

The Localization of a Commutative Ring

Anthony Bordg

May 6, 2022

Abstract

We formalize the localization [1, II, §4] of a commutative ring R with respect to a multiplicative subset (i.e. a submonoid of R seen as a multiplicative monoid).

This localization is itself a commutative ring and we build the natural homomorphism of rings from R to its localization.

Contents

1	The Localization of a Commutative Ring	1
1.1	Localization	1
1.2	The Natural Homomorphism from a Ring to Its Localization	33

2	Acknowledgements	37
----------	-------------------------	-----------

theory *Localization*

imports *Main HOL-Algebra.Group HOL-Algebra.Ring HOL-Algebra.AbelCoset*
begin

Contents:

- We define the localization of a commutative ring R with respect to a multiplicative subset, i.e. with respect to a submonoid of R (seen as a multiplicative monoid), cf. [*rec-rng-of-frac*].
- We prove that this localization is a commutative ring (cf. [*crng-rng-of-frac*]) equipped with a homomorphism of rings from R (cf. [*rng-to-rng-of-frac-is-ring-hom*]).

1 The Localization of a Commutative Ring

1.1 Localization

locale *submonoid = monoid M* **for** M (**structure**) +

fixes S

assumes *subset* : $S \subseteq \text{carrier } M$

and *m-closed* [*intro*, *simp*] : $\llbracket x \in S; y \in S \rrbracket \implies x \otimes y \in S$
and *one-closed* [*simp*] : $\mathbf{1} \in S$

lemma (**in** *submonoid*) *is-submonoid*: *submonoid* $M\ S$
by (*rule submonoid-axioms*)

locale *mult-submonoid-of-rng* = *ring* R + *submonoid* $R\ S$ **for** R **and** S

locale *mult-submonoid-of-crng* = *cring* R + *mult-submonoid-of-rng* $R\ S$ **for** R
and S

locale *eq-obj-rng-of-frac* = *cring* R + *mult-submonoid-of-crng* $R\ S$ **for** R (**structure**)
and S +
fixes *rel*
defines $rel \equiv (\text{carrier} = \text{carrier } R \times S, eq = \lambda(r,s) (r',s'). \exists t \in S. t \otimes ((s' \otimes r) \ominus (s \otimes r')) = \mathbf{0})$

lemma (**in** *abelian-group*) *minus-to-eq* :
assumes *abelian-group* G **and** $x \in \text{carrier } G$ **and** $y \in \text{carrier } G$ **and** $x \ominus y = \mathbf{0}$
shows $x = y$
by (*metis add.inv-solve-right assms(2) assms(3) assms(4) l-zero minus-eq zero-closed*)

lemma (**in** *eq-obj-rng-of-frac*) *equiv-obj-rng-of-frac*:
shows *equivalence* *rel*

proof

show $\bigwedge x. x \in \text{carrier } rel \implies x \text{.}_{=rel} x$

proof–

fix x

assume $x \in \text{carrier } rel$

then have $f1: \mathbf{1} \otimes ((snd\ x \otimes fst\ x) \ominus (snd\ x \otimes fst\ x)) = \mathbf{0}$

using *rel-def subset l-one minus-eq add.r-inv rev-subsetD*

by *auto*

moreover have $x = (fst\ x, snd\ x)$

by *simp*

thus $x \text{.}_{=rel} x$

using *rel-def one-closed f1*

by *auto*

qed

show $\bigwedge x\ y. x \text{.}_{=rel} y \implies x \in \text{carrier } rel \implies y \in \text{carrier } rel \implies y \text{.}_{=rel} x$

proof–

fix $x\ y$

assume $a1: x \text{.}_{=rel} y$ **and** $a2: x \in \text{carrier } rel$ **and** $a3: y \in \text{carrier } rel$

then obtain t **where** $f1: t \in S$ **and** $f2: t \otimes ((snd\ y \otimes fst\ x) \ominus (snd\ x \otimes fst\ y))$

= $\mathbf{0}$

using *rel-def*

by *fastforce*

then have $(snd\ x \otimes fst\ y) \ominus (snd\ y \otimes fst\ x) = \ominus ((snd\ y \otimes fst\ x) \ominus (snd\ x \otimes fst\ y))$

using *abelian-group.minus-add abelian-group.minus-minus*

```

    by (smt a2 a3 a-minus-def abelian-group.a-inv-closed add.inv-mult-group
is-abelian-group
    mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)
prod.collapse
    rel-def rev-subsetD subset)
  then have  $t \otimes ((snd\ x \otimes fst\ y) \ominus (snd\ y \otimes fst\ x)) = \mathbf{0}$ 
  using minus-zero r-minus f2
  by (smt a2 a3 f1 mem-Sigma-iff minus-closed partial-object.select-convs(1)
prod.collapse
    rel-def semiring-simprules(3) rev-subsetD subset)
  thus  $y \text{ .}=_rel\ x$ 
  using f1 rel-def
  by auto
qed
show  $\bigwedge x\ y\ z.$ 
 $x \text{ .}=_rel\ y \implies y \text{ .}=_rel\ z \implies x \in carrier\ rel \implies y \in carrier\ rel \implies z \in carrier\ rel$ 
 $rel \implies x \text{ .}=_rel\ z$ 
proof-
  fix  $x\ y\ z$ 
  assume  $a1:x \text{ .}=_rel\ y$  and  $a2:y \text{ .}=_rel\ z$  and  $a3:x \in carrier\ rel$  and  $a4:y \in carrier\ rel$ 
  and  $a5:z \in carrier\ rel$ 
  then obtain  $t$  where  $f1:t \in S$  and  $f2:t \otimes ((snd\ y \otimes fst\ x) \ominus (snd\ x \otimes fst\ y)) = \mathbf{0}$ 
  using rel-def
  by fastforce
  then obtain  $t'$  where  $f3:t' \in S$  and  $f4:t' \otimes ((snd\ z \otimes fst\ y) \ominus (snd\ y \otimes fst\ z)) = \mathbf{0}$ 
  using rel-def a2
  by fastforce
  then have  $t \otimes (snd\ y \otimes fst\ x) \ominus t \otimes (snd\ x \otimes fst\ y) = \mathbf{0}$ 
  using f1 subset r-distr f2
  by (smt a3 a4 a-minus-def abelian-group.a-inv-closed is-abelian-group mem-Sigma-iff
    monoid.m-closed monoid-axioms partial-object.select-convs(1) prod.collapse
r-minus rel-def
    subset-iff)
  then have  $t' \otimes (t \otimes (snd\ y \otimes fst\ x)) \ominus t' \otimes (t \otimes (snd\ x \otimes fst\ y)) = \mathbf{0}$ 
  using f3 subset r-distr
  by (smt a3 a4 a-minus-def f1 is-abelian-group mem-Sigma-iff minus-to-eq
    partial-object.select-convs(1) prod.collapse r-neg rel-def semiring-simprules(3)
subset-iff)
  then have  $f5:snd\ z \otimes (t' \otimes (t \otimes (snd\ y \otimes fst\ x))) \ominus snd\ z \otimes (t' \otimes (t \otimes (snd\ x \otimes fst\ y))) = \mathbf{0}$ 
  using a5 rel-def r-distr
  by (smt a3 a4 a-minus-def f1 f3 is-abelian-group mem-Sigma-iff minus-to-eq
    monoid.m-closed
    monoid-axioms partial-object.select-convs(1) prod.collapse r-neg subset
subset-iff)

```

have $t' \otimes (\text{snd } z \otimes \text{fst } y) \ominus t' \otimes (\text{snd } y \otimes \text{fst } z) = \mathbf{0}$
using $f3\ f4\ \text{subset}\ r\text{-distr}$
by ($\text{smt } a4\ a5\ a\text{-minus-def}\ \text{abelian-group.a-inv-closed}\ \text{is-abelian-group}\ \text{mem-Sigma-iff}$

$\text{monoid.m-closed}\ \text{monoid-axioms}\ \text{partial-object.select-convs}(1)\ \text{prod.collapse}$
 $r\text{-minus}\ \text{rel-def}$
 rev-subsetD

then have $t \otimes (t' \otimes (\text{snd } z \otimes \text{fst } y)) \ominus t \otimes (t' \otimes (\text{snd } y \otimes \text{fst } z)) = \mathbf{0}$
using $f1\ \text{subset}\ r\text{-distr}$
by ($\text{smt } a4\ a5\ a\text{-minus-def}\ f3\ \text{is-abelian-group}\ \text{mem-Sigma-iff}\ \text{minus-to-eq}$
 monoid.m-closed
 $\text{monoid-axioms}\ \text{partial-object.select-convs}(1)\ \text{prod.collapse}\ r\text{-neg}\ \text{rel-def}$
 subset-iff

then have $f6:\text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } z \otimes \text{fst } y))) \ominus \text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } y \otimes \text{fst } z))) = \mathbf{0}$
using $a3\ \text{rel-def}\ r\text{-distr}$
by ($\text{smt } a4\ a5\ a\text{-minus-def}\ f1\ f3\ \text{is-abelian-group}\ \text{mem-Sigma-iff}\ \text{minus-to-eq}$
 monoid.m-closed
 $\text{monoid-axioms}\ \text{partial-object.select-convs}(1)\ \text{prod.collapse}\ r\text{-neg}\ \text{subset}$
 subset-iff

have $\text{snd } z \otimes (t' \otimes (t \otimes (\text{snd } x \otimes \text{fst } y))) = \text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } z \otimes \text{fst } y)))$
using $\text{comm-monoid-axioms-def}[of\ R]\ f1\ f3\ \text{subset}\ a3\ a4\ a5\ m\text{-assoc}$
by ($\text{smt } m\text{-lcomm}\ \text{mem-Sigma-iff}\ \text{partial-object.select-convs}(1)\ \text{partial-object-ext-def}$
 rel-def
 $\text{semiring-simprules}(3)\ \text{rev-subsetD}\ \text{surjective-pairing}$

then have $\text{snd } z \otimes (t' \otimes (t \otimes (\text{snd } y \otimes \text{fst } x))) \ominus \text{snd } z \otimes (t' \otimes (t \otimes (\text{snd } x \otimes \text{fst } y))) \oplus$
 $\text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } z \otimes \text{fst } y))) \ominus \text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } y \otimes \text{fst } z)))$
 $=$
 $\text{snd } z \otimes (t' \otimes (t \otimes (\text{snd } y \otimes \text{fst } x))) \ominus \text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } y \otimes \text{fst } z)))$
using add.l-inv
by ($\text{smt } a3\ a4\ a5\ f1\ f3\ f5\ \text{is-abelian-group}\ \text{local.semiring-axioms}\ \text{mem-Sigma-iff}$
 minus-to-eq
 $\text{monoid.m-closed}\ \text{monoid-axioms}\ \text{partial-object.select-convs}(1)\ \text{prod.collapse}$
 rel-def
 $\text{semiring.semiring-simprules}(6)\ \text{subset}\ \text{subset-iff}$

then have $f7:\text{snd } z \otimes (t' \otimes (t \otimes (\text{snd } y \otimes \text{fst } x))) \ominus \text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } y \otimes \text{fst } z))) = \mathbf{0}$
using $f5\ f6$
by ($\text{smt } \langle \text{snd } z \otimes (t' \otimes (t \otimes (\text{snd } x \otimes \text{fst } y))) = \text{snd } x \otimes (t \otimes (t' \otimes (\text{snd } z \otimes \text{fst } y))) \rangle$
 $\langle t' \otimes (\text{snd } z \otimes \text{fst } y) \ominus t' \otimes (\text{snd } y \otimes \text{fst } z) = \mathbf{0} \rangle\ a4\ a5\ f3\ \text{is-abelian-group}$
 mem-Sigma-iff
 $\text{minus-to-eq}\ \text{partial-object.select-convs}(1)\ \text{prod.collapse}\ \text{rel-def}\ \text{semiring-simprules}(3)$
 $\text{subset}\ \text{subset-iff}$

moreover have $(t \otimes t' \otimes \text{snd } y) \otimes ((\text{snd } z \otimes \text{fst } x) \ominus (\text{snd } x \otimes \text{fst } z)) = ((t \otimes t' \otimes \text{snd } y) \otimes (\text{snd } z \otimes \text{fst } x)) \ominus ((t \otimes t' \otimes \text{snd } y) \otimes (\text{snd } x \otimes \text{fst } z))$

```

using r-distr f1 f3 subset a3 a4 a5 rel-def a-minus-def r-minus
by (smt SigmaE abelian-group.a-inv-closed is-abelian-group monoid.m-closed
monoid-axioms
  partial-object.select-convs(1) prod.sel(1) prod.sel(2) subset-iff)
moreover have f8:(t ⊗ t' ⊗ snd y) ⊗ (snd z ⊗ fst x) = snd z ⊗ (t' ⊗ (t ⊗
(snd y ⊗ fst x)))
using m-assoc comm-monoid-axioms-def[of R] f1 f3 subset a3 a4 a5 rel-def
rev-subsetD
by (smt SigmaE local.semiring-axioms m-lcomm partial-object.select-convs(1)
prod.sel(1)
  prod.sel(2) semiring.semiring-simprules(3))
moreover have f9:(t ⊗ t' ⊗ snd y) ⊗ (snd x ⊗ fst z) = snd x ⊗ (t ⊗ (t' ⊗
(snd y ⊗ fst z)))
using m-assoc comm-monoid-axioms-def[of R] f1 f3 subset a3 a4 a5 rel-def
rev-subsetD
by (smt SigmaE m-comm monoid.m-closed monoid-axioms partial-object.select-convs(1)
prod.sel(1)
  prod.sel(2))
then have f10:(t ⊗ t' ⊗ snd y) ⊗ (snd z ⊗ fst x) ⊖ (t ⊗ t' ⊗ snd y) ⊗ (snd
x ⊗ fst z) = 0
using f7 f8 f9
by simp
moreover have t ⊗ t' ⊗ snd y ∈ S
using f1 f3 a4 rel-def m-closed
by (simp add: mem-Times-iff)
then have (t ⊗ t' ⊗ snd y) ⊗ (snd z ⊗ fst x ⊖ snd x ⊗ fst z) = 0
using r-distr subset rev-subsetD f10 calculation(2)
by auto
thus x .=rel z
using rel-def ⟨t ⊗ t' ⊗ snd y ∈ S⟩
by auto
qed
qed

