Arithmetic for Z*

R.D. Arthan
ICL,
Eskdale Road,
Winnersh,
Berks.
RG11 5TT
rda@win.icl.co.uk

26 February 1996

1 INTRODUCTION

In the two editions of the Z Reference Manual, [4, 5], and in the current Committee Draft of the Z standard (CD), the defining properties of the elementary operations on the integers are "omitted". An earlier version of this document, Z Standards Document D-142, presented one version of the omitted details.

It was agreed in a Z Panel meeting at Limerick in 1995 that a slightly adjusted version of the treatment in D-142 should be adopted in an early revision of the CD. It was also agreed then that the set of integers should be defined as a subset of a given set of numbers so as to allow arithmetic operations to be axiomatised on supersets of the integers.

In February 1996, the Toolkit Subcommittee met in London, to work out the details of the revision to the CD agreed at Limerick. Working through some of the consequences of the discussions at Limerick against an earlier draft of this document resulted in the following observations and decisions:

1. At Limerick, it was suggested that the integer operators such as addition be made total over the integers. This would force an axiomatisation of the reals, say, to use different operator symbols from the integer ones. It was strongly felt at the London meeting that this was not acceptable and that the conceptual overhead of defining the operators in an extensible way was more than justified for the proposed revision to the CD.

2. The original draft of this document made some mistaken statements about the treatment of integer division in [5]. The definition given in that draft has advantages but does not appear to be the one of choice. An intermediate (privately circulated) revision to this document proposed only to define *div* and *mod* for natural operands; however, there was a strong feeling that, while there is no perfect definition of these operators for negative operands, the position taken in the Z reference manual is a defensible one. It was agreed to give a definition conformant with the laws in [5] in the proposed revision to the CD.

---

*Author's reference: DS/FMU/IED/WRK055; Z Document reference: D-188;This version of 26/2/96 supersedes an earlier version, D-142, dated 29/6/93. Reformatted 29/2/96.

3. A side effect of item 2 is that *abs* is no longer required within the toolkit itself and so it was agreed not to propose its inclusion.

4. Most of the changes to the original draft of this document are motivated by a desire to let users define arithmetic systems of their own devising which extend the integers. It was agreed that a simple treatment of the reals should be produced as a proof of concept by adapting parts of the material in [6].

This document addresses items 1, 2 and 3 above, by proposing a replacement for page 158 of the CD (as at version 1.2). Section 2 below contains the relevant material in a format close to that of the CD. This constitutes a first attempt to formulate the agreed proposal for revision to the CD. Because of the format change, some motivational discussion has been omitted; readers are referred to the original draft for this background material.

For comparison with other approaches, section 3 below gives a simple-minded axiomatisation of the reals from first principles. This is **not** an agreed proposal of the Toolkit Subcommittee, it is simply presented for its own interest and to illustrate one way of defining an arithmetic system extending the integers.

2 PROPOSED DEFINITIONS OF INTEGER ARITHMETIC

Pages 3-6 below constitute the proposal for revising the CD to cover integer arithmetic along lines agreed by the Toolkit Subcommittee. These pages are intended to replace page 158 of version 1.2 of the CD.

Notes

1. The set of general numbers has been called $\mathbb{A}$ because a longer name was felt by the subcommittee to be inelegant.

2. It is necessary to assert that *0* and *1* are integers in the definition of addition etc. Previously, this was guaranteed by their type, but that does not hold when we take $\mathbb{Z}$ to be a subset of $\mathbb{A}$. With the language as is, the other integer literals are slightly problematic. A simple solution is simply to insist, informally, that tools and logics supplying axioms for these literals must do so in a way which is consistent with the obvious definition schema for them. A sentence to this effect is given on page 4 below.

3. All the Z in this document except the fixity declarations has been type-checked. The type-checker used has a syntax which requires semi-colons between declarations in a signature and between the clauses in a predicate parts. These semi-colons should not be necessary in the standard.

4. The fixity declarations are my best attempt at transcribing what is already in the CD.

5. In the standard it is proposed that the symbol for arithmetic negation be a short minus sign. I have had to use $\sim$ because no suitable variant on the minus sign was available.

