Regular Paper

代数幾何の形式化について
On the Formalizations of Algebraic Geometry

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: 8.1.11 and MML Version: 5.65.1394
Received: December 16, 2021. Accepted: May 16, 2022.

Abstract

In the article we formalized introductory basic definitions and propositions of Algebraic Geometry. The formalization in the article is covered the first half of chapter 1 of [1]. Namely "Algebraic Set", "Ideal of an Algebraic Set" and related propositions. Throughout the article we denote k^n a set theoretical n-ple product of a field or ring k. In actual coding Funcs(n, k) is regarded as k^n. We introduced modified evaluation function (E_eval) for multivariate Polynomial and its first argument requires Element of Polynom-Ring(n,k) to avoid using transformation of Polynomial attribute to Element of Polynomial Ring.

1　はじめに

代数幾何の初歩的な定義と関連の命題群とその証明の形式化を行った．対象として扱う空間は可換環，体 k の直積集合 k^n をとる．k^n の点は k の要素の n 個の対 (n-tuple) に対応する．具体的には代数的集合と k^n の部分集合を零点に持つ多項式から生成されるイデアルの定義と関連の命題群とその証明の形式化を行った．形式化の過程で多変数多項式環に関連する定理で証明の困難な点も考察する．

2　アフィン代数幾何の形式化概略

2.1　形式化の動機

代数幾何の形式化は以下の点で重要と考える．

i) Mizar ライブラリに未だ形式化されていない.

ii) 可換代数の具体的応用例を与え，また可換代数論，多項式環の命題群の形式化

iii) 楕円曲線論も代数曲線の例であり，代数幾何の形式化が符号理論，学習理論など工学的分野で応用される事が期待される.

iv) 他の証明検証システムでは ISABEL によるスキーム論が形式化されている [2]．本稿ではより具体性のある古典的代数幾何を題材に形式化を行い応用し易いライブラリ構築を目指す.

2.2 形式化の範囲

2.2.1 対象となる空間

幾何として対象となるのはアフィン空間であり, 体 k に対し，アフィン空間として k^n をとり理論を展開する．k^n をベクトル空間とみて $GL(n,k)$ の作用と k^n とベクトルの平行移動の合成を変換群とする幾何である．本形式化ではアフィン幾何に関連する内容には触れず, 単なる k の要素の n 個の対 (n-tuple) の集合として形式化を進める．従ってベクトル空間を要求しないので k は体である必要はなく, 可換環で成り立つ定理は k は可換環としている．n 個の対 n-tuple は $n \to k$ として形式化する．これは n 変数多項式への代入との親和性を優先した．全空間 k^n はすべての $n \to k$ となり Funcs(n,k) により形式化した．一方既存 MML で数ベクトル空間 n-VectSp_overk は [3] に於いて定義，形式化されている．しかしながら n-VectSp_overk の点は Seg $n \to k$ で形式化され k^n の n-tuple と 0 を基点とする, しないの食い違いがあり効率よく既存線形空間論のライブラリからの結果が利用できない.

2.2.2 形式化の項目

i) 代数的集合

ii) 既約な代数的集合

iii) i),ii) に付随した命題群の形式化

形式化の過程で認識された困難な点は後述し考察を加える.

2.2.3 形式化の底本選定

本形式化で参考，底本とした教科書は

i) Fulton の教科書「代数曲線」[1]

ii) 秋月康夫，中井喜和，永田雅宜の教科書「代数幾何学」[4]

Fulton の教科書 i) は世界的に定評があり ii) は i) の構成と重なり，証明の細部の省略も少なく i) の参考書として利用できる.

2.3 形式化の実際

2.3.1 多項式の零点集合, 多項式の集合の共通零点の形式化

一変数の多項式の零点集合は *Roots* として POLYNOM5:def 10 で形式化されているが，n 変数の多項式に対応するように拡張し新規に定義した.

Listing 1. ALGGEO_1 - def 6

```
definition ::Zero set of f
  let R,n;
  let f be Polynomial of n,R;
  func Roots(f) −> Subset of Funcs(n,[#]R) equals
  {x where x is Function of n,R : eval(f,x) = 0.R};
end;
```

この関数によって以下の多項式の集合 S に対する共通零点集合，即ち S の要素すべてに零点となる点を共通零点すべてを定義する．この定義の形式化には関数 Zero_ を導入して S の要素の共通零点定義することから始める.

