FORMALIZED MATHEMATICS
Vol.1, No.5, November–December 1990
Université Catholique de Louvain

Properties of Fields

Józef Białas[1]
University of Łódź

Summary. The second part of considerations concerning groups and fields. It includes a definition and properties of commutative field F as a structure defined by: the set, a support of F, containing two different elements, by two binary operations $+_F$, $\cdot_F$ on this set, called addition and multiplication, and by two elements from the support of F, $\mathbf{0}_F$ being neutral for addition and $\mathbf{1}_F$ being neutral for multiplication. This structure is named a field if $\langle$the support of F, $+_F$, $\mathbf{0}_F\rangle$ and $\langle$the support of F, $\cdot_F$, $\mathbf{1}_F\rangle$ are commutative groups and multiplication has the property of left-hand and right-hand distributivity with respect to addition. It is demonstrated that the field F satisfies the definition of a field in the axiomatic approach.

MML Identifier: REALSET2.

The articles [4], [2], [3], and [1] provide the notation and terminology for this paper. A field structure is said to be a field if:

(Def.1) there exists an at least 2-elements set A and there exists a binary operation o_1 of A and there exists an element n_1 of A and there exists a binary operation o_2 of A preserving $A \setminus \{n_1\}$ and there exists an element n_2 of $A \setminus \mathrm{single}(n_1)$ such that it $= \mathrm{field}(A, o_1, o_2, n_1, n_2)$ and $\mathrm{group}(A, o_1, n_1)$ 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 $B = A \setminus \mathrm{single}(n_1)$ and $e = n_2$ and $P = o_2 \restriction_{n_1} A$ holds $\mathrm{group}(B, P, e)$ is a group and for all elements x, y, z of A holds $o_2(\langle x, o_1(\langle y, z\rangle)\rangle) = o_1(\langle o_2(\langle x, y\rangle), o_2(\langle x, z\rangle)\rangle)$ and $o_2(\langle o_1(\langle x, y\rangle), z\rangle) = o_1(\langle o_2(\langle x, z\rangle), o_2(\langle y, z\rangle)\rangle)$.

Next we state the proposition

(1) 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 o_1 of A and there exists an element n_1 of A and there exists a binary operation o_2 of A preserving $A \setminus \{n_1\}$ and there exists an element n_2 of $A \setminus \mathrm{single}(n_1)$ such

[1]Supported by RPBP.III-24.

ISSN 0777–4028

that $F = \mathrm{field}(A, o_1, o_2, n_1, n_2)$ and $\mathrm{group}(A, o_1, n_1)$ 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 $B = A \setminus \mathrm{single}(n_1)$ and $e = n_2$ and $P = o_2 \upharpoonright_{n_1} A$ holds $\mathrm{group}(B, P, e)$ is a group and for all elements x, y, z of A holds $o_2(\langle x, o_1(\langle y, z\rangle)\rangle) = o_1(\langle o_2(\langle x, y\rangle), o_2(\langle x, z\rangle)\rangle)$ and $o_2(\langle o_1(\langle x, y\rangle), z\rangle) = o_1(\langle o_2(\langle x, z\rangle), o_2(\langle y, z\rangle)\rangle)$.

Let F be a field. The support of F yielding an at least 2-elements set is defined by:

(Def.2) there exists a binary operation o_1 of the support of F and there exists an element n_1 of the support of F and there exists a binary operation o_2 of the support of F preserving the support of $F \setminus \{n_1\}$ and there exists an element n_2 of (the support of F) $\setminus \mathrm{single}(n_1)$ such that $F = \mathrm{field}(\text{the support of } F, o_1, o_2, n_1, n_2)$.

The following proposition is true

(2) For every field F and for every at least 2-elements set A holds $A =$ the support of F if and only if there exists a binary operation o_1 of A and there exists an element n_1 of A and there exists a binary operation o_2 of A preserving $A \setminus \{n_1\}$ and there exists an element n_2 of $A \setminus \mathrm{single}(n_1)$ such that $F = \mathrm{field}(A, o_1, o_2, n_1, n_2)$.

