FORMALIZED MATHEMATICS
Vol.1, No.3, May–August 1990
Université Catholique de Louvain

Group and Field Definitions

Józef Białas[1]
Łódź University

Summary. The article contains exactly the same definitions of group and field as those in [3]. These definitions were prepared without the help of the definitions and properties of *Nat* and *Real* modes icluded in the MML. This is the first of a series of articles in which we are going to introduce the concept of the set of real numbers in a elementary axiomatic way.

MML Identifier: `REALSET1`.

The terminology and notation used here are introduced in the following papers: [4], [1], and [2]. Let x be arbitrary. The functor single(x) yields a set and is defined as follows:

single(x) $= \{x\}$.

One can prove the following proposition

(1) For arbitrary x holds single(x) $= \{x\}$.

Let X, Y be sets. The functor $X \# Y$ yields a set and is defined by:

$X \# Y = [\!: X, Y :\!]$.

We now state several propositions:

(2) For all sets X, Y holds $X \# Y = [\!: X, Y :\!]$.

(3) For arbitrary z and for every set A holds $z \in A \# A$ if and only if there exist arbitrary x, y such that $x \in A$ and $y \in A$ and $z = \langle x, y \rangle$.

(4) For every set X and for every subset A of X holds $A \# A \subseteq X \# X$.

(5) For every set X such that $X = \emptyset$ holds $X \# X = \emptyset$.

(6) For every set X such that $X \# X = \emptyset$ holds $X = \emptyset$.

(7) For every set X holds $X \# X = \emptyset$ if and only if $X = \emptyset$.

Let X be a set. A binary operation of X is a function from $X \# X$ into X.

The following propositions are true:

[1]Supported by RPBP III.24 C9

ISSN 0777–4028

(8) For every set X and for every function F from $X\#X$ into X holds F is a binary operation of X.

(9) For every set X and for every function F holds F is a function from $X\#X$ into X if and only if F is a binary operation of X.

(10) For every set X and for every function F from $X\#X$ into X and for arbitrary x such that $x \in X\#X$ holds $F(x) \in X$.

(11) For every set X and for every binary operation F of X there exists a subset A of X such that for arbitrary x such that $x \in A\#A$ holds $F(x) \in A$.

Let X be a set, and let F be a binary operation of X, and let A be a subset of X. We say that F is in A if and only if:

for arbitrary x such that $x \in A\#A$ holds $F(x) \in A$.

Next we state a proposition

(12) For every set X and for every binary operation F of X and for every subset A of X holds F is in A if and only if for arbitrary x such that $x \in A\#A$ holds $F(x) \in A$.

Let X be a set, and let F be a binary operation of X. A subset of X is said to be a set closed w.r.t. F if:

for arbitrary x such that $x \in \text{it}\#\text{it}$ holds $F(x) \in \text{it}$.

The following propositions are true:

(13) For every set X and for every binary operation F of X and for every subset A of X holds A is a set closed w.r.t. F if and only if for arbitrary x such that $x \in A\#A$ holds $F(x) \in A$.

(14) For every set X and for every binary operation F of X and for every set A closed w.r.t. F holds $F \restriction (A\#A)$ is a binary operation of A.

Let X be a set, and let F be a binary operation of X, and let A be a set closed w.r.t. F. The functor $F \restriction A$ yielding a binary operation of A, is defined by:

$F \restriction A = F \restriction (A\#A)$.

The following propositions are true:

(15) For every set X and for every binary operation F of X and for every set A closed w.r.t. F holds $F \restriction A = F \restriction (A\#A)$.

(16) For every set X and for every binary operation F of X and for every subset A of X such that A is a set closed w.r.t. F holds $F \restriction (A\#A)$ is a binary operation of A.

(17) For every set X and for every binary operation F of X and for every set A closed w.r.t. F holds $F \restriction A$ is a binary operation of A.

We consider group structures which are systems

$\langle$ a carrier, an addition, a zero $\rangle$

where the carrier is a non-empty set, the addition is a binary operation of the carrier, and the zero is an element of the carrier. Let A be a non-empty set, and let og be a binary operation of A, and let ng be an element of A. The functor group(A, og, ng) yielding a group structure, is defined as follows:

$A =$ the carrier of group(A, og, ng) and $og =$ the addition of group(A, og, ng) and $ng =$ the zero of group(A, og, ng).

