JOURNAL OF FORMALIZED MATHEMATICS
Volume 9, Released 1997, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Correctness of the Generic Algorithms of Brown and Henrici Concerning Addition and Multiplication in Fraction Fields

Christoph Schwarzweller
University of Tübingen
Tübingen

Summary. We prove the correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields of gcd-domains. For that we first prove some basic facts about divisibility in integral domains and introduce the concept of amplesets. After that we are able to define gcd-domains and to prove the theorems of Brown and Henrici which are crucial for the correctness of the algorithms. In the last section we define Mizar functions mirroring their input/output behaviour and prove properties of these functions that ensure the correctness of the algorithms.

MML Identifier: GCD_1.

WWW: http://mizar.org/JFM/Vol9/gcd_1.html

The articles [3], [5], [4], [2], and [1] provide the notation and terminology for this paper.

1. Basics

Let us observe that every non empty multiplicative loop structure which is commutative and right unital is also left unital.

Let us note that every non empty double loop structure which is commutative and right distributive is also distributive and every non empty double loop structure which is commutative and left distributive is also distributive.

Let us observe that every ring is well unital.

One can verify that $\mathbb{R}_{\mathrm{F}}$ is integral domain-like.

Let us note that there exists a non empty double loop structure which is strict, Abelian, add-associative, right zeroed, right complementable, associative, commutative, integral domain-like, distributive, well unital, non degenerated, and field-like.

In the sequel R denotes an integral domain-like commutative ring and c denotes an element of R.

The following proposition is true

(1) Let R be an integral domain-like commutative ring and a, b, c be elements of R such that $a \neq 0_R$. Then

(i) if $a \cdot b = a \cdot c$, then $b = c$, and

(ii) if $b \cdot a = c \cdot a$, then $b = c$.

Let R be a non empty groupoid and let x, y be elements of R. The predicate $x \mid y$ is defined by:

(Def. 1) There exists an element z of R such that $y = x \cdot z$.

Let R be a well unital non empty multiplicative loop structure and let x, y be elements of R. Let us note that the predicate $x \mid y$ is reflexive.

Let R be a non empty multiplicative loop structure and let x be an element of R. We say that x is unital if and only if:

(Def. 2) $x \mid \mathbf{1}_R$.

Let R be a non empty multiplicative loop structure and let x, y be elements of R. We say that x is associated to y if and only if:

(Def. 3) $x \mid y$ and $y \mid x$.

Let us note that the predicate x is associated to y is symmetric. We introduce x is not associated to y as an antonym of x is associated to y.

Let R be a well unital non empty multiplicative loop structure and let x, y be elements of R. Let us note that the predicate x is associated to y is reflexive.

Let R be an integral domain-like commutative ring and let x, y be elements of R. Let us assume that $y \mid x$. And let us assume that $y \neq 0_R$. The functor $\frac{x}{y}$ yields an element of R and is defined by:

(Def. 4) $\frac{x}{y} \cdot y = x$.

One can prove the following propositions:

(2) Let R be an associative non empty multiplicative loop structure and a, b, c be elements of R. If $a \mid b$ and $b \mid c$, then $a \mid c$.

(3) Let R be a commutative associative non empty multiplicative loop structure and a, b, c, d be elements of R. If $b \mid a$ and $d \mid c$, then $b \cdot d \mid a \cdot c$.

(4) Let R be an associative non empty multiplicative loop structure and a, b, c be elements of R. If a is associated to b and b is associated to c, then a is associated to c.

(5) Let R be an associative non empty multiplicative loop structure and a, b, c be elements of R. If $a \mid b$, then $c \cdot a \mid c \cdot b$.

(6) Let R be a non empty multiplicative loop structure and a, b be elements of R. Then $a \mid a \cdot b$ and if R is commutative, then $b \mid a \cdot b$.

(7) Let R be an associative non empty multiplicative loop structure and a, b, c be elements of R. If $a \mid b$, then $a \mid b \cdot c$.