```

definition *eq-class-of-rng-of-frac*:: - ⇒ 'a ⇒ 'b ⇒ -set (infix |₁ 10)
where $r \mid_{rel} s \equiv \{(r', s') \in \text{carrier } rel. (r, s) \text{ .=}_{rel} (r', s')\}$

lemma *class-of-to-rel*:
shows $\text{class-of}_{rel} (r, s) = (r \mid_{rel} s)$
using *eq-class-of-def*[of rel] *eq-class-of-rng-of-frac-def*[of rel]
by auto

lemma (in *eq-obj-rng-of-frac*) *zero-in-mult-submonoid*:
assumes $0 \in S$ **and** $(r, s) \in \text{carrier } rel$ **and** $(r', s') \in \text{carrier } rel$
shows $(r \mid_{rel} s) = (r' \mid_{rel} s')$
proof
show $(r \mid_{rel} s) \subseteq (r' \mid_{rel} s')$
proof
fix x

```

assume a1:  $x \in (r \mid_{rel} s)$ 
have  $\mathbf{0} \otimes (s' \otimes fst\ x \ominus snd\ x \otimes r') = \mathbf{0}$ 
  using l-zero subset rel-def a1 eq-class-of-rng-of-frac-def
  by (smt abelian-group.minus-closed assms(3) is-abelian-group l-null mem-Collect-eq
mem-Sigma-iff
      monoid.m-closed monoid-axioms old.prod.case partial-object.select-convs(1)
subset-iff surjective-pairing)
  thus  $x \in (r' \mid_{rel} s')$ 
  using assms(1) assms(3) rel-def eq-class-of-rng-of-frac-def
  by (smt SigmaE a1 eq-object.select-convs(1) l-null mem-Collect-eq minus-closed
old.prod.case
      partial-object.select-convs(1) prod.collapse semiring-simprules(3) subset
subset-iff)
qed
show  $(r' \mid_{rel} s') \subseteq (r \mid_{rel} s)$ 
proof
  fix x
  assume a1:  $x \in (r' \mid_{rel} s')$ 
  have  $\mathbf{0} \otimes (s \otimes fst\ x \ominus snd\ x \otimes r) = \mathbf{0}$ 
  using l-zero subset rel-def a1 eq-class-of-rng-of-frac-def
  by (metis (no-types, lifting) BNF-Def.Collect-case-prodD assms(2) l-null
mem-Sigma-iff
      minus-closed partial-object.select-convs(1) semiring-simprules(3) rev-subsetD)
  thus  $x \in (r \mid_{rel} s)$ 
  using assms(1) assms(2) rel-def eq-class-of-rng-of-frac-def
  by (smt SigmaE a1 eq-object.select-convs(1) l-null mem-Collect-eq minus-closed
old.prod.case
      partial-object.select-convs(1) prod.collapse semiring-simprules(3) subset
subset-iff)
qed
qed

```

definition *set-eq-class-of-rng-of-frac*:: $- \Rightarrow$ *-set (set'-class'-of1)*
where *set-class-of_{rel}* $\equiv \{(r \mid_{rel} s) \mid r\ s, (r, s) \in carrier\ rel\}$

lemma *elem-eq-class*:

```

assumes equivalence S and  $x \in carrier\ S$  and  $y \in carrier\ S$  and  $x \cdot_S y$ 
shows  $class-of_S\ x = class-of_S\ y$ 
proof
show  $class-of_S\ x \subseteq class-of_S\ y$ 
proof
  fix z
  assume  $z \in class-of_S\ x$ 
  then have  $y \cdot_S z$ 
  using assms eq-class-of-def[of S x] equivalence.sym[of S x y] equivalence.trans
  by (metis (mono-tags, lifting) mem-Collect-eq)
thus  $z \in class-of_S\ y$ 
  using  $\langle z \in class-of_S\ x \rangle$ 

```

```

    by (simp add: eq-class-of-def)
qed
show class-ofS y ⊆ class-ofS x
proof
  fix z
  assume z ∈ class-ofS y
  then have x .=S z
    using assms eq-class-of-def equivalence.trans
    by (metis (mono-tags, lifting) mem-Collect-eq)
  thus z ∈ class-ofS x
    using ⟨z ∈ class-ofS y⟩
    by (simp add: eq-class-of-def)
qed
qed

lemma (in abelian-group) four-elem-comm:
  assumes a ∈ carrier G and b ∈ carrier G and c ∈ carrier G and d ∈ carrier
  G
  shows a ⊖ c ⊕ b ⊖ d = a ⊕ b ⊖ c ⊖ d
  using assms a-assoc a-comm
  by (simp add: a-minus-def)

lemma (in abelian-monoid) right-add-eq:
  assumes a = b
  shows c ⊕ a = c ⊕ b
  using assms
  by simp

lemma (in abelian-monoid) right-minus-eq:
  assumes a = b
  shows c ⊖ a = c ⊖ b
  by (simp add: assms)

lemma (in abelian-group) inv-add:
  assumes a ∈ carrier G and b ∈ carrier G
  shows ⊖ (a ⊕ b) = ⊖ a ⊖ b
  using assms minus-add
  by (simp add: a-minus-def)

lemma (in abelian-group) right-inv-add:
  assumes a ∈ carrier G and b ∈ carrier G and c ∈ carrier G
  shows c ⊖ a ⊖ b = c ⊖ (a ⊕ b)
  using assms
  by (simp add: a-minus-def add.m-assoc local.minus-add)

context eq-obj-rng-of-frac
begin

definition carrier-rng-of-frac:: - partial-object

```

where $\text{carrier-rng-of-frac} \equiv (\text{carrier} = \text{set-class-of_rel})$

definition $\text{mult-rng-of-frac}:: [-\text{set}, -\text{set}] \Rightarrow -\text{set}$

where $\text{mult-rng-of-frac } X Y \equiv$
 $\text{let } x' = (\text{SOME } x. x \in X) \text{ in}$
 $\text{let } y' = (\text{SOME } y. y \in Y) \text{ in}$
 $(\text{fst } x' \otimes \text{fst } y')|_{\text{rel}} (\text{snd } x' \otimes \text{snd } y')$

definition $\text{rec-monoid-rng-of-frac}:: - \text{monoid}$

where $\text{rec-monoid-rng-of-frac} \equiv (\text{carrier} = \text{set-class-of_rel}, \text{mult} = \text{mult-rng-of-frac},$
 $\text{one} = (\mathbf{1}|_{\text{rel}} \mathbf{1}))$

lemma $\text{member-class-to-carrier}$:

assumes $x \in (r |_{\text{rel}} s)$ **and** $y \in (r' |_{\text{rel}} s')$
shows $(\text{fst } x \otimes \text{fst } y, \text{snd } x \otimes \text{snd } y) \in \text{carrier } \text{rel}$
using $\text{assms } \text{rel-def } \text{eq-class-of-rng-of-frac-def}$
by $(\text{metis } (\text{no-types}, \text{lifting}) \text{Product-Type.Collect-case-prodD } m\text{-closed } \text{mem-Sigma-iff})$

$\text{partial-object.select-convs}(1) \text{ semiring-simprules}(3))$

lemma $\text{member-class-to-member-class}$:

assumes $x \in (r |_{\text{rel}} s)$ **and** $y \in (r' |_{\text{rel}} s')$
shows $(\text{fst } x \otimes \text{fst } y |_{\text{rel}} \text{snd } x \otimes \text{snd } y) \in \text{set-class-of_rel}$
using $\text{assms } \text{member-class-to-carrier}[\text{of } x \ r \ s \ y \ r' \ s'] \text{ set-eq-class-of-rng-of-frac-def}[\text{of } \text{rel}]$
 $\text{eq-class-of-rng-of-frac-def}$
by auto

lemma $\text{closed-mult-rng-of-frac}$:

assumes $(r, s) \in \text{carrier } \text{rel}$ **and** $(t, u) \in \text{carrier } \text{rel}$
shows $(r |_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} (t |_{\text{rel}} u) \in \text{set-class-of_rel}$

proof –

have $(r, s) \text{.}=\text{rel } (r, s)$
using $\text{assms}(1) \text{equiv-obj-rng-of-frac equivalence-def}[\text{of } \text{rel}]$
by blast
then have $(r, s) \in (r |_{\text{rel}} s)$
using $\text{assms}(1)$
by $(\text{simp add: eq-class-of-rng-of-frac-def})$
then have $f1:\exists x. x \in (r |_{\text{rel}} s)$
by auto
have $f2:\exists y. y \in (t |_{\text{rel}} u)$
using $\text{assms}(2) \text{equiv-obj-rng-of-frac equivalence.refl eq-class-of-rng-of-frac-def}$
by fastforce
show $(r |_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} (t |_{\text{rel}} u) \in \text{set-class-of_rel}$
using $f1 \ f2 \ \text{rec-monoid-rng-of-frac-def } \text{mult-rng-of-frac-def}[\text{of } (r |_{\text{rel}} s) (t |_{\text{rel}} u)]$
 $\text{set-eq-class-of-rng-of-frac-def}[\text{of } \text{rel}] \ \text{member-class-to-member-class}[\text{of } x' \ r \ s \ y'$
 $t \ u]$
by $(\text{metis } (\text{mono-tags}, \text{lifting}) \text{mem-Collect-eq } \text{member-class-to-carrier } \text{monoid.select-convs}(1))$

someI-ex)

qed

lemma *non-empty-class*:
assumes $(r, s) \in \text{carrier } rel$
shows $(r \mid_{rel} s) \neq \{\}$
using *assms eq-class-of-rng-of-frac-def equiv-obj-rng-of-frac equivalence.refl*
by *fastforce*

lemma *mult-rng-of-frac-fundamental-lemma*:
assumes $(r, s) \in \text{carrier } rel$ **and** $(r', s') \in \text{carrier } rel$
shows $(r \mid_{rel} s) \otimes_{\text{rec-monoid-rng-of-frac}} (r' \mid_{rel} s') = (r \otimes r' \mid_{rel} s \otimes s')$
proof –
have $f1:(r \mid_{rel} s) \neq \{\}$
using *assms(1) non-empty-class*
by *auto*
have $(r' \mid_{rel} s') \neq \{\}$
using *assms(2) non-empty-class*
by *auto*
then have $\exists x \in (r \mid_{rel} s). \exists x' \in (r' \mid_{rel} s'). (r \mid_{rel} s) \otimes_{\text{rec-monoid-rng-of-frac}} (r' \mid_{rel} s') =$
 $(fst\ x \otimes fst\ x' \mid_{rel} snd\ x \otimes snd\ x')$
using *f1 rec-monoid-rng-of-frac-def*
by *(metis monoid.select-convs(1) mult-rng-of-frac-def some-in-eq)*
then obtain x **and** x' **where** $f2:x \in (r \mid_{rel} s)$ **and** $f3:x' \in (r' \mid_{rel} s')$
and $(r \mid_{rel} s) \otimes_{\text{rec-monoid-rng-of-frac}} (r' \mid_{rel} s') = (fst\ x \otimes fst\ x' \mid_{rel} snd\ x \otimes$
 $snd\ x')$
by *blast*
then have $(r, s) \text{ .}=_rel (fst\ x, snd\ x)$
using *rel-def*
by *(metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def)*
then obtain t **where** $f4:t \in S$ **and** $f5:t \otimes ((snd\ x \otimes r) \ominus (s \otimes fst\ x)) = \mathbf{0}$
using *rel-def*
by *auto*
have $(r', s') \text{ .}=_rel (fst\ x', snd\ x')$
using *rel-def f3*
by *(metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def)*
then obtain t' **where** $f6:t' \in S$ **and** $f7:t' \otimes (snd\ x' \otimes r' \ominus s' \otimes fst\ x') = \mathbf{0}$
using *rel-def*
by *auto*
have $f8:t \in \text{carrier } R$
using *f4 subset rev-subsetD*
by *auto*
have $f9:snd\ x \otimes r \in \text{carrier } R$
using *subset rev-subsetD f2 assms(1)*
by *(metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def*
mem-Sigma-iff
partial-object.select-convs(1) rel-def semiring-simprules(3))

have $f10: \ominus (s \otimes \text{fst } x) \in \text{carrier } R$
using $\text{assms}(1)$ $\text{subset rev-subsetD } f2$
by ($\text{metis (no-types, lifting) BNF-Def.Collect-case-prodD abelian-group.a-inv-closed}$

$\text{eq-class-of-rng-of-frac-def is-abelian-group mem-Sigma-iff monoid.m-closed}$
 monoid-axioms
 $\text{partial-object.select-convs}(1)$ rel-def)
then have $t \otimes (\text{snd } x \otimes r) \ominus t \otimes (s \otimes \text{fst } x) = \mathbf{0}$
using $f8$ $f9$ $f10$ $f5$ $r\text{-distr}[of \text{snd } x \otimes r \ominus (s \otimes \text{fst } x) t]$ $a\text{-minus-def}$ $r\text{-minus}[of t s \otimes \text{fst } x]$
by ($\text{smt BNF-Def.Collect-case-prodD assms}(1)$ $\text{eq-class-of-rng-of-frac-def } f2$
 mem-Sigma-iff
 $\text{partial-object.select-convs}(1)$ $\text{rel-def semiring-simprules}(3)$ subset subset-iff)
then have $f11: t \otimes (\text{snd } x \otimes r) = t \otimes (s \otimes \text{fst } x)$
by ($\text{smt BNF-Def.Collect-case-prodD assms}(1)$ $\text{eq-class-of-rng-of-frac-def } f2$ $f8$
 is-abelian-group
 $\text{mem-Sigma-iff minus-to-eq monoid.m-closed monoid-axioms partial-object.select-convs}(1)$
 $\text{rel-def subset subset-iff}$)
have $f12: t' \in \text{carrier } R$
using $f6$ $\text{subset rev-subsetD}$
by auto
have $f13: \text{snd } x' \otimes r' \in \text{carrier } R$
using $\text{assms}(2)$ $f3$ $\text{subset rev-subsetD}$
by ($\text{metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def}$

$\text{mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs}(1)$
 rel-def)
have $f14: \ominus (s' \otimes \text{fst } x') \in \text{carrier } R$
using $\text{assms}(2)$ $f3$ $\text{subset rev-subsetD}$
by ($\text{metis (no-types, lifting) BNF-Def.Collect-case-prodD abelian-group.a-inv-closed}$

