Regular Paper

イデアルの準素分解

On Primary Decomposition

渡瀬 泰成 [1,*]
Yasushige Watase[1,*]

1 東京都杉並区松ノ木 3-21-6

* yasushige.watase@gmail.com

Proof checked by Mizar Version: 8.1.14 and MML Version: 5.76.1452
Received: December 15, 2023. Accepted: March 15, 2024.

要約

We formalized the so-called Primary Decomposition of Ideal appeared in the chapter 4 of [1]. we call an ideal $\mathfrak{a}$ of a commutative ring with the unit element, has a primary decomposition when such a finite set of primary ideals $\{\mathfrak{q}_i\}$ that $\mathfrak{a} = \cap\{\mathfrak{q}_i\}$ holds. A decomposition is called minimal when $\sqrt{\mathfrak{q}_\mathfrak{i}}$ are all distinct and $\mathfrak{q}_\mathfrak{i} \not\supseteq \bigcap_{j\neq i}^{n} \mathfrak{q}_j$ hold. This paper describes process of developing formal proofs for existence of a primary decomposition and its minimality.

1 序論

イデアルの分解とは数の素因数分解や整数環のイデアル分解 ($(6) = (2)\cap(3)$) と類似の概念である．イデアル $\mathfrak{a}$ の分解は $\mathfrak{a}$ とは異なるイデアル $\mathfrak{b}, \mathfrak{c}$ の共通部分に等しい ($\mathfrak{a} = \mathfrak{b}\cap\mathfrak{c}$) ときに $\mathfrak{a}$ は $\mathfrak{b}$ と $\mathfrak{c}$ に分解されると考える．整数環では素イデアルが極大イデアルであり，極大イデアルは準素イデアルとなることが知られているので素因数分解は準素分解の例となる．一般の可換環の場合，有限個の準素イデアル $\{\mathfrak{q}_\mathfrak{i}\}$ の共通部分によりイデアルの分解されていることを準素分解という．準素分解があれば分解の成分である $\{\mathfrak{q}_\mathfrak{i}\}$ 元の数を最小化した最短表現（言い換えれば 1 つでも分解の成分が欠けると分解を成さない.）が存在する．準素分解で重要な内容は, 与えられた準素分解から最短表現を構成する手順が存在すること, 及び最短表現の一意性と言われる準素分解成分の根基をとり出現する素イデアル（素因子）達は準素分解によらないという性質である．これらの内容の形式化が本稿の目的となる．形式化は一般の可換環でのイデアルの準素分解を文献 [1] を参考にして実施した．

2 準備

以下本稿では可換環といえば単位元を持つ非自明な環を指し A で表す．イデアルはドイツ文字 $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{p}, \mathfrak{q}...)$ を用い $\mathfrak{I}\,(A)$ は環 A のすべてのイデアルからなる集合を表す．$\mathfrak{P}$ は冪集合をとる場合用いる．イデアルの有限集合 $\{\mathfrak{q}_i \mid i \in I, I(\text{有限添数集合})\}$ を $\{\mathfrak{q}_i\}$ と略記する．

2.1 半順序集合に関する準備

$\mathfrak{I}$ にはイデアルが包含関係に関し反射的かつ推移的かつ反対称的を満たすので半順序の構造が入り $(\mathfrak{I}, <) = (\#\mathfrak{I}, \mathrm{RelIncl}(\mathfrak{I})\#)$ と Mizar にて形式化される．この事実によって $(\mathfrak{I}, <)$ に極大イデアルが存在することが Zorn の補題を用いて証明される．イデアルの束はイデアル論の証明で重要な役割をはたしている．以下では本論で有用となる一般の半順序集合 (X, R) で成り立つ性質を述べる．(ここで X は集合で R は X 上の関係である.)

性質 2.1. (既に Mizar で形式化されている事項はそのアーティクルと定理の番号を附した．今回形式化した定理や定義はアーティクル名として IDEAL3 として引用した.)

(i) $\mathrm{Poset}(\mathrm{X}, \mathrm{R})$ の有限集合は極小元を持つ．（cf. BAGORDER:7）．

(ii) 極小元の表現は述語，「半順序集合 X の部分集合 M における極小元 $x0$」は次のように形式化される：$x0$ is_minimal_wrt $M, \mathrm{RelIncl}(X)$. (cf. WAYBEL_4 : def 25).

(iii) Poset の有限部分集合 M 中の極小元のなす集合は minimals(M) として形式化される．(cf. DILWORTH:def 9).

(iv) Poset X の部分集合 S の任意の元よりも大なる X の元全体を UpperCone S と表記する．

(v) $\mathfrak{I}(A)$ の部分集合 S に対して $(\mathrm{S}, \subset)$ は半順序集合となる．

Poset X の部分集合を S として minimals(S) と UpperCone(S) を利用して以下の定理が成り立つ．

定理 2.1 (補題 6.1)**.** Upper を以下の様に定義する．(cf. IDEAL_3:def 9)

$$\begin{array}{cccc} \mathrm{Upper}: & \mathrm{minimals}(S) & \longrightarrow & \mathfrak{P}(S) \\ & \Psi & & \Psi \\ & x & \longmapsto & \mathrm{UpperCone}\{x\} \cup \{x\} \end{array}$$

この時

$$\bigcup \mathrm{Upper}(S) = S$$

が成り立つ．(cf. IDEAL_3:30)

2.2 イデアルに関する定義や性質

性質 2.2. ここではイデアルの既約, 準素イデアルの定義と性質を述べる.

以下 $\mathfrak{a}, \mathfrak{b}, \mathfrak{q}, \mathfrak{m}$ は任意の A のイデアルとする.

(*i*) $\mathfrak{a}$ が既約であるとは
$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ となる $\mathfrak{a}$ を含むイデアル $\mathfrak{b}, \mathfrak{c}$ が存在しない.

(*ii*) $\mathfrak{q}$ が準素イデアルとは
$xy \in \mathfrak{q} \Longrightarrow x \in \mathfrak{q} \vee \exists n \in N \ st \ y^n \in \mathfrak{q}$ (cf. IDEAL_2 : def 4).

(*iii*) $\mathfrak{a}$ の $\mathfrak{b}$ の商 $(\mathfrak{a} \colon \mathfrak{b})$ は以下の集合で定まるイデアルである. Mizar では $(\mathfrak{a} \ \% \ \mathfrak{b})$ と表記する.

$$(\mathfrak{a} \colon \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\} \quad \text{(cf. IDEAL\_1 : def 23).}$$

(iv) $\mathfrak{a}$ の根基 $\sqrt{\mathfrak{a}}$ は以下の集合で定まるイデアルである.

$$\sqrt{\mathfrak{a}} = \{x \in A \colon x^k \in \mathfrak{a} \text{ for some } k \in \mathbb{N}\} \quad \text{(cf. IDEAL\_1 : def 24).}$$

(v) $\mathfrak{q}$ が準素イデアルのとき $\sqrt{\mathfrak{q}}$ は素イデアルとなり, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ なるとき $\mathfrak{q}$ を $\mathfrak{p}$-準素, または $\mathfrak{p}$-primary という. (cf. IDEAL_2 : def 6).

