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

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* : $S \subseteq$ *carrier M*

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

lemma (**in** *submonoid*) *is-submonoid*: *submonoid M S*
⟨*proof*⟩

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 $rel \equiv (\!|carrier = carrier\ R \times S,\ eq = \lambda(r,s)\ (r',s').\ \exists\, t{\in}S.\ t \otimes ((s' \otimes r) \ominus (s \otimes r')) = \mathbf{0}|\!)$

lemma (**in** *abelian-group*) *minus-to-eq* :
assumes *abelian-group G* **and** $x \in carrier\ G$ **and** $y \in carrier\ G$ **and** $x \ominus y = \mathbf{0}$
shows $x = y$
⟨*proof*⟩

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

definition *eq-class-of-rng-of-frac*:: - ⇒ *'a* ⇒ *'b* ⇒ *-set* (**infix** $|_1$ *10*)
where $r\ |_{rel}\ s \equiv \{(r', s') \in carrier\ rel.\ (r, s) .\!=_{rel} (r', s')\}$

lemma *class-of-to-rel*:
shows $class\text{-}of_{rel}\ (r, s) = (r\ |_{rel}\ s)$
⟨*proof*⟩

lemma (**in** *eq-obj-rng-of-frac*) *zero-in-mult-submonoid*:
assumes $\mathbf{0} \in S$ **and** $(r, s) \in carrier\ rel$ **and** $(r', s') \in carrier\ rel$
shows $(r\ |_{rel}\ s) = (r'\ |_{rel}\ s')$
⟨*proof*⟩

definition *set-eq-class-of-rng-of-frac*:: - ⇒ *-set* (*set'-class'-of*$_1$)
where $set\text{-}class\text{-}of_{rel} \equiv \{(r\ |_{rel}\ s)|\ r\ s.\ (r, s) \in carrier\ rel\}$

lemma *elem-eq-class*:
assumes *equivalence S* **and** $x \in carrier\ S$ **and** $y \in carrier\ S$ **and** $x .\!=_S y$
shows $class\text{-}of_S\ x = class\text{-}of_S\ y$
⟨*proof*⟩

lemma (**in** *abelian-group*) *four-elem-comm*:
assumes $a \in carrier\ G$ **and** $b \in carrier\ G$ **and** $c \in carrier\ G$ **and** $d \in carrier$

G
shows $a \ominus c \oplus b \ominus d = a \oplus b \ominus c \ominus d$
⟨*proof*⟩

lemma (**in** *abelian-monoid*) *right-add-eq*:
assumes $a = b$
shows $c \oplus a = c \oplus b$
⟨*proof*⟩

lemma (**in** *abelian-monoid*) *right-minus-eq*:
assumes $a = b$
shows $c \ominus a = c \ominus b$
⟨*proof*⟩

lemma (**in** *abelian-group*) *inv-add*:
assumes $a \in$ *carrier* G **and** $b \in$ *carrier* G
shows $\ominus\ (a \oplus b) = \ominus\ a \ominus b$
⟨*proof*⟩

lemma (**in** *abelian-group*) *right-inv-add*:
assumes $a \in$ *carrier* G **and** $b \in$ *carrier* G **and** $c \in$ *carrier* G
shows $c \ominus a \ominus b = c \ominus (a \oplus b)$
⟨*proof*⟩

context *eq-obj-rng-of-frac*
begin

definition *carrier-rng-of-frac*:: - *partial-object*
where *carrier-rng-of-frac* ≡ (|*carrier* = $\textit{set-class-of}_{rel}$|)

definition *mult-rng-of-frac*:: [-*set*, -*set*] ⇒ -*set*
where *mult-rng-of-frac* X Y ≡
let $x' = (\textit{SOME}\ x.\ x \in X)$ *in*
let $y' = (\textit{SOME}\ y.\ y \in Y)$ *in*
$(\textit{fst}\ x' \otimes \textit{fst}\ y')|_{rel}\ (\textit{snd}\ x' \otimes \textit{snd}\ y')$

definition *rec-monoid-rng-of-frac*:: - *monoid*
where *rec-monoid-rng-of-frac* ≡ (|*carrier* = $\textit{set-class-of}_{rel}$, *mult* = *mult-rng-of-frac*, *one* = $(\mathbf{1}|_{rel}\ \mathbf{1})$|)

lemma *member-class-to-carrier*:
assumes $x \in (r\ |_{rel}\ s)$ **and** $y \in (r'\ |_{rel}\ s')$
shows $(\textit{fst}\ x \otimes \textit{fst}\ y, \textit{snd}\ x \otimes \textit{snd}\ y) \in$ *carrier rel*
⟨*proof*⟩