$\text{eq-class-of-rng-of-frac-def is-abelian-group mem-Sigma-iff monoid.m-closed}$
 monoid-axioms
 $\text{partial-object.select-convs}(1)$ rel-def)
then have $t' \otimes (\text{snd } x' \otimes r') \ominus t' \otimes (s' \otimes \text{fst } x') = \mathbf{0}$
using $f12$ $f13$ $f14$ $f7$ $r\text{-distr}[of \text{snd } x' \otimes r' \ominus (s' \otimes \text{fst } x') t']$ $a\text{-minus-def}$
 $r\text{-minus}[of t' s' \otimes \text{fst } x']$
by ($\text{smt BNF-Def.Collect-case-prodD assms}(2)$ $\text{eq-class-of-rng-of-frac-def } f3$
 mem-Sigma-iff
 $\text{partial-object.select-convs}(1)$ $\text{rel-def semiring-simprules}(3)$ subset subset-iff)
then have $f15: t' \otimes (\text{snd } x' \otimes r') = t' \otimes (s' \otimes \text{fst } x')$
by ($\text{smt BNF-Def.Collect-case-prodD assms}(2)$ $\text{eq-class-of-rng-of-frac-def } f3$ $f12$
 is-abelian-group
 $\text{mem-Sigma-iff minus-to-eq monoid.m-closed monoid-axioms partial-object.select-convs}(1)$
 $\text{rel-def subset subset-iff}$)
have $t' \otimes t \in S$
using $f4$ $f6$ $m\text{-closed}$
by auto
then have $f16: t' \otimes t \in \text{carrier } R$

```

using subset rev-subsetD
by auto
have f17:(snd x ⊗ snd x') ⊗ (r ⊗ r') ∈ carrier R
using assms f2 f3
by (metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def
mem-Sigma-iff
monoid.m-closed monoid-axioms partial-object.select-convs(1) rel-def subset
subset-iff)
have f18:(s ⊗ s') ⊗ (fst x ⊗ fst x') ∈ carrier R
using assms f2 f3
by (metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def
mem-Sigma-iff
monoid.m-closed monoid-axioms partial-object.select-convs(1) rel-def subset
subset-iff)
then have f19:(t' ⊗ t) ⊗ ((snd x ⊗ snd x') ⊗ (r ⊗ r') ⊖ (s ⊗ s') ⊗ (fst x ⊗
fst x')) =
((t' ⊗ t) ⊗ (snd x ⊗ snd x')) ⊗ (r ⊗ r') ⊖ (t' ⊗ t) ⊗ ((s ⊗ s') ⊗ (fst x ⊗ fst
x'))
using f16 f17 f18 r-distr m-assoc r-minus a-minus-def
by (smt BNF-Def.Collect-case-prodD assms(1) assms(2) eq-class-of-rng-of-frac-def
f14 f2 f3
m-comm mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)
rel-def
subset subset-iff)
then have f20:(t' ⊗ t) ⊗ (snd x ⊗ snd x') ⊗ (r ⊗ r') = (t' ⊗ t) ⊗ (snd x ⊗ r
⊗ snd x' ⊗ r')
using m-assoc m-comm f16 assms rel-def f2 f3
by (smt BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def mem-Sigma-iff

partial-object.select-convs(1) semiring-simprules(3) subset subset-iff)
then have ((t' ⊗ t) ⊗ (snd x ⊗ snd x')) ⊗ (r ⊗ r') = t' ⊗ ((t ⊗ snd x ⊗ r) ⊗
snd x' ⊗ r')
using m-assoc assms f2 f3 rel-def f8 f12
by (smt BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def mem-Sigma-iff
monoid.m-closed
monoid-axioms partial-object.select-convs(1) subset subset-iff)
then have f21:((t' ⊗ t) ⊗ (snd x ⊗ snd x')) ⊗ (r ⊗ r') = t' ⊗ (t ⊗ s ⊗ fst x)
⊗ snd x' ⊗ r'
using f11 m-assoc
by (smt BNF-Def.Collect-case-prodD assms(1) assms(2) eq-class-of-rng-of-frac-def
f12 f2 f3 f8
mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)
rel-def subset subset-iff)
moreover have (t' ⊗ t) ⊗ ((s ⊗ s') ⊗ (fst x ⊗ fst x')) = (t' ⊗ s' ⊗ fst x') ⊗ t
⊗ s ⊗ fst x
using assms f2 f3 f8 f12 m-assoc m-comm rel-def
by (smt BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def mem-Sigma-iff
monoid.m-closed
monoid-axioms partial-object.select-convs(1) subset subset-iff)

```

then have $(t' \otimes t) \otimes ((s \otimes s') \otimes (fst\ x \otimes fst\ x')) = (t' \otimes snd\ x' \otimes r') \otimes t \otimes s \otimes fst\ x$
using *f15 m-assoc*
by (*smt BNF-Def.Collect-case-prodD assms(2) eq-class-of-rng-of-frac-def f12 f3 mem-Sigma-iff*
partial-object.select-convs(1) rel-def subset subset-iff)
then have $f22:(t' \otimes t) \otimes ((s \otimes s') \otimes (fst\ x \otimes fst\ x')) = t' \otimes ((t \otimes snd\ x \otimes r) \otimes snd\ x' \otimes r')$
using *m-assoc m-comm assms*
by (*smt BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def f12 f2 f21 f3 f8 mem-Sigma-iff*
partial-object.select-convs(1) rel-def semiring-simprules(3) subset subset-iff)
then have $f23:(t' \otimes t) \otimes ((snd\ x \otimes snd\ x') \otimes (r \otimes r') \ominus (s \otimes s') \otimes (fst\ x \otimes fst\ x')) = \mathbf{0}$
using *f19 f21 f22*
by (*metis* $\langle t' \otimes t \otimes (snd\ x \otimes snd\ x') \otimes (r \otimes r') = t' \otimes (t \otimes snd\ x \otimes r \otimes snd\ x' \otimes r') \rangle$
a-minus-def f16 f18 r-neg semiring-simprules(3))
have $f24:(r \otimes r', s \otimes s') \in carrier\ rel$
using *assms rel-def*
by *auto*
have $f25:(fst\ x \otimes fst\ x', snd\ x \otimes snd\ x') \in carrier\ rel$
using *f2 f3 member-class-to-carrier*
by *auto*
then have $(r \otimes r', s \otimes s') \dot{=}_{rel} (fst\ x \otimes fst\ x', snd\ x \otimes snd\ x')$
using *f23 f24 rel-def* $\langle t' \otimes t \in S \rangle$
by *auto*
then have $class_of_{rel} (r \otimes r', s \otimes s') = class_of_{rel} (fst\ x \otimes fst\ x', snd\ x \otimes snd\ x')$
using *f24 f25 equiv-obj-rng-of-frac elem-eq-class[of rel (r \otimes r', s \otimes s') (fst\ x \otimes fst\ x', snd\ x \otimes snd\ x')]*
eq-class-of-rng-of-frac-def
by *auto*
then have $(r \otimes r' \mid_{rel} s \otimes s') = (fst\ x \otimes fst\ x' \mid_{rel} snd\ x \otimes snd\ x')$
using *class-of-to-rel[of rel]*
by *auto*
thus *?thesis*
using $\langle (r \mid_{rel} s) \otimes_{rec-monoid-rng-of-frac} (r' \mid_{rel} s') = (fst\ x \otimes fst\ x' \mid_{rel} snd\ x \otimes snd\ x') \rangle$
trans sym
by *auto*
qed

lemma *member-class-to-assoc:*

assumes $x \in (r \mid_{rel} s)$ **and** $y \in (t \mid_{rel} u)$ **and** $z \in (v \mid_{rel} w)$
shows $((fst\ x \otimes fst\ y) \otimes fst\ z \mid_{rel} (snd\ x \otimes snd\ y) \otimes snd\ z) = (fst\ x \otimes (fst\ y \otimes fst\ z) \mid_{rel} snd\ x \otimes (snd\ y \otimes snd\ z))$
using *assms m-assoc subset rel-def rev-subsetD*
by (*smt BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def mem-Sigma-iff*)

partial-object.select-convs(1)

lemma *assoc-mult-rng-of-frac:*

assumes $(r, s) \in \text{carrier rel}$ **and** $(t, u) \in \text{carrier rel}$ **and** $(v, w) \in \text{carrier rel}$
shows $((r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} (t \mid_{\text{rel}} u)) \otimes_{\text{rec-monoid-rng-of-frac}} (v \mid_{\text{rel}} w) =$
 $(r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} ((t \mid_{\text{rel}} u) \otimes_{\text{rec-monoid-rng-of-frac}} (v \mid_{\text{rel}} w))$

proof –

have $((r \otimes t) \otimes v, (s \otimes u) \otimes w) = (r \otimes (t \otimes v), s \otimes (u \otimes w))$
using *assms m-assoc*
by (*metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs(1) rel-def rev-subsetD subset*)
then have $f1:((r \otimes t) \otimes v \mid_{\text{rel}} (s \otimes u) \otimes w) = (r \otimes (t \otimes v) \mid_{\text{rel}} s \otimes (u \otimes w))$
by *simp*
have $f2:((r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} (t \mid_{\text{rel}} u)) \otimes_{\text{rec-monoid-rng-of-frac}} (v \mid_{\text{rel}} w) =$
 $((r \otimes t) \otimes v \mid_{\text{rel}} (s \otimes u) \otimes w)$
using *assms mult-rng-of-frac-fundamental-lemma rel-def*
by *auto*
have $f3:(r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} ((t \mid_{\text{rel}} u) \otimes_{\text{rec-monoid-rng-of-frac}} (v \mid_{\text{rel}} w)) =$
 $(r \otimes (t \otimes v) \mid_{\text{rel}} s \otimes (u \otimes w))$
using *assms mult-rng-of-frac-fundamental-lemma rel-def*
by *auto*
thus *?thesis*
using $f1 f2 f3$
by *simp*

qed

lemma *left-unit-mult-rng-of-frac:*

assumes $(r, s) \in \text{carrier rel}$
shows $\mathbf{1}_{\text{rec-monoid-rng-of-frac}} \otimes_{\text{rec-monoid-rng-of-frac}} (r \mid_{\text{rel}} s) = (r \mid_{\text{rel}} s)$
using *assms subset rev-subsetD rec-monoid-rng-of-frac-def mult-rng-of-frac-fundamental-lemma[of 1 1 r s]*
l-one[of r] l-one[of s] rel-def
by *auto*

lemma *right-unit-mult-rng-of-frac:*

assumes $(r, s) \in \text{carrier rel}$
shows $(r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} \mathbf{1}_{\text{rec-monoid-rng-of-frac}} = (r \mid_{\text{rel}} s)$
using *assms subset rev-subsetD rec-monoid-rng-of-frac-def mult-rng-of-frac-fundamental-lemma[of r s 1 1]*
r-one[of r] r-one[of s] rel-def
by *auto*

lemma *monoid-rng-of-frac:*

shows *monoid (rec-monoid-rng-of-frac)*
proof

show $\bigwedge x y. x \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies$
 $y \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies x \otimes_{\text{rec-monoid-rng-of-frac}} y \in \text{carrier}$
 $\text{rec-monoid-rng-of-frac}$
using $\text{rec-monoid-rng-of-frac-def closed-mult-rng-of-frac}$
by $(\text{smt mem-Collect-eq partial-object.select-convs}(1) \text{ set-eq-class-of-rng-of-frac-def})$
show $\bigwedge x y z. x \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies$
 $y \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies$
 $z \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies$
 $x \otimes_{\text{rec-monoid-rng-of-frac}} y \otimes_{\text{rec-monoid-rng-of-frac}} z =$
 $x \otimes_{\text{rec-monoid-rng-of-frac}} (y \otimes_{\text{rec-monoid-rng-of-frac}} z)$
using $\text{assoc-mult-rng-of-frac}$
by $(\text{smt mem-Collect-eq partial-object.select-convs}(1) \text{ rec-monoid-rng-of-frac-def}$
 $\text{ set-eq-class-of-rng-of-frac-def})$
show $\mathbf{1}_{\text{rec-monoid-rng-of-frac}} \in \text{carrier } \text{rec-monoid-rng-of-frac}$
using $\text{rec-monoid-rng-of-frac-def rel-def set-eq-class-of-rng-of-frac-def}$
by fastforce
show $\bigwedge x. x \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies \mathbf{1}_{\text{rec-monoid-rng-of-frac}} \otimes_{\text{rec-monoid-rng-of-frac}}$
 $x = x$
using $\text{left-unit-mult-rng-of-frac}$
by $(\text{smt mem-Collect-eq partial-object.select-convs}(1) \text{ rec-monoid-rng-of-frac-def}$
 $\text{ set-eq-class-of-rng-of-frac-def})$
show $\bigwedge x. x \in \text{carrier } \text{rec-monoid-rng-of-frac} \implies x \otimes_{\text{rec-monoid-rng-of-frac}} \mathbf{1}_{\text{rec-monoid-rng-of-frac}}$
 $= x$
using $\text{right-unit-mult-rng-of-frac}$
by $(\text{smt mem-Collect-eq partial-object.select-convs}(1) \text{ rec-monoid-rng-of-frac-def}$
 $\text{ set-eq-class-of-rng-of-frac-def})$
qed

lemma $\text{comm-mult-rng-of-frac}$:

assumes $(r, s) \in \text{carrier } \text{rel}$ **and** $(r', s') \in \text{carrier } \text{rel}$
shows $(r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} (r' \mid_{\text{rel}} s') = (r' \mid_{\text{rel}} s') \otimes_{\text{rec-monoid-rng-of-frac}}$
 $(r \mid_{\text{rel}} s)$

proof –

have $f1: (r \mid_{\text{rel}} s) \otimes_{\text{rec-monoid-rng-of-frac}} (r' \mid_{\text{rel}} s') = (r \otimes r' \mid_{\text{rel}} s \otimes s')$

using $\text{assms mult-rng-of-frac-fundamental-lemma}$

by simp

have $f2: (r' \mid_{\text{rel}} s') \otimes_{\text{rec-monoid-rng-of-frac}} (r \mid_{\text{rel}} s) = (r' \otimes r \mid_{\text{rel}} s' \otimes s)$

using $\text{assms mult-rng-of-frac-fundamental-lemma}$

by simp

have $f3: r \otimes r' = r' \otimes r$

using $\text{assms rel-def m-comm}$

by simp

have $f4: s \otimes s' = s' \otimes s$

using $\text{assms rel-def subset rev-subsetD m-comm}$

by $(\text{metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs}(1))$

thus $?thesis$

using $f1 f2 f3 f4$

by simp

qed

lemma *comm-monoid-rng-of-frac*:

shows *comm-monoid* (*rec-monoid-rng-of-frac*)

using *comm-monoid-def Group.comm-monoid-axioms-def monoid-rng-of-frac comm-mult-rng-of-frac*

by (*smt mem-Collect-eq partial-object.select-convs(1) rec-monoid-rng-of-frac-def set-eq-class-of-rng-of-frac-def*)

definition *add-rng-of-frac*:: [-set, -set] \Rightarrow -set

where *add-rng-of-frac* $X Y \equiv$

let $x' = (\text{SOME } x. x \in X)$ *in*

let $y' = (\text{SOME } y. y \in Y)$ *in*

$(\text{snd } y' \otimes \text{fst } x' \oplus \text{snd } x' \otimes \text{fst } y') \mid_{\text{rel}} (\text{snd } x' \otimes \text{snd } y')$

definition *rec-rng-of-frac*:: - ring

where *rec-rng-of-frac* \equiv

$(\mid \text{carrier} = \text{set-class-of}_{\text{rel}}, \text{mult} = \text{mult-rng-of-frac}, \text{one} = (\mathbf{1} \mid_{\text{rel}} \mathbf{1}), \text{zero} = (\mathbf{0} \mid_{\text{rel}} \mathbf{1}), \text{add} = \text{add-rng-of-frac} \mid)$

lemma *add-rng-of-frac-fundamental-lemma*:

assumes $(r, s) \in \text{carrier rel}$ **and** $(r', s') \in \text{carrier rel}$

shows $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') = (s' \otimes r \oplus s \otimes r' \mid_{\text{rel}} s \otimes s')$

proof –

have $\exists x' \in (r \mid_{\text{rel}} s). \exists y' \in (r' \mid_{\text{rel}} s'). (r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') = (\text{snd } y' \otimes \text{fst } x' \oplus \text{snd } x' \otimes \text{fst } y' \mid_{\text{rel}} \text{snd } x' \otimes \text{snd } y')$

using *assms rec-rng-of-frac-def add-rng-of-frac-def*[*of* $(r \mid_{\text{rel}} s) (r' \mid_{\text{rel}} s')$]

by (*metis non-empty-class ring-record-simps(12) some-in-eq*)

then obtain x' **and** y' **where** $f1: x' \in (r \mid_{\text{rel}} s)$ **and** $f2: y' \in (r' \mid_{\text{rel}} s')$ **and**