(vi) $\sqrt{\mathfrak{a}} = \cap\{\mathfrak{p}' \mid \mathfrak{p}' \in SpecA, \mathfrak{a} \subset \mathfrak{p}'\}$ が成り立つので (cf. TOPZARI1:18), $\mathfrak{q}$ が $\mathfrak{p}$-準素ならば $\mathfrak{p}$ は $\mathfrak{q}$ を含む最小の素イデアルである.

(vii) $\sqrt{\mathfrak{a}}$ が極大イデアルならば $\mathfrak{a}$ は準素イデアル. (cf. IDEAL_2 : 23).

(viii) $\mathfrak{m}$ を極大イデアル, n を正の整数とする. $\mathfrak{m}^n$ は準素イデアル. (cf. IDEAL_2 : 35).

(ix) 有限個の準素イデアルの共通部分はまた準素イデアルとなる. (cf. IDEAL_2 : def 6).

定義 2.1. イデアル $\mathfrak{b}$ を固定して写像 $(\%\mathfrak{b}) \colon \mathfrak{I}(A) \to \mathfrak{I}(A)$ を以下の様に定義する.

$$\begin{array}{cccc} (\%\mathfrak{b})\colon & \mathrm{Ideal}(A) & \longrightarrow & \mathrm{Ideal}(A) \\ & \Cup & & \Cup \\ & \mathfrak{b} & \longmapsto & (\mathfrak{a} \colon \mathfrak{b}) \end{array}$$

この写像は $\mathfrak{P}(\mathfrak{I}(A))$ から $\mathfrak{P}(\mathfrak{I}(A))$ への写像 $\{\mathfrak{a}_i\} \longrightarrow \{(\mathfrak{a}_{\mathrm{i}} \colon \mathfrak{b})\}$ を誘導する.

定義 2.2. 写像 sqrt(A) を以下の様に定義する.

$$\begin{array}{cccc} \mathrm{sqrt(A)}\colon & \mathrm{Ideal}(A) & \longrightarrow & \mathrm{Ideal}(A) \\ & \Cup & & \Cup \\ & \mathfrak{a} & \longmapsto & \sqrt{\mathfrak{a}} \end{array}$$

この写像は $\mathfrak{P}(\mathfrak{I}(A))$ から $\mathfrak{P}(\mathfrak{I}(A))$ への写像 $\{\mathfrak{a}_i\} \longrightarrow \{\sqrt{\mathfrak{a}_i}\}$ を誘導する.

3 準素分解

3.1 準素分解の形式化状況

Mizar 以外の定理証明系 (PVS), Mizar, Isabelle HOL, LEAN でのイデアルの分解に関する形式化の状況を簡単に言及する．一分解整域 UFD の既約元による分解はいずれの PVS で形式化されている．イデアルの分解は LEAN におけるデデキント整域でのイデアル分解を モノイドの一意分解の特殊な場合として形式化している [2]. 本稿で扱っている準素分解は整域を仮定していない可換環での議論であり Mizar 以外の定理証明系での形式化はない．代数多様体の既約成分もイデアルの分解と同様の内容であり代数幾何の分野での既存形式化を Isabelle HOL で調べたがスキーム論の形式化に重きを置き具体的な準素分解には言及はない [3]. Mizar ではアフィン代数的集合を扱った [4] に代数的集合の既約成分が素イデアルとなることの形式化がある．高階論理に基礎を置く Isabelle HOL でのスキーム論の構成では位相空間の圏から環の圏への関手である層の形式化を主に扱いスキーム論以前の代数曲線や曲面のような多項式環を対象とした形式化は無いのが現状である．

3.2 準素分解の概要

イデアル $\mathfrak{a}$ が有限個の準素イデアル $\{\mathfrak{q}_\mathfrak{i}\}$ の共通部分に等しくなるときイデアルは準素イデアルにより分解されるという．$\{\mathfrak{q}_\mathfrak{i}\}$ の根基を取って現れる素イデアル $\{\mathfrak{q}_\mathfrak{i}\}$ を通常 $\mathfrak{a}$ の素因子と呼ぶ．本編では特に $\mathfrak{a}$ の分解に現れる $\{\mathfrak{q}_\mathfrak{i}\}$ を準素因子と呼ぶこととする．任意のイデアルが準素分解を持つとは限らない事が知られており準素分解を持つイデアルを準素分解可能という．これらを定義としてまとめる．

定義 3.1. イデアル $\mathfrak{a}$ が準素分解可能とは準素イデアルからなる有限集合 $\{\mathfrak{q}_i\}$ が存在し $\mathfrak{a} = \cap\{\mathfrak{q}_i\}$ が成り立つことをいう．

準素分解はイデアル $\mathfrak{a}$ の根基の素因子分解を与えている．この説明には次の定理が必要である．

定理 3.1. 任意のイデアルの有限列 F_i に対して，

$$\sqrt{\cap\{\mathfrak{q}_i\}} = \cap\sqrt{\mathfrak{q}_i}$$

が成り立つ．

定理を準素分解可能なイデアル $\mathfrak{a}$ に適応すると

$$\sqrt{\mathfrak{a}} = \cap\sqrt{\mathfrak{q}_i}$$

が成り立ち準素イデアルの根基が素イデアルとなり $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ と置くと

$$\sqrt{\mathfrak{a}} = \cap\mathfrak{p}_i$$

となる．$\mathfrak{p}_i$ を素因子と呼ぶ．$\mathfrak{a}$ の根基が $\mathfrak{p}_i$ により素因子分解されたことが分かる．しかしながら素因子の $\mathfrak{p}_i$ には重複があり得るので重複を持たない様に所与の $\{\mathfrak{q}_i\}$ を変形して重複ない準素イデアルの集合 $\{\tilde{\mathfrak{q}}_k\}$ を構成する．重複ばかりでなく更に $\{\tilde{\mathfrak{q}}_k\}$ には以下に定義する最短であることを課す．

定義 3.2. 準素分解可能イデアル $\mathfrak{a}$ の準素分解 $\mathfrak{q}_i$ が最短であるとは， (cf. IDEAL_3:def 17)

(i) $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ $(i \neq j)$ これを radical-distinct と呼ぶ.

(ii) $\mathfrak{q}_\mathrm{i} \not\supseteq \bigcap_{j\neq i}^{n} \mathfrak{q}_j$

を満たすときを云う．これは最短な分解は１つでも準素因子が欠けると共通部分が $\mathfrak{a}$ と成らないことを意味している．

以上の準素イデアルの分解をつぎの３つの段階に分けて形式化を行う.

