1 A correction to the handout on $\mathbb{Z}_{11}$

In the handout on $\mathbb{Z}_{11}$, where I define "field", I forgot to include the axiom that $0 \neq 1$. This axiom is not needed for $\mathbb{R}$, because it follows from the axioms of Part II. (Precisely: assume that $0 = 1$; NZ3 implies that $1 \in \mathbb{N}$. Then NZ1 implies that $1 > 0$. Then Or1 implies that $0 < 1$. Furthermore, Or5 implies that $\sim (0 < 1 \wedge 0 \geq 1)$. Since $0 < 1$, it follows that $\sim 0 \geq 1$. Since $0 = 1$, we find that $1 = 0$—using SEE—so $1 < 0 \vee 1 = 0$, and then Or2 implies $1 \leq 0$. But then Or3 implies $0 \geq 1$. So we have proved, assuming that $0 = 1$, that $0 \geq 1 \wedge (\sim 0 \geq 1)$, which is a contradiction. Hence $0 \neq 1$.)

2 Homework assignment no. 10, due on Thursday November 30

1. We would like to define the ***ordered pair*** (x, y) of two objects x, y to be a set, having the property that

$$(\forall x)(\forall y)(\forall u)(\forall v)\Big((x,y) = (u,v) \Leftrightarrow (x = u \wedge y = v)\Big)\,. \qquad (2.0.1)$$

It does not matter how the ordered pair is defined, as long as (2.0.1) holds. Here are five possible ways of defining (x, y), of which some work and some do not. ("Works" means "it is such that (2.0.1) holds.")

(i) $(\forall x)(\forall y)\Big((x,y) = \{x,y\}\Big)$,

(ii) $(\forall x)(\forall y)((x,y) = \{\{x\},\{x,y\}\})$,

(iii) $(\forall x)(\forall y)((x,y) = \{x,\{x,y\}\})$,

(iv) $(\forall x)(\forall y)((x,y) = \{x,\{y\}\})$.

(v) $(\forall x)(\forall y)((x,y) = \{x,\{y,\emptyset\}\})$.

Prove that (i) does not work, and (ii) works. Determine whether (iii), (iv) and (v) work. (In each of the three cases, prove that the definition works, or prove that it does not.)

2. A ***field*** is a system $\mathbb{F}$ of objects on which there are defined (a) members of $\mathbb{F}$ called 0 ("zero") and 1 ("one"), and (b) operations of addition (sending x, y to $x + y$), subtraction (sending x, y to $x - y$), multiplication (sending x, y to $x \times y$, also written as $x \cdot y$, or just xy), and

division (sending x, y to $\frac{x}{y}$), in such a way that all the thirteen "axioms of arithmetic, Part I," hold (with $\mathbb{F}$ instead of $\mathbb{R}$), as well as the "fourtheenth axiom" $\boxed{0 \neq 1}$.

If n is a natural number, then $\mathbb{Q}(\sqrt{n})$ is the set of all real numbers of the form $a + b\sqrt{n}$, $a, b \in \mathbb{Q}$. (In other words, the set $\mathbb{Q}(\sqrt{n})$ is defined by $\boxed{\mathbb{Q}(\sqrt{n}) = \{x : x \in \mathbb{R} \wedge (\exists a \in \mathbb{Q})(\exists b \in \mathbb{Q})(x = a + b\sqrt{n})\}}$.)

(i) Prove that $\mathbb{Q}(\sqrt{2})$ is a field. (NOTE: The operations of addition, subtraction, multiplication, and division are defined as in $\mathbb{R}$, because after all the members of $\mathbb{Q}(\sqrt{2})$ are real numbers, so you can add, subtract and multiply any two members x, y of $\mathbb{Q}(\sqrt{2})$, and you can divide x by y if $y \neq 0$. Then most of the axioms are trivially true, and you do not need to waste time proving them. The only ones that require proof are Add1, Sub1, Mul1, and Div1, so all you have to do is prove these four axioms, with $\mathbb{Q}(\sqrt{2})$ instead of $\mathbb{R}$, of course.)

