent to $(\forall x \in \mathbf{R})$.

There will be **16** axioms. The first twelve of them do not involve "$\in \mathcal{P}$" at all, and are known as the **field axioms**. The last four have to do with "$\in \mathcal{P}$," i.e. with positivity, which is what will enable us later to define the *order relation* $>$ on $\mathbf{R}$, by letting $x > y$ if there is a z such that $x = y + z$ and $z \in \mathcal{P}$. So Axioms 13 through 16 are the *order axioms*. More precisely,

DEFINITION A. A system of objects on which there are binary operations $+$ and $.$, and objects 0, 1, such that Axioms A1 to A12 hold is called a *field*.

DEFINITION B. A system of objects on which there are binary operations $+$ and $.$, objects 0, 1, and a subset $\mathcal{P}$, such that Axioms A1 to A16 hold is called an *ordered field*.

So Axioms A13,14,15,16 are the extra postulates that have to be added to those of a field in order to get an ordered field. So we will call them *the order axioms of an ordered field*.

And here, finally, are the 16 axioms:

A1. $(\forall x)(\forall y)(\exists z)(x + y = z)$.

A2. $(\forall x)(\forall y)(\exists z)(x.y = z)$.

A3. $(\forall x)(\forall y)(x + y = y + x)$.

A4. $(\forall x)(\forall y)(x.y = y.x)$.

A5. $(\forall x)(\forall y)(\forall z)\Big((x + y) + z = x + (y + z)\Big)$.

A6. $(\forall x)(\forall y)(\forall z)\Big((x.y).z = x.(y.z)\Big)$.

A7. $(\forall x)(\forall y)(\forall z)\Big((x + y).z = x.z + y.z\Big)$.

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

[1] See Handout 2 for an explanation of the meaning of the word "term"

A9. $(\forall x)(\exists y)(x + y = 0)$.

A10. $(\forall x)(1.x = x)$.

A11. $(\forall x)\Big(x \neq 0 \rightarrow (\exists y)(x.y = 1)\Big)$.

A12. $1 \neq 0$.

A13. $(\forall x)(\forall y)\Big((x \in \mathcal{P} \wedge y \in \mathcal{P}) \Longrightarrow x + y \in \mathcal{P}\Big)$.

A14. $(\forall x)(\forall y)\Big((x \in \mathcal{P} \wedge y \in \mathcal{P}) \Longrightarrow x.y \in \mathcal{P}\Big)$.

A15. $(\forall x)(x \in \mathcal{P} \vee x = 0 \vee (\forall y)(x + y = 0 \Longrightarrow y \in \mathcal{P}))$.

A16. $0 \notin \mathcal{P}$.

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

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

COMMENTS: Axioms A1 and A2 say that addition and multiplication are binary operations *defined on the whole universe of numbers*. To understand thet importance of this, we can compare with other operations that can be defined on the real numbers, such as division or exponentiation, that are only "partially defined." For example, the quotient $\frac{x}{y}$ is not going to be defined for all x and y, but only when $y \neq 0$. (So at some point we will prove: $(\forall x)(\forall y)\Big(y \neq 0 \Longrightarrow (\exists z)(z = \frac{x}{y})\Big)$.) Similarly, the exponential x^y is going to be defined for all real numbers x and all *positive* real numbrs y (which means that there will be a theorem saying that $(\forall x)(\forall y)\Big(y \in \mathcal{P} \Longrightarrow (\exists z)(z = x^y\Big)$.)