1) 素因子の集合を構成

2) 最短条件 i) の実現.

3) 最短条件 ii) の実現.

素因子の重複ない表現の形式化と最短条件を達成するのかが当面の課題となる．解決の手順の概略は文献 [1] の 51 頁の最後の段落から 52 頁の最初の段落に示されているのでこれに従うが手順を具体化するには幾らかの関数の準備が必要となる．即ち第 1 段階の重複のない素因子の表現は準素因子の写像 sqrt(A) による像として重複を取り除く．最短条件 i) の実現のためには素因子毎に根基を取ってその因子となる準素因子をグループ化しグループ毎に準素因子の共通部分をとり新たな準素因子を構成する．最短条件 ii) の実現に新たな構成した準素因子を組み合わせ的に余分な因子を除く手順を関数化して形式化する.

3.3 準素分解の形式化

3.3.1 素因子の重複の除去

準素分解可能なイデアル $\mathfrak{a}$ で $\{\mathfrak{q}_\mathrm{i}\}$ が準素因子のとき,

定義 3.3. $\sqrt{\mathfrak{q}_\mathrm{i}} = \mathfrak{p}_\mathrm{i}$ と置き関数 $\mathrm{sqrt}(A)$ による集合 $\{\mathfrak{q}_\mathrm{i}\}$ の像は相異なる素イデアルからなる集合となりこれを prime_divset($\mathfrak{q}_\mathrm{i}$) と表記する.

従って prime_divset($\mathfrak{q}_\mathrm{i}$) $= \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k\}$ が素因子となり形式化は以下の通りである.

Listing 1. IDEAL_3:def 4 - Def.4

```
definition
  let A;
  let q be non empty finite Subset of PRIMARY(A);
  func prime_divset(q) -> non empty finite Subset of Spectrum A equals
::IDEAL_3:def 4
  (sqrt(A)).:q;
end;
```

3.3.2 最短条件 i) の実現.

イデアル $\mathfrak{a}$ の準素因子を $\{\mathfrak{q}_\mathrm{i}\}$ とする. $\{\mathfrak{q}_\mathrm{i}\}$ の元の根基をとって等しくなるものを集めてグループ分けを以下で定義する写像 PFactors よって行う. 別々のグループから元を取って $\mathfrak{q}_1, \mathfrak{q}_2$ とすると $\sqrt{\mathfrak{q}_1} \neq \sqrt{\mathfrak{q}_2}$ となっている.

定義 3.4. 準素分解可能イデアル $\mathfrak{a} = \cap \mathfrak{q}_i$ のとき, 単射 PFactors を定義する.

$$\begin{array}{cccc} \mathrm{PFactors}(\mathfrak{q}_\mathrm{i}): & \mathrm{prime\_divset}(\mathfrak{q}_\mathrm{i}) & \longrightarrow & \mathrm{PRIMARY}(A) \\ & \Cup & & \Cup \\ & \mathfrak{p} & \longmapsto & (\mathrm{sqrt(A)})^{-1}\mathfrak{p} \cap \{\mathfrak{q}_\mathrm{i}\} \end{array}$$

集合で書き下せば以下の様に成っており実質 $\{\mathfrak{q}_i\}$ を素因子 $\mathfrak{p}$ の順に並び替えたもに成っている.

$$\{\mathfrak{q}_i\} = \{\ \underbrace{\mathfrak{q}_{1_1} \cdots \mathfrak{q}_{1_r}}_{\substack{\mathfrak{p}_1-primary \\ =\mathrm{PFactors}(\mathfrak{p}_1)}}\ ,\ \underbrace{\mathfrak{q}_{2_1} \cdots \mathfrak{q}_{2_s}}_{\substack{\mathfrak{p}_2-primary \\ =\mathrm{PFactors}(\mathfrak{p}_2)}}\ , \cdots ,\ \underbrace{\mathfrak{q}_{k_1} \cdots \mathfrak{q}_{k_t}}_{\substack{\mathfrak{p}_k-primary \\ =\mathrm{PFactors}(\mathfrak{p}_k)}}\ \}$$

PFactors の形式化は以下の通りである.

Listing 2. IDEAL_3:def 5 - Def.5

```
  let A;
  let q be non empty finite Subset of PRIMARY(A);
  func PFactors(q) −> Function of prime_divset(q), bool PRIMARY(A) means
:: IDEAL_3:def 5
  for x be Element of prime_divset(q) holds ex p1 be prime Ideal of A st
  x = p1 & it.x = (sqrt(A))"{p1} /\ q;
  end;
```

次に性質 2.2. vii) を利用すると PFactors で分けられた $\mathfrak{p}_j$-primary グループの共通部分を取ると $\cap\{\mathfrak{q}_{i_1} \cdots \mathfrak{q}_{i_j}\}$ は再び $\mathfrak{p}_j$-primary イデアルとなる. これを $\tilde{\mathfrak{q}}_j$ と表す. 各グループの共通部分をとると新たに準素イデアルの集合 $\{\tilde{\mathfrak{q}}_j\}$ が出来上がる. これがもとの $\mathfrak{a}$ の準素分解になることも証明され $k \neq j$ ならば $\sqrt{\tilde{\mathfrak{q}}_j} \neq \sqrt{\tilde{\mathfrak{q}}_k}$ が成り立ち最短条件 i) が実現する. 素因子から対応するグループの共通部分を取る写像 Red を以下の様に定義する.

定義 3.5. 更に単射 PFactors を利用して単射 Red 定義する.

$$\begin{array}{cccc} \mathrm{Red}(\mathfrak{q}_\mathrm{i}): & \mathrm{prime\_divset}(\mathfrak{q}_\mathrm{i}) & \longrightarrow & \mathrm{PRIMARY}(A) \\ & \Cup & & \Cup \\ & \mathfrak{p} & \longmapsto & \cap(\mathrm{PFactors})(\mathfrak{p}) \end{array}$$

Listing 3. IDEAL_3:def 6 - Def 6

```
definition
   let A;
   let q be non empty finite Subset of PRIMARY(A);
   func Red(q) −> Function of prime_divset(q), PRIMARY(A) means
:: IDEAL_3:def 6
   for x be Element of prime_divset(q) holds it.x = meet((PFactors(q)).x);
end;
```

準素因子 $\{\mathfrak{q}_i\}$ の写像 Red による像は以下の様になる.

$$\mathrm{Red}\{\mathfrak{q}_i\} = \{ \underbrace{\cap\{\mathfrak{q}_{1_1}\cdots\mathfrak{q}_{1_j}\}}_{\tilde{\mathfrak{q}_1}}, \underbrace{\cap\{\mathfrak{q}_{2_1}\cdots\mathfrak{q}_{2_s}\}}_{\tilde{\mathfrak{q}_2}}, \cdots, \underbrace{\cap\{\mathfrak{q}_{k_1}\cdots\mathfrak{q}_{k_t}\}}_{\tilde{\mathfrak{q}_k}}\}$$

片々根基を取ると $\mathfrak{q} = \cap\{\tilde{\mathfrak{q}}_j\}$ となり $\{\tilde{\mathfrak{q}}_j\}$ が準素分解となり，且また最短条件 i) を実現している．このことを定理として以下の様に形式化した.