Let F be a field. The functor $+_F$ yielding a binary operation of the support of F
is defined as follows:

(Def.3) there exists an element n_1 of the support of F and there exists a binary operation o_2 of the support of F preserving the support of $F \setminus \{n_1\}$ and there exists an element n_2 of the support of $F \setminus \mathrm{single}(n_1)$ such that $F = \mathrm{field}(\text{the support of } F, +_F, o_2, n_1, n_2)$.

Next we state the proposition

(3) For every field F and for every binary operation o_1 of the support of F holds $o_1 = +_F$ if and only if there exists an element n_1 of the support of F and there exists a binary operation o_2 of the support of F preserving the support of $F \setminus \{n_1\}$ and there exists an element n_2 of the support of $F \setminus \mathrm{single}(n_1)$ such that $F = \mathrm{field}(\text{the support of } F, o_1, o_2, n_1, n_2)$.

Let F be a field. The functor $\mathbf{0}_F$ yielding an element of the support of F is defined by:

(Def.4) there exists a binary operation o_2 of the support of F preserving the support of $F \setminus \{\mathbf{0}_F\}$ and there exists an element n_2 of the support of $F \setminus \mathrm{single}(\mathbf{0}_F)$ such that $F = \mathrm{field}(\text{the support of } F, +_F, o_2, \mathbf{0}_F, n_2)$.

Next we state the proposition

(4) For every field F and for every element n_1 of the support of F holds $n_1 = \mathbf{0}_F$ if and only if there exists a binary operation o_2 of the support of F preserving the support of $F \setminus \{n_1\}$ and there exists an element n_2 of

the support of $F \setminus \mathrm{single}(n_1)$ such that $F = \mathrm{field}(\text{the support of } F, +_F, o_2, n_1, n_2)$.

Let F be a field. The functor $\cdot_F$ yields a binary operation of the support of F preserving the support of $F \setminus \{\mathbf{0}_F\}$and is defined as follows:

(Def.5) there exists an element n_2 of the support of $F \setminus \mathrm{single}(\mathbf{0}_F)$ such that $F = \mathrm{field}(\text{the support of } F, +_F, \cdot_F, \mathbf{0}_F, n_2)$.

We now state the proposition

(5) For every field F and for every binary operation o_2 of the support of F preserving the support of $F \setminus \{\mathbf{0}_F\}$ holds $o_2 = \cdot_F$ if and only if there exists an element n_2 of the support of $F \setminus \mathrm{single}(\mathbf{0}_F)$ such that $F = \mathrm{field}(\text{the support of } F, +_F, o_2, \mathbf{0}_F, n_2)$.

Let F be a field. The functor $\mathbf{1}_F$ yielding an element of the support of $F \setminus \mathrm{single}(\mathbf{0}_F)$ is defined as follows:

(Def.6) $F = \mathrm{field}(\text{the support of } F, +_F, \cdot_F, \mathbf{0}_F, \mathbf{1}_F)$.

The following propositions are true:

(6) For every field F and for every element n_2 of the support of $F \setminus \mathrm{single}(\mathbf{0}_F)$ holds $n_2 = \mathbf{1}_F$ if and only if $F = \mathrm{field}(\text{the support of } F, +_F, \cdot_F, \mathbf{0}_F, n_2)$.

(7) For every field F holds $F = \mathrm{field}(\text{the support of } F, +_F, \cdot_F, \mathbf{0}_F, \mathbf{1}_F)$.

(8) For every field F holds $\mathrm{group}(\text{the support of } F, +_F, \mathbf{0}_F)$ is a group.

(9) For every field F and for every non-empty set B and for every binary operation P of B and for every element e of B such that $B =$ the support of $F \setminus \mathrm{single}(\mathbf{0}_F)$ and $e = \mathbf{1}_F$ and $P = \cdot_F \restriction_{\mathbf{0}_F}$ the support of F holds $\mathrm{group}(B, P, e)$ is a group.

(10) Let F be a field. Let x, y, z be elements of the support of F. Then
  (i) $\cdot_F(\langle x, +_F(\langle y, z\rangle)\rangle) = +_F(\langle \cdot_F(\langle x, y\rangle), \cdot_F(\langle x, z\rangle)\rangle)$,
  (ii) $\cdot_F(\langle +_F(\langle x, y\rangle), z\rangle) = +_F(\langle \cdot_F(\langle x, z\rangle), \cdot_F(\langle y, z\rangle)\rangle)$.

