

Nagata Factoriality

Arthur Freitas Ramos* David Barros Hulak
Ruy J. G. B. de Queiroz

April 30, 2026

Abstract

This entry formalizes a prime-generated version of Nagata’s factoriality theorem in Isabelle/HOL. It develops the basic theory of prime-generated multiplicative sets, packages a wrapper interface around the AFP entry `Localization_Ring`, and proves record-based descent theorems showing that factoriality descends from a localization to the base ring under prime-generated and prime-or-unit hypotheses on the multiplicative set. The theorem package also includes closure-based corollaries for arbitrary and finite families of prime generators. The application layer specializes this framework to polynomial rings, both for localization away the polynomial variable X and for localizations generated by constant prime polynomials.

Contents

1	Overview	2
2	Prime-generated multiplicative sets	2
3	Localization helper lemmas	3
4	Record-based Nagata descent lemmas	6
5	Polynomial applications	12
6	Constant-prime localization applications	13
7	Nagata-factoriality scaffolding	15

*Maintainer: arfreita@microsoft.com

1 Overview

This entry formalizes a prime-generated version of Nagata's factoriality theorem for noetherian domains, following the classical commutative-algebra framework developed by Nagata, Samuel, and Matsumura.[2, 3, 1] It packages the descent theorem itself, closure-based corollaries for prime-generated multiplicative sets, and abstract polynomial applications for localization away the polynomial variable X and for localizations generated by constant prime polynomials.

theory *Prime-Generated*

imports *HOL-Computational-Algebra.Factorial-Ring*

begin

2 Prime-generated multiplicative sets

This theory isolates the reusable combinatorial layer behind Nagata's factoriality theorem. The full localization argument is developed in later theories; here we focus on the multiplicative sets generated by prime elements and on the closure lemmas that do not depend on any localization API.

definition *avoids* :: 'a :: comm-semiring-1 set \Rightarrow 'a \Rightarrow bool **where**
avoids S p \longleftrightarrow ($\forall s \in S. \neg p \text{ dvd } s$)

definition *prime-generated* :: 'a :: comm-semiring-1 set \Rightarrow bool **where**
prime-generated S \longleftrightarrow
($\forall s \in S. \exists M. (\forall q. q \in \# M \longrightarrow q \in S \wedge \text{prime-elem } q) \wedge \text{prod-mset } M = s$)

inductive-set *mult-submonoid-closure* :: 'a :: comm-monoid-mult set \Rightarrow 'a set **for** A **where**

one-closed: $1 \in \text{mult-submonoid-closure } A$

| *generator*: $a \in A \Longrightarrow a \in \text{mult-submonoid-closure } A$

| *mult-closed*:

$a \in \text{mult-submonoid-closure } A \Longrightarrow b \in \text{mult-submonoid-closure } A \Longrightarrow$

$a * b \in \text{mult-submonoid-closure } A$

definition *powers-set* :: 'a :: monoid-mult \Rightarrow 'a set **where**

powers-set p = {x. $\exists n. x = p \wedge n$ }

lemma *prime-generatedI*:

assumes $\bigwedge s. s \in S \Longrightarrow \exists M. (\forall q. q \in \# M \longrightarrow q \in S \wedge \text{prime-elem } q) \wedge \text{prod-mset } M = s$

shows *prime-generated* S

<proof>

lemma *prime-generatedE*:

assumes *prime-generated* S s \in S

obtains M **where** ($\forall q. q \in \# M \longrightarrow q \in S \wedge \text{prime-elem } q$) $\text{prod-mset } M = s$

<proof>

```

lemma prime-generated-powers-set:
  assumes prime-elem p
  shows prime-generated (powers-set p)
  ⟨proof⟩

lemma prime-generated-mult-submonoid-closure:
  assumes  $\bigwedge q. q \in A \implies \text{prime-elem } q$ 
  shows prime-generated (mult-submonoid-closure A)
  ⟨proof⟩

lemma zero-notin-prime-generated:
  assumes prime-generated S
  shows  $(0 :: 'a :: \text{semidom}) \notin S$ 
  ⟨proof⟩

end
theory Localization-Interface
  imports
    HOL-Algebra.Ring-Divisibility
    HOL-Algebra.QuotRing
    Localization-Ring.Localization
begin

```

3 Localization helper lemmas

The AFP entry *Localization-Ring.Localization* develops localizations as quotient rings in the HOL-Algebra hierarchy. For the present development we package a small wrapper layer at the level of equality of representatives, denominator rescaling, units coming from the multiplicative set, and injectivity of the canonical map.

```

context eq-obj-rng-of-frac
begin