定理 3.2.

$$\cap\{\mathfrak{q}_i\} = \cap\mathrm{Red}_{\mathfrak{p}_k\in\mathrm{prime\_divset}(\mathfrak{q})}(\mathfrak{p}_k)$$

が成り立つ.

Listing 4. IDEAL_3:27 - Th.27

```
theorem :: IDEAL_3:27
  for q be non empty finite Subset of PRIMARY(A) holds
  meet q = meet rng Red(q);
```

$\{\tilde{\mathfrak{q}}_j\}$ の作り方から最短条件 i) を満たしている．ここで更に集合 $\{\tilde{\mathfrak{q}}_j\}$ の極小元から成る集合を定義すると, これもまた準素分解を与え最短条件 i) を満たすので出来るだけ取り回しの良い簡約した準素分解を構成することが出来る.

定義 3.6. $\{\mathfrak{q}_i\}$ を準素イデアルの集合として写像 Red の像 $\{\tilde{\mathfrak{q}}_j\}$ を包含関係による半順序集合となり $\{\tilde{\mathfrak{q}}_j\}$ の極小元から成る集合を $\mathrm{minimalRed}(\mathfrak{q}_\mathrm{i})$ と定義する.

Listing 5. IDEAL_3:def 18 - Def.18

```
definition
  let A;
  let q be non empty finite Subset of PRIMARY(A);
  func minimalRed(q) −> non empty finite Subset of Ideals(A) equals
:: IDEAL_3:def 18
  minimals(RelStr(# rng Red(q),RelIncl(rng Red(q)) #));
end;
```

$\mathrm{minimalRed}(\mathfrak{q}_\mathrm{i})$ を用いると以下の定理が成り立つ.

定理 3.3. 任意の準素イデアルの有限集合 $\{\mathfrak{q}_\mathrm{i}\}$ に対して,

$$\cap\{\mathfrak{q}_\mathrm{i}\} = \cap\mathrm{minimalRed}(\mathfrak{q}_\mathrm{i})$$

が成り立ち $\mathrm{minimalRed}(\mathfrak{q}_\mathrm{i})$ が準素分解を与えている事を示している.

定理 3.4. 任意の準素イデアルの有限集合 $\{\mathfrak{q}_\mathrm{i}\}$ に対して,

$\mathrm{minimalRed}(\mathfrak{q}_\mathrm{i})$ は radicaldistinct.

が成り立つ.

定理の形式化例：

Listing 6. IDEAL_3:43 - Th.43

```
theorem :: IDEAL_3:43
  for q be non empty finite Subset of PRIMARY(A)
  holds minimalRed(q) is radical−distinct;
```

定理 3.3, 3.4 により 最短条件 i) を満たす準素分解 $\mathrm{minimalRed}(\mathfrak{q}_\mathrm{i})$ が構成された.

3.3.3 最短条件 ii) の実現．

前節で $\mathfrak{a} = \cap\{\tilde{\mathfrak{q}}_j\}$ が成り立つこと最短条件 i) を満たすことをみたので， $\mathfrak{a} \neq \cap_{i\neq j}\{\tilde{\mathfrak{q}}_j\}$ の証明が残った．極小元の共通部分を扱うので極小性から他の理論例えば束論を援用しての証明を模索したが解決出来なかった．最短条件 ii) の実現のため以下の手順を遂行すればよい．

手順 1. *Set* $N = \sharp\{\tilde{\mathfrak{q}}_j\}$, $i = 1$;
while $i \leq N$;
  if $\mathfrak{a} = \cap_{i\neq j}\{\tilde{\mathfrak{q}}_j\}$ *then Swap* $\tilde{\mathfrak{q}}_j$ *to A* $\wedge$ i++
  else $i++$;
end;

この手順は有限のイデアルの集合として以下の２つの関数により実現する．

Listing 7. IDEAL_3:def 26 - Def.26

```
definition
  let A;
  let n be Nat;
  let S be Element of (Ideals A)* ;
  func Trimming(S,n) -> Function of (Ideals A)* , (Ideals A)* means
:: IDEAL_3:def 26
  for x be Element of (Ideals A)* holds it.x = Trimming(x);
end;
```

有限集合を計算しやすいように入力を有限列にして手順１．を帰納的に以下の関数で定義する．

Listing 8. IDEAL_3:def 25 - Def.25

```
definition
  let A;
  let S be Element of (Ideals A)* ;
  func Trimming(S) -> Element of (Ideals A)* equals
:: IDEAL_3:def 25
  (Del(S,1))^<*(the carrier of A)*> if meet(rng Del(S,1)) = meet rng S
  otherwise (Del(S,1))^<*S.1*>;
end;
```

この手順の正当性を証明するればすくとも最短条件 ii) を満足する分解が得られる．

4 考察

前章の 3.3.3. で言及したが, イデアル $\mathfrak{a}$ の準素分解で準素因子が極小元で分解が表現された場合は既に最短表現（分解の因子が 1 つでも欠けると分解にならない）になっていると予想していたが証明には至らなかった．この原因は詳細に分析していないが, 極小元を準備して分解を構成した主な理由は分解を保ちながら準素因子の数を減らす為で最短条件 i) の証明では効果的であったが最短条件 ii) では巧く機能しなかった．
いま $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ を $\mathfrak{a}$ の準素分解の素因子とするとき, $\mathfrak{p}_1$ が素因子の中で極小元であるとき $\mathfrak{p}_2$ は埋没因子という．準素因子 $\mathfrak{q}_1$，$\mathfrak{q}_2$ がそれぞれ $\mathfrak{p}_1$-primary と $\mathfrak{p}_2$-primary であったとすると根基を取ると $\mathfrak{p}_2$ は $\sqrt{\mathfrak{a}}$ の素因子には現れず埋没する．準素因子で考えると $\mathfrak{q}_2$ が欠けていてもいいのか，欠くことが出来ないのか代数の計算で判断出来ない（出来なかった）

ので一つ一つ準素因子取り除いて分解が保たれているか判定ルーチンが入用となり前章の手順１を必要とした．20 世紀初頭の数学証明は手順１の様な構成的なものが見受けられ（クロネッカーの多変数多項式の既約分解のアルゴリズム等）, 20 世紀初頭のイデアル論, 整数論の証明においては Mizar で形式化が出来ることが多いと思われる．

今後は手順１の正当性の証明．本稿では含まなかったが一意性定理, イデアル $\mathfrak{a}$ に対し異なる最短な分解があってもそれらの素因子は同一であることを示した定理である．これも大事な定理であり形式化を行う．

参考文献

[1] Atiyah MF, Macdonald IG. Introduction to Commutative Algebra. vol. 2. Addison-Wesley Reading; 1969.