(8) For all elements a, b of R such that $b \mid a$ and $b \neq 0_R$ holds $\frac{a}{b} = 0_R$ iff $a = 0_R$.

(9) For every element a of R such that $a \neq 0_R$ holds $\frac{a}{a} = \mathbf{1}_R$.

(10) For every non degenerated integral domain-like commutative ring R and for every element a of R holds $\frac{a}{\mathbf{1}_R} = a$.

(11) Let a, b, c be elements of R such that $c \neq 0_R$. Then

(i) if $c \mid a \cdot b$ and $c \mid a$, then $\frac{a \cdot b}{c} = \frac{a}{c} \cdot b$, and

(ii) if $c \mid a \cdot b$ and $c \mid b$, then $\frac{a \cdot b}{c} = a \cdot \frac{b}{c}$.

(12) For all elements a, b, c of R such that $c \neq 0_R$ and $c \mid a$ and $c \mid b$ and $c \mid a+b$ holds $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$.

(13) For all elements a, b, c of R such that $c \neq 0_R$ and $c \mid a$ and $c \mid b$ holds $\frac{a}{c} = \frac{b}{c}$ iff $a = b$.

(14) For all elements a, b, c, d of R such that $b \neq 0_R$ and $d \neq 0_R$ and $b \mid a$ and $d \mid c$ holds $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.

(15) For all elements a, b, c of R such that $a \neq 0_R$ and $a \cdot b \mid a \cdot c$ holds $b \mid c$.

(16) For every element a of R such that a is associated to 0_R holds $a = 0_R$.

(17) For all elements a, b of R such that $a \neq 0_R$ and $a \cdot b = a$ holds $b = \mathbf{1}_R$.

(18) For all elements a, b of R holds a is associated to b iff there exists c such that c is unital and $a \cdot c = b$.

(19) For all elements a, b, c of R such that $c \neq 0_R$ and $c \cdot a$ is associated to $c \cdot b$ holds a is associated to b.

2. AmpleSets

Let R be a non empty multiplicative loop structure and let a be an element of R. The functor Classes a yields a subset of R and is defined by:

(Def. 5) For every element b of R holds $b \in$ Classes a iff b is associated to a.

Let R be a well unital non empty multiplicative loop structure and let a be an element of R. Note that Classes a is non empty.

The following proposition is true

(20) Let R be an associative non empty multiplicative loop structure and a, b be elements of R. If Classes a meets Classes b, then Classes a = Classes b.

Let R be a non empty multiplicative loop structure. The functor Classes R yielding a family of subsets of R is defined as follows:

(Def. 6) For every subset A of R holds $A \in$ Classes R iff there exists an element a of R such that A = Classes a.

Let R be a non empty multiplicative loop structure. One can check that Classes R is non empty.

Next we state the proposition

(21) Let R be a well unital non empty multiplicative loop structure and X be a subset of R. If $X \in$ Classes R, then X is non empty.

Let R be an associative well unital non empty multiplicative loop structure. A non empty subset of R is said to be an amp set of R if it satisfies the conditions (Def. 7).

(Def. 7)(i) For every element a of R holds there exists an element of it which is associated to a, and

(ii) for all elements x, y of it such that $x \neq y$ holds x is not associated to y.

Let R be an associative well unital non empty multiplicative loop structure. A non empty subset of R is said to be an AmpleSet of R if:

(Def. 8) It is an amp set of R and $\mathbf{1}_R \in$ it.

The following three propositions are true:

(22) Let R be an associative well unital non empty multiplicative loop structure and A_1 be an AmpleSet of R. Then

(i) $\mathbf{1}_R \in A_1$,

(ii) for every element a of R holds there exists an element of A_1 which is associated to a, and

(iii) for all elements x, y of A_1 such that $x \neq y$ holds x is not associated to y.

(23) Let R be an associative well unital non empty multiplicative loop structure, A_1 be an AmpleSet of R, and x, y be elements of A_1. If x is associated to y, then $x = y$.