The following propositions are true:

(18) For every non-empty set A and for every binary operation og of A and for every element ng of A and for every GR being a group structure holds $GR =$ group(A, og, ng) if and only if $A =$ the carrier of GR and $og =$ the addition of GR and $ng =$ the zero of GR.

(19) For every non-empty set A and for every binary operation og of A and for every element ng of A holds group(A, og, ng) is a group structure and $A =$ the carrier of group(A, og, ng) and $og =$ the addition of group(A, og, ng) and $ng =$ the zero of group(A, og, ng).

A group structure is called a group if:

there exists a non-empty set A and there exists a binary operation og of A and there exists an element ng of A such that it $=$ group(A, og, ng) and for all elements a, b, c of A holds $og(\langle og(\langle a, b\rangle), c\rangle) = og(\langle a, og(\langle b, c\rangle)\rangle)$ and for every element a of A holds $og(\langle a, ng\rangle) = a$ and $og(\langle ng, a\rangle) = a$ and for every element a of A there exists an element b of A such that $og(\langle a, b\rangle) = ng$ and $og(\langle b, a\rangle) = ng$ and for all elements a, b of A holds $og(\langle a, b\rangle) = og(\langle b, a\rangle)$.

Let D be a group. The carrier of D yields a non-empty set and is defined as follows:

there exists a binary operation od of the carrier of D and there exists an element nd of the carrier of D such that $D =$ group(the carrier of D, od, nd).

The following two propositions are true:

(20) For every group D and for every non-empty set A holds
$A =$ the carrier of D
if and only if there exists a binary operation od of A and there exists an element nd of A such that $D =$ group(A, od, nd).

(21) For every group D holds the carrier of D is a non-empty set and there exists a binary operation od of the carrier of D and there exists an element nd of the carrier of D such that $D =$ group(the carrier of D, od, nd).

Let D be a group. The functor $+_D$ yielding a binary operation of the carrier of D, is defined as follows:

there exists an element nd of the carrier of D such that
$D =$ group(the carrier of $D, +_D, nd$) .

The following propositions are true:

(22) For every group D and for every binary operation od of the carrier of D holds $od = +_D$ if and only if there exists an element nd of the carrier of D such that $D =$ group(the carrier of D, od, nd).

(23) For every group D holds $+_D$ is a binary operation of the carrier of D and there exists an element nd of the carrier of D such that
$D =$ group(the carrier of $D, +_D, nd$) .

Let D be a group. The functor $\mathbf{0}_D$ yielding an element of the carrier of D, is defined by:

$D = \mathrm{group}(\text{the carrier of } D, +_D, \mathbf{0}_D)$.

Next we state a number of propositions:

(24) For every group D and for every element ng of the carrier of D holds $ng = \mathbf{0}_D$ if and only if $D = \mathrm{group}(\text{the carrier of } D, +_D, ng)$.

(25) For every group D holds $\mathbf{0}_D$ is an element of the carrier of D and $D = \mathrm{group}(\text{the carrier of } D, +_D, \mathbf{0}_D)$.

(26) For every group D holds $D = \mathrm{group}(\text{the carrier of } D, +_D, \mathbf{0}_D)$.

(27) For every group D and for every non-empty set A and for every binary operation og of A and for every element ng of A such that $D = \mathrm{group}(A, og, ng)$ holds the carrier of $D = A$ and $+_D = og$ and $\mathbf{0}_D = ng$.

(28) For every group D and for all elements a, b, c of the carrier of D holds $+_D(\langle +_D(\langle a, b \rangle), c \rangle) = +_D(\langle a, +_D(\langle b, c \rangle) \rangle)$.

(29) For every group D and for every element a of the carrier of D holds $+_D(\langle a, \mathbf{0}_D \rangle) = a$ and $+_D(\langle \mathbf{0}_D, a \rangle) = a$.

(30) For every group D and for every element a of the carrier of D there exists an element b of the carrier of D such that $+_D(\langle a, b \rangle) = \mathbf{0}_D$ and $+_D(\langle b, a \rangle) = \mathbf{0}_D$.

(31) For every group D and for all elements a, b of the carrier of D holds $+_D(\langle a, b \rangle) = +_D(\langle b, a \rangle)$.

(32) There exist arbitrary x, y such that $x \neq y$.

(33) There exists a non-empty set A such that for every element z of A holds $A \setminus \mathrm{single}(z)$ is a non-empty set.