[2] Baanen A, Dahmen SR, Narayanan A, di Capriglio FAENMM. A Formalization of Dedekind Domains and Class Groups of Global Fields. J Autom Reason. 2022;66(4):611–637. Available from: `https://doi.org/10.1007/s10817-022-09644-0`.

[3] Ballarin C, (Editor), et al. The Isabelle/HOL Algebra Library. 2023;Available from: `https://isabelle.in.tum.de/library/HOL/HOL-Algebra/outline.pdf`.

[4] Watase Y. Introduction to Algebraic Geometry. Formaliz Math. 2023;31(1):67–73. Available from: `https://doi.org/10.2478/forma-2023-0007`.

Mizar article information

Mizar Mathematical Library (MML)

Works in Progress

IDEAL_3 On Primay Ideal Decomposition
by Y.Watase

We formalized the so-called Primary Decomposition of Ideal appeared in the chapter 4 of [1]. we call an ideal $\mathfrak{a}$ of a commutative ring with the unit element, has a primary decomposition when such a finite set of primary ideals $\{\mathfrak{q}_i\}$ that $\mathfrak{a} = \cap\{\mathfrak{q}_i\}$ holds. A decomposition is called minimal when $\sqrt{\mathfrak{q}_\mathfrak{i}}$ are all distinct and $\mathfrak{q}_\mathfrak{i} \not\supseteq \bigcap_{j\neq i}^{n} \mathfrak{q}_j$ hold. This paper describes process of developing formal proofs for existence of a primary decomposition and its minimality.

Listing 9. IDEAL_3 - abstract

```
:: On Primary Ideals. {P}art {II}
:: by Yasushige Watase
::
:: Received June 30, 2021
:: Copyright (c) 2021-2023 Association of Mizar Users
:: (Stowarzyszenie Uzytkownikow Mizara, Bialystok, Poland).
:: This code can be distributed under the GNU General Public Licence
:: version 3.0 or later, or the Creative Commons Attribution-ShareAlike
```

environ

vocabularies ARYTM_3, FUNCT_1, RELAT_1, CARD_3, XBOOLE_0, TARSKI, XCMPLX_0, STRUCT_0, SUBSET_1, SUPINF_2, NAT_1, CARD_1, ARYTM_1, FINSEQ_1, SETFAM_1, INT_2, BINOP_1, GROUP_4, NUMBERS, IDEAL_1, ZFMISC_1, FUNCSDOM, CARD_FIL, SQUARE_1, RING_2, XXREAL_0, TOPZARI1, LATTICEA, PARTFUN1, IDEAL_2, INT_3, ORDINAL4, LATTICE3, CHORD, FINSEQ_3, MOEBIUS1, UPROOTS, FINSET_1, FSM_1, MATROID0, TERMORD, WAYBEL_4, WELLORD2, DILWORTH, JORDAN4, ORDERS_2, ORDERS_1,
IDEAL_3;

notations TARSKI, XBOOLE_0, SUBSET_1, SETFAM_1, FUNCT_1, RELAT_1, ORDINAL1, RELSET_1, PARTFUN1, WELLORD2, FUNCT_2, DOMAIN_1, FINSET_1, CARD_1, ORDERS_1, NUMBERS, XCMPLX_0, XXREAL_0, FINSEQ_1, EQREL_1, FINSEQ_2, FINSEQOP, FINSEQ_3, RVSUM_1, PRE_POLY, STRUCT_0, ALGSTR_0, ORDERS_2, RLVECT_1, GROUP_1, VECTSP_1, VECTSP_2, WAYBEL_4, YELLOW_1, GCD_1, VECTSP10, UPROOTS, INT_3, IDEAL_1, RING_1, DILWORTH, RING_2, TOPZARI1, IDEAL_2;

constructors RELSET_1, FINSEQOP, FINSOP_1, WSIERP_1, WAYBEL_4, GCD_1, DILWORTH, IDEAL_2;

registrations XBOOLE_0, ORDINAL1, RELSET_1, XREAL_0, NAT_1, STRUCT_0, CARD_1, VECTSP_1, ALGSTR_1, SUBSET_1, ALGSTR_0, IDEAL_1, RING_2, INT_3, RING_1, TOPZARI1, FINSEQ_1, FINSEQ_5, IDEAL_2, FINSET_1, FUNCT_2, RELAT_1, FOMODEL0, ORDERS_2;

requirements NUMERALS, SUBSET, BOOLE, ARITHM, REAL;

definitions TARSKI, IDEAL_1, STRUCT_0, XBOOLE_0,SUBSET_1;

equalities STRUCT_0, FINSEQ_1, ALGSTR_0;

expansions TARSKI, FUNCT_2, IDEAL_1, STRUCT_0, XBOOLE_0, SUBSET_1, TOPZARI1, FUNCT_1, RING_1;

theorems RLVECT_1, IDEAL_1, FUNCT_2, TARSKI, FUNCT_1, NAT_1, RING_1, XBOOLE_0, FINSEQ_1, ORDINAL1, XBOOLE_1, RING_2, RELAT_1, SETFAM_1, TOPZARI1, FINSEQ_5, PARTFUN1, FINSEQ_3, FINSEQ_2, TOPREALA, CARD_1, IDEAL_2, SUBSET_1, ZFMISC_1, FINSEQOP, TARSKI_0, CARD_2, CARD_FIN, SETWISEO, AOFA_L00, DILWORTH, WELLORD2, ORDERS_2,
WAYBEL_4, BAGORDER, ORDINAL6;

schemes NAT_1, RECDEF_1, FUNCT_2;

begin *:: Preliminaries: Some Properties of Ideals*

reserve R **for** commutative Ring;
reserve A **for non** degenerated commutative Ring;
reserve I,J,q **for** Ideal **of** A;
reserve M,M1,M2 **for** Ideal **of** A/q;