(24) For every AmpleSet A_1 of R holds 0_R is an element of A_1.

Let R be an associative well unital non empty multiplicative loop structure, let A_1 be an AmpleSet of R, and let x be an element of R. The functor $\mathrm{NF}(x,A_1)$ yielding an element of R is defined as follows:

(Def. 9) $\mathrm{NF}(x,A_1) \in A_1$ and $\mathrm{NF}(x,A_1)$ is associated to x.

One can prove the following two propositions:

(25) For every AmpleSet A_1 of R holds $\mathrm{NF}(0_R,A_1) = 0_R$ and $\mathrm{NF}(\mathbf{1}_R,A_1) = \mathbf{1}_R$.

(26) For every AmpleSet A_1 of R and for every element a of R holds $a \in A_1$ iff $a = \mathrm{NF}(a,A_1)$.

Let R be an associative well unital non empty multiplicative loop structure and let A_1 be an AmpleSet of R. We say that A_1 is multiplicative if and only if:

(Def. 10) For all elements x, y of A_1 holds $x \cdot y \in A_1$.

We now state the proposition

(27) Let A_1 be an AmpleSet of R. Suppose A_1 is multiplicative. Let x, y be elements of A_1. If $y \mid x$ and $y \neq 0_R$, then $\frac{x}{y} \in A_1$.

3. GCD-DOMAINS

Let R be a non empty multiplicative loop structure. We say that R is gcd-like if and only if the condition (Def. 11) is satisfied.

(Def. 11) Let x, y be elements of R. Then there exists an element z of R such that $z \mid x$ and $z \mid y$ and for every element z_1 of R such that $z_1 \mid x$ and $z_1 \mid y$ holds $z_1 \mid z$.

Let us note that there exists an integral domain which is gcd-like.

Let us observe that there exists a non empty multiplicative loop structure which is gcd-like, associative, commutative, and well unital.

Let us observe that there exists a non empty multiplicative loop with zero structure which is gcd-like, associative, commutative, and well unital.

Let us observe that every field-like add-associative right zeroed right complementable left unital right unital left distributive right distributive commutative non empty double loop structure is gcd-like.

One can verify that there exists a non empty double loop structure which is gcd-like, associative, commutative, well unital, integral domain-like, well unital, distributive, non degenerated, Abelian, add-associative, right zeroed, and right complementable.

A gcdDomain is a gcd-like integral domain-like non degenerated commutative ring.

Let R be a gcd-like associative well unital non empty multiplicative loop structure, let A_1 be an AmpleSet of R, and let x, y be elements of R. The functor $\mathrm{gcd}_{A_1}(x,y)$ yields an element of R and is defined by the conditions (Def. 12).

(Def. 12)(i) $\mathrm{gcd}_{A_1}(x,y) \in A_1$,

(ii) $\mathrm{gcd}_{A_1}(x,y) \mid x$,

(iii) $\mathrm{gcd}_{A_1}(x,y) \mid y$, and

(iv) for every element z of R such that $z \mid x$ and $z \mid y$ holds $z \mid \mathrm{gcd}_{A_1}(x,y)$.

In the sequel R denotes a gcdDomain.

The following propositions are true:

(29)[1] For every AmpleSet A_1 of R and for all elements a, b, c of R such that $c \mid \gcd_{A_1}(a,b)$ holds $c \mid a$ and $c \mid b$.

(30) For every AmpleSet A_1 of R and for all elements a, b of R holds $\gcd_{A_1}(a,b) = \gcd_{A_1}(b,a)$.

(31) For every AmpleSet A_1 of R and for every element a of R holds $\gcd_{A_1}(a,0_R) = \mathrm{NF}(a,A_1)$ and $\gcd_{A_1}(0_R,a) = \mathrm{NF}(a,A_1)$.

(32) For every AmpleSet A_1 of R holds $\gcd_{A_1}(0_R,0_R) = 0_R$.