6. There is a stylistic question about whether to write $\forall\ D \mid A \bullet B$ or $\forall\ D \bullet A \Rightarrow B$. I have chosen the latter for uniformity with the rest of the toolkit definitions.

7. I make no claim that the axiomatisation given here is minimal in any sense. Indeed, there is some quite deliberate redundancy, e.g., the definition of the additive structure of the integers asserts commutativity of addition even though that can be derived from the other axioms.

Name

$\mathbb{A}$	*the set of all numbers*
$\mathbb{Z}$	*the set of integers*

Definition

z

$[\mathbb{A}]$

z

$\mathbb{Z} : \mathbb{P}\ \mathbb{A}$

Description

The given set $\mathbb{A}$ provides a supply of elements for use in specifying number systems.

$\mathbb{Z}$ is the set of integers, i.e., positive, negative and zero whole numbers.

The integers are characterised by the axioms for the their additive structure given on page 4.

Number systems which extend the integers may be specified as supersets of $\mathbb{Z}$.

Name

$\mathbb{N}$	*the set of natural numbers*
$+$	*addition*
$\sim$	*arithmetic negation*

Definition

$$\mathit{fixity\ leftfun\ 30}\ \_ + \_$$
$$\mathit{fixity\ leftfun\ 50}\ \sim \_$$

z

$$
\begin{array}{lll}
\multicolumn{3}{l}{\_ + \_ : \mathbb{A} \times \mathbb{A} \nrightarrow \mathbb{A};} \\
\multicolumn{3}{l}{\sim \_ : \mathbb{A} \nrightarrow \mathbb{A};} \\
\multicolumn{3}{l}{\mathbb{N} : \mathbb{P}\ \mathbb{Z}} \\
\hline
 & & (\mathbb{Z} \times \mathbb{Z}) \lhd (\_ + \_) \in \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}; \\
 & & \mathbb{Z} \lhd (\sim \_) \in \mathbb{Z} \to \mathbb{Z}; \\
 & & \{\mathit{0},\ \mathit{1}\} \subseteq \mathbb{Z}; \\
 & & \\
\forall i, j, k : \mathbb{Z} & \bullet & (i + j) + k = i + (j + k) \\
 & \land & i + j = j + i \\
 & \land & i + \sim i = \mathit{0} \\
 & \land & i + \mathit{0} = i; \\
 & & \\
\forall h : \mathbb{P}\ \mathbb{Z} & \bullet & \mathit{1} \in h \land (\forall i, j : h \bullet\ i + j \in h \land \sim i \in h) \Rightarrow h = \mathbb{Z}; \\
 & & \\
 & & \mathbb{N} = \bigcap \{s : \mathbb{P}\ \mathbb{Z} \mid \mathit{0} \in s \land \{i{:}s \bullet i + \mathit{1}\} \subseteq s\}; \\
 & & \\
 & & \sim \mathit{1} \notin \mathbb{N}
\end{array}
$$

Description

The operators $+$ and $\sim$ are well-defined and take integer values on integer operands; the literals $\mathit{0}$ and $\mathit{1}$ are integers.

The integers form a commutative group under $+$, with $\sim$ as inverse operation and $\mathit{0}$ as identity element.

Any subgroup of the integers which contains $\mathit{1}$ is equal to the whole group.

The set of natural numbers is the smallest set of integers which contains $\mathit{0}$ and is closed under the operation of adding $\mathit{1}$.

$\sim\mathit{1}$ is not a natural number.

These assertions may be shown to imply that the group of integers is an infinite cyclic group with one generator, $\mathit{1}$. Any two infinite cyclic groups are isomorphic, thus the above properties characterise the additive structure of the integers up to isomorphism. See, for example, [1] for the elementary theory of groups including the relevant facts about infinite cyclic groups.

