MATHEMATICS 300 — Introduction to Mathematical Reasoning

H. J. Sussmann — SPRING 2000

HANDOUT NO. 6 — March 27, 2000

THE AXIOMS FOR EQUALITY

We will always assume the validity of the following four axioms about equality.

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

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

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

Eq4. If x and y are different variables, $p(x)$ is a formula that does not contain y and has no x-quantifiers, and $p(y)$ is a formula that results from $p(x)$ by substituting y for x in some or all the occurrences of x, then $\forall x \forall y(x = y \rightarrow (p(x) \leftrightarrow p(y))$ is an axiom.

THE AXIOMS OF REAL NUMBER ARITHMETIC AND OTHER NUMBER SYSTEMS

We would like to be able to prove various properties of the real numbers and other number systems. We will do this by starting with some *axioms* or *postulates*, and then using them to prove *theorems*.

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 other number systems.

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

- two primitive constants, namely, "0" and "1,"
- two primitive 1-variable function symbols, namely, "$-$" and "inverse". (We write x^{-1} for "inverse(x)".)
- two primitive infix[1] binary function symbols, namely, "$+$" and "$.$",
- two primitive infix binary predicates, namely, "$=$" and "$<$".

In addition, we use "$S \neq T$"—if S, T are terms—as an abbreviation of "$\sim S = T$".

[1] "Infix" means that we write the function symbol between the two arguments; for example, we write $x + y$ rather than $+(x, y)$.

There will be **18** axioms. The first twelve of them do not involve "$<$" at all, and are known as the **field axioms**. Axioms 13 to 17 have to do with "$<$," i.e. with the *order relation* on $\mathbb{R}$. $x = y + z$ and $z \in \mathcal{P}$. So Axioms 13 through 17 are the *order axioms*. Axiom 18 is the *completeness axiom*.

More precisely,

DEFINITION A. A system of objects on which there are binary operations $+$ and $.$, one-variable functions $-$ and $^{-1}$, 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 $.$, one-variable functions $-$ and $^{-1}$, objects 0, 1, and a binary predicate $<$ such that Axioms A1 to A17 hold is called an *ordered field*.

So Axioms A13,14,15,17 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*.

Notice also that Axioms 1 to 10 and Axiom 12 do not talk about $^{-1}$.

DEFINITION C. A system of objects on which there are binary operations $+$ and $.$, a one-variable function $-$, and objects 0, 1, such that Axioms A1 to A10 and A12 hold is called an *ring*[2].

And here, finally, are the first 17 axioms. (We will discuss the completeness axiom later.)

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

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

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

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

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

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

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

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

A9. $\forall x (x.1 = x)$.

A10. $\forall x (x + (-x) = 0)$.

A11. $\forall x (x \neq 0 \rightarrow (x.x^{-1} = 1))$.

A12. $0 \neq 1$.

A13. $\forall x (\sim x < x)$.

A14. $\forall x \forall y \forall z ((x < y \wedge y < z) \rightarrow x < z)$.

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

A16. $\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$.

A17. $\forall x \forall y \forall z ((x < y \wedge 0 < z) \rightarrow x.z < y.z)$.

[2] For the algebra experts: it is really called a "commutative ring with identity."