lemma *member-class-to-member-class*:
assumes $x \in (r\ |_{rel}\ s)$ **and** $y \in (r'\ |_{rel}\ s')$
shows $(\textit{fst}\ x \otimes \textit{fst}\ y\ |_{rel}\ \textit{snd}\ x \otimes \textit{snd}\ y) \in \textit{set-class-of}_{rel}$
⟨*proof*⟩

lemma *closed-mult-rng-of-frac* :
assumes $(r, s) \in carrier\ rel$ **and** $(t, u) \in carrier\ rel$
shows $(r\ |_{rel}\ s) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (t\ |_{rel}\ u) \in set\text{-}class\text{-}of_{rel}$
⟨*proof*⟩

lemma *non-empty-class*:
assumes $(r, s) \in carrier\ rel$
shows $(r\ |_{rel}\ s) \neq \{\}$
⟨*proof*⟩

lemma *mult-rng-of-frac-fundamental-lemma*:
assumes $(r, s) \in carrier\ rel$ **and** $(r', s') \in carrier\ rel$
shows $(r\ |_{rel}\ s) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (r'\ |_{rel}\ s') = (r \otimes r'\ |_{rel}\ s \otimes s')$
⟨*proof*⟩

lemma *member-class-to-assoc*:
assumes $x \in (r\ |_{rel}\ s)$ **and** $y \in (t\ |_{rel}\ u)$ **and** $z \in (v\ |_{rel}\ w)$
shows $((fst\ x \otimes fst\ y) \otimes fst\ z\ |_{rel}\ (snd\ x \otimes snd\ y) \otimes snd\ z) = (fst\ x \otimes (fst\ y \otimes fst\ z)\ |_{rel}\ snd\ x \otimes (snd\ y \otimes snd\ z))$
⟨*proof*⟩

lemma *assoc-mult-rng-of-frac*:
assumes $(r, s) \in carrier\ rel$ **and** $(t, u) \in carrier\ rel$ **and** $(v, w) \in carrier\ rel$
shows $((r\ |_{rel}\ s) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (t\ |_{rel}\ u)) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (v\ |_{rel}\ w) =$
$(r\ |_{rel}\ s) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} ((t\ |_{rel}\ u) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (v\ |_{rel}\ w))$
⟨*proof*⟩

lemma *left-unit-mult-rng-of-frac*:
assumes $(r, s) \in carrier\ rel$
shows $\mathbf{1}_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (r\ |_{rel}\ s) = (r\ |_{rel}\ s)$
⟨*proof*⟩

lemma *right-unit-mult-rng-of-frac*:
assumes $(r, s) \in carrier\ rel$
shows $(r\ |_{rel}\ s) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} \mathbf{1}_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} = (r\ |_{rel}\ s)$
⟨*proof*⟩

lemma *monoid-rng-of-frac*:
shows *monoid* (*rec-monoid-rng-of-frac*)
⟨*proof*⟩

lemma *comm-mult-rng-of-frac*:
assumes $(r, s) \in carrier\ rel$ **and** $(r', s') \in carrier\ rel$
shows $(r\ |_{rel}\ s) \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (r'\ |_{rel}\ s') = (r'\ |_{rel}\ s') \otimes_{rec\text{-}monoid\text{-}rng\text{-}of\text{-}frac} (r\ |_{rel}\ s)$
⟨*proof*⟩

lemma *comm-monoid-rng-of-frac*:
shows *comm-monoid* (*rec-monoid-rng-of-frac*)
⟨*proof*⟩

definition *add-rng-of-frac*:: [-*set*, -*set*] ⇒ -*set*
where *add-rng-of-frac X Y* ≡
let x' = (*SOME x*. $x \in X$) *in*
let y' = (*SOME y*. $y \in Y$) *in*
(*snd* y' ⊗ *fst* x' ⊕ *snd* x' ⊗ *fst* y') $|_{rel}$ (*snd* x' ⊗ *snd* y')

definition *rec-rng-of-frac*:: - *ring*
where *rec-rng-of-frac* ≡
(|*carrier* = *set-class-of*$_{rel}$, *mult* = *mult-rng-of-frac*, *one* = ($\mathbf{1}|_{rel}$ $\mathbf{1}$), *zero* = ($\mathbf{0}$ $|_{rel}$ $\mathbf{1}$), *add* = *add-rng-of-frac* |)

lemma *add-rng-of-frac-fundamental-lemma*:
assumes $(r, s) \in$ *carrier rel* **and** $(r', s') \in$ *carrier rel*
shows $(r \;|_{rel}\; s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r' \;|_{rel}\; s') = (s' \otimes r \oplus s \otimes r' \;|_{rel}\; s \otimes s')$
⟨*proof*⟩

lemma *closed-add-rng-of-frac*:
assumes $(r, s) \in$ *carrier rel* **and** $(r', s') \in$ *carrier rel*
shows $(r \;|_{rel}\; s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r' \;|_{rel}\; s') \in$ *set-class-of*$_{rel}$
⟨*proof*⟩