Listing 2. ALGGEO_1 - def 7

```
definition ::Zero set of S ={F1,F2,...Fn}
  let R,n,S;
  func Zero_(S) −> Subset of Funcs(n,[#]R) equals
:: ALGGEO_1:def 7
  meet {Roots(f) where f is Polynomial of n,R : f in S};
end;
```

関数 Zero_ では，任意の S の要素 $x : n \to k$ で多項式の集合 F の要素を評価しているが，Polynomial of n, k が S に属するという条件で言い換えている．多項式環 $k[X_1, X_2 \dots X_n]$ の要素は Mizar での属性は Polynomial of n, k ではなく Element of Polynom-Ring(n, k) となる．Element of Polynom-Ring(n, k) 属性のままで計算する場合 Polynomial 属性を引数にとる既存評価関数 eval は利用できず不便なので，Element of Polynom-Ring 属性を引数にとる評価関数 E_eval を導入しておく.

Listing 3. ALGGEO_1 - def 4

```
definition
  let n be Ordinal, L be right_zeroed add−associative right_complementable
  well−unital distributive non trivial doubleLoopStr;
  let f be Element of Polynom−Ring (n,L),x be Function of n,L;
  func E_eval(f,x) −> Element of L means
:: ALGGEO_1:def 4
  ex p be Polynomial of n,L st p = f & it = eval(p,x);
end;
```

このように Element of Polynom-Ring(n, k) 属性に対応した定義だと有限の多項式の列 F に対する評価も以下のように定義可能となる.

Listing 4. ALGGEO_1 - def 5

```
definition
   let R,n,F,x;
   func E_eval(F,x) −> FinSequence of the carrier of R means
:: ALGGEO_1:def 5
   dom it = dom F & for i be Nat st i in dom F holds it.i = E_eval(F/.i,x);
 end;
```

多項式環の要素の属性で共通零点集合の定義を言い換えると以下の通りである.

定理 1

$$Zero\_(S) = \{x \in k^n | \forall f(\text{element of Polynomial Ring}) \wedge f \in S, E\_eval(f, x) = 0.R\}$$

2.3.2 代数的集合

定義 1 k を体とし，k^n の部分集合 V が n 変数多項式環 $k[x_1, x_2 \ldots x_n]$ の有限個の部分集合 $S = \{F_1(x_1, x_2 \ldots x_n), \cdots F_r(x_1, x_2 \ldots x_n)\}$ の要素 F_i 達の共通零点となるとき V を代数的集合という.

k^n の部分集合が代数的集合であるという述語は以下の attr と mode を用いて形式化した．attr zero_points_derived は点集合が零点から由来した集合であるという性質を記述し，代数的集合は零点由来の集合を表すものとして mode で定義した.

Listing 5. ALGGEO_1 - Th.16

```
definition
  let R,n;
  let IT be Subset of Funcs(n,[#]R);
  attr IT is zero_points_derived means
:: ALGGEO_1:def 8
  ex S be non empty Subset of Polynom−Ring(n,R) st IT = Zero_(S);
end;

registration
  let R,n;
  cluster zero_points_derived for non empty Subset of Funcs(n,[#]R);
end;

definition
  let n,R;
  mode Algebraic_Set of n,R is
  zero_points_derived non empty Subset of Funcs(n,[#]R);
end;
```

2.3.3 零点集合の性質

零点集合の性質として命題群が証明される．以下はその例である.

命題 1

$$\forall f, g \in R[x_1, x_2, \ldots x_n], \text{Zero\_}(fg) = \text{Zero\_}(f) \cup \text{Zero\_}(g) \ holds.$$

Mizar での形式化は,

Listing 6. ALGGEO_1 - Th.21

```
theorem :: ALGGEO_1:21
    for R be non degenerated domRing, f,g be Polynomial of n,R holds
    Zero_({f∗'g}) = Zero_({f}) \/ Zero_({g});
```

命題 2

$$\forall a = (a_1, a_2, \ldots, a_n) \in R^n, \mathrm{Zero\_}(\{\mathrm{x_1} - \mathrm{a_1}, \mathrm{x_2} - \mathrm{a_2}, \ldots, \mathrm{x_n} - \mathrm{a_n}\}) = \mathrm{a}\ \textit{holds}.$$

Mizar での形式化は,

Listing 7. ALGGEO_1 - Th.24

```
theorem :: ALGGEO_1:24
    for a be Function of n,R holds Zero_(polyset(a)) = {a};
```

ここでは $\{\mathrm{x_1} - \mathrm{a_1}, \mathrm{x_2} - \mathrm{a_2}, \ldots, \mathrm{x_n} - \mathrm{a_n}\}$ を polyset(a) と関数化してしまっているが, 要素 $x_i - a_i$ は以下の HILBASIS : def3 で定義されている単項式 1_1 [5] を利用して形式化を行った.

