FORMALIZED MATHEMATICS
Vol. 28, No. 1, Pages 79–87, 2020
DOI: 10.2478/forma-2020-0006

sciendo
https://www.sciendo.com/

Rings of Fractions and Localization

Yasushige Watase
Suginami-ku Matsunoki
3-21-6 Tokyo, Japan

Summary. This article formalized rings of fractions in the Mizar system [3], [4]. A construction of the ring of fractions from an integral domain, namely a quotient field was formalized in [7].

This article generalizes a construction of fractions to a ring which is commutative and has zero divisor by means of a multiplicatively closed set, say S, by known manner. Constructed ring of fraction is denoted by $S\tilde{}R$ instead of $S^{-1}R$ appeared in [1], [6]. As an important example we formalize a ring of fractions by a particular multiplicatively closed set, namely $R \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of R. The resulted local ring is denoted by $R_{\mathfrak{p}}$. In our Mizar article it is coded by $R\tilde{}\mathfrak{p}$ as a synonym.

This article contains also the formal proof of a universal property of a ring of fractions, the total-quotient ring, a proof of the equivalence between the total-quotient ring and the quotient field of an integral domain.

MSC: 13B30 16S85 68V20

Keywords: rings of fractions; localization; total-quotient ring; quotient field

MML identifier: RINGFRAC, version: 8.1.09 5.60.1371

1. Preliminaries: Units, Zero Divisors and Multiplicatively-closed Set

From now on R, R_1 denote commutative rings, A, B denote non degenerated, commutative rings, o, o_1, o_2 denote objects, r, r_1, r_2 denote elements of R, a, a_1, a_2, b, b_1 denote elements of A, f denotes a function from R into R_1, and $\mathfrak{p}$ denotes an element of the spectrum of A.

Let R be a commutative ring and r be an element of R. We say that r is zero-divisible if and only if

ISSN 1426–2630(Print), 1898-9934(Online)

(Def. 1) there exists an element r_1 of R such that $r_1 \neq 0_R$ and $r \cdot r_1 = 0_R$.

Let A be a non degenerated, commutative ring. Let us observe that there exists an element of A which is zero-divisible.

Let us consider A.

A zero-divisor of A is a zero-divisible element of A. Now we state the propositions:

(1) 0_A is a zero-divisor of A.

(2) 1_A is not a zero-divisor of A.

Let us consider A. The functor ZeroDivSet(A) yielding a subset of A is defined by the term

(Def. 2) $\{a$, where a is an element of $A : a$ is a zero-divisor of $A\}$.

The functor NonZeroDivSet(A) yielding a subset of A is defined by the term

(Def. 3) $\Omega_A \setminus (\mathrm{ZeroDivSet}(A))$.

Let us note that ZeroDivSet(A) is non empty and NonZeroDivSet(A) is non empty.

Now we state the propositions:

(3) $0_A \notin \mathrm{NonZeroDivSet}(A)$. The theorem is a consequence of (1).

(4) If A is an integral domain, then $\{0_A\} = \mathrm{ZeroDivSet}(A)$. The theorem is a consequence of (1).

(5) $\{1_R\}$ is multiplicatively closed.

Let us consider R. One can check that there exists a non empty subset of R which is multiplicatively closed.

Let us consider A. Let V be a subset of A. We say that V is without zero if and only if

(Def. 4) $0_A \notin V$.

Let us observe that there exists a non empty, multiplicatively closed subset of A which is without zero.

Now we state the propositions:

(6) $\Omega_A \setminus \mathfrak{p}$ is multiplicatively closed.

(7) Let us consider a proper ideal J of A. Then multClSet(J, a) is multiplicatively closed.

Let us consider A. One can check that NonZeroDivSet(A) is multiplicatively closed.

Let us consider R. The functor UnitSet(R) yielding a subset of R is defined by the term

(Def. 5) $\{a$, where a is an element of $R : a$ is a unit of $R\}$.

Let us observe that UnitSet(R) is non empty.

Now we state the proposition:

(8) If $r_1 \in \mathrm{UnitSet}(R)$, then r_1 is right mult-cancelable.

PROOF: Consider r_2 such that $r_2 \cdot r_1 = 1_R$. For every elements u, v of R such that $u \cdot r_1 = v \cdot r_1$ holds $u = v$. □

Let us consider R. Let r be an element of R. Assume $r \in \mathrm{UnitSet}(R)$. The functor recip($r$) yielding an element of R is defined by

(Def. 6) $it \cdot r = 1_R$.