$f3: (r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') = (\text{snd } y' \otimes \text{fst } x' \oplus \text{snd } x' \otimes \text{fst } y' \mid_{\text{rel}} \text{snd } x' \otimes \text{snd } y')$

by *auto*

then have $(r, s) \cdot_{\text{rel}} x'$

using *f1 rel-def eq-class-of-rng-of-frac-def*[*of rel r s*]

by *auto*

then obtain t **where** $f4: t \in S$ **and** $f5: t \otimes (\text{snd } x' \otimes r \ominus s \otimes \text{fst } x') = \mathbf{0}$

using *rel-def*

by *auto*

have $(r', s') \cdot_{\text{rel}} y'$

using *f2 rel-def eq-class-of-rng-of-frac-def*[*of rel r' s'*]

by *auto*

then obtain t' **where** $f6: t' \in S$ **and** $f7: t' \otimes (\text{snd } y' \otimes r' \ominus s' \otimes \text{fst } y') = \mathbf{0}$

using *rel-def*

by *auto*

then have $f8: t \otimes t' \in S$

using *m-closed f4 f6*

by *simp*

then have $(s' \otimes r \oplus s \otimes r', s \otimes s') \cdot_{\text{rel}} (\text{snd } y' \otimes \text{fst } x' \oplus \text{snd } x' \otimes \text{fst } y', \text{snd } x' \otimes \text{snd } y')$

proof –

```

have f9: $t' \otimes s' \otimes \text{snd } y' \in \text{carrier } R$ 
  using f6 assms(2) f2 subset rev-subsetD eq-class-of-rng-of-frac-def rel-def
  by fastforce
have f10: $\text{snd } x' \otimes r \in \text{carrier } R$ 
  using assms(1) f1 rel-def subset rev-subsetD
by (metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def

      mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3))
have f11: $s \otimes \text{fst } x' \in \text{carrier } R$ 
  using assms(1) subset rev-subsetD f1 rel-def
by (metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def

      mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3))
have  $t \otimes (\text{snd } x' \otimes r \ominus s \otimes \text{fst } x') = t \otimes (\text{snd } x' \otimes r) \ominus t \otimes (s \otimes \text{fst } x')$ 
  using f9 f10 f11 f4 subset rev-subsetD r-distr[of snd x' \otimes r s \otimes fst x' t]
a-minus-def
  r-minus[of t s \otimes fst x']
  by (smt add.inv-closed monoid.m-closed monoid-axioms r-distr)
then have f12: $(t' \otimes s' \otimes \text{snd } y') \otimes (t \otimes (\text{snd } x' \otimes r \ominus s \otimes \text{fst } x')) =$ 
 $t' \otimes s' \otimes \text{snd } y' \otimes t \otimes (\text{snd } x' \otimes r) \ominus (t' \otimes s' \otimes \text{snd } y' \otimes t \otimes (s \otimes \text{fst } x'))$ 
  using f9 r-distr[of - - t' \otimes s' \otimes snd y'] rel-def r-minus a-minus-def
  by (smt abelian-group.minus-to-eq f10 f11 f4 f5 is-abelian-group m-assoc
monoid.m-closed
      monoid-axioms r-neg r-null subset subset-iff)
have f13: $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \in \text{carrier } R$ 
  using assms f1 f2 subset rev-subsetD
by (metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def

      mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)
rel-def)
have f14: $(s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \in \text{carrier } R$ 
  using assms f1 f2 subset rev-subsetD
by (metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def

      mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)
rel-def)
then have  $(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x')) =$ 
 $(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r)) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x'))$ 
  using f13 f14 f8 subset rev-subsetD r-distr rel-def r-minus a-minus-def
  by (smt add.inv-closed semiring-simprules(3))
have f15: $s \otimes s' \in \text{carrier } R$ 
  using assms rel-def subset rev-subsetD
  by auto
have f16: $\text{snd } y' \otimes \text{fst } x' \in \text{carrier } R$ 
  using f1 f2 rel-def subset rev-subsetD[of - S] monoid.m-closed[of R snd y' fst
x']
  by (metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def

```



```

      mem-Sigma-iff monoid-axioms partial-object.select-convs(1))
have f17:t ∈ carrier R
  using f4 subset rev-subsetD
  by auto
have f18:t' ∈ carrier R
  using f6 subset rev-subsetD
  by auto
have f19:s ∈ carrier R
  using assms(1) rel-def subset
  by auto
have f20:s' ∈ carrier R
  using assms(2) rel-def subset
  by auto
have f21:snd y' ∈ carrier R
  using f2 rel-def subset rev-subsetD
by (metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def

      mem-Sigma-iff partial-object.select-convs(1))
have f22:fst x' ∈ carrier R
  using f1 rel-def
  by (metis (no-types, lifting) Product-Type.Collect-case-prodD eq-class-of-rng-of-frac-def
mem-Sigma-iff
      partial-object.select-convs(1))
  then have f23:(t ⊗ t') ⊗ ((s ⊗ s') ⊗ (snd y' ⊗ fst x')) = t' ⊗ s' ⊗ snd y' ⊗
t ⊗ (s ⊗ fst x')
    using f17 f18 f19 f20 f21 m-assoc m-comm
  by (smt BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def f1 f4 f6 mem-Sigma-iff

      partial-object.select-convs(1) rel-def semiring-simprules(3) subset-iff)
  have f24:(t ⊗ t') ⊗ ((snd x' ⊗ snd y') ⊗ (s' ⊗ r)) = t' ⊗ s' ⊗ snd y' ⊗ t ⊗
(snd x' ⊗ r)
    using f17 f18 f20 f21 m-assoc m-comm
  by (smt BNF-Def.Collect-case-prodD assms(1) eq-class-of-rng-of-frac-def f1
f2 f4 f6
      mem-Sigma-iff partial-object.select-convs(1) rel-def semiring-simprules(3)
subset subset-iff)
  then have (t ⊗ t') ⊗ ((snd x' ⊗ snd y') ⊗ (s' ⊗ r)) ⊖ (t ⊗ t') ⊗ ((s ⊗ s') ⊗
(snd y' ⊗ fst x'))=
    (t' ⊗ s' ⊗ snd y' ⊗ t ⊗ (snd x' ⊗ r)) ⊖ (t' ⊗ s' ⊗ snd y' ⊗ t ⊗ (s ⊗ fst x'))
    using f23 f24
  by simp
  then have f25:(t' ⊗ s' ⊗ snd y') ⊗ (t ⊗ (snd x' ⊗ r ⊖ s ⊗ fst x')) =
    (t ⊗ t') ⊗ ((snd x' ⊗ snd y') ⊗ (s' ⊗ r)) ⊖ (t ⊗ t') ⊗ ((s ⊗ s') ⊗ (snd y' ⊗
fst x'))
    using f12
  by simp
  have f26:(t ⊗ t') ⊗ ((snd x' ⊗ snd y') ⊗ (s ⊗ r')) ⊖ (t ⊗ t') ⊗ ((s ⊗ s') ⊗
(snd x' ⊗ fst y')) =

```

$t \otimes s \otimes \text{snd } x' \otimes t' \otimes (\text{snd } y' \otimes r') \ominus (t \otimes s \otimes \text{snd } x' \otimes t' \otimes (s' \otimes \text{fst } y'))$
by (*smt BNF-Def.Collect-case-prodD assms(2) eq-class-of-rng-of-frac-def f1 f17 f18 f19 f2*)
m-assoc m-comm mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1) rel-def subset subset-iff
have *f27*: $\text{snd } y' \otimes r' \in \text{carrier } R$
using *assms(2) f21 rel-def*
by *auto*
have *f28*: $s' \otimes \text{fst } y' \in \text{carrier } R$
using *f20 assms(2)*
by (*metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def f2*)
mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1) rel-def
then have $t' \otimes (\text{snd } y' \otimes r' \ominus s' \otimes \text{fst } y') = t' \otimes (\text{snd } y' \otimes r') \ominus t' \otimes (s' \otimes \text{fst } y')$
using *f18 f27 f28 r-minus[of t' s' \otimes fst y']*
by (*simp add: a-minus-def r-distr*)
then have *f29*: $(t \otimes s \otimes \text{snd } x') \otimes (t' \otimes (\text{snd } y' \otimes r' \ominus s' \otimes \text{fst } y')) = (t \otimes s \otimes \text{snd } x') \otimes (t' \otimes (\text{snd } y' \otimes r') \ominus t' \otimes (s' \otimes \text{fst } y'))$
by *simp*
have $t \otimes s \otimes \text{snd } x' \in \text{carrier } R$
using *f17 f19 f1 subset assms(1) eq-class-of-rng-of-frac-def f4 rel-def*
by *fastforce*
then have *f30*: $(t \otimes s \otimes \text{snd } x') \otimes (t' \otimes (\text{snd } y' \otimes r' \ominus s' \otimes \text{fst } y')) = (t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r')) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y'))$
using *f26 f29 r-distr*
by (*smt <t' \otimes (snd y' \otimes r' \ominus s' \otimes fst y') = t' \otimes (snd y' \otimes r') \ominus t' \otimes (s' \otimes fst y')>*)
a-minus-def abelian-group.minus-to-eq f18 f27 f28 f7 is-abelian-group m-assoc monoid.m-closed
monoid-axioms r-neg semiring-simprules(15))
then have *f31*: $((t' \otimes s' \otimes \text{snd } y') \otimes (t \otimes (\text{snd } x' \otimes r \ominus s \otimes \text{fst } x'))) \oplus ((t \otimes s \otimes \text{snd } x') \otimes (t' \otimes (\text{snd } y' \otimes r' \ominus s' \otimes \text{fst } y')))$
 $= ((t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r))) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x')) \oplus ((t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r')) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')))$
using *f25 f30*
by *simp*
have *f32*: $(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r)) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x'))$
 $= (t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r)) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x')$
using *f17 f18 r-distr*
by (*simp add: <t \otimes t' \otimes (snd x' \otimes snd y' \otimes (s' \otimes r)) \ominus s \otimes s' \otimes (snd y' \otimes fst x') = t \otimes t' \otimes (snd x' \otimes snd y' \otimes (s' \otimes r)) \ominus t \otimes t' \otimes (s \otimes s' \otimes (snd y' \otimes fst x'))>*)
have *f33*: $(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r')) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x'))$

$(\text{snd } x' \otimes \text{fst } y') =$
 $(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y'))$
using $r\text{-distr}[of - - t \otimes t']$ $f17$ $f18$ $a\text{-minus-def}$ $r\text{-minus}$
by $(\text{smt BNF-Def.Collect-case-prodD abelian-group.a-inv-closed assms}(1)$
 $\text{assms}(2)$
 $\text{eq-class-of-rng-of-frac-def } f1$ $f2$ $\text{is-abelian-group mem-Sigma-iff partial-object.select-convs}(1)$
 $\text{rel-def semiring-simprules}(3)$ $\text{subset subset-iff})$
have $f34:(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r') = (\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes$
 $r) \oplus (\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r')$
using $r\text{-distr}$
by $(\text{metis (no-types, lifting) BNF-Def.Collect-case-prodD assms}(1) \text{ assms}(2)$
 $\text{eq-class-of-rng-of-frac-def}$
 $f1$ $f2$ $\text{mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs}(1)$
 rel-def
 $\text{subset subset-iff})$
then have $(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r')) =$
 $(t \otimes t') \otimes (\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \oplus (t \otimes t') \otimes (\text{snd } x' \otimes \text{snd } y') \otimes (s$
 $\otimes r')$
by $(\text{smt BNF-Def.Collect-case-prodD assms}(1) \text{ assms}(2) \text{ eq-class-of-rng-of-frac-def}$
 $f1$ $f17$ $f18$
 $f2$ $m\text{-assoc mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs}(1)$
 $r\text{-distr rel-def subset subset-iff})$
have $f35:(s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x' \oplus \text{snd } x' \otimes \text{fst } y') = (s \otimes s') \otimes (\text{snd } y' \otimes$
 $\text{fst } x') \oplus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')$
using $r\text{-distr } f19$ $f20$
by $(\text{metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def}$
 $f1$ $f2$
 $\text{mem-Sigma-iff partial-object.select-convs}(1) \text{ rel-def semiring-simprules}(3)$
 $\text{subset subset-iff})$
then have $f36:(t \otimes t') \otimes (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x' \oplus \text{snd } x' \otimes \text{fst } y') =$
 $(t \otimes t') \otimes (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus (t \otimes t') \otimes (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst}$
 $y')$
by $(\text{smt BNF-Def.Collect-case-prodD assms}(1) \text{ assms}(2) \text{ eq-class-of-rng-of-frac-def}$
 $f1$ $f17$ $f18$ $f2$
 $\text{mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs}(1)$
 $r\text{-distr rel-def}$
 $\text{subset subset-iff})$
have $f37:(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst}$
 $x')) \in \text{carrier } R$
by $(\text{simp add: } f13$ $f14$ $f17$ $f18)$
have $f38:(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst}$
 $y')) \in \text{carrier } R$
using $\langle t \otimes s \otimes \text{snd } x' \in \text{carrier } R \rangle$ $f30$ $f33$ $f7$ zero-closed
by auto
have $f39:(t \otimes t') \otimes ((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r)) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes$
 $(\text{snd } y' \otimes \text{fst } x')) \in \text{carrier } R$
by $(\text{simp add: } f32$ $f37)$
have $\text{snd } x' \otimes \text{snd } y' \in \text{carrier } R$

using *f1 f2 subset rev-subsetD*
by (*metis (no-types, lifting) BNF-Def.Collect-case-prodD eq-class-of-rng-of-frac-def*)

mem-Sigma-iff partial-object.select-convs(1) rel-def semiring-simprules(3)
have $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (snd\ y' \otimes fst\ x'))$
 \oplus