The numeric literals $\mathit{2}, \mathit{3}, \mathit{4}, \ldots$ must be taken to be defined by: $\mathit{2} = \mathit{1} + \mathit{1}, \mathit{3} = \mathit{2} + \mathit{1}, \mathit{4} = \mathit{3} + \mathit{1}, \ldots$

Name

$-$	*subtraction*
$\leq, <, \geq, >$	*arithmetic comparisons*

Definition

$$\begin{array}{l}
\mathit{fixity\ leftfun\ 30}\ _ - _ \\
\mathit{fixity\ rel}\ _ \leq _ \\
\mathit{fixity\ rel}\ _ < _ \\
\mathit{fixity\ rel}\ _ \geq _ \\
\mathit{fixity\ rel}\ _ > _
\end{array}$$

z

$$\_ - \_ : \mathbb{A} \times \mathbb{A} \nrightarrow \mathbb{A}$$

$$\begin{array}{l}
(\mathbb{Z} \times \mathbb{Z}) \lhd (_ - _) \in \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}; \\
\forall i, j : \mathbb{Z} \bullet i - j = i + {\sim}j
\end{array}$$

z

$$\_ \leq \_, \_ < \_, \_ \geq \_, \_ > \_ : \mathbb{A} \leftrightarrow \mathbb{A}$$

$$\begin{array}{lll}
\forall i, j : \mathbb{Z} & \bullet & (i \leq j \Leftrightarrow j - i \in \mathbb{N}) \\
 & \land & (i < j \Leftrightarrow i + 1 \leq j) \\
 & \land & (i \geq j \Leftrightarrow j \leq i) \\
 & \land & (i > j \Leftrightarrow j < i)
\end{array}$$

Description

For all integers i and j, $i - j$ is well-defined and is equal to $i + {\sim}j$.

For all integers i and j, $i \leq j$ holds if and only if the difference, $j - i$, is a natural number.

The remaining arithmetic comparisons are defined in terms of $\leq$.

Name

$*$	*multiplication*
div	*integer division*
mod	*modulus*

Definition

$$\begin{array}{l} \mathit{fixity\ leftfun\ 40\ \_ * \_} \\ \mathit{fixity\ leftfun\ 40\ \_\ div\ \_} \\ \mathit{fixity\ leftfun\ 40\ \_\ mod\ \_} \end{array}$$

z

$$\_ * \_ : \mathbb{A} \times \mathbb{A} \nrightarrow \mathbb{A}$$

$$\begin{array}{lll} & & (\mathbb{Z} \times \mathbb{Z}) \lhd (\_ * \_) \in \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}; \\ & & \\ \forall i, j, k : \mathbb{Z} & \bullet & (i * j) * k = i * (j * k) \\ & \land & i * j = j * i \\ & \land & i * (j + k) = i{*}j + i{*}k \\ & \land & 1 * i = i \end{array}$$

z

$$\_\ \mathit{div}\ \_, \_\ \mathit{mod}\ \_ : \mathbb{A} \times \mathbb{A} \nrightarrow \mathbb{A}$$

$$\begin{array}{lll} & & (\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) \lhd (\_\ \mathit{div}\ \_) \in \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}; \\ & & (\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) \lhd (\_\ \mathit{mod}\ \_) \in \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}; \\ & & \\ \forall i : \mathbb{Z}; j : \mathbb{Z} \setminus \{0\} & \bullet & i = (i\ \mathit{div}\ j) * j + i\ \mathit{mod}\ j \\ & \land & (0 \le i\ \mathit{mod}\ j < j \lor 0 \ge i\ \mathit{mod}\ j > j) \end{array}$$

The multiplication operator $*$ is well-defined and takes integer values on integer operands.

Multiplication on the integers is characterised as the, necessarily unique, operation under which the integers become a commutative ring with 1 as identity element for the multiplication.

For any integers i and j, $i\ \mathit{div}\ j$ and $i\ \mathit{mod}\ j$ are defined and are integers provided $j \neq 0$.

When defined and not 0, $i\ \mathit{mod}\ j$ has the same sign as j. This means that $i\ \mathit{div}\ j$ is the largest integer no greater than the rational number i/j. In other words, division rounds towards $-\infty$.

3 REALS

What follows is **not** part of the proposed revision to the CD endorsed by the Toolkit Subcommittee.