(33) For every AmpleSet A_1 of R and for every element a of R holds $\gcd_{A_1}(a,\mathbf{1}_R) = \mathbf{1}_R$ and $\gcd_{A_1}(\mathbf{1}_R,a) = \mathbf{1}_R$.

(34) For every AmpleSet A_1 of R and for all elements a, b of R holds $\gcd_{A_1}(a,b) = 0_R$ iff $a = 0_R$ and $b = 0_R$.

(35) Let A_1 be an AmpleSet of R and a, b, c be elements of R. Suppose b is associated to c. Then $\gcd_{A_1}(a,b)$ is associated to $\gcd_{A_1}(a,c)$ and $\gcd_{A_1}(b,a)$ is associated to $\gcd_{A_1}(c,a)$.

(36) For every AmpleSet A_1 of R and for all elements a, b, c of R holds $\gcd_{A_1}(\gcd_{A_1}(a,b),c) = \gcd_{A_1}(a,\gcd_{A_1}(b,c))$.

(37) For every AmpleSet A_1 of R and for all elements a, b, c of R holds $\gcd_{A_1}(a \cdot c, b \cdot c)$ is associated to $c \cdot (\gcd_{A_1}(a,b))$.

(38) For every AmpleSet A_1 of R and for all elements a, b, c of R such that $\gcd_{A_1}(a,b) = \mathbf{1}_R$ holds $\gcd_{A_1}(a,b \cdot c) = \gcd_{A_1}(a,c)$.

(39) For every AmpleSet A_1 of R and for all elements a, b, c of R such that $c = \gcd_{A_1}(a,b)$ and $c \neq 0_R$ holds $\gcd_{A_1}(\frac{a}{c}, \frac{b}{c}) = \mathbf{1}_R$.

(40) For every AmpleSet A_1 of R and for all elements a, b, c of R holds $\gcd_{A_1}(a + b \cdot c, c) = \gcd_{A_1}(a,c)$.

4. THE THEOREMS OF BROWN AND HENRICI

Next we state two propositions:

(41) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of R. Suppose $\gcd_{A_1}(r_1,r_2) = \mathbf{1}_R$ and $\gcd_{A_1}(s_1,s_2) = \mathbf{1}_R$ and $r_2 \neq 0_R$ and $s_2 \neq 0_R$. Then $\gcd_{A_1}(r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)}, r_2 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)}) = \gcd_{A_1}(r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)}, \gcd_{A_1}(r_2,s_2))$.

(42) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of R. Suppose $\gcd_{A_1}(r_1,r_2) = \mathbf{1}_R$ and $\gcd_{A_1}(s_1,s_2) = \mathbf{1}_R$ and $r_2 \neq 0_R$ and $s_2 \neq 0_R$. Then $\gcd_{A_1}(\frac{r_1}{\gcd_{A_1}(r_1,s_2)} \cdot \frac{s_1}{\gcd_{A_1}(s_1,r_2)}, \frac{r_2}{\gcd_{A_1}(s_1,r_2)} \cdot \frac{s_2}{\gcd_{A_1}(r_1,s_2)}) = \mathbf{1}_R$.

5. CORRECTNESS OF THE ALGORITHMS

Let R be a gcd-like associative well unital non empty multiplicative loop structure, let A_1 be an AmpleSet of R, and let x, y be elements of R. We say that x, y are canonical w.r.t. A_1 if and only if:

(Def. 13) $\gcd_{A_1}(x,y) = \mathbf{1}_R$.

The following proposition is true

(43) Let A_1, A'_1 be AmpleSets of R and x, y be elements of R. Then x, y are canonical w.r.t. A_1 if and only if x, y are canonical w.r.t. A'_1.

[1] The proposition (28) has been removed.

Let R be a gcd-like associative well unital non empty multiplicative loop structure and let x, y be elements of R. We say that x, y are co-prime if and only if:

(Def. 14) There exists an AmpleSet A_1 of R such that $\gcd_{A_1}(x,y) = \mathbf{1}_R$.