$(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')) =$
 $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r)) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (snd\ y' \otimes$
fst x')) \oplus
 $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s \otimes r')) \ominus (t \otimes t') \otimes ((s \otimes s') \otimes (snd\ x' \otimes$
fst y'))

using *f32 f33 ⟨snd x' ⊗ snd y' ∈ carrier R⟩ ⟨t ⊗ s ⊗ snd x' ∈ carrier R⟩*
assms(2) f17 f18 f19
f25 f30 f5 f7 f9 l-zero r-null rel-def zero-closed
apply *clarsimp*
using *l-zero semiring-simprules(3) by presburger*
then have *f40:((t' ⊗ s' ⊗ snd y') ⊗ (t ⊗ (snd x' ⊗ r ⊕ s ⊗ fst x'))) ⊕*
 $((t \otimes s \otimes snd\ x') \otimes (t' \otimes (snd\ y' \otimes r' \ominus s' \otimes fst\ y'))) =$
 $((t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (snd\ y' \otimes fst\ x'))) \oplus$
 $((t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')))$
using *f31*
by (*simp add: f32 f33*)
have *f41:(snd x' ⊗ snd y') ⊗ (s' ⊗ r) ⊕ (s ⊗ s') ⊗ (snd y' ⊗ fst x') ∈ carrier*
R
by (*simp add: f13 f14*)
have *f42:(snd x' ⊗ snd y') ⊗ (s ⊗ r') ⊕ (s ⊗ s') ⊗ (snd x' ⊗ fst y') ∈ carrier*
R
by (*smt BNF-Def.Collect-case-prodD abelian-group.minus-closed assms(1)*)
assms(2)
eq-class-of-rng-of-frac-def f1 f2 is-abelian-group mem-Sigma-iff partial-object.select-convs(1)

rel-def semiring-simprules(3) subset subset-iff)
then have $(t' \otimes s' \otimes snd\ y') \otimes (t \otimes (snd\ x' \otimes r \oplus s \otimes fst\ x')) \oplus$
 $(t \otimes s \otimes snd\ x') \otimes (t' \otimes (snd\ y' \otimes r' \ominus s' \otimes fst\ y')) =$
 $(t \otimes t') \otimes (((snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (snd\ y' \otimes fst\ x')) \oplus$
 $((snd\ x' \otimes snd\ y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')))$
using *r-distr[of (snd x' ⊗ snd y') ⊗ (s' ⊗ r) ⊕ (s ⊗ s') ⊗ (snd y' ⊗ fst x')*
 $(snd\ x' \otimes snd\ y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')\ t \otimes t']$
f17 f18 f40 f41 f42
by *simp*
have $(snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (snd\ y' \otimes fst\ x') \oplus (snd\ x' \otimes$
 $snd\ y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (snd\ x' \otimes fst\ y') =$
 $(snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \oplus (snd\ x' \otimes snd\ y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes$
 $(snd\ y' \otimes fst\ x') \ominus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')$
using *four-elem-comm[of (snd x' ⊗ snd y') ⊗ (s' ⊗ r) (snd x' ⊗ snd y') ⊗*
 $(s \otimes r') (s \otimes s') \otimes (snd\ y' \otimes fst\ x') (s \otimes s') \otimes (snd\ x' \otimes fst\ y')]$
by (*smt BNF-Def.Collect-case-prodD assms eq-class-of-rng-of-frac-def f1 f2*)
mem-Sigma-iff partial-object.select-convs(1) rel-def semiring-simprules(3)
subset subset-iff)

then have $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus (\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y') =$
 $((\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \oplus (\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r')) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')$
by blast
then have $f43:(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus (\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y') =$
 $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')$
using f34
by simp
have $(\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r') \in \text{carrier } R$
using $\langle \text{snd } x' \otimes \text{snd } y' \in \text{carrier } R \rangle \text{ assms}(2) f19 \text{ rel-def}$
by auto
have $(s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y') \in \text{carrier } R$
by $(\text{metis } (\text{no-types, lifting}) \text{BNF-Def.Collect-case-prodD assms eq-class-of-rng-of-frac-def f1 f2 mem-Sigma-iff partial-object.select-convs}(1) \text{ rel-def}$
 $\text{semiring-simprules}(3) \text{ subset subset-iff})$
then have $f43\text{bis}:(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r) \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus ((\text{snd } x' \otimes \text{snd } y') \otimes (s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')) =$
 $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')$
using a-assoc a-minus-def f41 f43
by $(\text{smt } \langle \text{snd } x' \otimes \text{snd } y' \otimes (s \otimes r') \in \text{carrier } R \rangle \text{ add.l-inv-ex add.m-closed minus-equality})$
have $f44:s \otimes s' \otimes (\text{snd } y' \otimes \text{fst } x') \in \text{carrier } R$
by (simp add: f14)
have $f45:s \otimes s' \otimes (\text{snd } x' \otimes \text{fst } y') \in \text{carrier } R$
by $(\text{metis } (\text{no-types, lifting}) \text{BNF-Def.Collect-case-prodD assms eq-class-of-rng-of-frac-def f1 f2 mem-Sigma-iff partial-object.select-convs}(1) \text{ rel-def}$
 $\text{semiring-simprules}(3) \text{ subset subset-iff})$
then have $\ominus ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')) =$
 $\ominus ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x')) \ominus ((s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y'))$
using f44 f45 inv-add
by auto
then have $\ominus ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')) =$
 $\ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')$
using l-minus[of s \otimes s']
by $(\text{simp add: a-minus-def f15 f16 f45})$
then have $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y') =$
 $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r') \ominus ((s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \oplus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y'))$
using right-inv-add $\langle \text{snd } x' \otimes \text{snd } y' \in \text{carrier } R \rangle \text{ assms}(2) f13 f19 f34 f44 f45 \text{ rel-def}$
by auto
then have $(\text{snd } x' \otimes \text{snd } y') \otimes (s' \otimes r \oplus s \otimes r') \ominus (s \otimes s') \otimes (\text{snd } y' \otimes \text{fst } x') \ominus (s \otimes s') \otimes (\text{snd } x' \otimes \text{fst } y')$

$x' \oplus (s \otimes s') \otimes (snd\ x' \otimes fst\ y') =$
 $(snd\ x' \otimes snd\ y') \otimes (s' \otimes r \oplus s \otimes r') \oplus ((s \otimes s') \otimes (snd\ y' \otimes fst\ x' \oplus snd$
 $x' \otimes fst\ y'))$
using *r-distr*
by (*simp add: f35*)
then have $((snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \oplus (s \otimes s') \otimes (snd\ y' \otimes fst\ x')) \oplus$
 $((snd\ x' \otimes snd\ y') \otimes (s \otimes r') \oplus (s \otimes s') \otimes (snd\ x' \otimes fst\ y'))$
 $= (snd\ x' \otimes snd\ y') \otimes (s' \otimes r \oplus s \otimes r') \oplus ((s \otimes s') \otimes (snd\ y' \otimes fst\ x' \oplus snd$
 $x' \otimes fst\ y'))$
using *f43bis*
by *simp*
then have $(t \otimes t') \otimes (((snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \oplus (s \otimes s') \otimes (snd\ y' \otimes$
 $fst\ x')) \oplus ((snd\ x' \otimes snd\ y') \otimes (s \otimes r') \oplus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')))$
 $= (t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r \oplus s \otimes r') \oplus ((s \otimes s') \otimes (snd\ y' \otimes$
 $fst\ x' \oplus snd\ x' \otimes fst\ y')))$
by *simp*
then have $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r) \oplus (s \otimes s') \otimes (snd\ y' \otimes fst$
 $x')) \oplus$
 $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s \otimes r') \oplus (s \otimes s') \otimes (snd\ x' \otimes fst\ y')) =$
 $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r \oplus s \otimes r') \oplus ((s \otimes s') \otimes (snd\ y' \otimes$
 $fst\ x' \oplus snd\ x' \otimes fst\ y')))$
using *r-distr[of - - t \otimes t'] f17 f18 <t' \otimes s' \otimes snd\ y' \otimes (t \otimes (snd\ x' \otimes r \oplus s
 $\otimes fst\ x')) \oplus t \otimes s \otimes snd\ x' \otimes (t' \otimes (snd\ y' \otimes r' \oplus s' \otimes fst\ y')) = t \otimes t' \otimes (snd$
 $x' \otimes snd\ y' \otimes (s' \otimes r) \oplus s \otimes s' \otimes (snd\ y' \otimes fst\ x') \oplus (snd\ x' \otimes snd\ y' \otimes (s \otimes r')$
 $\oplus s \otimes s' \otimes (snd\ x' \otimes fst\ y'))\rangle f40$
by *auto*
then have $(t' \otimes s' \otimes snd\ y') \otimes (t \otimes (snd\ x' \otimes r \oplus s \otimes fst\ x')) \oplus$
 $(t \otimes s \otimes snd\ x') \otimes (t' \otimes (snd\ y' \otimes r' \oplus s' \otimes fst\ y')) =$
 $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r \oplus s \otimes r') \oplus (s \otimes s') \otimes (snd\ y' \otimes fst$
 $x' \oplus snd\ x' \otimes fst\ y'))$
using *f40*
by *simp*
then have $(t \otimes t') \otimes ((snd\ x' \otimes snd\ y') \otimes (s' \otimes r \oplus s \otimes r') \oplus (s \otimes s') \otimes$
 $(snd\ y' \otimes fst\ x' \oplus snd\ x' \otimes fst\ y')) = 0$
using *f5 f7*
by (*simp add: <t \otimes s \otimes snd\ x' \in carrier R> f9*)
thus *?thesis*
using *rel-def f8*
by *auto*
qed
then have $(s' \otimes r \oplus s \otimes r' \mid_{rel\ s \otimes s'}) = (snd\ y' \otimes fst\ x' \oplus snd\ x' \otimes fst\ y' \mid_{rel$
 $snd\ x' \otimes snd\ y')$
proof–
have $(s' \otimes r \oplus s \otimes r', s \otimes s') \in carrier\ rel$
using *assms rel-def submonoid.m-closed*
by (*smt add.m-closed m-closed mem-Sigma-iff monoid.m-closed monoid-axioms*
partial-object.select-conv(1)
rev-subsetD subset)
have $(snd\ y' \otimes fst\ x' \oplus snd\ x' \otimes fst\ y', snd\ x' \otimes snd\ y') \in carrier\ rel$*

```

using rel-def f1 f2 subset submonoid.m-closed eq-class-of-rng-of-frac-def
by (smt Product-Type.Collect-case-prodD add.m-closed mem-Sigma-iff mem-
ber-class-to-carrier
    partial-object.select-convs(1) semiring-simprules(3) rev-subsetD)
thus ?thesis
using elem-eq-class[of rel] equiv-obj-rng-of-frac
by (metis ⟨(s' ⊗ r ⊕ s ⊗ r', s ⊗ s') .=_rel (snd y' ⊗ fst x' ⊕ snd x' ⊗ fst y',
snd x' ⊗ snd y')⟩
    ⟨(s' ⊗ r ⊕ s ⊗ r', s ⊗ s') ∈ carrier rel⟩ class-of-to-rel)
qed
thus ?thesis
using f3
by simp
qed

```

lemma *closed-add-rng-of-frac*:

```

assumes (r, s) ∈ carrier rel and (r', s') ∈ carrier rel
shows (r |rel s) ⊕rec-rng-of-frac (r' |rel s') ∈ set-class-ofrel
proof –
have f1:(r |rel s) ⊕rec-rng-of-frac (r' |rel s') = (s' ⊗ r ⊕ s ⊗ r' |rel s ⊗ s')
using assms add-rng-of-frac-fundamental-lemma
by simp
have f2:s' ⊗ r ⊕ s ⊗ r' ∈ carrier R
using assms rel-def
by (metis (no-types, lifting) add.m-closed mem-Sigma-iff monoid.m-closed
monoid-axioms
    partial-object.select-convs(1) rev-subsetD subset)
have f3:s ⊗ s' ∈ S
using assms rel-def submonoid.m-closed
by simp
from f2 and f3 have (s' ⊗ r ⊕ s ⊗ r', s ⊗ s') ∈ carrier rel
by (simp add: rel-def)
thus ?thesis
using set-eq-class-of-rng-of-frac-def f1
by auto
qed

```

lemma *closed-rel-add*:

```

assumes (r, s) ∈ carrier rel and (r', s') ∈ carrier rel
shows (s' ⊗ r ⊕ s ⊗ r', s ⊗ s') ∈ carrier rel
proof –
have s ⊗ s' ∈ S
using assms rel-def submonoid.m-closed
by simp
have s' ⊗ r ⊕ s ⊗ r' ∈ carrier R
using assms rel-def
by (metis (no-types, lifting) add.m-closed mem-Sigma-iff monoid.m-closed
monoid-axioms
    partial-object.select-convs(1) rev-subsetD subset)