```

```

lemma fraction-eq-iff-rel:
  assumes  $(r, s) \in \text{carrier } \text{rel}$ 
  and  $(r', s') \in \text{carrier } \text{rel}$ 
  shows  $(r \mid_{\text{rel}} s) = (r' \mid_{\text{rel}} s') \iff (r, s) \text{.}=\text{rel } (r', s')$ 
  ⟨proof⟩

```

```

lemma fraction-zero-rep [simp]:
  assumes  $s \in S$ 
  shows  $(\mathbf{0} \mid_{\text{rel}} s) = \mathbf{0}_{\text{rec-rng-of-frac}}$ 
  ⟨proof⟩

```

```

lemma fraction-surj:
  assumes  $x \in \text{carrier } \text{rec-rng-of-frac}$ 
  shows  $\exists r \in \text{carrier } R. \exists s \in S. x = (r \mid_{\text{rel}} s)$ 

```

<proof>

lemma *fraction-rescale:*

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

and $s' \in S$

shows $(r \mid_{\text{rel}} s) = (s' \otimes r \mid_{\text{rel}} s' \otimes s)$

<proof>

lemma *fraction-mult-rep:*

assumes $rs: (r, s) \in \text{carrier rel}$

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

shows $(r \mid_{\text{rel}} s) \otimes_{\text{rec-rng-of-frac}} (r' \mid_{\text{rel}} s') =$
 $(r \otimes_R r' \mid_{\text{rel}} s \otimes_R s')$

<proof>

lemma *map-mul-fraction:*

assumes $a\text{-in}: a \in \text{carrier } R$

and $rs: (r, s) \in \text{carrier rel}$

shows $\text{rng-to-rng-of-frac } a \otimes_{\text{rec-rng-of-frac}} (r \mid_{\text{rel}} s) = (a \otimes_R r \mid_{\text{rel}} s)$

<proof>

lemma *fraction-mul-map:*

assumes $rs: (r, s) \in \text{carrier rel}$

and $a\text{-in}: a \in \text{carrier } R$

shows $(r \mid_{\text{rel}} s) \otimes_{\text{rec-rng-of-frac}} \text{rng-to-rng-of-frac } a = (r \otimes_R a \mid_{\text{rel}} s)$

<proof>

lemma *fraction-eq-iff-cross-multiply:*

assumes $rs: (r, s) \in \text{carrier rel}$

and $rs': (r', s') \in \text{carrier rel}$

and $\text{zero-notin}: \mathbf{0} \notin S$

and $\text{no-zero-div}: \forall a \in \text{carrier } R. \forall b \in \text{carrier } R. a \otimes b = \mathbf{0} \longrightarrow a = \mathbf{0} \vee b =$

$\mathbf{0}$

shows $(r \mid_{\text{rel}} s) = (r' \mid_{\text{rel}} s') \iff s' \otimes_R r = s \otimes_R r'$

<proof>

lemma *fraction-eq-zero-iff:*

assumes $rs: (r, s) \in \text{carrier rel}$

and $\text{zero-notin}: \mathbf{0} \notin S$

and $\text{no-zero-div}: \forall a \in \text{carrier } R. \forall b \in \text{carrier } R. a \otimes b = \mathbf{0} \longrightarrow a = \mathbf{0} \vee b =$

$\mathbf{0}$

shows $(r \mid_{\text{rel}} s) = \mathbf{0}_{\text{rec-rng-of-frac}} \iff r = \mathbf{0}$

<proof>

lemma *map-eq-zero-iff:*

assumes $a\text{-in}: a \in \text{carrier } R$

and $\text{zero-notin}: \mathbf{0} \notin S$

and $\text{no-zero-div}: \forall a' \in \text{carrier } R. \forall b' \in \text{carrier } R. a' \otimes b' = \mathbf{0} \longrightarrow a' = \mathbf{0} \vee$

$b' = \mathbf{0}$

shows $\text{rng-to-rng-of-frac } a = \mathbf{0}_{\text{rec-rng-of-frac}} \iff a = \mathbf{0}$
 ⟨proof⟩

lemma *dvd-map-iff*:

assumes *a-in*: $a \in \text{carrier } R$

and *b-in*: $b \in \text{carrier } R$

and *zero-notin*: $\mathbf{0} \notin S$

and *no-zero-div*: $\forall a' \in \text{carrier } R. \forall b' \in \text{carrier } R. a' \otimes b' = \mathbf{0} \implies a' = \mathbf{0} \vee b' = \mathbf{0}$

shows $\text{rng-to-rng-of-frac } a \text{ divides}_{\text{rec-rng-of-frac}} \text{rng-to-rng-of-frac } b \iff (\exists s \in S. a \text{ divides}_R (s \otimes_R b))$