Thanks to these two axioms, if you have a term such as $1+1$, you can be sure (by specializing (A1) to $x = 1$, $y = 1$) that $(\exists z)(1 + 1 = z)$. Once you know this, Rule 6 enables you to introduce a constant symbol (for example, the symbol "2") for which

$$1 + 1 = 2\,.$$

Axioms A3 and A4 are the *commutative laws* of addition and multiplication.
Axioms A5 and A6 are the *associative laws* of addition and multiplication.
Axiom A7 is the *distributive law* of multiplication with respect to addition.
Axiom A8 says that 0 is an additive identity, that is, that adding 0 to any number leaves the number unchanged.
Axiom A9 says that every real number has an additive inverse.
Axiom A10 says that 1 is a mutiplicative identity, that is, that mutiplying any number by 1 leaves the number unchanged.
Axiom A11 says that every nonzero real number has a multiplicative inverse.
Axiom A12 says that 0 and 1 are different. If you do not believe that A12 is necessary, take a look at the other axioms. Notice that they would all be satisfied if $\mathbf{R}$ consisted of just 0 and nothing else, and 1 was equal to 0. So unless we put in Axiom A12 we will never be able to prove that $1 \neq 0$.
Axiom A13 says that the sum of two positive numbers is positive.
Axiom A14 says that the product of two positive numbers is positive.
Axioms A15 says that every number x is either positive, negative, or zero. We say it in a roundabout way because we have not yet defined what we mean by a "negative number." Instead of saying "x is negative," we say "$(\forall y)(x + y = 0 \Longrightarrow y \in \mathcal{P})$."
Axiom A16 says that 0 is not positive.

If you recall the definitions of "field" and "ordered field" given above (Definitions A and B), we can summarize them as follows:

A. *A* **field** *is a system of objects —or "numbers"— on which two binary operations "+" and "," ("addition" and "multiplication") are specified, both of which are commutative and associative, and such that multiplication is distributive with respect to addition, as well as two different* [2] *numbers* 0 *and* 1 *that are, respectively, identity elements for the addition and multiplication operations, and are such that every number has an additive inverse and every nonzero number has a multiplicative inverse.*

B. *An* **ordered field** *is a field in which, in addition, a set* $\mathcal{P}$ *of numbers —called the set of positive numbers— is specified, in such a way that the sum and the product of two positive numbers is positive,* 0 *is not positive, and every nonzero number is either positive or the additive inverse of a positive number.*

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 "additive inverse":

DEFINITION: An *additive inverse* of a number x is a number y such that $x + y = 0$.

DEFINITION: A *multiplicative inverse* of a number x is a number y such that $x.y = 1$.

We can then prove:

THEOREM 1. *The additive inverse of every number is unique.* In formal language:

$$(\forall x)(\forall y)(\forall z)\Big((x + y = 0 \wedge x + z = 0) \Longrightarrow y = z\Big) .$$

(This just says that any two additive inverses of x must be the same.)

PROOF (WITH SHORTCUTS): Suppose x is an arbitrary number, and y, z are additive inverses of x. We have to prove that $y = z$. Now, the fact that y and z are additive inverses of x means that $x + y = 0$ and $x + z = 0$. Then

$$\begin{aligned}
y &= 0 + y && \text{(by Axiom A8)}\\
&= (x + z) + y && \text{(by Rule 8, because } 0 = x + z\text{)}\\
&= (z + x) + y && \text{(by Axiom A3)}\\
&= z + (x + y) && \text{(by Axiom A5)}\\
&= z + 0 && \text{(by Rule 8, because } x + y = 0\text{)}\\
&= 0 + z && \text{(by Axiom A3)}\\
&= z && \text{(by Axiom A8)}.
\end{aligned}$$

Q.E.D.

REMARK. The letters "Q.E.D." are often used to indicate the end of a proof. They stand for the Latin words "quod erat demonstrandum," which mean "which is what was to be proved."

[2] The fact that 0 and 1 are different is Axiom A12.

THEOREM 2. *The multiplicative inverse of every number is unique.* In formal language:

$$(\forall x)(\forall y)(\forall z)\Big((x.y=1 \wedge x.z=1) \Longrightarrow y=z\Big)\,.$$

PROOF (WITH SHORTCUTS): Suppose x is an arbitrary number, and y, z are multiplicative inverses of x. We have to prove that $y=z$. Now, the fact that y and z are multiplicative inverses of x means that $x.y=1$ and $x.z=1$. Then

$$\begin{aligned} y &= 1.y \\ &= (x.z).y \\ &= (z.x).y \\ &= z.(x.y) \\ &= z.1 \\ &= 1.z \\ &= z\,. \end{aligned}$$

Q.E.D.