In [6], an axiomatisation of the reals is given supported by a battery of definitions introducing nomenclature for partial orders, algebraic structures of various sorts and many other things. What follows is is an experiment to see how complicated it is to axiomatise the real numbers without building up the supporting definitions. This serves at least to illustrate the approach of introducing number systems as supersets of $\mathbb{Z}$.

The axiomatisation will actually fit in one axiomatic box on one page, but I have split it over three boxes to give room for some narrative. The three boxes correspond to the following three properties of the real numbers:

1. the reals form a field;
2. the field of reals may be linearly ordered in a way which is compatible with addition and multiplication, in a certain sense; to define such a linear order,it is sufficient to find an additively and multiplicatively closed set, P, of *positive elements*, such that the sets P, $-P$ and $\{0\}$ partition the field.
3. any non-empty set of reals, which is bounded below with respect to the order given in property 2, possesses a greatest lower bound.

These properties characterise the real numbers up to isomorphism. It is a consequence of properties 1 and 2 that the reals contain a subring isomorphic to the integers. In the present context, we insist that the reals actually contain the integers — a state of affairs which can be be arranged by a trivial adaptation of any of the usual constructions of the reals.

Axiomatisations of the reals very similar to the one given here may be found in elementary calculus textbooks. See, for example, [3]. A proof that the axiomatisation does characterise the reals is less frequent in elementary textbooks, but may be found, for example, in [2].

I have used the symbol $\div$ for real division. The symbol / might be preferred, but it is presumably reserved for its use in schema renaming.

I have use the name *inf* for the infimum or greatest lower bound function, rather than *glb*. *inf* seems to be more prevalent in the calculus literature and avoids conflicting with other potential uses of *glb*. The axiomatic description for *inf* could be replaced with an axiom saying that the infimum exists for any set that is bounded below; however, I felt it was pleasant for each of the axioms to be captured in a paragraph which actually defines something, rather than just constrains what we already have.

Name

$\mathbb{R}$	*the set of real numbers*
$\div$	*real division*

Definition

$$\mathit{fixity\ leftfun\ 40}\ \_ \div \_$$

z

$$\mathbb{R} : \mathbb{P}_{1}\ \mathbb{A};$$
$$\_ \div \_ : \mathbb{A} \times \mathbb{A} \nrightarrow \mathbb{A}$$

$$(\mathbb{R} \times \mathbb{R}) \lhd (\_ + \_) \in \mathbb{R} \times \mathbb{R} \to \mathbb{R};$$
$$(\mathbb{R} \times \mathbb{R}) \lhd (\_ * \_) \in \mathbb{R} \times \mathbb{R} \to \mathbb{R};$$
$$(\mathbb{R} \times \mathbb{R} \setminus \{0\}) \lhd (\_ \div \_) \in \mathbb{R} \times \mathbb{R} \setminus \{0\} \to \mathbb{R};$$
$$\mathbb{R} \lhd (\sim \_) \in \mathbb{R} \to \mathbb{R};$$
$$\mathbb{Z} \subseteq \mathbb{R};$$

$$\begin{array}{lll} \forall x, y, z : \mathbb{R} & \bullet & (x + y) + z = x + (y + z) \\ & \wedge & x + y = y + z \\ & \wedge & x + \sim x = 0 \\ & \wedge & x + 0 = x; \end{array}$$

$$\begin{array}{lll} \forall x, y, z : \mathbb{R} & \bullet & (x * y) * z = x * (y * z) \\ & \wedge & x * y = y * x \\ & \wedge & x * (y + z) = x*y + x*z \\ & \wedge & 1 * x = x; \end{array}$$

$$\forall x : \mathbb{R};\ y : \mathbb{R} \setminus \{0\} \bullet \quad (x \div y) * y = x$$

Description

The real numbers extend the ring of integers and form a field under the extended arithmetic operators together with the division operator $\div$.

Together, with the axioms given on pages 9 and 10 the axioms on this page characterise the real numbers up to isomorphism. For further mathematical background and a proof of this characterisation, see, for example, [2].