⟨proof⟩

lemma *image-submonoid-is-unit*:

assumes $x \in \text{rng-to-rng-of-frac } S$

shows $x \in \text{Units rec-rng-of-frac}$

⟨proof⟩

lemma *map-submonoid-elem-is-unit*:

assumes $s \in S$

shows $\text{rng-to-rng-of-frac } s \in \text{Units rec-rng-of-frac}$

⟨proof⟩

lemma *map-unit-is-unit*:

assumes *u-unit*: $u \in \text{Units } R$

shows $\text{rng-to-rng-of-frac } u \in \text{Units rec-rng-of-frac}$

⟨proof⟩

lemma *fraction-unit-numerator-is-unit*:

assumes *u-unit*: $u \in \text{Units } R$

and *s-in*: $s \in S$

shows $(u \text{ |}_{\text{rel}} s) \in \text{Units rec-rng-of-frac}$

⟨proof⟩

lemma *map-inj-on*:

assumes $\mathbf{0} \notin S$

and $\forall a \in \text{carrier } R. \forall b \in \text{carrier } R. a \otimes b = \mathbf{0} \implies a = \mathbf{0} \vee b = \mathbf{0}$

shows *inj-on* $\text{rng-to-rng-of-frac } (\text{carrier } R)$

⟨proof⟩

end

end

theory *Nagata-Lemmas*

imports *Localization-Interface*

begin

4 Record-based Nagata descent lemmas

definition *ring-avoids* ::

$('a, 'b)$ ring-scheme $\Rightarrow 'a$ set $\Rightarrow 'a \Rightarrow \text{bool}$

where

$\text{ring-avoids } R \ S \ p \longleftrightarrow (\forall s \in S. \neg p \text{ divides}_R s)$

definition *ring-prime-generated* ::

$('a, 'b)$ ring-scheme $\Rightarrow 'a$ set $\Rightarrow \text{bool}$

where

$\text{ring-prime-generated } R \ S \longleftrightarrow$

$(\forall s \in S. \exists fs.$

$\text{set } fs \subseteq S \wedge$

$(\forall q \in \text{set } fs. \text{ring-prime}_R q) \wedge$

$\text{foldr } (\otimes_R) \ fs \ \mathbf{1}_R = s)$

lemma *ring-prime-generatedI*:

assumes $\bigwedge s. s \in S \implies \exists fs.$

$\text{set } fs \subseteq S \wedge$

$(\forall q \in \text{set } fs. \text{ring-prime}_R q) \wedge$

$\text{foldr } (\otimes_R) \ fs \ \mathbf{1}_R = s$

shows $\text{ring-prime-generated } R \ S$

$\langle \text{proof} \rangle$

lemma *ring-prime-generatedE*:

assumes $\text{ring-prime-generated } R \ S \ s \in S$

obtains fs **where**

$\text{set } fs \subseteq S$

$\forall q \in \text{set } fs. \text{ring-prime}_R q$

$\text{foldr } (\otimes_R) \ fs \ \mathbf{1}_R = s$

$\langle \text{proof} \rangle$

definition *ring-powers-set* ::

$('a, 'b)$ ring-scheme $\Rightarrow 'a \Rightarrow 'a$ set

where

$\text{ring-powers-set } R \ p = \{x. \exists n::\text{nat}. x = p [\frown]_R n\}$

inductive-set *ring-mult-submonoid-closure* ::

$('a, 'b)$ ring-scheme $\Rightarrow 'a$ set $\Rightarrow 'a$ set

for R **and** A

where

one-closed: $\mathbf{1}_R \in \text{ring-mult-submonoid-closure } R \ A$

| *generator*: $a \in A \implies a \in \text{ring-mult-submonoid-closure } R \ A$

| *mult-closed*:

$a \in \text{ring-mult-submonoid-closure } R \ A \implies$

$b \in \text{ring-mult-submonoid-closure } R \ A \implies$

$a \otimes_R b \in \text{ring-mult-submonoid-closure } R \ A$

lemma *ring-mult-submonoid-closure-subset*:

assumes *ring-R*: ring R
and *A-sub*: $A \subseteq \text{carrier } R$
shows *ring-mult-submonoid-closure* $R \ A \subseteq \text{carrier } R$
 ⟨*proof*⟩

lemma *ring-mult-submonoid-closure-submonoid*:
assumes *ring-R*: ring R
and *A-sub*: $A \subseteq \text{carrier } R$
shows *submonoid* $R \ (\text{ring-mult-submonoid-closure } R \ A)$
 ⟨*proof*⟩

lemma *foldr-mult-right*:
assumes *ring-R*: ring R
and *xs-sub*: set $xs \subseteq \text{carrier } R$
and *y-in*: $y \in \text{carrier } R$
shows *foldr* $(\otimes_R) \ xs \ y =$
 foldr $(\otimes_R) \ xs \ \mathbf{1}_R \ \otimes_R \ y$
 ⟨*proof*⟩

lemma *ring-powers-submonoid*:
assumes *ring-R*: ring R
and *p-in*: $p \in \text{carrier } R$
shows *submonoid* $R \ (\text{ring-powers-set } R \ p)$
 ⟨*proof*⟩

lemma *ring-prime-generated-powers-set*:
assumes *ring-R*: ring R
and *p-in*: $p \in \text{carrier } R$
and *hp*: *ring-prime* $_R \ p$
shows *ring-prime-generated* $R \ (\text{ring-powers-set } R \ p)$
 ⟨*proof*⟩

lemma *ring-prime-generated-mult-submonoid-closure*:
assumes *ring-R*: ring R
and *A-sub*: $A \subseteq \text{carrier } R$
and *hprime*: $\bigwedge q. q \in A \implies \text{ring-prime}_R \ q$
shows *ring-prime-generated* $R \ (\text{ring-mult-submonoid-closure } R \ A)$
 ⟨*proof*⟩

locale *nagata-localization* = *eq-obj-rng-of-frac* $R \ S + \text{domain } R$ **for** R (**structure**)
and S
begin

lemma *no-zero-divisors*:
 $\forall a \in \text{carrier } R. \forall b \in \text{carrier } R. a \otimes_R b = \mathbf{0} \implies a = \mathbf{0} \vee b = \mathbf{0}$
 ⟨*proof*⟩

lemma *multlist-closed*:
assumes *xs-sub*: set $xs \subseteq \text{carrier } R$

shows $\text{foldr } (\otimes_R) \text{ xs } \mathbf{1}_R \in \text{carrier } R$
<proof>

lemma *multlist-mem-submonoid*:

assumes fs-sub : $\text{set fs} \subseteq S$
shows $\text{foldr } (\otimes_R) \text{ fs } \mathbf{1}_R \in S$
<proof>

lemma *multlist-nonzero-of-prime-factors*:

assumes fs-sub : $\text{set fs} \subseteq S$
and hf : $\forall q \in \text{set fs. ring-prime}_R q$
shows $\text{foldr } (\otimes_R) \text{ fs } \mathbf{1}_R \neq \mathbf{0}$
<proof>

lemma *zero-notin-submonoid-of-prime-generated*:

assumes hS : $\text{ring-prime-generated } R S$
shows $\mathbf{0} \notin S$
<proof>

lemma *zero-notin-submonoid-of-prime-or-unit*:

assumes hS : $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
shows $\mathbf{0} \notin S$
<proof>

lemma *ring-prime-imp-ring-irreducible*:

assumes p-in : $p \in \text{carrier } R$
and hp : $\text{ring-prime}_R p$
shows $\text{ring-irreducible}_R p$
<proof>

lemma *prime-of-irreducible-of-dvd-mem*:

assumes hS : $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
and p-in : $p \in \text{carrier } R$
and hp : $\text{ring-irreducible}_R p$
and s-in : $s \in S$
and p-dvd-s : $p \text{ divides}_R s$
shows $\text{ring-prime}_R p$
<proof>

lemma *prime-of-irreducible-of-dvd-prime-factors*:

assumes fs-sub : $\text{set fs} \subseteq S$
and hf : $\forall q \in \text{set fs. ring-prime}_R q$
and p-in : $p \in \text{carrier } R$
and hp : $\text{ring-irreducible}_R p$
and hdiv : $p \text{ divides}_R \text{foldr } (\otimes_R) \text{ fs } \mathbf{1}_R$
shows $\text{ring-prime}_R p$
<proof>

lemma *prime-of-irreducible-of-dvd-mem-prime-generated*:

assumes hS : *ring-prime-generated* $R S$
and p -in: $p \in \text{carrier } R$
and hp : *ring-irreducible* $_R p$
and s -in: $s \in S$
and p -dvd- s : $p \text{ divides}_R s$
shows *ring-prime* $_R p$
 ⟨*proof*⟩