:: Generarization of ZMATRLIN:42
theorem *:: IDEAL_3:1*
for I **be** Ideal **of** A
for F **be** FinSequence **of** A
st for i **being** Nat **st** i in dom F **holds** F.i in I **holds** Sum F in I;

definition
let A;
func sqrt(A) −> Function **of** Ideals(A),Ideals(A) **means**
:: IDEAL_3:def 1

```
  for x be Element of Ideals (A) holds it.x = sqrt x;
end;

theorem :: IDEAL_3:2
    for I be Ideal of A, F be non empty FinSequence of Ideals(A) holds
    rng((%I)*F) <> {} & rng F <> {} &
    meet rng((%I)*F) c= the carrier of A;

::[AM]Ex.1.12. iv) (/\F_i % I) = /\(F_i % I)
theorem :: IDEAL_3:3
    for I be Ideal of A, F be non empty FinSequence of Ideals(A) holds
    (%I).(meet rng F) = meet rng((%I)*F);

theorem :: IDEAL_3:4
    for I be Ideal of A, F be non empty FinSequence of Ideals(A) holds
    rng((sqrt(A))*F) <> {} & rng F <> {};

registration
  let A;
  let a be non empty FinSequence of Ideals(A);
  cluster meet (rng a) -> add-closed left-ideal right-ideal for Subset of A;
end;

reserve x for object;

theorem :: IDEAL_3:5
   x in Ideals A iff x is Ideal of A;

theorem :: IDEAL_3:6
   x in PRIMARY(A) iff x is primary Ideal of A;

theorem :: IDEAL_3:7
    PRIMARY(A) c= Ideals (A);


theorem :: IDEAL_3:8
   x in Spectrum A iff x is prime Ideal of A;

theorem :: IDEAL_3:9
    for I be Ideal of A, F be non empty FinSequence of Ideals(A) holds
    (sqrt(A)).(meet rng F) = meet rng((sqrt(A))*F);

theorem :: IDEAL_3:10
    for I be Ideal of A, F be non empty FinSequence of Ideals(A) holds
    (%I)*F is non empty FinSequence of Ideals(A);

definition
  let A;
  let I be Ideal of A;
  attr I is primary_decomposable means
:: IDEAL_3:def 2

  ex q be non empty finite Subset of PRIMARY(A) st
  I = meet q;
end;


registration
  let A be non degenerated commutative Ring;
  cluster primary_decomposable for Ideal of A;
end;

definition
  let A;
  let I be primary_decomposable Ideal of A;
  let q be non empty finite Subset of PRIMARY(A);
  pred q is_a_primary_decomposition_of I means
:: IDEAL_3:def 3
```

```
  I = meet q;
end;

reserve F for FinSequence of Ideals(A);

::Th2SPEC2:
:: Spectrum(A) c= Ideals(A)

reserve x for Element of A,
        o for object;

definition
  let A;
  let q be non empty finite Subset of PRIMARY(A);
  func prime_divset(q) -> non empty finite Subset of Spectrum A equals
:: IDEAL_3:def 4

  (sqrt(A)).:q;
end;


definition
  let A;
  let q be non empty finite Subset of PRIMARY(A);
func PFactors(q) -> Function of prime_divset(q), bool PRIMARY(A) means
:: IDEAL_3:def 5

  for x be Element of prime_divset(q) holds ex p1 be prime Ideal of A st
  x = p1 & it.x = (sqrt(A))"{p1} /\ q;
  end;

theorem :: IDEAL_3:11
   for q be non empty finite Subset of PRIMARY(A),
   x1,x2 be Element of prime_divset(q) holds
   x1 <> x2 implies (PFactors(q)).x1 /\ (PFactors(q)).x2 = {};

registration
  let A;
  let q be non empty finite Subset of PRIMARY(A);
  cluster PFactors(q) -> one-to-one;
end;

theorem :: IDEAL_3:12
   for q be non empty finite Subset of PRIMARY(A) holds
   union(rng (PFactors(q))) = q;

theorem :: IDEAL_3:13
    for p1 be prime Ideal of A holds
    (sqrt(A))"{p1} /\ PRIMARY(A) = PRIMARY(A,p1);

theorem :: IDEAL_3:14
   for q be non empty finite Subset of PRIMARY(A),
   p be prime Ideal of A st p in prime_divset(q) holds
   (PFactors(q)).p is non empty finite Subset of PRIMARY(A,p) &
   (PFactors(q)).p = PRIMARY(A,p) /\ q;

theorem :: IDEAL_3:15
   for q be non empty finite Subset of PRIMARY(A),
   p be prime Ideal of A st p in prime_divset(q) holds
   meet((PFactors(q)).p) in PRIMARY(A,p);

definition
   let A;
   let q be non empty finite Subset of PRIMARY(A);
   func Red(q) -> Function of prime_divset(q), PRIMARY(A) means
:: IDEAL_3:def 6

   for x be Element of prime_divset(q) holds it.x = meet((PFactors(q)).x);
```

```
end;

theorem :: IDEAL_3:16
  for q be non empty finite Subset of PRIMARY(A),
  x1,x2 be Element of prime_divset(q) holds
  (Red(q)).x1 = (Red(q)).x2 implies x1 = x2;

registration
 let A;
 let q be non empty finite Subset of PRIMARY(A);
 cluster Red(q) -> one-to-one;
end;

theorem :: IDEAL_3:17
  for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
  p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
  p1 in prime_divset(q1) holds card (prime_divset(q1) \{p1}) = n;

::theorem Th9B:
:: for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
:: p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
:: p1 in prime_divset(q1) holds
:: not (PFactors(q1)).p1 c=
:: union rng((PFactors(q1))|(prime_divset(q1) \{p1}))

theorem :: IDEAL_3:18
  for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
  p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
  p1 in prime_divset(q1) holds
  rng((PFactors(q1))|(prime_divset(q1) \{p1})) /\ {(PFactors(q1)).p1} = {} &
  rng (PFactors(q1)) =
  rng((PFactors(q1))|(prime_divset(q1) \{p1})) \/ {(PFactors(q1)).p1};

theorem :: IDEAL_3:19
  for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
  p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
  p1 in prime_divset(q1) holds
  (PFactors(q1)).p1 misses union rng((PFactors(q1))|(prime_divset(q1) \{p1}));

theorem :: IDEAL_3:20
  for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
  p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
  p1 in prime_divset(q1) holds
  rng((Red(q1))|(prime_divset(q1) \{p1})) /\ {(Red(q1)).p1} = {} &
  rng (Red(q1)) = rng((Red(q1))|(prime_divset(q1) \{p1})) \/ {(Red(q1)).p1} &
  rng(Red(q1)) /\ {(Red(q1)).p1} = {(Red(q1)).p1} &
  rng (Red(q1)) \ {(Red(q1)).p1} = rng((Red(q1))|(prime_divset(q1) \{p1}));

theorem :: IDEAL_3:21
  for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
  p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
  p1 in prime_divset(q1) holds
  meet rng Red(q1)
   = meet rng((Red(q1))|(prime_divset(q1) \{p1})) /\ (Red(q1)).p1;

::theorem Th10A0:
:: for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