A PROOF OF THEOREM 1 WITHOUT SHORTCUTS: We have to prove the following:

$$(\forall x)(\forall y)(\forall z)((x+y=0 \wedge x+z=0) \Longrightarrow y=z)\,. \qquad (@)$$

Here is a proof:

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

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

(3) $(\forall x)(\forall y)\Big(x+y=y+x\Big)$.

(4) Let a be arbitrary.

(5) Let u be arbitrary.

(6) Let v be arbitrary.

(7) Assume $a+u=0 \wedge a+v=0$.

(8) $(a+u=0 \wedge a+v=0) \Longrightarrow a+u=0$.

(9) $(a+u=0 \wedge a+v=0) \Longrightarrow a+v=0$.

(10) $a+u=0$.

(11) $a+v=0$.

(12) $0+v=v$

(13) $(\forall y)\Big(v+y=y+v\Big)$.

(14) $v+0=0+v$.

(15) $v+0=v$.

(16) $v+(a+u)=v$

(17) $(\forall y)(\forall z)\Big(v+(y+z)=(v+y)+z\Big)$.

(18) $(\forall z)\Big(v+(a+z)=(v+a)+z\Big)$.

(19) $v+(a+u)=(v+a)+u$.

(20) $v+a=a+v$.

(21) $v+(a+u)=(a+v)+u$.

(22) $v+(a+u)=0+u$.

(23) $0+u=u$.

(24) $v+(a+u)=u$.

(25) $u+0=u$.

(26) $v+(a+u)=u$.

(27) $u=v$.

(28) $(a+u=0 \wedge a+v=0) \Longrightarrow u=v$.

(29) $(\forall z)(a+u=0 \wedge a+z=0) \Longrightarrow u=z$.

(30) $(\forall y)(\forall z)(a+y=0 \wedge a+z=0) \Longrightarrow y=z$.

(31) $(\forall x)(\forall y)(\forall z)(x+y=0 \wedge x+z=0) \Longrightarrow y=z$.

Q.E.D.

PROBLEM 1: provide the missing justifications for the steps in the proof with shortcuts of Theorem 2.

PROBLEM 2: provide the missing justifications for the steps in the proof of Theorem 1 without shortcuts.

PROBLEM 3: give a proof without shortcuts of Theorem 2.

Next, recall that the notation

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

means "there is one and only one x such that $p(x)$." (For example: if our universe of discourse is the set of all people —alive or dead— and $p(x, y)$ means "y is x's mother," $q(x, y)$ means "y is x's brother," and $g(x, y)$ means "y is x's grandfather," then $(\forall x)(\exists! y)p(x, y)$ says that "everybody has one and only one mother," which is true. On the other hand, $(\forall x)(\exists! y)q(x, y)$ says that "everybody has one and only one brother," which is not true, because some people have no brothers at all, and other people have more that one brother. Finally, $(\forall x)(\exists! y)g(x, y)$ says that "everybody has one and only one grandfather," which is not true, because people [3] have *two* grandfathers.)

THEOREM 3. *Every number has a unique additive inverse.* In formal language:

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

PROOF: Suppose x is an arbitrary number. By Axiom A9, x has an additive inverse. By Theorem 1, this inverse is unique. Q.E.D.

THEOREM 4. *Every nonzero number has a unique multiplicative inverse.* In formal language:

$$(\forall x)\Big(x \neq 0 \Longrightarrow (\exists! y)(x.y = 1)\Big)\,.$$

PROOF: Suppose x is an arbitrary nonzero number. By Axiom A11, x has a multiplicative inverse. By Theorem 2, this inverse is unique. Q.E.D.