(11) For every field F and for all elements a, b, c of the support of F holds $+_F(\langle +_F(\langle a, b\rangle), c\rangle) = +_F(\langle a, +_F(\langle b, c\rangle)\rangle)$.

(12) For every field F and for all elements a, b of the support of F holds $+_F(\langle a, b\rangle) = +_F(\langle b, a\rangle)$.

(13) For every field F and for every element a of the support of F holds $+_F(\langle a, \mathbf{0}_F\rangle) = a$ and $+_F(\langle \mathbf{0}_F, a\rangle) = a$.

(14) For every field F and for every element a of the support of F there exists an element b of the support of F such that $+_F(\langle a, b\rangle) = \mathbf{0}_F$ and $+_F(\langle b, a\rangle) = \mathbf{0}_F$.

Let F be an at least 2-elements set. A set is said to be a one-element subset of F if:

(Def.7) there exists an element x of F such that it $= \mathrm{single}(x)$.

We now state the proposition

(15) For every at least 2-elements set F and for every one-element subset A of F holds $F \setminus A$ is a non-empty set.

Let F be an at least 2-elements set, and let A be a one-element subset of F. Then $F \setminus A$ is a non-empty set.

The following proposition is true

(16) For every at least 2-elements set F and for every element x of F holds single(x) is a one-element subset of F.

Let F be an at least 2-elements set, and let x be an element of F. Then single(x) is a one-element subset of F.

The following propositions are true:

(20)[2] For every field F and for all elements a, b, c of the support of $F \setminus$ single($\mathbf{0}_F$) holds $\cdot_F(\langle \cdot_F(\langle a, b \rangle), c \rangle) = \cdot_F(\langle a, \cdot_F(\langle b, c \rangle) \rangle)$.

(21) For every field F and for all elements a, b of the support of $F \setminus$single($\mathbf{0}_F$) holds $\cdot_F(\langle a, b \rangle) = \cdot_F(\langle b, a \rangle)$.

(22) For every field F and for every element a of the support of $F \setminus$single($\mathbf{0}_F$) holds $\cdot_F(\langle a, \mathbf{1}_F \rangle) = a$ and $\cdot_F(\langle \mathbf{1}_F, a \rangle) = a$.

(23) For every field F and for every element a of the support of $F \setminus$ single($\mathbf{0}_F$) there exists an element b of the support of $F \setminus$single($\mathbf{0}_F$) such that $\cdot_F(\langle a, b \rangle) = \mathbf{1}_F$ and $\cdot_F(\langle b, a \rangle) = \mathbf{1}_F$.

Let F be a field. The functor $-_F$ yielding a function from the support of F into the support of F is defined by:

(Def.8) for every element x of the support of F holds $+_F(\langle x, -_F(x) \rangle) = \mathbf{0}_F$.

One can prove the following propositions:

(24) For every field F and for every element x of the support of F holds $+_F(\langle x, -_F(x) \rangle) = \mathbf{0}_F$.

(25) For every field F and for every function S from the support of F into the support of F holds $S = -_F$ if and only if for every element x of the support of F holds $+_F(\langle x, S(x) \rangle) = \mathbf{0}_F$.

(26) For every field F and for every element x of the support of F and for every element y of the support of F such that $+_F(\langle x, y \rangle) = \mathbf{0}_F$ holds $y = -_F(x)$.

(27) For every field F and for every element x of the support of F holds $x = -_F(-_F(x))$.

(28) For every field F and for all elements a, b of the support of F holds $+_F(\langle a, b \rangle)$ is an element of the support of F and $\cdot_F(\langle a, b \rangle)$ is an element of the support of F and $-_F(a)$ is an element of the support of F.

(29) For every field F and for all elements a, b, c of the support of F holds $\cdot_F(\langle a, +_F(\langle b, -_F(c) \rangle) \rangle) = +_F(\langle \cdot_F(\langle a, b \rangle), -_F(\cdot_F(\langle a, c \rangle)) \rangle)$.

(30) For every field F and for all elements a, b, c of the support of F holds $\cdot_F(\langle +_F(\langle a, -_F(b) \rangle), c \rangle) = +_F(\langle \cdot_F(\langle a, c \rangle), -_F(\cdot_F(\langle b, c \rangle)) \rangle)$.