A non-empty set is said to be an at least 2-elements set if:
for every element x of it holds it $\setminus \mathrm{single}(x)$ is a non-empty set.

We now state two propositions:

(34) For every non-empty set A holds A is an at least 2-elements set if and only if for every element x of A holds $A \setminus \mathrm{single}(x)$ is a non-empty set.

(35) For every non-empty set A such that for every element x of A holds $A \setminus \mathrm{single}(x)$ is a non-empty set holds A is an at least 2-elements set.

We consider field structures which are systems

⟨ a carrier, an addition, a multiplication, a zero, a unit ⟩

where the carrier is an at least 2-elements set, the addition is a binary operation of the carrier, the multiplication is a binary operation of the carrier, the zero is an element of the carrier, and the unit is an element of the carrier. Let A be an at least 2-elements set, and let od, om be binary operations of A, and let nd be an element of A, and let nm be an element of $A \setminus \mathrm{single}(nd)$. The functor $\mathrm{field}(A, od, om, nd, nm)$ yielding a field structure, is defined as follows:

$A =$ the carrier of $\mathrm{field}(A, od, om, nd, nm)$ and $od =$ the addition of $\mathrm{field}(A, od, om, nd, nm)$ and $om =$ the multiplication of $\mathrm{field}(A, od, om, nd, nm)$ and

nd = the zero of field(A, od, om, nd, nm) and nm = the unit of field(A, od, om, nd, nm).

We now state two propositions:

(36) Let A be an at least 2-elements set. Let od, om be binary operations of A. Then for every element nd of A and for every element nm of $A \setminus \text{single}(nd)$ and for every F being a field structure holds $F = \text{field}(A, od, om, nd, nm)$ if and only if A = the carrier of F and od = the addition of F and om = the multiplication of F and nd = the zero of F and nm = the unit of F.

(37) Let A be an at least 2-elements set. Let od, om be binary operations of A. Let nd be an element of A. Let nm be an element of $A \setminus \text{single}(nd)$. Then

(i) field(A, od, om, nd, nm) is a field structure,
(ii) A = the carrier of field(A, od, om, nd, nm),
(iii) od = the addition of field(A, od, om, nd, nm),
(iv) om = the multiplication of field(A, od, om, nd, nm),
(v) nd = the zero of field(A, od, om, nd, nm),
(vi) nm = the unit of field(A, od, om, nd, nm).

Let X be an at least 2-elements set, and let F be a binary operation of X, and let x be an element of X. We say that F is binary operation preserving x if and only if:

$X \setminus \text{single}(x)$ is a set closed w.r.t. F and $F \restriction ((X \setminus \text{single}(x)) \# (X \setminus \text{single}(x)))$ is a binary operation of $X \setminus \text{single}(x)$.

Next we state two propositions:

(38) For every at least 2-elements set X and for every binary operation F of X and for every element x of X holds F is binary operation preserving x if and only if $X \setminus \text{single}(x)$ is a set closed w.r.t. F and $F \restriction ((X \setminus \text{single}(x)) \# (X \setminus \text{single}(x)))$ is a binary operation of $X \setminus \text{single}(x)$.

(39) For every set X and for every subset A of X there exists a binary operation F of X such that for arbitrary x such that $x \in A \# A$ holds $F(x) \in A$.

Let X be a set, and let A be a subset of X. A binary operation of X is said to be a binary operation of X preserving A if:

for arbitrary x such that $x \in A \# A$ holds it$(x) \in A$.

One can prove the following two propositions:

(40) For every set X and for every subset A of X and for every binary operation F of X holds F is a binary operation of X preserving A if and only if for arbitrary x such that $x \in A \# A$ holds $F(x) \in A$.

(41) For every set X and for every subset A of X and for every binary operation F of X preserving A holds $F \restriction (A \# A)$ is a binary operation of A.

Let X be a set, and let A be a subset of X, and let F be a binary operation of X preserving A. The functor $F \restriction A$ yielding a binary operation of A, is defined as follows:

$F \restriction A = F \restriction (A\#A)$.

We now state two propositions:

(42) For every set X and for every subset A of X and for every binary operation F of X preserving A holds $F \restriction A = F \restriction (A\#A)$.

(43) For every at least 2-elements set A and for every element x of A there exists a binary operation F of A such that for arbitrary y such that $y \in (A \setminus \mathrm{single}(x))\#(A \setminus \mathrm{single}(x))$ holds $F(y) \in A \setminus \mathrm{single}(x)$.