lemma *dvd-of-localization-dvd*:
assumes hS : $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
and p -in: $p \in \text{carrier } R$
and a -in: $a \in \text{carrier } R$
and hp : *ring-irreducible* $_R p$
and $havoid$: *ring-avoids* $R S p$
and $hdiv$: *rng-to-rng-of-frac* $p \text{ divides}_{\text{rec-rng-of-frac}} \text{rng-to-rng-of-frac } a$
shows $p \text{ divides}_R a$
 ⟨*proof*⟩

lemma *prime-of-localization-prime*:
assumes hS : $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
and p -in: $p \in \text{carrier } R$
and hp : *ring-irreducible* $_R p$
and $havoid$: *ring-avoids* $R S p$
and $hploc$: *ring-prime* $_{\text{rec-rng-of-frac}} (\text{rng-to-rng-of-frac } p)$
shows *ring-prime* $_R p$
 ⟨*proof*⟩

lemma *dvd-of-mul-eq-prime-factors*:
assumes fs -sub: $\text{set } fs \subseteq S$
and hf : $\forall q \in \text{set } fs. \text{ring-prime}_R q$
and p -in: $p \in \text{carrier } R$
and a -in: $a \in \text{carrier } R$
and hp : *ring-irreducible* $_R p$
and $hnot$: $\forall q \in \text{set } fs. \neg p \text{ divides}_R q$
and c -in: $c \in \text{carrier } R$
and hEq : $\text{foldr } (\otimes_R) fs \mathbf{1}_R \otimes_R a = p \otimes_R c$
shows $p \text{ divides}_R a$
 ⟨*proof*⟩

lemma *dvd-of-localization-dvd-prime-generated*:
assumes hS : *ring-prime-generated* $R S$
and p -in: $p \in \text{carrier } R$
and a -in: $a \in \text{carrier } R$
and hp : *ring-irreducible* $_R p$
and $havoid$: *ring-avoids* $R S p$
and $hdiv$: *rng-to-rng-of-frac* $p \text{ divides}_{\text{rec-rng-of-frac}} \text{rng-to-rng-of-frac } a$
shows $p \text{ divides}_R a$
 ⟨*proof*⟩

lemma *map-irreducible-not-unit-of-zero-notin*:
assumes *zero-notin*: $\mathbf{0} \notin S$
and *loc-dom*: *domain rec-rng-of-frac*
and *p-in*: $p \in \text{carrier } R$
and *hp*: *ring-irreducible_R p*
and *havoid*: *ring-avoids R S p*
shows *rng-to-rng-of-frac p* $\notin \text{Units rec-rng-of-frac}$
<proof>

lemma *map-irreducible-not-unit*:
assumes *hS*: $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
and *loc-dom*: *domain rec-rng-of-frac*
and *p-in*: $p \in \text{carrier } R$
and *hp*: *ring-irreducible_R p*
and *havoid*: *ring-avoids R S p*
shows *rng-to-rng-of-frac p* $\notin \text{Units rec-rng-of-frac}$
<proof>

lemma *localization-irreducible-of-irreducible*:
assumes *hS*: $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
and *loc-dom*: *domain rec-rng-of-frac*
and *p-in*: $p \in \text{carrier } R$
and *hp*: *ring-irreducible_R p*
and *havoid*: *ring-avoids R S p*
shows *ring-irreducible_{rec-rng-of-frac} (rng-to-rng-of-frac p)*
<proof>

lemma *nagata-key-lemma*:
assumes *hS*: $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$
and *loc-fd*: *factorial-domain rec-rng-of-frac*
and *p-in*: $p \in \text{carrier } R$
and *hp*: *ring-irreducible_R p*
shows *ring-prime_R p*
<proof>

lemma *split-prime-factors-of-mul-eq*:
assumes *fs-sub*: *set fs* $\subseteq S$
and *hf*: $\forall q \in \text{set } fs. \text{ring-prime}_R q$
and *p-in*: $p \in \text{carrier } R$
and *a-in*: $a \in \text{carrier } R$
and *b-in*: $b \in \text{carrier } R$
and *hEq*: $p \otimes_R \text{foldr } (\otimes_R) fs \mathbf{1}_R = a \otimes_R b$
shows $\exists fs1 fs2 a' b'.$
 $fs <\sim\sim> fs1 @ fs2 \wedge$
 $\text{set } fs1 \subseteq S \wedge (\forall q \in \text{set } fs1. \text{ring-prime}_R q) \wedge$
 $\text{set } fs2 \subseteq S \wedge (\forall q \in \text{set } fs2. \text{ring-prime}_R q) \wedge$
 $a' \in \text{carrier } R \wedge b' \in \text{carrier } R \wedge$
 $a = \text{foldr } (\otimes_R) fs1 \mathbf{1}_R \otimes_R a' \wedge$