THEOREM 5. *For every number x, we have $x.0 = 0$.* In formal language:

$$(\forall x)(x.0 = 0)\,.$$

PROOF: Suppose x is an arbitrary number. Since $0 + 0 = 0$ by Axiom A8, we have $x.(0 + 0) = x.0$ (using Axiom Eq1, specialized to $x.0$, to get $x.0 = x.0$, and then Rule 8 to plug in $0 + 0$ instead of the first 0; the specialization of $(\forall x)(x = x)$ to $x.0$ is justified because Axiom A2 implies $(\exists y)(x.0 = y)$, so we can introduce a constant a for which $x.0 = a$, and then we can specialize $(\forall x)(x = x)$ to get $a = a$, and using Rule 8 we then get $x.0 = x.0$).

Now Axiom A7 implies $x.(0 + 0) = x.0 + x.0$. So Rule 8 gives us

$$x.0 + x.0 = x.0\,.$$

Now we can add te additive inverse of $x.0$ to both sides. More precisely, we can specialize Axiom A9 to get $(\exists y)(x.0 + y = 0)$. (Why?) Then we can use Rule 6 to introduce a constant b such that $x.0 + b = 0$. We then have $0 = x.0 + b = (x.0 + x.0) + b = x.0 + (x.0 + b) = x.0 + 0 = 0 + x.0 = x.0$, using Rule 8, Axiom A5, Rule 8, Axiom A3 and Axiom A8, in that order. Q.E.D.

PROBLEM 4: Answer the question that appears in the proof of Theorem 5.

We know from Theorem 3 that every number has a unique additive inverse. Let us give a name to the additive inverse of 1. Let us call it -1.

[3] except in some rare cases, such as some ancient Egyptian kings.

THEOREM 6. $(-1).(-1) = 1$.

PROOF. We know that $1 + (-1) = 0$. Axiom A3 then implies $(-1) + 1 = 0$, so 1 is the additive inverse of -1. Suppose we prove that

$$(-1) + (-1).(-1) = 0\,. \tag{1}$$

This would tell us that $(-1).(-1)$ is also an additive inverse of -1. Since the additive inverse is unique, we would get $(-1).(-1) = 1$, as desired.

So all we need to do is prove (1). But this is easy:

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

using Axioms A3, Rule 8, Axiom A7, and Theorem 5. Q.E.D.

THEOREM 7. $1 \in \mathcal{P}$.

PROOF. Axiom A15 says that either $1 \in \mathcal{P}$, or $1 = 0$, or $-1 \in \mathcal{P}$. The possibility that $1 = 0$ is excluded by Axiom A12. If $1 \in \mathcal{P}$ then we got what we wanted.

So the only case left for us to consider is when $-1 \in \mathcal{P}$. But in this case $(-1).(-1) \in \mathcal{P}$ by Axiom A14. Theorem 6 tells us that $(-1).(-1) = 1$. So $1 \in \mathcal{P}$. So we have shown that $1 \in \mathcal{P}$ in all possible cases. Q.E.D.

THEOREM 8. $-1 \notin \mathcal{P}$.

PROOF. Suppose $-1 \in \mathcal{P}$. We already know that $1 \in \mathcal{P}$. Then Axiom A13 implies that $1 + (-1) \in \mathcal{P}$. So $0 \in \mathcal{P}$. But this is impossible, because Axiom A16 says that $0 \notin \mathcal{P}$.

We now introduce the symbols 2, 3 and 4 as abbreviations for $1 + 1$, $2 + 1$ and $3 + 1$, respectively.

PROBLEM 5: Prove that $2 \neq 0$.

PROBLEM 6: Prove that $2 + 2 = 4$.

PROBLEM 7: Prove that $2.2 = 4$.

PROBLEM 8: Prove that

$$(\forall x)(x \in \mathcal{P} \Longrightarrow (\exists y)(\exists z)(y \in \mathcal{P} \wedge z \in \mathcal{P} \wedge y + z = x)\,.$$

(Hint, you may wish to take $y = z = \frac{x}{2}$. But we don't yet know what "$\frac{x}{2}$" means, so you have to get around that. The result of Problem 5 may be useful here.)