:: p1 be prime Ideal of A st card prime_divset(q1) = n+1 &
:: p1 in (prime_divset(q1)) holds
:: ex qn be non empty finite Subset of PRIMARY(A) st
:: (prime_divset(q1) \{p1}) = prime_divset(qn) &
:: qn = q1 \(PFactors(q1)).p1 &
:: PFactors(qn) = (PFactors(q1))|(prime_divset(q1) \{p1}) &
:: union rng(PFactors(qn)) = q1 \(PFactors(q1)).p1


definition
 let A;
```

```
  let q be non empty finite Subset of PRIMARY(A);
attr q is minlength means
:: IDEAL_3:def 7

  card q =1 or
  for q1 be Element of q holds meet(q \ {q1}) c/= q1;
end;

::theorem Th001:
:: for q1 be non empty finite Subset of PRIMARY(A), p1 be prime Ideal of A
:: st prime_divset(q1) = {p1} holds q1 c= PRIMARY(A,p1)

theorem :: IDEAL_3:22
   for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
   p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
   p1 in prime_divset(q1) holds card (prime_divset(q1) \{p1}) = n;

theorem :: IDEAL_3:23
   for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
   p1 be prime Ideal of A
   st card prime_divset(q1) = n+1 & p1 in (prime_divset(q1)) holds
   ex qn be non empty finite Subset of PRIMARY(A) st
   (prime_divset(q1) \{p1}) = prime_divset(qn) & qn = q1 \(PFactors(q1)).p1;

theorem :: IDEAL_3:24
   for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
   p1 be prime Ideal of A
   st card prime_divset(q1) = n+1 & p1 in (prime_divset(q1)) holds
   ex qn be non empty finite Subset of PRIMARY(A) st
   (prime_divset(q1) \{p1}) = prime_divset(qn) & qn = q1 \(PFactors(q1)).p1 &
   union rng((PFactors(q1))|(prime_divset(q1) \{p1})) = q1 \(PFactors(q1)).p1;

theorem :: IDEAL_3:25
   for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
   p1 be prime Ideal of A st card prime_divset(q1) = n+1 &
   p1 in (prime_divset(q1)) holds
   ex qn be non empty finite Subset of PRIMARY(A) st
   (prime_divset(q1) \{p1}) = prime_divset(qn) &
   qn = q1 \(PFactors(q1)).p1 &
   PFactors(qn) = (PFactors(q1))|(prime_divset(q1) \{p1}) &
   union rng(PFactors(qn)) = q1 \(PFactors(q1)).p1;

theorem :: IDEAL_3:26
    for q be non empty finite Subset of PRIMARY(A) holds
    meet (union(rng PFactors(q))) = meet rng Red(q);

::theorem Th9B:
:: for q1 be non empty finite Subset of PRIMARY(A), n be non zero Nat,
:: p1 be prime Ideal of A st card(prime_divset(q1)) = n+1 &
:: p1 in prime_divset(q1) holds
:: not (PFactors(q1)).p1 c=
:: union rng((PFactors(q1))|(prime_divset(q1) \{p1}))

theorem :: IDEAL_3:27
   for q be non empty finite Subset of PRIMARY(A) holds
   meet q = meet rng Red(q);

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


::theorem Th12:
:: for q be non empty finite Subset of PRIMARY(A) holds
:: meet minimals(InclPoset(rng Red(q))) = meet rng Red(q);


:: func UpperCone(S) -> Subset of A equals
:::: ORDERS_2:def 8
:: {a1 : for a2 st a2 in S holds a2 <
```

```
::theorem :: ORDERS_2:51
:: a is_minimal_in the InternalRel of A iff for b holds not b < a;


::theorem Th2K:
:: for S be non empty Subset of Ideals(A),
:: x be Element of RelStr(# S,RelIncl(S) #) holds
:: x in minimals(RelStr(# S,RelIncl(S) #)) implies
:: x is_minimal_in S & x is_minimal_wrt S,RelIncl(S)

theorem :: IDEAL_3:28
   for S be non empty finite Subset of Ideals(A) holds
   minimals(RelStr(# S,RelIncl(S) #)) <> {};

definition
   let A;
   let S be non empty finite Subset of Ideals(A);
   func minimals(S) -> non empty Subset of Ideals(A) equals
:: IDEAL_3:def 8

   minimals(RelStr(# S,RelIncl(S) #));
end;

definition
  let A;
  let S be non empty finite Subset of Ideals(A);
  func Upper(S) -> Function of minimals(S), bool S
  means
:: IDEAL_3:def 9

  for x be Element of minimals(S) holds
  ex x1 be Element of RelStr(# S,RelIncl(S) #) st
  x = x1 & it.x = UpperCone({x1}) \/ {x1};
end;

theorem :: IDEAL_3:29
   for S be non empty finite Subset of Ideals(A) holds
   Upper(S) is one-to-one;

registration
  let A;
  let S be non empty finite Subset of Ideals(A);
  cluster Upper(S) -> one-to-one;
end;

theorem :: IDEAL_3:30
   for S be non empty finite Subset of Ideals(A) holds
   union rng Upper(S) = S;

definition
   let A;
   let q be non empty finite Subset of PRIMARY(A);
   let a be Element of rng Red(q);
   func Lower(a) -> Subset of rng Red(q) equals
:: IDEAL_3:def 10

   {I where I is Element of rng Red(q) : I c< a };
end;

theorem :: IDEAL_3:31
   for S be non empty Subset of Ideals(A) holds
   RelStr(# S,RelIncl(S) #) is Poset;

definition
  let A;
  let S be non empty finite Subset of Spectrum A;
attr S is without-embedded-prime means
```

```
:: IDEAL_3:def 11

  for x,y be Element of S holds (x c/= y & y c/= x);
end;

definition
  let A;
  let q be non empty finite Subset of PRIMARY(A);
attr q is reduced means
:: IDEAL_3:def 12

  card q =1 or
  for q1 be Element of q holds meet(q \ {q1}) c/= q1;
end;

definition
  let A;
  let q be non empty finite Subset of PRIMARY(A);
attr q is radical-distinct means
:: IDEAL_3:def 13

  card q =1 or
  for q1,q2 be Element of q st q1 <> q2 holds ex I1,I2 be Ideal of A st
  q1 = I1 & q2 = I2 & sqrt I1 <> sqrt I2;
end;

definition
  let A;
  let S be non empty finite Subset of PRIMARY(A);
attr S is minimal means
:: IDEAL_3:def 14

  S is radical-distinct reduced or
  S is reduced radical-distinct;
end;

definition
  let A;
  let q be non empty finite Subset of Ideals(A);
attr q is reduced means
:: IDEAL_3:def 15

  card q =1 or
  for q1 be Element of q holds meet(q \ {q1}) c/= q1;
end;

definition
  let A;
  let q be non empty finite Subset of Ideals(A);
attr q is radical-distinct means
:: IDEAL_3:def 16

  card q =1 or
  for q1,q2 be Element of q st q1 <> q2 holds ex I1,I2 be Ideal of A st
  q1 = I1 & q2 = I2 & sqrt I1 <> sqrt I2;
end;

definition
  let A;
  let S be non empty finite Subset of Ideals(A);
attr S is minimal means
:: IDEAL_3:def 17

  S is radical-distinct reduced or
  S is reduced radical-distinct;
end;

::Lm12:
:: for q be non empty finite Subset of PRIMARY(A)
```