```

thus *?thesis*
using *rel-def*
by (*simp add: ‹s ⊗ s' ∈ S›*)
qed

lemma *assoc-add-rng-of-frac:*

assumes $(r, s) \in \text{carrier rel}$ **and** $(r', s') \in \text{carrier rel}$ **and** $(r'', s'') \in \text{carrier rel}$
shows $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') \oplus_{\text{rec-rng-of-frac}} (r'' \mid_{\text{rel}} s'') =$
 $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} ((r' \mid_{\text{rel}} s') \oplus_{\text{rec-rng-of-frac}} (r'' \mid_{\text{rel}} s''))$

proof –

have $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') = (s' \otimes r \oplus s \otimes r' \mid_{\text{rel}} s \otimes s')$
using *assms(1) assms(2) add-rng-of-frac-fundamental-lemma*
by *simp*
then have $f1:(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') \oplus_{\text{rec-rng-of-frac}} (r'' \mid_{\text{rel}} s'') =$
 $(s'' \otimes (s' \otimes r \oplus s \otimes r') \oplus (s \otimes s') \otimes r'' \mid_{\text{rel}} (s \otimes s') \otimes s'')$
using *assms add-rng-of-frac-fundamental-lemma closed-rel-add*
by *simp*
have $(r' \mid_{\text{rel}} s') \oplus_{\text{rec-rng-of-frac}} (r'' \mid_{\text{rel}} s'') = (s'' \otimes r' \oplus s' \otimes r'' \mid_{\text{rel}} s' \otimes s'')$
using *assms(2) assms(3) add-rng-of-frac-fundamental-lemma*
by *simp*
then have $f2:(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} ((r' \mid_{\text{rel}} s') \oplus_{\text{rec-rng-of-frac}} (r'' \mid_{\text{rel}} s''))$
 $=$
 $((s' \otimes s'') \otimes r \oplus s \otimes (s'' \otimes r' \oplus s' \otimes r'') \mid_{\text{rel}} s \otimes (s' \otimes s''))$
using *assms add-rng-of-frac-fundamental-lemma closed-rel-add*
by *simp*
have $f3:(s \otimes s') \otimes s'' = s \otimes (s' \otimes s'')$
using *m-assoc subset assms rel-def*
by (*metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs(1) rev-subsetD*)
have $s'' \otimes (s' \otimes r \oplus s \otimes r') \oplus (s \otimes s') \otimes r'' = (s' \otimes s'') \otimes r \oplus s \otimes (s'' \otimes r'$
 $\oplus s' \otimes r'')$
by (*smt a-assoc assms m-comm mem-Sigma-iff monoid.m-assoc monoid.m-closed monoid-axioms*
partial-object.select-convs(1) r-distr rel-def subset subset-iff)
thus *?thesis*
using *f1 f2 f3*
by *simp*
qed

lemma *add-rng-of-frac-zero:*

shows $(\mathbf{0} \mid_{\text{rel}} \mathbf{1}) \in \text{set-class-of rel}$
by (*metis (no-types, lifting) closed-mult-rng-of-frac mem-Sigma-iff monoid.simps(2) one-closed*
partial-object.select-convs(1) rec-monoid-rng-of-frac-def rel-def right-unit-mult-rng-of-frac semiring-simprules(4) zero-closed)

lemma *l-unit-add-rng-of-frac:*

assumes $(r, s) \in \text{carrier rel}$
shows $\mathbf{0}_{\text{rec-rng-of-frac}} \oplus_{\text{rec-rng-of-frac}} (r \mid_{\text{rel}} s) = (r \mid_{\text{rel}} s)$
proof –

have $(\mathbf{0} \mid_{rel} \mathbf{1}) \oplus_{rec-rng-of-frac} (r \mid_{rel} s) = (s \otimes \mathbf{0} \oplus \mathbf{1} \otimes r \mid_{rel} \mathbf{1} \otimes s)$
using *assms add-rng-of-frac-fundamental-lemma*
by *(simp add: rel-def)*
then have $(\mathbf{0} \mid_{rel} \mathbf{1}) \oplus_{rec-rng-of-frac} (r \mid_{rel} s) = (r \mid_{rel} s)$
using *assms rel-def subset*
by *auto*
thus *?thesis*
using *rec-rng-of-frac-def*
by *simp*
qed

lemma *r-unit-add-rng-of-frac:*
assumes $(r, s) \in carrier\ rel$
shows $(r \mid_{rel} s) \oplus_{rec-rng-of-frac} \mathbf{0}_{rec-rng-of-frac} = (r \mid_{rel} s)$
proof –
have $(r \mid_{rel} s) \oplus_{rec-rng-of-frac} (\mathbf{0} \mid_{rel} \mathbf{1}) = (\mathbf{1} \otimes r \oplus s \otimes \mathbf{0} \mid_{rel} s \otimes \mathbf{1})$
using *assms add-rng-of-frac-fundamental-lemma*
by *(simp add: rel-def)*
then have $(r \mid_{rel} s) \oplus_{rec-rng-of-frac} (\mathbf{0} \mid_{rel} \mathbf{1}) = (r \mid_{rel} s)$
using *assms rel-def subset*
by *auto*
thus *?thesis*
using *rec-rng-of-frac-def*
by *simp*
qed

lemma *comm-add-rng-of-frac:*
assumes $(r, s) \in carrier\ rel$ **and** $(r', s') \in carrier\ rel$
shows $(r \mid_{rel} s) \oplus_{rec-rng-of-frac} (r' \mid_{rel} s') = (r' \mid_{rel} s') \oplus_{rec-rng-of-frac} (r \mid_{rel} s)$
proof –
have $f1: (r \mid_{rel} s) \oplus_{rec-rng-of-frac} (r' \mid_{rel} s') = (s' \otimes r \oplus s \otimes r' \mid_{rel} s \otimes s')$
using *assms add-rng-of-frac-fundamental-lemma*
by *simp*
have $f2: (r' \mid_{rel} s') \oplus_{rec-rng-of-frac} (r \mid_{rel} s) = (s \otimes r' \oplus s' \otimes r \mid_{rel} s' \otimes s)$
using *assms add-rng-of-frac-fundamental-lemma*
by *simp*
thus *?thesis*
using *f1 f2*
by *(metis (no-types, lifting) add.m-comm assms(1) assms(2) m-comm mem-Sigma-iff*
partial-object.select-convs(1) rel-def semiring-simprules(3) rev-subsetD sub-
set)
qed

lemma *class-of-zero-rng-of-frac:*
assumes $s \in S$
shows $(\mathbf{0} \mid_{rel} s) = \mathbf{0}_{rec-rng-of-frac}$
proof –
have $f1: (\mathbf{0}, s) \in carrier\ rel$

using *assms rel-def*
by *simp*
have $\mathbf{1} \otimes (\mathbf{1} \otimes \mathbf{0} \ominus s \otimes \mathbf{0}) = \mathbf{0}$
using *assms local.ring-axioms rev-subsetD ring.ring-simprules(14) subset*
by *fastforce*
then have $(\mathbf{0}, s) \text{.}=\text{rel} (\mathbf{0}, \mathbf{1})$
using *rel-def submonoid.one-closed*
by *auto*
thus *?thesis*
using *elem-eq-class equiv-obj-rng-of-frac f1 rec-rng-of-frac-def*
by *(metis (no-types, lifting) class-of-to-rel mem-Sigma-iff one-closed partial-object.select-convs(1)*

rel-def ring-record-simps(11))
qed

lemma *r-inv-add-rng-of-frac*:
assumes $(r, s) \in \text{carrier } \text{rel}$
shows $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (\ominus r \mid_{\text{rel}} s) = \mathbf{0}_{\text{rec-rng-of-frac}}$
proof –
have $(\ominus r, s) \in \text{carrier } \text{rel}$
using *assms rel-def*
by *simp*
then have $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (\ominus r \mid_{\text{rel}} s) = (s \otimes r \oplus s \otimes \ominus r \mid_{\text{rel}} s \otimes s)$
using *assms add-rng-of-frac-fundamental-lemma*
by *simp*
then have $(r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (\ominus r \mid_{\text{rel}} s) = (\mathbf{0} \mid_{\text{rel}} s \otimes s)$
using *r-minus[of s r] assms rel-def subset rev-subsetD r-neg*
by *auto*
thus *?thesis*
using *class-of-zero-rng-of-frac assms rel-def submonoid.m-closed*
by *simp*
qed

lemma *l-inv-add-rng-of-frac*:
assumes $(r, s) \in \text{carrier } \text{rel}$
shows $(\ominus r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r \mid_{\text{rel}} s) = \mathbf{0}_{\text{rec-rng-of-frac}}$
proof –
have $(\ominus r, s) \in \text{carrier } \text{rel}$
using *assms rel-def*
by *simp*
then have $(\ominus r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r \mid_{\text{rel}} s) = (s \otimes \ominus r \oplus s \otimes r \mid_{\text{rel}} s \otimes s)$
using *assms add-rng-of-frac-fundamental-lemma*
by *simp*
then have $(\ominus r \mid_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r \mid_{\text{rel}} s) = (\mathbf{0} \mid_{\text{rel}} s \otimes s)$
using *r-minus[of s r] assms rel-def subset rev-subsetD l-neg*
by *auto*
thus *?thesis*
using *class-of-zero-rng-of-frac assms rel-def submonoid.m-closed*
by *simp*

qed

lemma *abelian-group-rng-of-frac*:

shows *abelian-group (rec-rng-of-frac)*

proof

show $\bigwedge x y. \llbracket x \in \text{carrier (add-monoid rec-rng-of-frac)};$
 $y \in \text{carrier (add-monoid rec-rng-of-frac)} \rrbracket$

$\implies x \otimes_{\text{add-monoid rec-rng-of-frac}} y$
 $\in \text{carrier (add-monoid rec-rng-of-frac)}$

using *closed-add-rng-of-frac*

by (*smt mem-Collect-eq monoid.select-convs(1) partial-object.select-convs(1)*)

rec-rng-of-frac-def

set-eq-class-of-rng-of-frac-def)

show $\bigwedge x y z.$

$\llbracket x \in \text{carrier (add-monoid rec-rng-of-frac)};$
 $y \in \text{carrier (add-monoid rec-rng-of-frac)};$
 $z \in \text{carrier (add-monoid rec-rng-of-frac)} \rrbracket$

$\implies x \otimes_{\text{add-monoid rec-rng-of-frac}} y \otimes_{\text{add-monoid rec-rng-of-frac}} z =$
 $x \otimes_{\text{add-monoid rec-rng-of-frac}} (y \otimes_{\text{add-monoid rec-rng-of-frac}} z)$

using *assoc-add-rng-of-frac*

by (*smt mem-Collect-eq monoid.simps(1) partial-object.select-convs(1) rec-rng-of-frac-def*

set-eq-class-of-rng-of-frac-def)

show $\mathbf{1}_{\text{add-monoid rec-rng-of-frac}} \in \text{carrier (add-monoid rec-rng-of-frac)}$

using *add-rng-of-frac-zero* **by** (*simp add: rec-rng-of-frac-def*)

show $\bigwedge x. x \in \text{carrier (add-monoid rec-rng-of-frac)} \implies$

$\mathbf{1}_{\text{add-monoid rec-rng-of-frac}} \otimes_{\text{add-monoid rec-rng-of-frac}} x = x$

using *l-unit-add-rng-of-frac*

by (*smt mem-Collect-eq monoid.select-convs(1) monoid.select-convs(2) partial-object.select-convs(1)*

rec-rng-of-frac-def set-eq-class-of-rng-of-frac-def)

rec-rng-of-frac-def set-eq-class-of-rng-of-frac-def)

show $\bigwedge x. x \in \text{carrier (add-monoid rec-rng-of-frac)} \implies$

$x \otimes_{\text{add-monoid rec-rng-of-frac}} \mathbf{1}_{\text{add-monoid rec-rng-of-frac}} = x$

using *r-unit-add-rng-of-frac*

by (*smt mem-Collect-eq monoid.select-convs(1) monoid.select-convs(2) partial-object.select-convs(1)*

rec-rng-of-frac-def set-eq-class-of-rng-of-frac-def)

rec-rng-of-frac-def set-eq-class-of-rng-of-frac-def)

show $\bigwedge x y. \llbracket x \in \text{carrier (add-monoid rec-rng-of-frac)};$
 $y \in \text{carrier (add-monoid rec-rng-of-frac)} \rrbracket$

$\implies x \otimes_{\text{add-monoid rec-rng-of-frac}} y = y \otimes_{\text{add-monoid rec-rng-of-frac}} x$

using *comm-add-rng-of-frac*

by (*smt mem-Collect-eq monoid.select-convs(1) partial-object.select-convs(1)*)

rec-rng-of-frac-def

set-eq-class-of-rng-of-frac-def)

show $\text{carrier (add-monoid rec-rng-of-frac)} \subseteq \text{Units (add-monoid rec-rng-of-frac)}$

proof

show $x \in \text{Units (add-monoid rec-rng-of-frac)}$ **if** $x \in \text{carrier (add-monoid rec-rng-of-frac)}$ **for** x

proof –

have $x \in \text{set-class-of}_{rel}$
using *that rec-rng-of-frac-def by simp*
then obtain r **and** s **where** $f1:(r, s) \in \text{carrier } rel$ **and** $f2:x = (r \mid_{rel} s)$
using *set-eq-class-of-rng-of-frac-def*
by *(smt mem-Collect-eq)*
then have $f3:(r \mid_{rel} s) \oplus_{rec-rng-of-frac} (\ominus r \mid_{rel} s) = \mathbf{0}_{rec-rng-of-frac}$
using $f1$ *r-inv-add-rng-of-frac[of r s]*
by *simp*
have $f4:(\ominus r \mid_{rel} s) \oplus_{rec-rng-of-frac} (r \mid_{rel} s) = \mathbf{0}_{rec-rng-of-frac}$
using $f1$ *l-inv-add-rng-of-frac[of r s]*
by *simp*
then have $\exists y \in \text{set-class-of}_{rel}. y \oplus_{rec-rng-of-frac} x = \mathbf{0}_{rec-rng-of-frac} \wedge x$
 $\oplus_{rec-rng-of-frac} y = \mathbf{0}_{rec-rng-of-frac}$
using $f2$ $f3$ $f4$
by *(metis (no-types, lifting) abelian-group.a-inv-closed class-of-zero-rng-of-frac*

closed-add-rng-of-frac f1 is-abelian-group mem-Sigma-iff partial-object.select-convs(1)

rel-def r-unit-add-rng-of-frac zero-closed)
thus $x \in \text{Units}$ *(add-monoid rec-rng-of-frac)*
using *rec-rng-of-frac-def that by (simp add: Units-def)*
qed
qed
qed

lemma *r-distr-rng-of-frac:*
assumes $(r, s) \in \text{carrier } rel$ **and** $(r', s') \in \text{carrier } rel$ **and** $(r'', s'') \in \text{carrier } rel$
shows $((r \mid_{rel} s) \oplus_{rec-rng-of-frac} (r' \mid_{rel} s')) \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'') =$
 $(r \mid_{rel} s) \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'') \oplus_{rec-rng-of-frac} (r' \mid_{rel} s') \otimes_{rec-rng-of-frac}$
 $(r'' \mid_{rel} s'')$
proof –
have $(r \mid_{rel} s) \oplus_{rec-rng-of-frac} (r' \mid_{rel} s') = (s' \otimes r \oplus s \otimes r' \mid_{rel} s \otimes s')$
using *assms(1) assms(2) add-rng-of-frac-fundamental-lemma*
by *simp*
then have $f1:((r \mid_{rel} s) \oplus_{rec-rng-of-frac} (r' \mid_{rel} s')) \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'')$
 $=$
 $((s' \otimes r \oplus s \otimes r') \otimes r'' \mid_{rel} (s \otimes s') \otimes s'')$
using *assms mult-rng-of-frac-fundamental-lemma*
by *(simp add: closed-rel-add rec-monoid-rng-of-frac-def rec-rng-of-frac-def)*
have $f2:(r \mid_{rel} s) \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'') = (r \otimes r'' \mid_{rel} s \otimes s'')$
using *assms(1) assms(3) mult-rng-of-frac-fundamental-lemma*
by *(simp add: rec-monoid-rng-of-frac-def rec-rng-of-frac-def)*
have $f3:(r' \mid_{rel} s') \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'') = (r' \otimes r'' \mid_{rel} s' \otimes s'')$
using *assms(2) assms(3) mult-rng-of-frac-fundamental-lemma*
by *(simp add: rec-monoid-rng-of-frac-def rec-rng-of-frac-def)*
have $f4:(r \otimes r'', s \otimes s'') \in \text{carrier } rel$
using *rel-def assms(1) assms(3) submonoid.m-closed*
by *simp*
have $f5:(r' \otimes r'', s' \otimes s'') \in \text{carrier } rel$