lemma *closed-rel-add*:
assumes $(r, s) \in$ *carrier rel* **and** $(r', s') \in$ *carrier rel*
shows $(s' \otimes r \oplus s \otimes r', s \otimes s') \in$ *carrier rel*
⟨*proof*⟩

lemma *assoc-add-rng-of-frac*:
assumes $(r, s) \in$ *carrier rel* **and** $(r', s') \in$ *carrier rel* **and** $(r'', s'') \in$ *carrier rel*
shows $(r \;|_{rel}\; s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r' \;|_{rel}\; s') \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r''|_{rel}\; s'') =$
$(r \;|_{rel}\; s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} ((r' \;|_{rel}\; s') \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r'' \;|_{rel}\; s''))$
⟨*proof*⟩

lemma *add-rng-of-frac-zero*:
shows $(\mathbf{0} \;|_{rel}\; \mathbf{1}) \in$ *set-class-of*$_{rel}$
⟨*proof*⟩

lemma *l-unit-add-rng-of-frac*:
assumes $(r, s) \in$ *carrier rel*
shows $\mathbf{0}_{rec\text{-}rng\text{-}of\text{-}frac} \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r \;|_{rel}\; s) = (r \;|_{rel}\; s)$
⟨*proof*⟩

lemma *r-unit-add-rng-of-frac*:
assumes $(r, s) \in$ *carrier rel*
shows $(r \;|_{rel}\; s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} \mathbf{0}_{rec\text{-}rng\text{-}of\text{-}frac} = (r \;|_{rel}\; s)$

⟨*proof*⟩

lemma *comm-add-rng-of-frac*:
  assumes $(r,\ s) \in$ *carrier rel* **and** $(r',\ s') \in$ *carrier rel*
  shows $(r\ |_{rel}\ s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r'\ |_{rel}\ s') = (r'\ |_{rel}\ s') \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r\ |_{rel}\ s)$
⟨*proof*⟩

lemma *class-of-zero-rng-of-frac*:
  assumes $s \in S$
  shows $(\mathbf{0}\ |_{rel}\ s) = \mathbf{0}_{rec\text{-}rng\text{-}of\text{-}frac}$
⟨*proof*⟩

lemma *r-inv-add-rng-of-frac*:
  assumes $(r,\ s) \in$ *carrier rel*
  shows $(r\ |_{rel}\ s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (\ominus\ r\ |_{rel}\ s) = \mathbf{0}_{rec\text{-}rng\text{-}of\text{-}frac}$
⟨*proof*⟩

lemma *l-inv-add-rng-of-frac*:
  assumes $(r,\ s) \in$ *carrier rel*
  shows $(\ominus\ r\ |_{rel}\ s) \oplus_{rec\text{-}rng\text{-}of\text{-}frac} (r\ |_{rel}\ s) = \mathbf{0}_{rec\text{-}rng\text{-}of\text{-}frac}$
⟨*proof*⟩

lemma *abelian-group-rng-of-frac*:
  shows *abelian-group* (*rec-rng-of-frac*)
⟨*proof*⟩

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

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

lemma *rng-rng-of-frac*:
  shows *ring* (*rec-rng-of-frac*)
⟨*proof*⟩

lemma *crng-rng-of-frac*:
  shows *cring* (*rec-rng-of-frac*)
  ⟨*proof*⟩

lemma *simp-in-frac*:

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

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 $r \equiv (r \mid_{rel} \mathbf{1})$

lemma *rng-to-rng-of-frac-is-ring-hom* :
shows *rng-to-rng-of-frac* $\in$ *ring-hom R rec-rng-of-frac*
$\langle proof \rangle$

lemma *Im-rng-to-rng-of-frac-unit*:
assumes $x \in$ *rng-to-rng-of-frac* ‘ S
shows $x \in$ *Units rec-rng-of-frac*
$\langle proof \rangle$

lemma *eq-class-to-rel*:
assumes $(r, s) \in$ *carrier* $R \times S$ **and** $(r', s') \in$ *carrier* $R \times S$ **and** $(r \mid_{rel} s) = (r' \mid_{rel} s')$
shows $(r, s) \mathrel{.=_{rel}} (r', s')$
$\langle proof \rangle$

lemma *rng-to-rng-of-frac-without-zero-div-is-inj*:
assumes $\mathbf{0} \notin S$ **and** $\forall a \in$ *carrier* $R. \forall b \in$ *carrier* $R.\ a \otimes b = \mathbf{0} \longrightarrow a = \mathbf{0} \vee b = \mathbf{0}$
shows *a-kernel R rec-rng-of-frac rng-to-rng-of-frac* $= \{\mathbf{0}\}$
$\langle proof \rangle$

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.