Let R be a gcdDomain and let x, y be elements of R. Let us note that the predicate x, y are co-prime is symmetric.

One can prove the following proposition

(44) For every AmpleSet A_1 of R and for all elements x, y of R such that x, y are co-prime holds $\gcd_{A_1}(x,y) = \mathbf{1}_R$.

Let R be a gcd-like associative well unital non empty multiplicative loop with zero structure, let A_1 be an AmpleSet of R, and let x, y be elements of R. We say that x, y are normalized w.r.t. A_1 if and only if:

(Def. 15) $\gcd_{A_1}(x,y) = \mathbf{1}_R$ and $y \in A_1$ and $y \neq 0_R$.

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let r_1, r_2, s_1, s_2 be elements of R. Let us assume that r_1, r_2 are co-prime and s_1, s_2 are co-prime and $r_2 = \mathrm{NF}(r_2,A_1)$ and $s_2 = \mathrm{NF}(s_2,A_1)$. The functor $\mathrm{add1}_{A_1}(r_1,r_2,s_1,s_2)$ yields an element of R and is defined by:

$$\text{(Def. 16)}\quad \mathrm{add1}_{A_1}(r_1,r_2,s_1,s_2) = \begin{cases} s_1, \text{ if } r_1 = 0_R, \\ r_1, \text{ if } s_1 = 0_R, \\ r_1 \cdot s_2 + r_2 \cdot s_1, \text{ if } \gcd_{A_1}(r_2,s_2) = \mathbf{1}_R, \\ 0_R, \text{ if } r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)} = 0_R, \\ \frac{r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)}}{\gcd_{A_1}(r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)}, \gcd_{A_1}(r_2,s_2))}, \text{ otherwise.} \end{cases}$$

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let r_1, r_2, s_1, s_2 be elements of R. Let us assume that r_1, r_2 are co-prime and s_1, s_2 are co-prime and $r_2 = \mathrm{NF}(r_2,A_1)$ and $s_2 = \mathrm{NF}(s_2,A_1)$. The functor $\mathrm{add2}_{A_1}(r_1,r_2,s_1,s_2)$ yields an element of R and is defined by:

$$\text{(Def. 17)}\quad \mathrm{add2}_{A_1}(r_1,r_2,s_1,s_2) = \begin{cases} s_2, \text{ if } r_1 = 0_R, \\ r_2, \text{ if } s_1 = 0_R, \\ r_2 \cdot s_2, \text{ if } \gcd_{A_1}(r_2,s_2) = \mathbf{1}_R, \\ \mathbf{1}_R, \text{ if } r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)} = 0_R, \\ \frac{r_2 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)}}{\gcd_{A_1}(r_1 \cdot \frac{s_2}{\gcd_{A_1}(r_2,s_2)} + s_1 \cdot \frac{r_2}{\gcd_{A_1}(r_2,s_2)}, \gcd_{A_1}(r_2,s_2))}, \text{ otherwise.} \end{cases}$$

The following propositions are true:

(45) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized w.r.t. A_1 and s_1, s_2 are normalized w.r.t. A_1. Then $\mathrm{add1}_{A_1}(r_1,r_2,s_1,s_2)$, $\mathrm{add2}_{A_1}(r_1,r_2,s_1,s_2)$ are normalized w.r.t. A_1.

(46) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized w.r.t. A_1 and s_1, s_2 are normalized w.r.t. A_1. Then $\mathrm{add1}_{A_1}(r_1,r_2,s_1,s_2) \cdot (r_2 \cdot s_2) = \mathrm{add2}_{A_1}(r_1,r_2,s_1,s_2) \cdot (r_1 \cdot s_2 + s_1 \cdot r_2)$.