A PROOF OF THEOREM 7 WITHOUT ANY SHORTCUTS

This is a pretty silly section, but you should read it anyhow.

The point of this section is to remind you that **a proof with shortcuts is basically an abbreviated form of a proof without shortcuts.** Ultimately, every proof with shortcuts can be translated into a proof without shortcuts. The problem with this is that the proofs without shortcuts are usually enormously long, and once you know how to do such proofs it would be a waste of time and energy to write them out in detail.

You should think of theorem-proving without shortcuts as a **ladder** that you can climb until you get to the higher level of doing proofs without shortcuts, in a more informal language. Once you are confidently settled at the top level, you can throw the ladder away, because you no longer need it. But, if you throw away the ladder before you get to the top, you will fall. (Or, if you prefer: **when you make things up without knowing how to justify them in terms of the basic rules and axioms, it shows, and I can tell.**)

So, to bring this point home, let us give a proof of Theorem 7 *directly from first principles, not using any shortcuts, and not even using previous theorems.* We will just use the axioms and the rules of inference, and nothing else.

Naturally, the strategy for the proof is basically the same as what we have already done. You can regard the proof of Theorem 7 given above as an *outline* of the "true" proof that will be presented now.

WARNING: this is going to be painful, because it's very long. But it is quite easy. Every step is in fact completely trivial.

And here is the proof.

