FORMALIZED MATHEMATICS
Volume 6, Number 3, 1997
Warsaw University - 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`.

The papers [4], [6], [5], [3], [1], and [2] provide the notation and terminology for this paper.

1. Basics

In this paper R denotes an integral domain and a, b, c denote elements of the carrier of R.

The following proposition is true

(1) For all elements a, b, c of the carrier of R such that $a \neq 0_R$ holds if $a \cdot b = a \cdot c$, then $b = c$ and if $b \cdot a = c \cdot a$, then $b = c$.

ISSN 1426–2630

Let R be an integral domain and let x, y be elements of the carrier of R. We say that x divides y if and only if:

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

Let us notice that the predicate x divides y is reflexive.

Let R be an integral domain and let x be an element of the carrier of R. We say that x is unital if and only if:

(Def. 2) x divides 1_R.

Let R be an integral domain and let x, y be elements of the carrier of R. We say that x is associated to y if and only if:

(Def. 3) x divides y and y divides x.

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

Let R be an integral domain and let x, y be elements of the carrier of R. Let us assume that y divides x. And let us assume that $y \neq 0_R$. The functor $\frac{x}{y}$ yielding an element of the carrier of R is defined as follows:

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

One can prove the following propositions:

(2) For all elements a, b, c of the carrier of R such that a divides b and b divides c holds a divides c.

(3) Let a, b, c, d be elements of the carrier of R. If b divides a and d divides c, then $b \cdot d$ divides $a \cdot c$.

(4) Let a, b, c be elements of the carrier of R. If a is associated to b and b is associated to c, then a is associated to c.

(5) For all elements a, b, c of the carrier of R such that a divides b holds $c \cdot a$ divides $c \cdot b$.

(6) For all elements a, b of the carrier of R holds a divides $a \cdot b$ and b divides $a \cdot b$.

(7) For all elements a, b, c of the carrier of R such that a divides b holds a divides $b \cdot c$.

(8) Let a, b be elements of the carrier of R. If b divides a and $b \neq 0_R$, then $\frac{a}{b} = 0_R$ iff $a = 0_R$.

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

(10) For every element a of the carrier of R holds $\frac{a}{1_R} = a$.

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

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

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

(12) Let a, b, c be elements of the carrier of R. Suppose $c \neq 0_R$ and c divides a and c divides b and c divides $a + b$. Then $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$.

(13) Let a, b, c be elements of the carrier of R. Suppose $c \neq 0_R$ and c divides a and c divides b. Then $\frac{a}{c} = \frac{b}{c}$ if and only if $a = b$.

(14) Let a, b, c, d be elements of the carrier of R. Suppose $b \neq 0_R$ and $d \neq 0_R$ and b divides a and d divides c. Then $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.

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

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

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

(18) Let a, b be elements of the carrier of R. Then a is associated to b if and only if there exists c such that c is unital and $a \cdot c = b$.

(19) For all elements a, b, c of the carrier 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 an integral domain and let a be an element of the carrier of R. The functor $\mathrm{Classes}\, a$ yields a subset of the carrier of R and is defined as follows:

(Def. 5) For every element b of the carrier of R holds $b \in \mathrm{Classes}\, a$ iff b is associated to a.

Let R be an integral domain and let a be an element of the carrier of R. Note that $\mathrm{Classes}\, a$ is non empty.

We now state the proposition

(20) For all elements a, b of the carrier of R such that $\mathrm{Classes}\, a \cap \mathrm{Classes}\, b \neq \emptyset$ holds $\mathrm{Classes}\, a = \mathrm{Classes}\, b$.

Let R be an integral domain. The functor $\mathrm{Classes}\, R$ yielding a family of subsets of the carrier of R is defined by the condition (Def. 6).

(Def. 6) Let A be a subset of the carrier of R. Then $A \in \mathrm{Classes}\, R$ if and only if there exists an element a of the carrier of R such that $A = \mathrm{Classes}\, a$.

Let R be an integral domain. One can check that $\mathrm{Classes}\, R$ is non empty.

We now state the proposition

(21) For every subset X of the carrier of R such that $X \in \mathrm{Classes}\, R$ holds X is non empty.

Let R be an integral domain. A non empty subset of the carrier 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 the carrier 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 integral domain. A non empty subset of the carrier of R is called an AmpleSet of R if:

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

In the sequel A_1 denotes an AmpleSet of R.

The following propositions are true:

(22) Let A_1 be an AmpleSet of R. Then

(i) $1_R \in A_1$,

(ii) for every element a of the carrier 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) For all elements x, y of A_1 such that x is associated to y holds $x = y$.

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

Let R be an integral domain, let A_1 be an AmpleSet of R, and let x be an element of the carrier of R. The functor $\mathrm{NF}(x, A_1)$ yields an element of the carrier of R and is defined as follows:

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

The following propositions are true:

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

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

Let R be an integral domain 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 $x \cdot y \in A_1$.