$$b = \text{foldr } (\otimes_R) \text{ fs2 } \mathbf{1}_R \otimes_R b' \wedge$$

$$p = a' \otimes_R b'$$

<proof>

lemma *localization-irreducible-of-irreducible-prime-generated:*

assumes *hS: ring-prime-generated R S*
and *loc-dom: domain rec-rng-of-frac*
and *p-in: p ∈ carrier R*
and *hp: ring-irreducible_R p*
and *havoid: ring-avoids R S p*
shows *ring-irreducible_{rec-rng-of-frac} (rng-to-rng-of-frac p)*
<proof>

lemma *prime-of-localization-prime-prime-generated:*

assumes *hS: ring-prime-generated R S*
and *p-in: p ∈ carrier R*
and *hp: ring-irreducible_R p*
and *havoid: ring-avoids R S p*
and *hploc: ring-prime_{rec-rng-of-frac} (rng-to-rng-of-frac p)*
shows *ring-prime_R p*
<proof>

lemma *nagata-key-lemma-prime-generated:*

assumes *hS: ring-prime-generated R S*
and *loc-fd: factorial-domain rec-rng-of-frac*
and *p-in: p ∈ carrier R*
and *hp: ring-irreducible_R p*
shows *ring-prime_R p*
<proof>

lemma *nagata-theorem:*

assumes *noeth: noetherian-domain R*
and *hS: ring-prime-generated R S*
and *loc-fd: factorial-domain rec-rng-of-frac*
shows *factorial-domain R*
<proof>

lemma *nagata-theorem-of-prime-or-unit:*

assumes *noeth: noetherian-domain R*
and *hS: $\bigwedge s. s \in S \implies \text{ring-prime}_R s \vee s \in \text{Units } R$*
and *loc-fd: factorial-domain rec-rng-of-frac*
shows *factorial-domain R*
<proof>

lemma *nagata-theorem-of-prime-generators:*

assumes *noeth: noetherian-domain R*
and *S-eq: S = ring-mult-submonoid-closure R A*
and *A-sub: A ⊆ carrier R*
and *hprime: $\bigwedge q. q \in A \implies \text{ring-prime}_R q$*

and *loc-fd: factorial-domain rec-rng-of-frac*
shows *factorial-domain R*
 ⟨*proof*⟩

lemma *nagata-theorem-of-finite-prime-generators:*
assumes *noeth: noetherian-domain R*
and *finA: finite A*
and *S-eq: S = ring-mult-submonoid-closure R A*
and *A-sub: A ⊆ carrier R*
and *hprime: ⋀q. q ∈ A ⇒ ring-prime_R q*
and *loc-fd: factorial-domain rec-rng-of-frac*
shows *factorial-domain R*
 ⟨*proof*⟩

end

end

theory *Polynomial-Applications*

imports

Nagata-Lemmas

HOL-Algebra.Polynomial-Divisibility

begin

5 Polynomial applications

This theory packages the first concrete application layer on top of the record-based Nagata descent theorem. The present results isolate the abstract “localize away X” step for HOL-Algebra polynomial rings, together with the standard field-coefficient specialization in which X is prime by the degree-one irreducibility criterion.

context *domain*

begin

lemma *polynomial-prime-X:*

assumes *K: subfield K R*

shows *ring-prime_{K[X]} X*

⟨*proof*⟩

lemma *polynomial-prime-generated-powers-X:*

assumes *K: subring K R*

and *hX: ring-prime_{K[X]} X*

shows *ring-prime-generated (K[X]) (ring-powers-set (K[X]) X)*

⟨*proof*⟩

end

locale *polynomial-away-X-localization =*

```

fixes  $R$  (structure) and  $P$  (structure) and  $S$  and  $K$ 
assumes poly-axioms: nagata-localization  $P$   $S$ 
  and base-axioms: domain  $R$ 
  and P-eq:  $P = K[X]$ 
  and S-eq:  $S = \text{ring-powers-set } (K[X])$   $X$ 
begin

```

```

abbreviation loc-ring where loc-ring  $\equiv$  eq-obj-rng-of-frac.rec-rng-of-frac  $P$   $S$ 