We introduce the notation r^{-1} as a synonym of recip(r).

Let u, v be elements of R. The functor u/v yielding an element of R is defined by the term

(Def. 7) $u \cdot \mathrm{recip}(u)$.

Let us consider a unit u of R and an element v of R. Now we state the propositions:

(9) If f inherits ring homomorphism, then $f(u)$ is a unit of R_1 and $f(u)^{-1} = f(u^{-1})$.

(10) If f inherits ring homomorphism, then $f(v \cdot (u^{-1})) = f(v) \cdot (f(u)^{-1})$. The theorem is a consequence of (9).

2. EQUIVALENCE RELATION OF FRACTIONS

In the sequel S denotes a non empty, multiplicatively closed subset of R.

Let us consider R and S. The functor Frac(S) yielding a subset of (the carrier of R) $\times$ (the carrier of R) is defined by

(Def. 8) for every set x, $x \in it$ iff there exist elements a, b of R such that $x = \langle a, b\rangle$ and $b \in S$.

Now we state the proposition:

(11) $\mathrm{Frac}(S) = \Omega_R \times S$.

Let us consider R and S. Let us observe that Frac(S) is non empty.

The functor frac1(S) yielding a function from R into Frac(S) is defined by

(Def. 9) for every object o such that $o \in$ the carrier of R holds $it(o) = \langle o, 1_R\rangle$.

From now on u, v, w, x, y, z denote elements of Frac(S).

Let us consider R and S. Let u, v be elements of Frac(S). The functor FracAdd(u, v) yielding an element of Frac(S) is defined by the term

(Def. 10) $\langle (u)_{\mathbf{1}} \cdot (v)_{\mathbf{2}} + (v)_{\mathbf{1}} \cdot (u)_{\mathbf{2}}, (u)_{\mathbf{2}} \cdot (v)_{\mathbf{2}}\rangle$.

One can verify that the functor is commutative.

The functor FracMult(u, v) yielding an element of Frac(S) is defined by the term

(Def. 11) $\langle (u)_{\mathbf{1}} \cdot (v)_{\mathbf{1}},\, (u)_{\mathbf{2}} \cdot (v)_{\mathbf{2}} \rangle$.

One can check that the functor is commutative.

Let us consider x and y. The functors: $x + y$ and $x \cdot y$ yielding elements of Frac(S) are defined by terms

(Def. 12) FracAdd(x, y),

(Def. 13) FracMult(x, y),

respectively. Now we state the propositions:

(12) FracAdd(x, FracAdd(y, z)) = FracAdd(FracAdd(x, y), z).

(13) FracMult(x, FracMult(y, z)) = FracMult(FracMult(x, y), z).

Let us consider R and S. Let x, y be elements of Frac(S). We say that $x =_{Fr_S} y$ if and only if

(Def. 14) there exists an element s_1 of R such that $s_1 \in S$ and $((x)_{\mathbf{1}} \cdot ((y)_{\mathbf{2}}) - (y)_{\mathbf{1}} \cdot ((x)_{\mathbf{2}})) \cdot s_1 = 0_R$.

Now we state the propositions:

(14) If $0_R \in S$, then $x =_{Fr_S} y$.

(15) $x =_{Fr_S} x$.

(16) If $x =_{Fr_S} y$, then $y =_{Fr_S} x$.

(17) If $x =_{Fr_S} y$ and $y =_{Fr_S} z$, then $x =_{Fr_S} z$.

Let us consider R and S. The functor EqRel(S) yielding an equivalence relation of Frac(S) is defined by

(Def. 15) $\langle u,\, v \rangle \in it$ iff $u =_{Fr_S} v$.

Now we state the propositions:

(18) $x \in [y]_{\mathrm{EqRel}(S)}$ if and only if $x =_{Fr_S} y$.

(19) $[x]_{\mathrm{EqRel}(S)} = [y]_{\mathrm{EqRel}(S)}$ if and only if $x =_{Fr_S} y$.

PROOF: Set $E = \mathrm{EqRel}(S)$. If $[x]_E = [y]_E$, then $x =_{Fr_S} y$. $x \in [y]_E$. □

(20) If $x =_{Fr_S} u$ and $y =_{Fr_S} v$, then FracMult(x, y) $=_{Fr_S}$ FracMult(u, v).

(21) If $x =_{Fr_S} u$ and $y =_{Fr_S} v$, then FracAdd(x, y) $=_{Fr_S}$ FracAdd(u, v).