Listing 8. ALGGEO_1 - def.10

```
definition
  let n,R;
  let a be Function of n,R, i be Element of n;
  func wpoly(a,i) -> Element of Polynom-Ring(n,R) equals
:: ALGGEO_1:def 10
  1_1(i,R) - (a.i)*1_(n,R);
end;
```

2.3.4 k^n の部分集合のイデアルの形式化

定義 2 k^n の部分集合 X をとり，X のすべて点でゼロとなる多項式全体を $\mathcal{I}(X)$ と定義し X のイデアルと称す.

この形式化は以下の様にの通り X のすべて点でゼロとなる多項式全体に対応付ける関数 Ideal_ を定義することによる.

Listing 9. ALGGEO_1 - def.11

```
definition ::Ideal of X c= Funcs(n,R);
  let R, n, X;
  func Ideal_X -> non empty Subset of Polynom-Ring(n,R) equals
  :Def11:
  {f where f is Polynomial of n,R : X c= Roots(f)};
```

$\mathcal{I}(X)$ は多項式環のイデアルになることが示され「X のイデアル」と呼ばれる所以である.

2.3.5 既約/可約な代数的集合

代数的集合に既約・可約の概念を以下のように定義する．はじめに可約を定義し，その否定により既約を定義する.

定義 3 k^n の代数的集合 V が可約であるとは代数的集合 V_1, V_2 が存在し V_1 $neq V_2 \wedge V = V_1 \cup V_2$ をみたすときをいう．V が可約でないとき既約という.

2.3.6 関数 Zero_ と関数 Ideal_ の相互作用

関数 Zero_ と関数 Ideal_ を用いた命題群が証明される．

命題 3 $X, Y \subset k^n, S \subset k[x_1, x_2 \dots x_n]$, V を k^n の代数的集合とする．この時以下が成立する．

1. $X \subset Y \Rightarrow \mathrm{Ideal\_}Y \subset \mathrm{Ideal\_}X$,
2. $\mathrm{Ideal\_}(\emptyset) = k[x_1, x_2 \dots x_n]$,
3. $(0) \subset \mathrm{Ideal\_}(k^n)$,
4. $\mathrm{Ideal\_}(\mathrm{Zero\_}(S)) \supset S$,
5. $\mathrm{Zero\_}(\mathrm{Ideal\_}(X)) \supset X$,
6. $\mathrm{Zero\_}(\mathrm{Ideal\_}(\mathrm{Zero\_}(S))) = \mathrm{Zero\_}S$,
7. $\mathrm{Ideal\_}(\mathrm{Zero\_}(\mathrm{Ideal\_}(X))) = \mathrm{Ideal\_}X$,
8. $V = \mathrm{Ideal\_}(\mathrm{Zero\_}V)$.

上記命題の項番 3. は k が無限体であれば等号が成立する．証明には以下の命題が必要である．

命題 4

$$\forall f \in k[x_1, x_2 \dots x_n] \wedge f \ is \ \text{non-zero} \Rightarrow \exists a \in k^n \ st \ f(a) \neq 0.k$$

命題 4. の証明は MML ライブラリーの既存定理から導出は今のところ成功していない．既存の多項式の評価関数では証明が出来ない．次節でこの問題を考察する．

3 多変数多項式の評価関数について

前節で取り上げた命題 4. の証明を難しくしている点を解説する．まずは問題を単純化し問題を考察する．

3.1 問題

命題 5 k を無限個の元を含む体，$f(x, y)$ を恒等 0 でない k 係数 2 変数の多項式とする．このとき $f(a, b) \neq 0$ となる (a, b) は無限個存在する．

この証明のスケッチは,「$f(a, y)$ が恒等 0 とならない様に $x = a$ を選ぶ，そうしてできた k[y] の多項式 $f(a, y)$ の零点の個数は次数を超えないので有限個よって $f(a, b) \neq 0$ となる (a, b) は無限個存在する.」

この証明で形式化できない点は $f(a, y)$ のように不定元を選択して評価することにある．$f(x, y)$ を $k[x][y]$ の多項式と見做すことは可能である．$\hat{f}_x(y) \in k[x][y]$ と表記する．しかしこれを一変数の多項式と考えて eval 関数では k[x] の要素を代入しての評価となる．