```

Once a localization of $K[X]$ at the powers of X has been fixed, Nagata's theorem reduces factoriality of $K[X]$ to factoriality of that localization, provided X is prime.

```

lemma polynomial-factorial-of-localized-X-factorial:
  assumes K: subring  $K$   $R$ 
    and noeth: noetherian-domain  $(K[X])$ 
    and hX: ring-prime $K[X]$   $X$ 
    and loc-fd: factorial-domain loc-ring
  shows factorial-domain  $(K[X])$ 
  <proof>

```

```

lemma polynomial-factorial-of-localized-X-factorial-field:
  assumes K: subfield  $K$   $R$ 
    and noeth: noetherian-domain  $(K[X])$ 
    and loc-fd: factorial-domain loc-ring
  shows factorial-domain  $(K[X])$ 
  <proof>

```

```

end

```

```

end

```

```

theory Fraction-Field-Applications

```

```

  imports

```

```

    Nagata-Lemmas

```

```

    Polynomial-Applications

```

```

    HOL-Algebra.Polynomial-Divisibility

```

```

begin

```

6 Constant-prime localization applications

This theory packages the constant-prime specialization of the polynomial application layer at the same level of abstraction as *Polynomial-Applications*: it specializes Nagata's theorem to multiplicative sets generated by constant prime polynomials and isolates the corresponding descent step for polynomial rings.

```

context domain

```

```

begin

```

lemma *polynomial-prime-generated-constant-closure*:
assumes *Ksub*: subring K R
and *A-sub*: $A \subseteq \text{carrier } (R \ (\!| \text{carrier} := K \!|))$
and *hprime*: $\bigwedge q. q \in A \implies \text{ring-prime}_{K[X]} \text{ (poly-of-const } q)$
shows
 $\text{ring-prime-generated } (K[X])$
 $(\text{ring-mult-submonoid-closure } (K[X]) \text{ (poly-of-const ' } A))$
 $\langle \text{proof} \rangle$

end

locale *polynomial-constant-prime-localization* =
fixes R (**structure**) **and** P (**structure**) **and** S **and** $K :: 'a \text{ set}$ **and** $A :: 'a \text{ set}$
assumes *poly-axioms*: nagata-localization P S
and *base-axioms*: domain R
and *P-eq*: $P = K[X]$
and *S-eq*: $S = \text{ring-mult-submonoid-closure } (K[X]) \text{ (ring.poly-of-const } (R \ (\!| \text{carrier} := K \!|)) \text{ ' } A)$
begin

abbreviation *const-poly* **where**
 $\text{const-poly} \equiv \text{ring.poly-of-const } (R \ (\!| \text{carrier} := K \!|))$

abbreviation *loc-ring* **where** $\text{loc-ring} \equiv \text{eq-obj-rng-of-frac.rec-rng-of-frac } P$ S

Once a localization of $K[X]$ at a constant-prime closure has been fixed, Nagata's theorem immediately reduces factoriality of $K[X]$ to factoriality of that localization.

lemma *polynomial-factorial-of-localized-constant-primes-factorial*:
assumes *Ksub*: subring K R
and *A-sub*: $A \subseteq \text{carrier } (R \ (\!| \text{carrier} := K \!|))$
and *noeth*: noetherian-domain $(K[X])$
and *hprime*: $\bigwedge q. q \in A \implies \text{ring-prime}_{K[X]} \text{ (const-poly } q)$
and *loc-fd*: factorial-domain *loc-ring*
shows factorial-domain $(K[X])$
 $\langle \text{proof} \rangle$

end

end

theory *Nagata-Factoriality*

imports

Prime-Generated

Nagata-Lemmas

Polynomial-Applications

Fraction-Field-Applications

HOL-Computational-Algebra.Polynomial

begin

7 Nagata-factoriality scaffolding

Nagata's factoriality theorem descends unique factorization from a localization to the base ring under a prime-generated hypothesis on the multiplicative set. The present entry now packages the prime-generated core, a wrapper layer over the AFP localization entry, and a record-based HOL-Algebra proof of both the prime-generated and prime-or-unit descent variants in *Nagata-Lemmas*. That theory now also packages theorem-level entry points for submonoid closures generated by prime families, including a finite-generator wrapper. The additional theories *Polynomial-Applications* and *Fraction-Field-Applications* package abstract polynomial applications for localization away X and for localizations generated by constant prime polynomials, cf. Nagata and Samuel.[2] [3]

lemma *prime-generated-constant-prime-polynomials:*

fixes $A :: 'a :: \text{semidom set}$

assumes $\bigwedge c. c \in A \implies \text{prime-elem } c$

shows *prime-generated* (*mult-submonoid-closure* $((\lambda c. [:c:]) \text{ ' } A)$)

<proof>

corollary *zero-notin-constant-prime-polynomial-closure:*

fixes $A :: 'a :: \text{idom set}$

assumes $\bigwedge c. c \in A \implies \text{prime-elem } c$

shows $0 \notin \text{mult-submonoid-closure } ((\lambda c. [:c:]) \text{ ' } A)$

<proof>

The last corollary isolates one of the key configurations in the constant-prime polynomial application: the multiplicative set generated by constant prime polynomials is prime-generated and therefore avoids zero.