The following proposition is true

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

3. GCD-Domains

Let R be an integral domain. 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 the carrier of R. Then there exists an element z of the carrier of R such that

(i) z divides x,

(ii) z divides y, and

(iii) for every element z_1 of the carrier of R such that z_1 divides x and z_1 divides y holds z_1 divides z.

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

A gcdDomain is a gcd-like integral domain.

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let x, y be elements of the carrier of R. The functor $\gcd_{A_1}(x, y)$ yielding an element of the carrier of R is defined by the conditions (Def. 12).

(Def. 12)(i) $\gcd_{A_1}(x, y) \in A_1$,

(ii) $\gcd_{A_1}(x, y)$ divides x,

(iii) $\gcd_{A_1}(x, y)$ divides y, and

(iv) for every element z of the carrier of R such that z divides x and z divides y holds z divides $\gcd_{A_1}(x, y)$.

In the sequel R is a gcdDomain.

The following propositions are true:

(28) Let A_1 be an AmpleSet of R and a, b be elements of the carrier of R. Then $\gcd_{A_1}(a, b)$ divides a and $\gcd_{A_1}(a, b)$ divides b.

(29) Let A_1 be an AmpleSet of R and a, b, c be elements of the carrier of R. If c divides $\gcd_{A_1}(a, b)$, then c divides a and c divides b.

(30) For every AmpleSet A_1 of R and for all elements a, b of the carrier 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 the carrier 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 the carrier of R holds $\gcd_{A_1}(a, 1_R) = 1_R$ and $\gcd_{A_1}(1_R, a) = 1_R$.

(34) Let A_1 be an AmpleSet of R and a, b be elements of the carrier of R. Then $\gcd_{A_1}(a, b) = 0_R$ if and only if $a = 0_R$ and $b = 0_R$.

(35) Let A_1 be an AmpleSet of R and a, b, c be elements of the carrier 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 the carrier 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 the carrier 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 the carrier of R such that $\gcd_{A_1}(a, b) = 1_R$ holds $\gcd_{A_1}(a, b \cdot c) = \gcd_{A_1}(a, c)$.

(39) Let A_1 be an AmpleSet of R and a, b, c be elements of the carrier of R. If $c = \gcd_{A_1}(a, b)$ and $c \neq 0_R$, then $\gcd_{A_1}(\frac{a}{c}, \frac{b}{c}) = 1_R$.

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

4. The Theorems of Brown and Henrici

The following propositions are true:

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

5. Correctness of the Algorithms

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let x, y be elements of the carrier of R. We say that x, y are canonical wrt A_1 if and only if:

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

Next we state the proposition

(43) Let A_1, A_1' be AmpleSet of R and x, y be elements of the carrier of R. Then x, y are canonical wrt A_1 if and only if x, y are canonical wrt A_1'.

Let R be a gcdDomain and let x, y be elements of the carrier of R. We say that x canonical y if and only if:

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

Let us observe that the predicate x canonical y is symmetric.

Next we state the proposition

(44) Let A_1 be an AmpleSet of R and x, y be elements of the carrier of R. If x canonical y, then $\gcd_{A_1}(x,y)=1_R$.

Let R be a gcdDomain, let A_1 be an AmpleSet of R, and let x, y be elements of the carrier of R. We say that x, y are normalized wrt A_1 if and only if:

(Def. 15) $\gcd_{A_1}(x,y)=1_R$ 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 the carrier of R. Let us assume that r_1 canonical r_2 and s_1 canonical s_2 and $r_2=\mathrm{NF}(r_2,A_1)$ and $s_2=\mathrm{NF}(s_2,A_1)$. The functor $\mathrm{add1}_{A_1}(r_1,r_2,s_1,s_2)$ yielding an element of the carrier of R is defined as follows:

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

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 the carrier of R. Let us assume that r_1 canonical r_2 and s_1 canonical s_2 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 the carrier of R and is defined by:

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

We now state two propositions:

(45) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of the carrier of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized wrt A_1 and s_1, s_2 are normalized wrt 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 wrt A_1.

(46) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of the carrier of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized wrt A_1 and s_1, s_2 are normalized wrt 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 the carrier of R. The functor $\mathrm{mult1}_{A_1}(r_1,r_2,s_1,s_2)$ yields an element of the carrier of R and is defined as follows:

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

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 the carrier of R. Let us assume that r_1 canonical r_2 and s_1 canonical s_2 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 the carrier of R and is defined as follows:

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

The following two propositions are true:

(47) Let A_1 be an AmpleSet of R and r_1, r_2, s_1, s_2 be elements of the carrier of R. Suppose A_1 is multiplicative and r_1, r_2 are normalized wrt A_1 and s_1, s_2 are normalized wrt 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 wrt A_1.

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

References

[1] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[2] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[3] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

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

[5] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[6] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received June 16, 1997