:: holds card(prime_divset(q)) is Nat

::theorem Th12:
:: for q be non empty finite Subset of PRIMARY(A)
:: holds prime_divset(q) = prime_divset(rng Red(q))

theorem *:: IDEAL_3:32*
for q **be non** empty finite Subset **of** PRIMARY(A)
st card(prime_divset(q)) > 1 **holds** rng Red(q) **is** radical−distinct;

theorem *:: IDEAL_3:33*
for q **be non** empty finite Subset **of** PRIMARY(A) **st** rng Red(q) <> {} **holds**
minimals(RelStr**(#** rng Red(q),RelIncl(rng Red(q)) #)) <> {} **&**
rng Red(q) **is non** empty finite Subset **of** Ideals(A);

definition
let A;
let q **be non** empty finite Subset **of** PRIMARY(A);
func minimalRed(q) **−>** **non** empty finite Subset **of** Ideals(A) **equals**
:: IDEAL_3:def 18

minimals(RelStr**(#** rng Red(q),RelIncl(rng Red(q)) #));
end;

definition
let A;
let q **be non** empty finite Subset **of** PRIMARY(A);
func RedRng(q) **−>** **non** empty finite Subset **of** Ideals(A) **equals**
:: IDEAL_3:def 19

rng Red(q);
end;

theorem *:: IDEAL_3:34*
for S **be non** empty finite Subset **of** Ideals(A),
a1 **be** Element **of** RelStr**(#** S,RelIncl(S) #) **st**
UpperCone({a1}) <> {}
holds a1 c= meet UpperCone({a1});

theorem *:: IDEAL_3:35*
for S **be non** empty finite Subset **of** Ideals(A),
a0 **be** Element **of** minimals(S) **holds** a0 = meet((Upper(S)).a0);

theorem *:: IDEAL_3:36*
for S **be non** empty finite Subset **of** Ideals(A),
a0 **be** Element **of** minimals(S), a **be set st** a in (Upper(S)).a0
holds a0 c= a;

theorem *:: IDEAL_3:37*
for q **be non** empty finite Subset **of** PRIMARY(A) **st**
card(minimals(RedRng(q))) = 1 **holds**
meet minimals(RedRng(q)) = meet (union rng Upper(RedRng(q)));

::theorem Th20Z:
:: for q be non empty finite Subset of PRIMARY(A),
:: a0 be Element of minimals(RedRng(q)) holds a0 = meet((Upper(RedRng(q))).a0)

theorem *:: IDEAL_3:38*
for S **be non** empty Subset **of** Ideals(A),
x **be** Element **of** RelStr**(#** S,RelIncl(S) #) **holds**
x in minimals(RelStr**(#** S,RelIncl(S) #)) **implies**
x is_minimal_in S **&** x is_minimal_wrt S,RelIncl(S);

theorem *:: IDEAL_3:39*
for q **be non** empty finite Subset **of** PRIMARY(A) **st** rng Red(q) <> {} **holds**
minimals(RelStr**(#** rng Red(q),RelIncl(rng Red(q)) #)) <> {} **&**
rng Red(q) **is non** empty finite Subset **of** Ideals(A);

```
theorem :: IDEAL_3:40
  for q be non empty finite Subset of PRIMARY(A)
  holds
  meet union(rng Upper(RedRng(q))) = meet minimalRed(q);

theorem :: IDEAL_3:41
  for q be non empty finite Subset of PRIMARY(A)
  holds meet q = meet minimalRed(q);

theorem :: IDEAL_3:42 :::::Copy from IDEAL_2, Th36
   for Q be primary Ideal of A holds
   sqrt Q is prime & for P be prime Ideal of A st Q c= P holds sqrt Q c= P;

theorem :: IDEAL_3:43
  for q be non empty finite Subset of PRIMARY(A)
  holds minimalRed(q) is radical-distinct;


theorem :: IDEAL_3:44
  for S be non empty finite Subset of Ideals(A),
  s1,s2 be Element of minimals(S) st s1 <> s2 holds
  ex x be Element of A st x in s1 \ s2;

theorem :: IDEAL_3:45
  for S be non empty finite Subset of Ideals(A),
  s1,s2 be Element of minimals(S) st s1 <> s2 holds
  s1 c/= s2 & s2 c/= s1;

:: non empty is important::::::::::
definition
 let A;
 let I be Ideal of A;
 attr I is primary_decomposable means
:: IDEAL_3:def 20

 ex q be non empty one-to-one FinSequence of PRIMARY(A) st
 I = meet rng q;
end;

registration
 let A be non degenerated commutative Ring;
 cluster primary_decomposable for Ideal of A;
end;

definition
 let A;
 let I be primary_decomposable Ideal of A;
 let q be non empty one-to-one FinSequence of PRIMARY(A);
 pred q is_a_primary_decomposition_of I means
:: IDEAL_3:def 21

 I = meet rng q;
end;

definition
 let A;
 let I be primary_decomposable Ideal of A;
 mode primary_decomposition of I -> non empty one-to-one
 FinSequence of PRIMARY(A) means
:: IDEAL_3:def 22

 I = meet rng it;
end;

definition
 let A;
 let I be primary_decomposable Ideal of A;
 mode primary_decomposition of I -> non empty one-to-one
 FinSequence of PRIMARY(A) means
```

```
:: IDEAL_3:def 23

  I = meet rng it;
end;


reserve I for primary_decomposable Ideal of A,
        S for primary_decomposition of I,
        x for Element of A,
        o for object;

definition
  let A;
  let S be non empty FinSequence of PRIMARY(A);
  func prime_div(S) -> non empty FinSequence of Spectrum A equals
:: IDEAL_3:def 24

  (sqrt(A))*S;
end;

definition
  let A;
  let S be Element of (Ideals A)* ;
  func Trimming(S) -> Element of (Ideals A)* equals
:: IDEAL_3:def 25

  (Del(S,1))^<*(the carrier of A)*> if meet(rng Del(S,1)) = meet rng S
  otherwise (Del(S,1))^<*S.1*>;
end;

::definition
:: let A;
:: let n be Nat;
:: let S be Element of (Ideals A)* ;
:: func Trimming(S,n) -> Function of (Ideals A)* , (Ideals A)* means
:::: IDEAL_3:def 26
:: for x be Element of (Ideals A)* holds it.x = Trimming(x);
::end;

definition
   let A;
   let n be Nat such that
 0 <> n;
   let S be Element of (Ideals A)* ;
   func Trimming(S,n) -> Element of (Ideals A)* means
:: IDEAL_3:def 27

   ex f being FinSequence of (Ideals A)* st
   it = f.len f & len f = n & f.1 = S &
   for i being Nat st i in dom f & i+1 in dom f holds
   f.(i+1) = Trimming(f/.i);
 end;
```