(1)	$(\forall x)\Big(x \in \mathcal{P} \vee x = 0 \vee (\forall y)(x + y = 0 \Longrightarrow y \in \mathcal{P})\Big)$.	(Axiom A15.)
(2)	$(\forall x)(\forall y)(\exists z)(x.y = z)$.	(Axiom A2.)
(3)	$(\forall x)(\forall y)(x + y = y + x)$.	(Axiom A3.)
(4)	$(\forall x)(\exists y)(x + y = 0)$.	(Axiom A9.)
(5)	$(\forall x)(\forall y)(\forall z)\Big((x + y).z = x.z + y.z\Big)$.	(Axiom A7.)
(6)	$(\forall x)(\forall y)\Big((x \in \mathcal{P} \wedge y \in \mathcal{P}) \Longrightarrow x.y \in \mathcal{P}\Big)$.	(Axiom A13).
(7)	$(\forall x)(1.x = x)$.	(Axiom A10.)
(8)	$(\forall x)(\forall y)(\forall z)\Big((x + y) + z = x + (y + z)\Big)$.	(Axiom A5.)
(9)	$\sim 1 = 0$.	(Axiom A12.)
(10)	$(\forall x)(0 + x = x)$.	(Axiom A8.)
(11)	$1 \in \mathcal{P} \vee 1 = 0 \vee (\forall y)(1 + y = 0 \Longrightarrow y \in \mathcal{P})$.	(Rule 4, from (1), specialized to $x = 1$.)
(12)	$(\forall y)(0 + y = y + 0)$.	(Rule 4, from (3), specialized to $x = 0$.)
(13)	$(\exists y)(1 + y = 0)$.	(Rule 4, from (4), specialized to $x = 1$.)
(14.1)	Assume $(\forall y)(1 + y = 0 \Longrightarrow y \in \mathcal{P})$.	(Preparation to apply Rule 3.)
(14.2.1)	Let a be such that $1 + a = 0$.	(Rule 6, from (13).)
(14.2.2)	$1 + a = 0 \Longrightarrow a \in \mathcal{P}$.	(Rule 4, from (14.1), specialized to $y = a$.)
(14.2.3)	$a \in \mathcal{P}$.	(Rule 2, from (14.2.1) and (14.2.2).)
(14.2.4)	$(\forall y)(\forall z)((0 + y).z = 0.z + y.z)$	(Rule 4, from (5), specialized to $x = 0$.)
(14.2.5)	$(\forall z)((0 + 0).z = 0.z + 0.z)$	(Rule 4, from (14.2.4), specialized to $y = 0$.)
(14.2.6)	$(0 + 0).a = 0.a + 0.a$	(Rule 4, from (14.2.5), specialized to $z = a$.)
(14.2.7)	$0 + 0 = 0$.	(Rule 4, from (10), specialized to $x = 0$.)
(14.2.8)	$0.a = 0.a + 0.a$.	(Rule 8, from (14.2.6) and (14.2.7).)
(14.2.9)	$(\forall y)(\exists z)(0.y = z)$.	(Rule 4, from (2), specialized to $x = 0$.)
(14.2.10)	$(\exists z)(0.a = z)$.	(Rule 4, from (14.2.9), specialized to $y = a$.)
(14.2.11.1)	Let b be such that $0.a = b$.	(Rule 6, from (14.2.10).)
(14.2.11.2)	$b = b + b$.	(Rule 8, from (14.2.8) and (14.2.11.1).
(14.2.11.3)	$(\exists y)(b + y = 0)$.	(Rule 4, from (4), specialized to $x = b$.)
(14.2.11.4.1)	Let c be such that $b + c = 0$.	(Rule 6, from (14.2.11.3).)
(14.2.11.4.2)	$(b + b) + c = 0$.	(Rule 8, from (14.2.11.2) and (14.2.11.4.1).
(14.2.11.4.3)	$(\forall y)(\forall z)\Big((b+y)+z = b+(y+z)\Big)$.	(Rule 4, from (8), specialized to $x = b$.)
(14.2.11.4.4)	$(\forall z)\Big((b+b)+z = b+(b+z)\Big)$.	(Rule 4, from (14.2.11.4.3), spec. to $y = b$.)
(14.2.11.4.5)	$(b+b)+c = b+(b+c)$.	(Rule 4, from (14.2.11.4.4), specialized to $z = c$.)
(14.2.11.4.6)	$(b + b) + c = b + 0$.	(Rule 8, from (14.2.11.4.1) and (14.2.11.4.5).)
(14.2.11.4.7)	$0 = b + 0$.	(Rule 8, from (14.2.11.4.2) and (14.2.11.4.6).)
(14.2.11.4.8)	$0 + b = b$.	(Rule 4, from (10), specialized to $x = b$.)
(14.2.11.4.9)	$0 + b = b + 0$.	(Rule 4, from (3), specialized to $x = b$.)
(14.2.11.4.10)	$b + 0 = b$.	(Rule 8, from (14.2.11.4.8) and (14.2.11.4.9).)
(14.2.11.4.11)	$0 = b$.	(Rule 8, from (14.2.11.4.7) and (14.2.11.4.10).)
(14.2.11.4.12)	$0 = 0.a$.	(Rule 8, from (14.2.11.1) and (14.2.11.4.11).)
(14.2.11.5)	$0 = 0.a$.	(Rule 6, from (14.2.11.4.1) and (14.2.11.4.12.)
(14.2.12)	$0 = 0.a$.	(Rule 6, from (14.2.11.1) and (14.2.11.5)
(14.2.13)	$0 = (1 + a).a$.	(Rule 8, from (14.2.1) and (14.2.12).)
(14.2.14)	$(\forall y)(\forall z)\Big((1 + y).z = 1.z + y.z\Big)$.	(Rule 4, from (5), specialized to $x = 1$.)
(14.2.15)	$(\forall z)\Big((1 + a).z = 1.z + a.z\Big)$.	(Rule 4, from (14.2.14), specialized to $y = a$.)
(14.2.16)	$(1 + a).a = 1.a + a.a$.	(Rule 4, from (14.2.15), specialized to $z = a$.)