(22) $(x + y) \cdot z =_{Fr_S} x \cdot z + y \cdot z$.

Let us consider R and S. The functors: $0_R^{S \times S}$ and $I_R^{S \times S}$ yielding elements of Frac(S) are defined by terms

(Def. 16) $\langle 0_R,\, 1_R \rangle$,

(Def. 17) $\langle 1_R,\, 1_R \rangle$,

respectively. Now we state the proposition:

(23) Let us consider an element s of S. If $x = \langle s,\, s \rangle$, then $x =_{Fr_S} I_R^{S \times S}$.

3. Construction of Ring of Fractions

Let us consider R and S. The functor FracRing(S) yielding a strict double loop structure is defined by

(Def. 18) the carrier of it = Classes EqRel(S) and $1_{it} = [I_R^{S \times S}]_{\mathrm{EqRel}(S)}$ and $0_{it} = [0_R^{S \times S}]_{\mathrm{EqRel}(S)}$ and for every elements x, y of it, there exist elements a, b of Frac(S) such that $x = [a]_{\mathrm{EqRel}(S)}$ and $y = [b]_{\mathrm{EqRel}(S)}$ and (the addition of it)$(x, y) = [a + b]_{\mathrm{EqRel}(S)}$ and for every elements x, y of it, there exist elements a, b of Frac(S) such that $x = [a]_{\mathrm{EqRel}(S)}$ and $y = [b]_{\mathrm{EqRel}(S)}$ and (the multiplication of it)$(x, y) = [a \cdot b]_{\mathrm{EqRel}(S)}$.

We introduce the notation $S{\sim}R$ as a synonym of FracRing(S).

One can verify that $S{\sim}R$ is non empty.

Now we state the proposition:

(24) $0_R \in S$ if and only if $S{\sim}R$ is degenerated. The theorem is a consequence of (19).

In the sequel a, b, c denote elements of Frac(S) and x, y, z denote elements of $S{\sim}R$.

Now we state the propositions:

(25) There exists an element a of Frac(S) such that $x = [a]_{\mathrm{EqRel}(S)}$.

(26) If $x = [a]_{\mathrm{EqRel}(S)}$ and $y = [b]_{\mathrm{EqRel}(S)}$, then $x \cdot y = [a \cdot b]_{\mathrm{EqRel}(S)}$. The theorem is a consequence of (19) and (20).

(27) $x \cdot y = y \cdot x$. The theorem is a consequence of (25) and (26).

(28) If $x = [a]_{\mathrm{EqRel}(S)}$ and $y = [b]_{\mathrm{EqRel}(S)}$, then $x + y = [a + b]_{\mathrm{EqRel}(S)}$. The theorem is a consequence of (19) and (21).

(29) $S{\sim}R$ is a ring.

Proof: $x + y = y + x$. $(x + y) + z = x + (y + z)$. $x + 0_{S\sim R} = x$. x is right complementable. $(x + y) \cdot z = x \cdot z + y \cdot z$. $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. $x \cdot (1_{S\sim R}) = x$ and $1_{S\sim R} \cdot x = x$. □

Let us consider R and S. One can verify that $S{\sim}R$ is commutative, Abelian, add-associative, right zeroed, right complementable, associative, well unital, and distributive.

Now we state the proposition:

(30) There exist elements r_1, r_2 of R such that

(i) $r_2 \in S$, and

(ii) $z = [\langle r_1, r_2 \rangle]_{\mathrm{EqRel}(S)}$.

The theorem is a consequence of (25).

In the sequel S denotes a without zero, non empty, multiplicatively closed subset of A.

Let us consider A and S. The canonical homomorphism of S into quotient field yielding a function from A into $S{\sim}A$ is defined by

(Def. 19) for every object o such that $o \in$ the carrier of A holds $it(o) = [(\mathrm{frac1}(S))(o)]_{\mathrm{EqRel}(S)}$.

Let us observe that the canonical homomorphism of S into quotient field is additive, multiplicative, and unity-preserving.

Now we state the propositions:

(31) Let us consider elements a, b of A. Then (the canonical homomorphism of S into quotient field)$(a - b)$ = (the canonical homomorphism of S into quotient field)(a) − (the canonical homomorphism of S into quotient field)(b).

(32) Suppose $0_A \notin S$. Then ker the canonical homomorphism of S into quotient field $\subseteq$ ZeroDivSet(A).