using *rel-def* *assms(2)* *assms(3)* *submonoid.m-closed*
by *simp*
from *f2* **and** *f3* **have** *f6*: $(r \mid_{rel} s) \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'') \oplus_{rec-rng-of-frac} (r' \mid_{rel} s') \otimes_{rec-rng-of-frac} (r'' \mid_{rel} s'')$
 $= ((s' \otimes s'') \otimes (r \otimes r'') \oplus (s \otimes s') \otimes (r' \otimes r'')) \mid_{rel} (s \otimes s'') \otimes (s' \otimes s'')$
using *assms f4 f5 submonoid.m-closed add-rng-of-frac-fundamental-lemma*
by *simp*
have $(s \otimes s'' \otimes (s' \otimes s')) \otimes ((s' \otimes r \oplus s \otimes r') \otimes r'') = (s \otimes s'' \otimes (s' \otimes s'))$
 $\otimes (s' \otimes r \otimes r'' \oplus s \otimes r' \otimes r'')$
using *assms rel-def subset rev-subsetD l-distr*
by (*smt mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)*)
then have *f7*: $(s \otimes s'' \otimes (s' \otimes s')) \otimes ((s' \otimes r \oplus s \otimes r') \otimes r'') =$
 $(s \otimes s'' \otimes (s' \otimes s')) \otimes (s' \otimes r \otimes r'') \oplus (s \otimes s'' \otimes (s' \otimes s')) \otimes (s \otimes r' \otimes r'')$
using *assms rel-def subset rev-subsetD submonoid.m-closed r-distr*
by (*smt mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)*)
have *f8*: $(s \otimes s' \otimes s'') \otimes (s' \otimes s'' \otimes (r \otimes r'')) \oplus s \otimes s'' \otimes (r' \otimes r'') =$
 $(s \otimes s' \otimes s'') \otimes (s' \otimes s'' \otimes (r \otimes r'')) \oplus (s \otimes s' \otimes s'') \otimes (s \otimes s'' \otimes (r' \otimes r''))$
using *assms rel-def subset rev-subsetD submonoid.m-closed r-distr*
by (*smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3)*)
have $(s \otimes s'' \otimes (s' \otimes s')) = (s \otimes (s'' \otimes s') \otimes s')$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-assoc*
by (*smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3)*)
then have *f9*: $(s \otimes s'' \otimes (s' \otimes s')) = (s \otimes s' \otimes (s'' \otimes s'))$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-comm m-assoc*
by (*smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3)*)
then have *f10*: $(s \otimes s'' \otimes (s' \otimes s')) \otimes (s' \otimes r \otimes r'') = (s \otimes s' \otimes s'') \otimes (s' \otimes$
 $s'' \otimes (r \otimes r''))$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-assoc m-comm*
by (*smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3)*)
have $(s \otimes s'' \otimes (r' \otimes r'')) = (s'' \otimes s \otimes (r' \otimes r''))$
using *assms rel-def subset rev-subsetD m-comm*
by (*metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs(1)*)
then have $(s \otimes s'' \otimes (s' \otimes s')) \otimes (s \otimes r' \otimes r'') = (s \otimes s' \otimes s'') \otimes (s \otimes s'' \otimes$
 $(r' \otimes r''))$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-comm m-assoc f9*
by (*smt mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1)*)
then have $((s \otimes s'' \otimes (s' \otimes s')) \otimes ((s' \otimes r \oplus s \otimes r') \otimes r'')) = (s \otimes s' \otimes s'')$
 $\otimes (s' \otimes s'' \otimes (r \otimes r'')) \oplus s \otimes s'' \otimes (r' \otimes r''))$
using *f7 f8 f10*
by *presburger*
then have $((s \otimes s'' \otimes (s' \otimes s')) \otimes ((s' \otimes r \oplus s \otimes r') \otimes r'')) \ominus (s \otimes s' \otimes s'')$
 $\otimes (s' \otimes s'' \otimes (r \otimes r'')) \oplus s \otimes s'' \otimes (r' \otimes r'')) = \mathbf{0}$
by (*smt a-minus-def assms(1) assms(2) assms(3) closed-rel-add mem-Sigma-iff*
partial-object.select-convs(1) r-neg rel-def semiring-simprules(3) rev-subsetD
subset)
then have *f11*: $\mathbf{1} \otimes (((s \otimes s'' \otimes (s' \otimes s')) \otimes ((s' \otimes r \oplus s \otimes r') \otimes r'')) \ominus (s \otimes$
 $s' \otimes s'') \otimes (s' \otimes s'' \otimes (r \otimes r'')) \oplus s \otimes s'' \otimes (r' \otimes r'')))) = \mathbf{0}$
by *simp*

have $f12:((s' \otimes r \oplus s \otimes r') \otimes r'', s \otimes s' \otimes s'') \in \text{carrier rel}$
using *assms closed-rel-add rel-def*
by *auto*
have $f13:(s' \otimes s'' \otimes (r \otimes r'') \oplus s \otimes s'' \otimes (r' \otimes r''), s \otimes s'' \otimes (s' \otimes s'')) \in$
carrier rel
by (*simp add: closed-rel-add f4 f5*)
have $1 \in S$
using *submonoid.one-closed*
by *simp*
then have $((s' \otimes r \oplus s \otimes r') \otimes r'', s \otimes s' \otimes s'') \dot{=}_{\text{rel}} (s' \otimes s'' \otimes (r \otimes r'') \oplus$
 $s \otimes s'' \otimes (r' \otimes r''), s \otimes s'' \otimes (s' \otimes s''))$
using *rel-def f11 f13 f12*
by *auto*
then have $((s' \otimes r \oplus s \otimes r') \otimes r'' |_{\text{rel}} s \otimes s' \otimes s'') = (s' \otimes s'' \otimes (r \otimes r'') \oplus s$
 $\otimes s'' \otimes (r' \otimes r'') |_{\text{rel}} s \otimes s'' \otimes (s' \otimes s''))$
using *elem-eq-class*
by (*metis class-of-to-rel equiv-obj-rng-of-frac f12 f13*)
thus *?thesis*
using *f1 f6*
by *simp*
qed

lemma *l-distr-rng-of-frac:*

assumes $(r, s) \in \text{carrier rel}$ **and** $(r', s') \in \text{carrier rel}$ **and** $(r'', s'') \in \text{carrier rel}$
shows $(r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}} ((r |_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' |_{\text{rel}} s')) =$
 $(r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}} (r |_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}}$
 $(r' |_{\text{rel}} s')$

proof –

have $(r |_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' |_{\text{rel}} s') = (s' \otimes r \oplus s \otimes r' |_{\text{rel}} s \otimes s')$
using *assms(1) assms(2) add-rng-of-frac-fundamental-lemma*
by *simp*
then have $f1:(r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}} ((r |_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}} (r' |_{\text{rel}} s'))$
 $=$
 $(r'' \otimes (s' \otimes r \oplus s \otimes r') |_{\text{rel}} s'' \otimes (s \otimes s'))$
using *assms mult-rng-of-frac-fundamental-lemma*
by (*simp add: closed-rel-add rec-monoid-rng-of-frac-def rec-rng-of-frac-def*)
have $f2:(r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}} (r |_{\text{rel}} s) = (r'' \otimes r |_{\text{rel}} s'' \otimes s)$
using *assms(1) assms(3) mult-rng-of-frac-fundamental-lemma*
by (*simp add: rec-monoid-rng-of-frac-def rec-rng-of-frac-def*)
have $f3:(r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}} (r' |_{\text{rel}} s') = (r'' \otimes r' |_{\text{rel}} s'' \otimes s')$
using *assms(2) assms(3) mult-rng-of-frac-fundamental-lemma*
by (*simp add: rec-monoid-rng-of-frac-def rec-rng-of-frac-def*)
have $f4:(r'' \otimes r, s'' \otimes s) \in \text{carrier rel}$
using *rel-def assms(1) assms(3) submonoid.m-closed*
by *simp*
have $f5:(r'' \otimes r', s'' \otimes s') \in \text{carrier rel}$
using *rel-def assms(2) assms(3) submonoid.m-closed*
by *simp*
from *f2* **and** *f3* **have** $f6:(r'' |_{\text{rel}} s'') \otimes_{\text{rec-rng-of-frac}} (r |_{\text{rel}} s) \oplus_{\text{rec-rng-of-frac}}$

$(r'' \mid_{rel} s'') \otimes_{rec-rng-of-frac} (r' \mid_{rel} s')$
 $= ((s'' \otimes s') \otimes (r'' \otimes r) \oplus (s'' \otimes s) \otimes (r'' \otimes r')) \mid_{rel} (s'' \otimes s) \otimes (s'' \otimes s')$
using *assms f4 f5 submonoid.m-closed add-rng-of-frac-fundamental-lemma*
by *simp*
have $(s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s' \otimes r \oplus s \otimes r')) = (s'' \otimes s \otimes (s'' \otimes s'))$
 $\otimes (r'' \otimes (s' \otimes r) \oplus r'' \otimes (s \otimes r'))$
using *assms rel-def subset rev-subsetD r-distr*
by *(smt mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1))*
then have $f7:(s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s' \otimes r \oplus s \otimes r')) =$
 $(s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s' \otimes r)) \oplus (s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s \otimes$
 $r'))$
using *assms rel-def subset rev-subsetD submonoid.m-closed r-distr*
by *(smt mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1))*
have $f8:(s'' \otimes s \otimes s') \otimes (s'' \otimes s' \otimes (r'' \otimes r) \oplus s'' \otimes s \otimes (r'' \otimes r')) =$
 $(s'' \otimes s \otimes s') \otimes (s'' \otimes s' \otimes (r'' \otimes r)) \oplus (s'' \otimes s \otimes s') \otimes (s'' \otimes s \otimes (r'' \otimes r'))$
using *assms rel-def subset rev-subsetD submonoid.m-closed r-distr*
by *(smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3))*
have $(s'' \otimes s \otimes (s'' \otimes s')) = (s'' \otimes (s \otimes s')) \otimes s'$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-assoc*
by *(smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3))*
then have $f9:(s'' \otimes s \otimes (s'' \otimes s')) = (s'' \otimes s'' \otimes (s \otimes s'))$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-comm m-assoc*
by *(smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3))*
then have $f10:(s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes s' \otimes r) = (s'' \otimes s \otimes s') \otimes (s'' \otimes$
 $s' \otimes (r'' \otimes r))$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-assoc m-comm*
by *(smt mem-Sigma-iff partial-object.select-convs(1) semiring-simprules(3))*
have $(s'' \otimes s \otimes (r'' \otimes r')) = (s \otimes s'' \otimes (r'' \otimes r'))$
using *assms rel-def subset rev-subsetD m-comm*
by *(metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs(1))*
then have $(s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes s \otimes r') = (s'' \otimes s \otimes s') \otimes (s'' \otimes s \otimes$
 $(r'' \otimes r'))$
using *assms rel-def subset rev-subsetD submonoid.m-closed m-comm m-assoc f9*
by *(smt mem-Sigma-iff monoid.m-closed monoid-axioms partial-object.select-convs(1))*
then have $((s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s' \otimes r \oplus s \otimes r'))) = (s'' \otimes (s \otimes s'))$
 $\otimes (s'' \otimes s' \otimes (r'' \otimes r) \oplus s'' \otimes s \otimes (r'' \otimes r'))$
using *f7 f8 f10*
by *(smt assms(1) assms(2) assms(3) m-assoc mem-Sigma-iff partial-object.select-convs(1) rel-def*
rev-subsetD subset)
then have $((s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s' \otimes r \oplus s \otimes r'))) \ominus (s'' \otimes (s \otimes s'))$
 $\otimes (s'' \otimes s' \otimes (r'' \otimes r) \oplus s'' \otimes s \otimes (r'' \otimes r')) = \mathbf{0}$
by *(smt a-minus-def assms(1) assms(2) assms(3) closed-rel-add mem-Sigma-iff partial-object.select-convs(1)*
r-neg rel-def semiring-simprules(3) rev-subsetD subset)
then have $f11:\mathbf{1} \otimes (((s'' \otimes s \otimes (s'' \otimes s')) \otimes (r'' \otimes (s' \otimes r \oplus s \otimes r'))) \ominus (s'' \otimes$
 $(s \otimes s')) \otimes (s'' \otimes s' \otimes (r'' \otimes r) \oplus s'' \otimes s \otimes (r'' \otimes r')))) = \mathbf{0}$
by *simp*
have $f12:(r'' \otimes (s' \otimes r \oplus s \otimes r'), s'' \otimes (s \otimes s')) \in carrier\ rel$

using *assms closed-rel-add rel-def*
by *auto*
have $f13:(s'' \otimes s' \otimes (r'' \otimes r) \oplus s'' \otimes s \otimes (r'' \otimes r'), s'' \otimes s \otimes (s'' \otimes s')) \in$
carrier rel
by (*simp add: closed-rel-add f4 f5*)
have $1 \in S$
using *submonoid.one-closed*
by *simp*
then have $(r'' \otimes (s' \otimes r \oplus s \otimes r'), s'' \otimes (s \otimes s')) \dot{=}_{rel} (s'' \otimes s' \otimes (r'' \otimes r)$
 $\oplus s'' \otimes s \otimes (r'' \otimes r'), s'' \otimes s \otimes (s'' \otimes s'))$
using *rel-def f11 f13 f12*
by *auto*
then have $(r'' \otimes (s' \otimes r \oplus s \otimes r') \mid_{rel} s'' \otimes (s \otimes s')) = (s'' \otimes s' \otimes (r'' \otimes r)$
 $\oplus s'' \otimes s \otimes (r'' \otimes r') \mid_{rel} s'' \otimes s \otimes (s'' \otimes s'))$
using *elem-eq-class*
by (*metis class-of-to-rel equiv-obj-rng-of-frac f12 f13*)
thus *?thesis*
using *f1 f6*
by *simp*
qed