[2]The propositions (17)–(19) became obvious.

(31) For every field F and for every element a of the support of F holds $\cdot_F(\langle a, \mathbf{0}_F \rangle) = \mathbf{0}_F$.

(32) For every field F and for every element a of the support of F holds $\cdot_F(\langle \mathbf{0}_F, a \rangle) = \mathbf{0}_F$.

(33) For every field F and for all elements a, b of the support of F holds $-_F(\cdot_F(\langle a, b \rangle)) = \cdot_F(\langle a, -_F(b) \rangle)$.

(34) For every field F holds $\cdot_F(\langle \mathbf{1}_F, \mathbf{0}_F \rangle) = \mathbf{0}_F$.

(35) For every field F holds $\cdot_F(\langle \mathbf{0}_F, \mathbf{1}_F \rangle) = \mathbf{0}_F$.

(36) For every field F and for all elements a, b of the support of F holds $\cdot_F(\langle a, b \rangle)$ is an element of the support of F.

(37) For every field F and for all elements a, b, c of the support of F holds $\cdot_F(\langle \cdot_F(\langle a, b \rangle), c \rangle) = \cdot_F(\langle a, \cdot_F(\langle b, c \rangle) \rangle)$.

(38) For every field F and for all elements a, b of the support of F holds $\cdot_F(\langle a, b \rangle) = \cdot_F(\langle b, a \rangle)$.

(39) For every field F and for every element a of the support of F holds $\cdot_F(\langle a, \mathbf{1}_F \rangle) = a$ and $\cdot_F(\langle \mathbf{1}_F, a \rangle) = a$.

Let F be a field. The functor $\overset{-1}{F}$ yielding a function from the support of $F \setminus \text{single}(\mathbf{0}_F)$ into the support of $F \setminus \text{single}(\mathbf{0}_F)$ is defined by:

(Def.9) for every element x of the support of $F \setminus \text{single}(\mathbf{0}_F)$ holds $\cdot_F(\langle x, \overset{-1}{F}(x) \rangle) = \mathbf{1}_F$.

One can prove the following propositions:

(40) For every field F and for every element x of the support of $F \setminus \text{single}(\mathbf{0}_F)$ holds $\cdot_F(\langle x, \overset{-1}{F}(x) \rangle) = \mathbf{1}_F$.

(41) For every field F and for every function S from the support of $F \setminus \text{single}(\mathbf{0}_F)$ into the support of $F \setminus \text{single}(\mathbf{0}_F)$ holds $S = \overset{-1}{F}$ if and only if for every element x of the support of $F \setminus \text{single}(\mathbf{0}_F)$ holds $\cdot_F(\langle x, S(x) \rangle) = \mathbf{1}_F$.

(42) For every field F and for every element x of the support of $F \setminus \text{single}(\mathbf{0}_F)$ and for every element y of the support of $F \setminus \text{single}(\mathbf{0}_F)$ such that $\cdot_F(\langle x, y \rangle) = \mathbf{1}_F$ holds $y = \overset{-1}{F}(x)$.

(43) For every field F and for every element x of the support of $F \setminus \text{single}(\mathbf{0}_F)$ holds $x = \overset{-1}{F}(\overset{-1}{F}(x))$.

(44) For every field F and for all elements a, b of the support of $F \setminus \text{single}(\mathbf{0}_F)$ holds $\cdot_F(\langle a, b \rangle)$ is an element of the support of $F \setminus \text{single}(\mathbf{0}_F)$ and $\overset{-1}{F}(a)$ is an element of the support of $F \setminus \text{single}(\mathbf{0}_F)$.

(45) For every field F and for all elements a, b, c of the support of F such that $+_F(\langle a, b \rangle) = +_F(\langle a, c \rangle)$ holds $b = c$.

(46) For every field F and for every element a of the support of $F \setminus \text{single}(\mathbf{0}_F)$ and for all elements b, c of the support of F such that $\cdot_F(\langle a, b \rangle) = \cdot_F(\langle a, c \rangle)$ holds $b = c$.

References

[1] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

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

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

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

Received June 20, 1990