(ii) Prove that every member α of $\mathbb{Q}(\sqrt{2})$ has a ***unique*** expression of the form $\alpha = a + b\sqrt{2}$. That is, prove that

$$(\forall \alpha)\Big(\alpha \in \mathbb{Q}(\sqrt{2}) \Rightarrow (\exists! a)(\exists! b)((a \in \mathbb{Q} \wedge b \in \mathbb{Q}) \wedge \alpha = a + b\sqrt{2})\Big).$$

Recall that "$(\exists! x)P(x)$" is read as "there exists a unique x such that $P(x)$", and it means

$$(\exists x)\Big(P(x) \wedge (\forall y)(P(y) \Rightarrow x = y)\Big).$$

(iii) Is it true that $\mathbb{Q}(\sqrt{n})$ is a field for every $n \in \mathbb{N}$? (Prove that the answer is "yes" or that the answer is "no".)

(iv) Is it true for every $n \in \mathbb{N}$ that every member α of $\mathbb{Q}(\sqrt{n})$ has a unique expression of the form $\alpha = a + b\sqrt{n}$? (Prove that the answer is "yes" or that the answer is "no".)

3. Is $\mathbb{Z}$ a field, with the usual operations of addition, subtraction and multiplication, and the same 0 and 1 as in $\mathbb{R}$? (Prove that the answer is "yes" or that the answer is "no". The key question here is whether it is possible to define an operation of division in $\mathbb{Z}$ such that Axioms Div1 and Div2 hold.)

3 The Axioms of Arithmetic

THE AXIOMS OF ARITHMETIC, PART I

ADDITION AXIOMS

Add1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x + y \in \mathbb{R}$.

Add2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x + y = y + x$.

Add3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x + y) + z = x + (y + z)$.

SUBTRACTION AXIOMS

Sub1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x - y \in \mathbb{R}$.

Sub2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x - y = z \Leftrightarrow x = y + z)$

MULTIPLICATION AXIOMS

Mul1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x \cdot y \in \mathbb{R}$.

Mul2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x \cdot y = y \cdot x$.

Mul3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

DIVISION AXIOMS

Div1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((\sim y = 0) \Rightarrow \frac{x}{y} \in \mathbb{R})$.

Div2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((\sim y = 0) \Rightarrow (\frac{x}{y} = z \Leftrightarrow x = y \cdot z))$.

DISTRIBUTIVE LAW

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

ZERO AND ONE AXIOMS

ZO1. $(\forall x \in \mathbb{R}) x + 0 = x$

ZO2. $(\forall x \in \mathbb{R}) x \cdot 1 = x$

THE AXIOMS OF ARITHMETIC, PART II

ORDER AXIOMS

Or1. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x > y \Leftrightarrow y < x)$

Or2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x \leq y \Leftrightarrow (x < y \vee x = y))$

Or3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x \geq y \Leftrightarrow y \leq x)$

Or4. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((x < y \vee x > y) \vee x = y)$

Or5. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \sim (x < y \wedge x \geq y)$

Or6. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((x < y \wedge y < z) \Rightarrow x < z)$

Or7. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x < y \Rightarrow x + z < y + z)$

Or8. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((x < y \wedge z > 0) \Rightarrow x \cdot z < y \cdot z)$

AXIOMS ABOUT INTEGERS AND NATURAL NUMBERS

NZ1. $(\forall x)(x \in \mathbb{N} \Leftrightarrow (x \in \mathbb{Z} \wedge x > 0))$

NZ2. $(\forall x \in \mathbb{Z})x \in \mathbb{R}$

NZ3. $0 \in \mathbb{Z}$

NZ4. $1 \in \mathbb{N}$

NZ5. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x + y \in \mathbb{Z}$

NZ6. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x - y \in \mathbb{Z}$

NZ7. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x \cdot y \in \mathbb{Z}$

NZ8. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(y \leq x \vee y \geq x + 1)$

NZ9. Let n be a variable, and let $P(n)$ be a formula that contains no n-quantifiers. Then

$$\Big(P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))\Big) \Rightarrow (\forall n \in \mathbb{N})P(n)\,.$$

NZ9'. ALTERNATIVE VERSION OF AXIOM NZ9: Let S be a subset of $\mathbb{N}$. Assume that $1 \in S \wedge (\forall n)(n \in S \Rightarrow n+1 \in S)$. Then $S = \mathbb{N}$.