lemma *rng-rng-of-frac:*
shows *ring (rec-rng-of-frac)*
proof –
have $f1:\forall x y z. x \in \text{carrier } \text{rec-rng-of-frac} \longrightarrow y \in \text{carrier } \text{rec-rng-of-frac} \longrightarrow z$
 $\in \text{carrier } \text{rec-rng-of-frac}$
 $\longrightarrow (x \oplus_{\text{rec-rng-of-frac}} y) \otimes_{\text{rec-rng-of-frac}} z = x \otimes_{\text{rec-rng-of-frac}} z \oplus_{\text{rec-rng-of-frac}}$
 $y \otimes_{\text{rec-rng-of-frac}} z$
using *r-distr-rng-of-frac rec-rng-of-frac-def*
by (*smt mem-Collect-eq partial-object.select-convs(1) set-eq-class-of-rng-of-frac-def*)
have $f2:\forall x y z. x \in \text{carrier } \text{rec-rng-of-frac} \longrightarrow y \in \text{carrier } \text{rec-rng-of-frac} \longrightarrow z$
 $\in \text{carrier } \text{rec-rng-of-frac}$
 $\longrightarrow z \otimes_{\text{rec-rng-of-frac}} (x \oplus_{\text{rec-rng-of-frac}} y) = z \otimes_{\text{rec-rng-of-frac}} x \oplus_{\text{rec-rng-of-frac}}$
 $z \otimes_{\text{rec-rng-of-frac}} y$
using *l-distr-rng-of-frac rec-rng-of-frac-def*
by (*smt mem-Collect-eq partial-object.select-convs(1) set-eq-class-of-rng-of-frac-def*)
then have *ring-axioms (rec-rng-of-frac)*
using *ring-axioms-def f1 f2*
by *auto*
thus *?thesis*
using *ring-def[of rec-rng-of-frac] abelian-group-rng-of-frac monoid-rng-of-frac*
rec-rng-of-frac-def
abelian-group-axioms-def rec-monoid-rng-of-frac-def eq-class-of-rng-of-frac-def
by (*simp add: Group.monoid-def*)
qed

lemma *crng-rng-of-frac:*
shows *cring (rec-rng-of-frac)*
using *cring-def[of rec-rng-of-frac] rng-rng-of-frac comm-monoid-rng-of-frac rec-rng-of-frac-def*

rec-monoid-rng-of-frac-def eq-class-of-rng-of-frac-def
by (*metis (no-types, lifting) comm-monoid.m-comm monoid.monoid-comm-monoidI*
monoid.select-convs(1)
partial-object.select-convs(1) ring.is-monoid)

lemma *simp-in-frac*:

assumes $(r, s) \in \text{carrier } \text{rel}$ **and** $s' \in S$
shows $(r \mid_{\text{rel}} s) = (s' \otimes r \mid_{\text{rel}} s' \otimes s)$

proof –

have $f1: (s' \otimes r, s' \otimes s) \in \text{carrier } \text{rel}$
using *assms rel-def submonoid.m-closed subset rev-subsetD*
by *auto*
have $(s' \otimes s) \otimes r \ominus s \otimes (s' \otimes r) = (s' \otimes s) \otimes r \ominus (s \otimes s') \otimes r$
using *assms subset rev-subsetD m-assoc[of s s' r] rel-def*
by (*metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs(1)*)
then have $(s' \otimes s) \otimes r \ominus s \otimes (s' \otimes r) = (s' \otimes s) \otimes r \ominus (s' \otimes s) \otimes r$
using *m-comm[of s s'] assms subset rev-subsetD rel-def*
by (*metis (no-types, lifting) mem-Sigma-iff partial-object.select-convs(1)*)
then have $(s' \otimes s) \otimes r \ominus s \otimes (s' \otimes r) = \mathbf{0}$
by (*metis (no-types, lifting) a-minus-def assms mem-Sigma-iff partial-object.select-convs(1)*)

r-neg rel-def semiring-simprules(3) rev-subsetD subset
then have $\mathbf{1} \otimes ((s' \otimes s) \otimes r \ominus s \otimes (s' \otimes r)) = \mathbf{0}$
by *simp*
then have $(r, s) \text{.}=\text{rel} (s' \otimes r, s' \otimes s)$
using *assms(1) f1 rel-def one-closed*
by *auto*
thus *?thesis*
using *elem-eq-class*
by (*metis assms(1) class-of-to-rel equiv-obj-rng-of-frac f1*)

qed

1.2 The Natural Homomorphism from a Ring to Its Localization

definition *rng-to-rng-of-frac* :: $'a \Rightarrow ('a \times 'a)$ *set where*
rng-to-rng-of-frac $r \equiv (r \mid_{\text{rel}} \mathbf{1})$

lemma *rng-to-rng-of-frac-is-ring-hom* :

shows *rng-to-rng-of-frac* \in *ring-hom* R *rec-rng-of-frac*

proof –

have $f1: \text{rng-to-rng-of-frac} \in \text{carrier } R \rightarrow \text{carrier } \text{rec-rng-of-frac}$
using *rng-to-rng-of-frac-def rec-rng-of-frac-def set-eq-class-of-rng-of-frac-def*
rel-def
by *fastforce*
have $f2: \forall x y. x \in \text{carrier } R \wedge y \in \text{carrier } R$
 $\longrightarrow \text{rng-to-rng-of-frac} (x \otimes_R y) = \text{rng-to-rng-of-frac } x \otimes_{\text{rec-rng-of-frac}} \text{rng-to-rng-of-frac } y$

```

proof(rule allI, rule allI, rule impI)
  fix x y
  assume x ∈ carrier R ∧ y ∈ carrier R
  have f1: rng-to-rng-of-frac (x ⊗R y) = (x ⊗ y |rel 1)
    using rng-to-rng-of-frac-def
    by simp
  have rng-to-rng-of-frac x ⊗rec-rng-of-frac rng-to-rng-of-frac y = (x |rel 1)
    ⊗rec-rng-of-frac (y |rel 1)
    using rng-to-rng-of-frac-def
    by simp
  then have rng-to-rng-of-frac x ⊗rec-rng-of-frac rng-to-rng-of-frac y = (x ⊗ y
|rel 1)
    using mult-rng-of-frac-fundamental-lemma
    by (simp add: ⟨x ∈ carrier R ∧ y ∈ carrier R⟩ rec-monoid-rng-of-frac-def
rec-rng-of-frac-def rel-def)
  thus rng-to-rng-of-frac (x ⊗R y) = rng-to-rng-of-frac x ⊗rec-rng-of-frac rng-to-rng-of-frac
y
    using f1
    by auto
qed
have f3: ∀ x y. x ∈ carrier R ∧ y ∈ carrier R
  → rng-to-rng-of-frac (x ⊕R y) = rng-to-rng-of-frac x ⊕rec-rng-of-frac rng-to-rng-of-frac
y
proof(rule allI, rule allI, rule impI)
  fix x y
  assume a: x ∈ carrier R ∧ y ∈ carrier R
  have f1: rng-to-rng-of-frac (x ⊕R y) = (x ⊕ y |rel 1)
    using rng-to-rng-of-frac-def
    by simp
  have rng-to-rng-of-frac x ⊕rec-rng-of-frac rng-to-rng-of-frac y = (x |rel 1)
    ⊕rec-rng-of-frac (y |rel 1)
    using rng-to-rng-of-frac-def
    by simp
  then have rng-to-rng-of-frac x ⊕rec-rng-of-frac rng-to-rng-of-frac y = (1 ⊗ x
⊕ 1 ⊗ y |rel 1 ⊗ 1)
    using mult-rng-of-frac-fundamental-lemma a
    eq-obj-rng-of-frac.add-rng-of-frac-fundamental-lemma eq-obj-rng-of-frac.rng-to-rng-of-frac-def

    eq-obj-rng-of-frac-axioms f1
    by fastforce
  then have rng-to-rng-of-frac x ⊕rec-rng-of-frac rng-to-rng-of-frac y = (x ⊕ y
|rel 1)
    using l-one a
    by simp
  thus rng-to-rng-of-frac (x ⊕R y) = rng-to-rng-of-frac x ⊕rec-rng-of-frac rng-to-rng-of-frac
y
    using f1
    by auto
qed

```

```

have rng-to-rng-of-frac 1 = (1 |rel 1)
  using rng-to-rng-of-frac-def
  by simp
then have rng-to-rng-of-frac 1R = 1rec-rng-of-frac
  using rec-rng-of-frac-def
  by simp
thus ?thesis
  using ring-hom-def[of R rec-rng-of-frac] f1 f2 f3 f4
  by simp
qed

lemma Im-rng-to-rng-of-frac-unit:
  assumes  $x \in \text{rng-to-rng-of-frac } S$ 
  shows  $x \in \text{Units rec-rng-of-frac}$ 
proof –
  obtain  $s$  where  $a1:s \in S$  and  $a2:x = (s \text{ |}_{rel} \mathbf{1})$ 
    using assms rng-to-rng-of-frac-def rel-def
    by auto
  then have  $(s \text{ |}_{rel} \mathbf{1}) \otimes_{rec-rng-of-frac} (\mathbf{1} \text{ |}_{rel} s) = (s \otimes \mathbf{1} \text{ |}_{rel} s \otimes \mathbf{1})$ 
    using mult-rng-of-frac-fundamental-lemma rec-monoid-rng-of-frac-def rec-rng-of-frac-def
  rel-def subset
    by auto
  then have  $f1:(s \text{ |}_{rel} \mathbf{1}) \otimes_{rec-rng-of-frac} (\mathbf{1} \text{ |}_{rel} s) = (\mathbf{1} \text{ |}_{rel} \mathbf{1})$ 
    using simp-in-frac a1 rel-def
    by auto
  have  $(\mathbf{1} \text{ |}_{rel} s) \otimes_{rec-rng-of-frac} (s \text{ |}_{rel} \mathbf{1}) = (s \otimes \mathbf{1} \text{ |}_{rel} s \otimes \mathbf{1})$ 
    using mult-rng-of-frac-fundamental-lemma rec-monoid-rng-of-frac-def rec-rng-of-frac-def
  rel-def
    subset a1
    by auto
  then have  $f2:(\mathbf{1} \text{ |}_{rel} s) \otimes_{rec-rng-of-frac} (s \text{ |}_{rel} \mathbf{1}) = (\mathbf{1} \text{ |}_{rel} \mathbf{1})$ 
    using simp-in-frac a1 rel-def
    by auto
  then have  $f3:\exists y \in \text{carrier rec-rng-of-frac. } y \otimes_{rec-rng-of-frac} x = \mathbf{1}_{rec-rng-of-frac}$ 
   $\wedge$ 
     $x \otimes_{rec-rng-of-frac} y = \mathbf{1}_{rec-rng-of-frac}$ 
    using rec-rng-of-frac-def f1 f2 a2 rel-def a1
  by (metis (no-types, lifting) class-of-zero-rng-of-frac closed-add-rng-of-frac l-unit-add-rng-of-frac

    mem-Sigma-iff monoid.select-convs(2) partial-object.select-convs(1) semir-
ing-simprules(4) zero-closed)
  have  $x \in \text{carrier rec-rng-of-frac}$ 
    using a2 a1 subset rev-subsetD rec-rng-of-frac-def
  by (metis (no-types, opaque-lifting) ring-hom-closed rng-to-rng-of-frac-def rng-to-rng-of-frac-is-ring-hom)
  thus ?thesis
    using Units-def[of rec-rng-of-frac] f3
    by auto
qed

```

lemma *eq-class-to-rel*:

assumes $(r, s) \in \text{carrier } R \times S$ **and** $(r', s') \in \text{carrier } R \times S$ **and** $(r \mid_{\text{rel}} s) = (r' \mid_{\text{rel}} s')$

shows $(r, s) \text{.}=\text{rel } (r', s')$

proof –

have $(r, s) \in (r \mid_{\text{rel}} s)$

using *assms(1) equiv-obj-rng-of-frac equivalence-def*

by (*metis (no-types, lifting) CollectI case-prodI eq-class-of-rng-of-frac-def partial-object.select-convs(1) rel-def*)

then have $(r, s) \in (r' \mid_{\text{rel}} s')$

using *assms(3)*

by *simp*

then have $(r', s') \text{.}=\text{rel } (r, s)$

by (*simp add: eq-class-of-rng-of-frac-def*)

thus *?thesis*

using *equiv-obj-rng-of-frac equivalence-def*

by (*metis (no-types, lifting) assms(1) assms(2) partial-object.select-convs(1) rel-def*)

qed

lemma *rng-to-rng-of-frac-without-zero-div-is-inj*:

assumes $0 \notin S$ **and** $\forall a \in \text{carrier } R. \forall b \in \text{carrier } R. a \otimes b = 0 \longrightarrow a = 0 \vee b = 0$

shows $a\text{-kernel } R \text{ rec-rng-of-frac rng-to-rng-of-frac} = \{0\}$

proof –

have $\{r \in \text{carrier } R. \text{rng-to-rng-of-frac } r = 0_{\text{rec-rng-of-frac}}\} \subseteq \{0\}$

proof(*rule subsetI*)

fix x

assume $a1: x \in \{r \in \text{carrier } R. \text{rng-to-rng-of-frac } r = 0_{\text{rec-rng-of-frac}}\}$

then have $(x, 1) \text{.}=\text{rel } (0, 1)$

using *rng-to-rng-of-frac-def rec-rng-of-frac-def eq-class-to-rel*

by *simp*

then obtain t **where** $f1:t \in S$ **and** $f2:t \otimes (1 \otimes x \oplus 1 \otimes 0) = 0$

using *rel-def*

by *auto*

have $f3:x \in \text{carrier } R$

using *a1*

by *simp*

then have $f4:t \otimes x = 0$

using *l-one r-zero f2*

by (*simp add: a-minus-def*)

have $t \neq 0$

using *f1 assms(1)*

by *auto*

then have $x = 0$

using *assms(2) f1 f3 f4 subset rev-subsetD*

by *auto*

thus $x \in \{0\}$

by *simp*

```

qed
have  $\{0\} \subseteq \{r \in \text{carrier } R. \text{rng-to-rng-of-frac } r = \mathbf{0}_{\text{rec-rng-of-frac}}\}$ 
  using subsetI rng-to-rng-of-frac-def rec-rng-of-frac-def
  by simp
then have  $\{r \in \text{carrier } R. \text{rng-to-rng-of-frac } r = \mathbf{0}_{\text{rec-rng-of-frac}}\} = \{0\}$ 
  using  $\langle \{r \in \text{carrier } R. \text{rng-to-rng-of-frac } r = \mathbf{0}_{\text{rec-rng-of-frac}}\} \subseteq \{0\} \rangle$ 
  by auto
thus ?thesis
  by (simp add: a-kernel-def kernel-def)
qed

end

end

```

2 Acknowledgements

The author was supported by the ERC Advanced Grant ALEXANDRIA (Project 742178) funded by the European Research Council and led by Professor Lawrence Paulson at the University of Cambridge, UK.

References

- [1] S. Lang. *Algebra*. Springer, revised third edition edition, 2002.