Name

$\mathbb{R}_+$, $\mathbb{R}_-$ *positive and negative real numbers*

Definition

z

$$
\begin{array}{|l}
\quad \mathbb{R}_+, \mathbb{R}_- : \mathbb{P}_1 \mathbb{A} \\
\hline
\quad (\mathbb{R}_+ \times \mathbb{R}_+) \lhd (\_ + \_) \in \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+; \\
\quad (\mathbb{R}_+ \times \mathbb{R}_+) \lhd (\_ * \_) \in \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+; \\
\\
\quad \mathbb{R}_- = (\sim\_) (\!| \mathbb{R}_+ |\!); \\
\\
\quad \mathbb{R}_- \cap \mathbb{R}_+ = \varnothing; \\
\quad \mathbb{R} = \mathbb{R}_- \cup \{0\} \cup \mathbb{R}_+; \\
\\
\forall x, y : \mathbb{R} \bullet \quad x \leq y \Leftrightarrow y + \sim x \in \mathbb{R}_+ \cup \{0\}
\end{array}
$$

Description

The set of positive real numbers is closed under addition and multiplication.

The set of negative real numbers comprises precisely the negatives of the positive real numbers.

The sets of positive and negative real numbers are disjoint and together with $\{0\}$, they partition $\mathbb{R}$.

These properties imply that $\mathbb{R}$ is an ordered field: for real numbers, x and y, $x \leq y$ holds if and only if the difference $y + \sim x$ is non-negative.

The ordering given by $\leq$ is total: for any x and y, either $x \leq y$ or $y \leq x$. Moreover, the ordering is compatible with addition and multiplication: if x $\leq$ y then $x + z \leq y + z$, for any z; if x $\leq$ y and also $0 \leq z$ then $x * z \leq y * z$.

Together, with the axioms given on pages 8 and 10 the axioms on this page characterise the real numbers up to isomorphism. For further mathematical background and a proof of this characterisation, see, for example, [2].

Name

inf *infimum, the greatest lower bound operator*

Definition

z

$$inf : \mathbb{P}_1\ \mathbb{R} \nrightarrow \mathbb{R}$$

$$dom\ inf = \{A : \mathbb{P}_1\ \mathbb{R} \mid \exists x : \mathbb{R} \bullet \{x\} \times A \subseteq (\_ \leq \_)\};$$

$$\begin{array}{lll} \forall A : \mathbb{P}_1\ \mathbb{R} & \bullet & (\exists x : \mathbb{R} \bullet \{x\} \times A \subseteq (\_ \leq \_)) \\ & \Rightarrow & \{inf\ A\} \times A \subseteq (\_ \leq \_) \\ & \wedge & (\forall y : \mathbb{R} \bullet \{y\} \times A \subseteq (\_ \leq \_) \Rightarrow y \leq inf\ A) \end{array}$$

Description

The domain of the infimum function comprises all non-empty sets of reals which are bounded below. (The idiom $\{x\} \times A \subseteq (\_ \leq \_)$ means that x is less than or equal to every element of A, i.e. x is a lower bound for A).

If a set, A, of reals is bounded below, then *inf* A is a greatest lower bound for A. *inf* A need not be a member of A.

Together, with the axioms given on pages 8 and 9 the axioms on this page characterise the real numbers up to isomorphism. For further mathematical background and a proof of this characterisation, see, for example, [2].

References

[1] P.M. Cohn. *Algebra*, volume 1. John Wiley & Sons, Inc., 1974.

[2] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert. *Numbers*. Springer-Verlag, 1990.

[3] Barry M. Mitchell. *Calculus without Analytic Geometry*. D.C. Heath & Co., 1969.

[4] J.M. Spivey. *The Z Notation: A Reference Manual*. Prentice-Hall, 1989.

[5] J.M. Spivey. *The Z Notation: A Reference Manual, Second Edition*. Prentice-Hall, 1992.

[6] Z Standards Document D-172. *Z Notation Mathematical Tool-kit*. Sam Valentine, Department of Computing, University of Brighton, March 1995.