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let r_1, r_2, s_1, s_2 be elements of R. The functor $\mathrm{mult1}_{A_1}(r_1,r_2,s_1,s_2)$ yielding an element of R is defined as follows:

$$\text{(Def. 18)}\quad \mathrm{mult1}_{A_1}(r_1,r_2,s_1,s_2) = \begin{cases} 0_R, \text{ if } r_1 = 0_R \text{ or } s_1 = 0_R, \\ r_1 \cdot s_1, \text{ if } r_2 = \mathbf{1}_R \text{ and } s_2 = \mathbf{1}_R, \\ \frac{r_1 \cdot s_1}{\gcd_{A_1}(r_1,s_2)}, \text{ if } s_2 \neq 0_R \text{ and } r_2 = \mathbf{1}_R, \\ \frac{r_1 \cdot s_1}{\gcd_{A_1}(s_1,r_2)}, \text{ if } r_2 \neq 0_R \text{ and } s_2 = \mathbf{1}_R, \\ \frac{r_1}{\gcd_{A_1}(r_1,s_2)} \cdot \frac{s_1}{\gcd_{A_1}(s_1,r_2)}, \text{ otherwise.} \end{cases}$$

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let r_1, r_2, s_1, s_2 be elements of R. Let us assume that r_1, r_2 are co-prime and s_1, s_2 are co-prime and $r_2 = \mathrm{NF}(r_2, A_1)$ and $s_2 = \mathrm{NF}(s_2, A_1)$. The functor $\mathrm{mult2}_{A_1}(r_1, r_2, s_1, s_2)$ yields an element of R and is defined by:

(Def. 19) $$\mathrm{mult2}_{A_1}(r_1,r_2,s_1,s_2) = \begin{cases} \mathbf{1}_R, \text{ if } r_1 = 0_R \text{ or } s_1 = 0_R, \\ \mathbf{1}_R, \text{ if } r_2 = \mathbf{1}_R \text{ and } s_2 = \mathbf{1}_R, \\ \frac{s_2}{\mathrm{gcd}_{A_1}(r_1,s_2)}, \text{ if } s_2 \neq 0_R \text{ and } r_2 = \mathbf{1}_R, \\ \frac{r_2}{\mathrm{gcd}_{A_1}(s_1,r_2)}, \text{ if } r_2 \neq 0_R \text{ and } s_2 = \mathbf{1}_R, \\ \frac{r_2}{\mathrm{gcd}_{A_1}(s_1,r_2)} \cdot \frac{s_2}{\mathrm{gcd}_{A_1}(r_1,s_2)}, \text{ otherwise.} \end{cases}$$

We now state four propositions:

(47) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized w.r.t. A_1 and s_1, s_2 are normalized w.r.t. A_1. Then $\mathrm{mult1}_{A_1}(r_1,r_2,s_1,s_2)$, $\mathrm{mult2}_{A_1}(r_1,r_2,s_1,s_2)$ are normalized w.r.t. A_1.

(48) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized w.r.t. A_1 and s_1, s_2 are normalized w.r.t. A_1. Then $\mathrm{mult1}_{A_1}(r_1,r_2,s_1,s_2) \cdot (r_2 \cdot s_2) = \mathrm{mult2}_{A_1}(r_1,r_2,s_1,s_2) \cdot (r_1 \cdot s_1)$.

(51)[2] Let F be an add-associative right zeroed right complementable Abelian distributive non empty double loop structure and x, y be elements of F. Then $(-x) \cdot y = -x \cdot y$ and $x \cdot -y = -x \cdot y$.

(53)[3] For every field-like commutative ring F and for all elements a, b of F such that $a \neq 0_F$ and $b \neq 0_F$ holds $a^{-1} \cdot b^{-1} = (b \cdot a)^{-1}$.

REFERENCES

[1] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[2] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/vectsp_2.html.

[3] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[4] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/rlvect_1.html.

[5] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

Received June 16, 1997

Published January 2, 2004

[2] The propositions (49) and (50) have been removed.
[3] The proposition (52) has been removed.