Let A be an at least 2-elements set, and let x be an element of A. A binary operation of A is called a binary operation of A preserving $A \setminus \{x\}$ if:

for arbitrary y such that $y \in (A \setminus \mathrm{single}(x))\#(A \setminus \mathrm{single}(x))$ holds $\mathrm{it}(y) \in A \setminus \mathrm{single}(x)$.

One can prove the following two propositions:

(44) For every at least 2-elements set A and for every element x of A and for every binary operation F of A holds F is a binary operation of A preserving $A \setminus \{x\}$ if and only if for arbitrary y such that $y \in (A \setminus \mathrm{single}(x))\#(A \setminus \mathrm{single}(x))$ holds $F(y) \in A \setminus \mathrm{single}(x)$.

(45) For every at least 2-elements set A and for every element x of A and for every binary operation F of A preserving $A \setminus \{x\}$ holds $F \restriction ((A \setminus \mathrm{single}(x))\#(A \setminus \mathrm{single}(x)))$ is a binary operation of $A \setminus \mathrm{single}(x)$.

Let A be an at least 2-elements set, and let x be an element of A, and let F be a binary operation of A preserving $A \setminus \{x\}$. The functor $F \restriction_x A$ yields a binary operation of $A \setminus \mathrm{single}(x)$ and is defined as follows:

$F \restriction_x A = F \restriction ((A \setminus \mathrm{single}(x))\#(A \setminus \mathrm{single}(x)))$.

One can prove the following proposition

(46) For every at least 2-elements set A and for every element x of A and for every binary operation F of A preserving $A \setminus \{x\}$ holds $F \restriction_x A = F \restriction ((A \setminus \mathrm{single}(x))\#(A \setminus \mathrm{single}(x)))$.

A field structure is said to be a field if:

there exists an at least 2-elements set A and there exists a binary operation od of A and there exists an element nd of A and there exists a binary operation om of A preserving $A \setminus \{nd\}$ and there exists an element nm of $A \setminus \mathrm{single}(nd)$ such that $\mathrm{it} = \mathrm{field}(A, od, om, nd, nm)$ and $\mathrm{group}(A, od, nd)$ is a group and for every non-empty set B and for every binary operation P of B and for every element e of B such that $B = A \setminus \mathrm{single}(nd)$ and $e = nm$ and $P = om \restriction_{nd} A$ holds $\mathrm{group}(B, P, e)$ is a group and for all elements x, y, z of A holds $om(\langle x, od(\langle y, z\rangle)\rangle) = od(\langle om(\langle x, y\rangle), om(\langle x, z\rangle)\rangle)$.

We now state two propositions:

(47) Let F be a group structure. Then F is a group if and only if there exists a non-empty set A and there exists a binary operation og of A and there exists an element ng of A such that $F = \mathrm{group}(A, og, ng)$ and for all elements a, b, c of A holds $og(\langle og(\langle a, b\rangle), c\rangle) = og(\langle a, og(\langle b, c\rangle)\rangle)$ and for every element a of A holds $og(\langle a, ng\rangle) = a$ and $og(\langle ng, a\rangle) = a$

and for every element a of A there exists an element b of A such that $og(\langle a,b\rangle) = ng$ and $og(\langle b,a\rangle) = ng$ and for all elements a, b of A holds $og(\langle a,b\rangle) = og(\langle b,a\rangle)$.

(48) Let F be a field structure. Then F is a field if and only if there exists an at least 2-elements set A and there exists a binary operation od of A and there exists an element nd of A and there exists a binary operation om of A preserving $A \setminus \{nd\}$ and there exists an element nm of $A \setminus \mathrm{single}(nd)$ such that $F = \mathrm{field}(A, od, om, nd, nm)$ and $\mathrm{group}(A, od, nd)$ is a group and for every non-empty set B and for every binary operation P of B and for every element e of B such that $B = A \setminus \mathrm{single}(nd)$ and $e = nm$ and $P = om \restriction_{nd} A$ holds $\mathrm{group}(B, P, e)$ is a group and for all elements x, y, z of A holds $om(\langle x, od(\langle y,z\rangle)\rangle) = od(\langle om(\langle x,y\rangle), om(\langle x,z\rangle)\rangle)$.

References

[1] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[2] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[3] Jean Dieudonné. *Foundations of Modern Analises.* Academic Press, New York and London, 1960.

[4] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received October 27, 1989