(14.2.17)	$0 = 1.a + a.a.$	(Rule 8, from (14.2.13) and (14.2.16).)
(14.2.18)	$1.a = a.$	(Rule 4, from (7), specializing to $x = a.$)
(14.2.19)	$0 = a + a.a.$	(Rule 8, from (14.2.17) and (14.2.18).)
(14.2.20)	$0 + 1 = 1.$	(Rule 4, from (10) specialized to $x = 1.$)
(14.2.21)	$0 + 1 = 1 + 0.$	(Rule 4, from (12) specialized to $y = 1.$)
(14.2.22)	$1 + 0 = 1.$	(Rule 8, from (14.2.20) and (14.2.21).)
(14.2.23)	$1 + (a + a.a) = 1.$	(Rule 8, from (14.2.19) and (14.2.22).)
(14.2.24)	$(\forall y)(\forall z)\Big((1 + y) + z = 1 + (y + z)\Big).$	(Rule 4, from (8), specialized to $x = 1.$)
(14.2.25)	$(\forall z)\Big((1 + a) + z = 1 + (a + z)\Big).$	(Rule 4, from (14.2.24), specialized to $y = a.$)
(14.2.26)	$(\forall y)(\exists z)(a.y = z).$	(Rule 4, from (2), specialized to $x = a.$)
(14.2.27)	$(\exists z)(a.a = z).$	(Rule 4, from (14.2.26), specialized to $y = a.$)
(14.2.28.1)	Let d be such that $a.a = d.$	(Rule 6, from (14.2.27).)
(14.2.28.2)	$(1 + a) + d = 1 + (a + d).$	(Rule 4, from (14.2.25), specialized to $z = d.$)
(14.2.28.3)	$1 + (a + d) = 1.$	(Rule 8, from (14.2.23) and (14.2.28.1).)
(14.2.28.4)	$(1 + a) + d = 1.$	(Rule 8, from (14.2.28.2) and (14.2.28.3).)
(14.2.28.5)	$0 + d = 1.$	(Rule 8, from (14.2.1) and (14.2.28.4).)
(14.2.28.6)	$0 + d = d.$	(Rule 4, from (10), specialized to $x = d.$)
(14.2.28.7)	$d = 1.$	(Rule 8, from (14.2.28.5) and (14.2.28.6).)
(14.2.28.8)	$a.a = 1.$	(Rule 8, from (14.2.28.1) and (14.2.28.7).)
(14.2.29)	$a.a = 1.$	(Rule 6, from (14.2.28.1) and (14.2.28.8).)
(14.2.30)	$(\forall y)\Big((a \in \mathcal{P} \wedge y \in \mathcal{P}) \Longrightarrow a.y \in \mathcal{P}\Big).$	(Rule 4, from (1), specialized to $x = a.$)
(14.2.31)	$(a \in \mathcal{P} \wedge a \in \mathcal{P}) \Longrightarrow a.a \in \mathcal{P}.$	(Rule 4, from (14.2.30), specialized to $x = a.$)
(14.2.32)	$a \in \mathcal{P} \Longrightarrow (a \in \mathcal{P} \wedge a \in \mathcal{P}).$	(Rule 1, tautology $\alpha \Longrightarrow (\alpha \wedge \alpha).$)
(14.2.33)	$a \in \mathcal{P} \wedge a \in \mathcal{P}.$	(Rule 2, from (14.2.3) and (14.2.32).)
(14.2.34)	$a.a \in \mathcal{P}.$	(Rule 2, from (14.2.31) and (14.2.33).)
(14.2.35)	$1 \in \mathcal{P}.$	(Rule 8, from (14.2.29) and (14.2.34).)
(14.3)	$1 \in \mathcal{P}.$	(Rule 6, from (14.2.1) and (14.2.35).)
(15)	$(\forall y)(y + 1 = 0 \Longrightarrow y \in \mathcal{P}) \Longrightarrow 1 \in \mathcal{P}.$	(Rule 3, from (14.1) and (14.3).)