係数部分を先 k の要素 a で eval 関数で評価したものを $\hat{f}_a(y)$ と表記すれば，これは $k[y]$ の要素として k の要素で評価される．$\hat{f}_a(y)$ を可能にする部分評価関数と言うべきものが必要である．この部分評価関数と既存関数が両立すること，即ち $f(a,b) = eval(f,(a,b))$ と $\hat{f}_a(y)$ が等しいことを確かめれば，命題 5. の証明の形式化も現実的となる．

4 今後の形式化

前章で考察した問題の解決が最優先の課題であり，提示した部分評価関数も Bag 演算を整備して応用のし易い関数として開発することである．Mizar の 40 年の長きにわたる歴史においてこの多項式の分野は取り扱いづらい分野の一つと思われる．形式化実績の積み重ね，汎用性のある有用なライブラリ構築が期待される．代数的集合の既約分解の導入にはイデアルの分解も関連するので準素イデアル [6] の続編も必要となる．代数幾何の形式化は可換環, 多項式環， ネター空間論にまたがる分野であり MML ライブラリを総動員し活用しないと形式化でいないので Mizar システムのみならずプログラミング技術も試される場である．

多項式環自体は具体的な題材であるが扱うには十分複雑な代数構造であることが形式化を通して工数がかさむことで理解される．より単純な代数構造上の幾何から形式化を進めるアプローチもある．半群上の幾何， 所謂トロピカル幾何や工程計画問題 [7] に応用される Max-Plus 代数の形式化を進めるアプローチも今後の考慮したい．

参考文献

[1] Fulton W. Algebraic Curves. The Benjamin/Cummings Publishing Company; 1969.

[2] Bordg A, Paulson L, Li W. Grothendieck's Schemes in Algebraic Geometry. Archive of Formal Proofs. 2021 Mar;`https://isa-afp.org/entries/Grothendieck_Schemes.html`, Formal proof development.

[3] Lango A, Bancerek G. Product of Families of Groups and Vector Spaces. Formalized Mathematics. 1992;3(**2**):235–240. Available from: `http://fm.mizar.org/1992-3/pdf3-2/prvect_1.pdf`.

[4] Akizuki Y, Nakai Y, Nagata M. Algebraic Geometry. Iwanami Shoten (in Japanese); 1987.

[5] Backer J, Rudnicki P. Hilbert Basis Theorem. Formalized Mathematics. 2001;9(**3**):583–589. Available from: `http://fm.mizar.org/2001-9/pdf9-3/hilbasis.pdf`.

[6] Watase Y. On Primary Ideals (in press). Formalized Mathematics. 2021;29(**2**).

[7] 小林 正典. Tropical geometry and its application to scheduling problem. 代数幾何学シンポジウム記録. 2021 jan;(2020):106–114. Available from: `https://ci.nii.ac.jp/naid/120006952786/`.

Mizar article information

Works in Progress

ALGGEO_1 Intrduction to Algebraic Geometry

by Yasushige Watase

Summary: In the article we formalized introductory basic definitions and propositions of Algebraic Geometry. The formalization in the article is covered the first half of chapter 1 of [1]. Namely "Algebraic Set", "Ideal of an Algebraic Set" and related propositions. Throughout the article we denote k^n a set theoretical n-ple product of a field or ring k. In actual coding Funcs(n, k) is regarded as k^n. We introduced modified evaluation function (E_eval) for multivariate Polynomial and its first argument requires Element of Polynom-Ring(n,k) to avoid using transformation of Polynomial attribute to Element of Polynomial Ring.