Separately, the theory *Localization-Interface* exposes an Isabelle/HOL wrapper around the AFP localization construction with lemmas for representative equality, numerator-denominator surjectivity, denominator rescaling, cross-multiplication in the domain case, units coming from both the multiplicative set and base-ring units, and injectivity of the canonical localization map under the usual domain hypotheses. On top of that, *Nagata-Lemmas* proves the descent lemmas needed for Nagata's theorem, together with a record-based multiplicative-closure API

$\llbracket \text{ring } ?R; ?A \subseteq \text{carrier } ?R; \bigwedge q. q \in ?A \implies \text{ring-prime } ?R \ q \rrbracket$
 $\implies \text{ring-prime-generated } ?R (\text{ring-mult-submonoid-closure } ?R \ ?A)$

for the constant-prime submonoids used in the fraction-field route, culminating in theorem statements

$\llbracket \text{nagata-localization } ?R \ ?S; \text{noetherian-domain } ?R; \rrbracket$

ring-prime-generated ?R ?S;
factorial-domain (eq-obj-rng-of-frac.rec-rng-of-frac ?R ?S)]
 \implies *factorial-domain* ?R

and

[[*nagata-localization* ?R ?S; *noetherian-domain* ?R;
 $\bigwedge s. s \in ?S \implies$ *ring-prime*_{?R} s \vee s \in *Units* ?R;
factorial-domain (eq-obj-rng-of-frac.rec-rng-of-frac ?R ?S)]
 \implies *factorial-domain* ?R

together with the prime-generator closure wrappers

[[*nagata-localization* ?R ?S; *noetherian-domain* ?R;
?S = *ring-mult-submonoid-closure* ?R ?A; ?A \subseteq *carrier* ?R;
 $\bigwedge q. q \in ?A \implies$ *ring-prime*_{?R} q;
factorial-domain (eq-obj-rng-of-frac.rec-rng-of-frac ?R ?S)]
 \implies *factorial-domain* ?R

and

[[*nagata-localization* ?R ?S; *noetherian-domain* ?R; *finite* ?A;
?S = *ring-mult-submonoid-closure* ?R ?A; ?A \subseteq *carrier* ?R;
 $\bigwedge q. q \in ?A \implies$ *ring-prime*_{?R} q;
factorial-domain (eq-obj-rng-of-frac.rec-rng-of-frac ?R ?S)]
 \implies *factorial-domain* ?R

. The theory *Polynomial-Applications* then specializes this framework to the polynomial ring case by proving

[[*domain* ?R; *subfield* ?K ?R]] \implies *pprime*_{?R} ?K X ?R

over fields and the abstract away-X descent theorem

[[*polynomial-away-X-localization* ?R ?P ?S ?K; *subring* ?K ?R;
noetherian-domain (?K [X] ?R); *pprime*_{?R} ?K X ?R;
factorial-domain (eq-obj-rng-of-frac.rec-rng-of-frac ?P ?S)]
 \implies *factorial-domain* (?K [X] ?R)

, while *Fraction-Field-Applications* packages the companion constant-prime closure theorem

[[*polynomial-constant-prime-localization* ?R ?P ?S ?K ?A; *subring* ?K ?R;
?A \subseteq *carrier* (?R(|*carrier* := ?K)); *noetherian-domain* (?K [X] ?R);
 $\bigwedge q. q \in ?A \implies$ *pprime*_{?R} ?K (*ring.poly-of-const* (?R(|*carrier* := ?K)) q);
factorial-domain (eq-obj-rng-of-frac.rec-rng-of-frac ?P ?S)]
 \implies *factorial-domain* (?K [X] ?R)

.

end

References

- [1] H. Matsumura. *Commutative Ring Theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.
- [2] M. Nagata. *Local Rings*, volume 13 of *Interscience Tracts in Pure and Applied Mathematics*. Interscience Publishers, New York, 1962.
- [3] P. Samuel. *Lectures on Unique Factorization Domains*, volume 30 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1964.