PROOF: For every o such that $o \in$ ker the canonical homomorphism of S into quotient field holds $o \in$ ZeroDivSet(A). □

(33) Suppose $0_A \notin S$ and A is an integral domain. Then

(i) ker the canonical homomorphism of S into quotient field $= \{0_A\}$, and

(ii) the canonical homomorphism of S into quotient field is one-to-one.

PROOF: ker the canonical homomorphism of S into quotient field $\subseteq$ ZeroDiv Set(A). ZeroDivSet$(A) = \{0_A\}$. For every objects x, y such that x, $y \in$ dom(the canonical homomorphism of S into quotient field) and (the canonical homomorphism of S into quotient field)(x) = (the canonical homomorphism of S into quotient field)(y) holds $x = y$. □

4. Localization in Terms of Prime Ideals

From now on $\mathfrak{p}$ denotes an element of the spectrum of A.

Let us consider A and $\mathfrak{p}$. The functor $\mathrm{Loc}(A, \mathfrak{p})$ yielding a subset of A is defined by the term

(Def. 20) $\Omega_A \setminus \mathfrak{p}$.

One can check that $\mathrm{Loc}(A, \mathfrak{p})$ is non empty and $\mathrm{Loc}(A, \mathfrak{p})$ is multiplicatively closed and $\mathrm{Loc}(A, \mathfrak{p})$ is without zero.

The functor $A{\sim}\mathfrak{p}$ yielding a ring is defined by the term

(Def. 21) $\mathrm{Loc}(A, \mathfrak{p}){\sim}A$.

One can verify that $A{\sim}\mathfrak{p}$ is non degenerated and $A{\sim}\mathfrak{p}$ is commutative.

The functor LocIdeal$(\mathfrak{p})$ yielding a subset of $\Omega_{A\sim\mathfrak{p}}$ is defined by the term

(Def. 22) $\{y$, where y is an element of $A{\sim}\mathfrak{p}$: there exists an element a of $\mathrm{Frac}(\mathrm{Loc}(A,\mathfrak{p}))$ such that $a \in \mathfrak{p} \times \mathrm{Loc}(A,\mathfrak{p})$ and $y = [a]_{\mathrm{EqRel}(\mathrm{Loc}(A,\mathfrak{p}))}\}$.

Observe that LocIdeal($\mathfrak{p}$) is non empty.

In the sequel a, m, n denote elements of $A{\sim}\mathfrak{p}$.

Now we state the propositions:

(34) LocIdeal($\mathfrak{p}$) is a proper ideal of $A{\sim}\mathfrak{p}$.

Proof: Reconsider $M = \mathrm{LocIdeal}(\mathfrak{p})$ as a subset of $A{\sim}\mathfrak{p}$. For every elements m, n of $A{\sim}\mathfrak{p}$ such that $m, n \in M$ holds $m + n \in M$. For every elements x, m of $A{\sim}\mathfrak{p}$ such that $m \in M$ holds $x \cdot m \in M$. M is proper by [2, (19)], (19). □

(35) Let us consider an object x. Suppose $x \in \Omega_{A\sim\mathfrak{p}} \setminus (\mathrm{LocIdeal}(\mathfrak{p}))$. Then x is a unit of $A{\sim}\mathfrak{p}$. The theorem is a consequence of (25) and (11).

(36) (i) $A{\sim}\mathfrak{p}$ is local, and

(ii) LocIdeal($\mathfrak{p}$) is a maximal ideal of $A{\sim}\mathfrak{p}$.

Proof: Reconsider $J = \mathrm{LocIdeal}(\mathfrak{p})$ as a proper ideal of $A{\sim}\mathfrak{p}$. $A{\sim}\mathfrak{p}$ is local. J is a maximal ideal of $A{\sim}\mathfrak{p}$ by [8, (8), (11)], (35). □

5. Universal Property of Ring of Fractions

From now on f denotes a function from A into B.

Now we state the proposition:

(37) Let us consider an element s of S. Suppose f inherits ring homomorphism and $f^{\circ}S \subseteq \mathrm{UnitSet}(B)$. Then $f(s)$ is a unit of B.

Let us consider A, B, S, and f. Assume f inherits ring homomorphism and $f^{\circ}S \subseteq \mathrm{UnitSet}(B)$. The functor UnivMap($S, f$) yielding a function from $S{\sim}A$ into B is defined by

(Def. 23) for every object x such that $x \in$ the carrier of $S{\sim}A$ there exist elements a, s of A such that $s \in S$ and $x = [\langle a, s\rangle]_{\mathrm{EqRel}(S)}$ and $it(x) = f(a) \cdot (f(s)^{-1})$.