(16) $$\Big(1 \in \mathcal{P} \vee 1 = 0 \vee (\forall y)(y + 1 = 0 \Longrightarrow y \in \mathcal{P})\Big) \Longrightarrow$$
$$\Bigg(\sim 1 = 0 \Longrightarrow \bigg(\Big((\forall y)(y + 1 = 0 \Longrightarrow y \in \mathcal{P}) \Longrightarrow 1 \in \mathcal{P}\Big) \Longrightarrow 1 \in \mathcal{P}\bigg)\Bigg).$$
(Instance of the tautology $(p \vee q \vee r) \Longrightarrow \Big((\sim q) \Longrightarrow ((r \Longrightarrow p) \Longrightarrow p)\Big).$)

(17) $\sim 1 = 0 \Longrightarrow \bigg(\Big((\forall y)(y + 1 = 0 \Longrightarrow y \in \mathcal{P}) \Longrightarrow 1 \in \mathcal{P}\Big) \Longrightarrow 1 \in \mathcal{P}\bigg).$ (Rule 2, from (11) and (16).)

(18) $\Big((\forall y)(y + 1 = 0 \Longrightarrow y \in \mathcal{P}) \Longrightarrow 1 \in \mathcal{P}\Big) \Longrightarrow 1 \in \mathcal{P}.$ (Rule 2, from (9) and (17).)

(19) $1 \in \mathcal{P}.$ (Rule 2, from (15) and (18).)

WE GOT THERE! WE DID IT! IT'S PROVED!

AND IT TOOK US ONLY 78 STEPS.

Q.E.D.

Of the sixteen axioms A1 to A16, which ones are true for our other number systems?

Axioms A1,2,3,4,5,6,7, and A10 are true in **all** of them. Axioms A8 and A12 are true in all them also but, technically, $0 \notin \mathbf{N}$, so we should not count A8 and A12 as holding there, because, when the universe is $\mathbf{N}$, 0 does not exist. Axiom A9 is true in $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$, but not in $\mathbf{N}$ or $\mathbf{N}_{\geq 0}$. Axiom A11 is true in $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$, but not in $\mathbf{N}$, $\mathbf{N}_{\geq 0}$ or $\mathbf{Z}$.

As for Axioms A13,1,4,15,16, they are true in $\mathbf{R}$ *and also in* $\mathbf{Q}$, if we define "positive" in the usual way. Are they true in other systems, e.g. in $\mathbf{C}$? Well, that would depend on what the set $\mathcal{P}$ is, that is, on how we might choose to define what it means for a complex number to be "positive." It turns out that *there is no way to do it.*

PROBLEM 9: Prove that there is no way to define a subset $\mathcal{P}$ of $\mathbf{C}$ so that Axioms A1 to A16 hold. (In other words, there is no way to make $\mathbf{C}$ into an ordered field.) Hint: suppose you could. Would i be positive?

We have seen that all the axioms A1 to A16 hold on $\mathbf{Q}$ as well as on $\mathbf{R}$. This means that, as far as Axioms A1 to A16 are concerned, one cannot distinguish between $\mathbf{R}$ and $\mathbf{Q}$. So, **as a system of axioms for R, A1-A16 is not strong enough to give us everything that is true in R, including those things that aren't true in Q.**

For example: the statement

$$(\forall x)(x \in \mathcal{P} \Longrightarrow (\exists y)(y.y = x))$$

(i.e. "every positive number has a square root") is true in $\mathbf{R}$ but not in $\mathbf{Q}$. So **this statement cannot be proved from A1-A16 alone** (because, if it could be proved from A1-A16, then it would be true in every number system where A1-A16 are true, and in particular in $\mathbf{Q}$).

What happens with the integers modulo m? We proved in class that

1. If m is prime then $\mathbf{Z}_m$ is a field.
2. If m is not prime then $\mathbf{Z}_m$ is not a field.

PROBLEM 10: Let $m \in \mathbf{N}$, $m > 1$. Prove that there is no way to define a subset $\mathcal{P}$ of $\mathbf{Z}_m$ so that Axioms A1 to A16 hold. (In other words, there is no way to make $\mathbf{Z}_m$ into an ordered field.)

PROBLEM 11: Find the multiplicative inverse of 35 (i.e. the equivalence class of 35) in Z_{89}.

PROBLEM 12: Find a nonzero member of $\mathbf{Z}_{124}$ that has no multiplicative inverse.

HAVE A HAPPY THANSKGIVING!