Now we state the propositions:

(38) If f inherits ring homomorphism and $f^{\circ}S \subseteq \mathrm{UnitSet}(B)$, then UnivMap($S, f$) is additive.

Proof: For every elements x, y of $S{\sim}A$, $(\mathrm{UnivMap}(S,f))(x+y) = (\mathrm{UnivMap}(S,f))(x) + (\mathrm{UnivMap}(S,f))(y)$. □

(39) If f inherits ring homomorphism and $f^{\circ}S \subseteq \mathrm{UnitSet}(B)$, then UnivMap($S, f$) is multiplicative.

Proof: For every elements x, y of $S{\sim}A$, $(\mathrm{UnivMap}(S,f))(x \cdot y) = (\mathrm{UnivMap}(S,f))(x) \cdot (\mathrm{UnivMap}(S,f))(y)$. □

(40) If f inherits ring homomorphism and $f^\circ S \subseteq \mathrm{UnitSet}(B)$, then $\mathrm{UnivMap}(S, f)$ is unity-preserving.
PROOF: $(\mathrm{UnivMap}(S, f))(1_{S\sim A}) = 1_B$. □

(41) If f inherits ring homomorphism and $f^\circ S \subseteq \mathrm{UnitSet}(B)$, then $\mathrm{UnivMap}(S, f)$ inherits ring homomorphism.

(42) Suppose f inherits ring homomorphism and $f^\circ S \subseteq \mathrm{UnitSet}(B)$. Then $f = (\mathrm{UnivMap}(S, f)) \cdot$ (the canonical homomorphism of S into quotient field).
PROOF: Set $g_1 = (\mathrm{UnivMap}(S, f)) \cdot$ (the canonical homomorphism of S into quotient field). For every object x such that $x \in \mathrm{dom}\, f$ holds $f(x) = g_1(x)$ by (19), (37), [5, (8)]. □

6. The Total-Quotient Ring and the Quotient Field of Integral Domain

Let us consider A. The functor $\mathrm{TotalQuotRing}(A)$ yielding a ring is defined by the term

(Def. 24) $\mathrm{NonZeroDivSet}(A) \sim A$.

Observe that $\mathrm{TotalQuotRing}(A)$ is non degenerated.

In the sequel x denotes an object.

Now we state the proposition:

(43) If A is a field, then $\mathrm{Ideals}\, A = \{\{0_A\}, \text{the carrier of } A\}$.
PROOF: If $x \in \mathrm{Ideals}\, A$, then $x \in \{\{0_A\}, \text{the carrier of } A\}$. If $x \in \{\{0_A\}, \text{the carrier of } A\}$, then $x \in \mathrm{Ideals}\, A$. □

From now on A denotes an integral domain.

(44) (i) $\mathrm{NonZeroDivSet}(A) = \Omega_A \setminus \{0_A\}$, and
(ii) $\mathrm{NonZeroDivSet}(A)$ is a without zero, non empty, multiplicatively closed subset of A.

The theorem is a consequence of (4).

(45) Let us consider an element a of A. Then $a \in \mathrm{NonZeroDivSet}(A)$ if and only if $a \neq 0_A$. The theorem is a consequence of (44).

(46) $\mathrm{TotalQuotRing}(A)$ is a field. The theorem is a consequence of (4), (30), and (19).

(47) Let us consider an integral domain A. Then the field of quotients of A is ring isomorphic to $\mathrm{TotalQuotRing}(A)$.
PROOF: Set $S = \mathrm{NonZeroDivSet}(A)$. Set $B =$ the field of quotients of A. Set $f =$ the canonical homomorphism of A into quotient field. $f^\circ S \subseteq \mathrm{UnitSet}(B)$. Reconsider $S = \mathrm{NonZeroDivSet}(A)$ as a without zero, non

empty, multiplicatively closed subset of A. UnivMap(S, f) inherits ring homomorphism. TotalQuotRing(A) is a field. Set $g = $ UnivMap(S, f). For every object y such that $y \in \Omega_B$ holds $y \in \operatorname{rng} g$. $\square$

References

[1] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.

[2] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[5] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

[6] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2nd edition, 1989.

[7] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.

[8] Yasushige Watase. Zariski topology. *Formalized Mathematics*, 26(**4**):277–283, 2018. doi:10.2478/forma-2018-0024.

Accepted January 13, 2020