Listing 10. ALGGEO_1 - abstract

```
:: Introduction to Algebraic Geometory I
:: by Yasushige Watase
::
:: Received May 27, 2019
:: Copyright (c) 2019–2021 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
:: License version 3.0 or later, subject to the binding interpretation
:: detailed in file COPYING.interpretation.
:: See COPYING.GPL and COPYING.CC–BY–SA for the full text of these
:: licenses, or see http://www.gnu.org/licenses/gpl.html and
:: http://creativecommons.org/licenses/by–sa/3.0/.

environ

 vocabularies NUMBERS, SUBSET_1, RELAT_1, ORDINAL4, FINSEQ_1, XBOOLE_0,
      FUNCT_1, XXREAL_0, TARSKI, NAT_1, ARYTM_3, ZFMISC_1, CARD_1, YELLOW_8,
      ORDINAL1, ARYTM_1, PRE_POLY, QC_LANG1, GROUP_1, ALGSTR_0, RLVECT_1,
      VECTSP_1, POLYNOM1, POLYNOM2, AFINSQ_1, FINSEQ_2, CARD_3, SQUARE_1,
      STRUCT_0, PARTFUN1, FINSET_1, SUPINF_2, FUNCOP_1, ALGSEQ_1, RATFUNC1,
      FUNCT_2, HILBASIS, VECTSP_2, CARD_FIL, RSSPACE, IDEAL_1, MESFUNC1, INT_2,
      SETFAM_1, XCMPLX_0, PRE_TOPC, POLYNOM5, LATTICES, BSPACE, NEWTON, RING_1,
      ALGGEO_1;

notations
      TARSKI,XBOOLE_0, XTUPLE_0, ZFMISC_1, SUBSET_1, SETFAM_1, RELAT_1, FUNCT_1,
      ORDINAL1, RELSET_1, PARTFUN1, MCART_1, FUNCT_2, BINOP_1, DOMAIN_1,
      FUNCOP_1, FUNCT_4, FINSET_1, CARD_1, PBOOLE, ORDERS_1, NUMBERS, XCMPLX_0,
      XXREAL_0, XREAL_0, NAT_1, INT_1, MEMBERED, VALUED_0, INT_2, NAT_D,
      CLASSES2, FINSEQ_1, FINSEQ_2, VALUED_1, RVSUM_1, AFINSQ_1, FINSEQ_7,
      PRE_POLY, STRUCT_0, ALGSTR_0, ORDERS_2,PRE_TOPC, RLVECT_1, GROUP_1,
      VECTSP_1, ALGSTR_1, VECTSP_2, GROUP_2, GROUP_3, POLYNOM1, ALGSEQ_1,
      PRVECT_1, BINOM, POLYNOM2, POLYNOM3, POLYNOM4, POLYNOM5, UPROOTS, GROUP_9,
      HURWITZ, IDEAL_1, RING_1, RING_2, POLYALG1, HILBASIS, POLYNOM7, GROEB_1,
      RATFUNC1, GROUP_1A, RING_4, HILB10_2, FIELD_1;

constructors
      TARSKI, XTUPLE_0, ZFMISC_1, SUBSET_1, SETFAM_1, RELAT_1, RELAT_2, RELSET_1,
      RECDEF_1, DOMAIN_1, ORDINAL2, FUNCT_4, PBOOLE, NAT_D, BINOP_2, FINSEQ_7,
      ORDERS_2, GROUP_1, GROUP_4, FVSUM_1, POLYNOM1, ALGSEQ_1, WAYBEL_4,
      PRVECT_1, QUOFIELD, BINOM, POLYNOM2, POLYNOM3, BAGORDER, POLYNOM4,
      POLYNOM5, UPROOTS, GROUP_9, HURWITZ, HILBASIS, POLYALG1, POLYNOM6,
      POLYNOM7, GROEB_1, RATFUNC1, GROUP_1A, RING_4, HILB10_2, FIELD_1;
```

registrations XBOOLE_0, RELAT_1, FUNCT_1, ORDINAL1, XREAL_0, NAT_1, CARD_1, VALUED_0, VALUED_1, RELSET_1, INT_1, STRUCT_0, VECTSP_1, PRE_POLY, MEMBERED, POLYNOM2, AFINSQ_1, ORDINAL2, POLYNOM6, HILB10_2, XXREAL_0, SUBSET_1, FUNCT_2, FINSEQ_1, FINSEQ_2, MATRIX11,FVSUM_1, AFINSQ_2, FUNCOP_1, ALGSTR_1, ALGSTR_0, HILBASIS, PRVECT_1, POLYNOM7, GCD_1, POLYNOM1, VECTSP_2, POLYALG1, RLVECT_1, GROUP_1A, PRE_CIRC, WAYBEL_2, IDEAL_1, RING_1, RING_2, POLYNOM3, XXREAL_2, UPROOTS,POLYNOM5, PBOOLE, BAGORDER, RELAT_2, ORDERS_2, GROEB_1, TERMORD, BINOM, GROUP_1, MOD_4, RINGCAT1, ALGSEQ_1;

requirements NUMERALS, SUBSET, ARITHM, REAL;

definitions TARSKI, XBOOLE_0, MEMBERED, RLVECT_1, ALGSTR_0, STRUCT_0, GROUP_1, VECTSP_1, SUBSET_1, FUNCT_2;

equalities FINSEQ_1, STRUCT_0, ALGSTR_0, POLYNOM1, VECTSP_1, FINSEQ_2, ORDINAL1, SUBSET_1, AFINSQ_1, XBOOLE_0, FUNCT_2, BINOP_1, FUNCOP_1;

expansions POLYNOM1, FUNCT_2, ORDINAL1,IDEAL_1, SUBSET_1,FUNCT_1, BINOP_1, VECTSP_2, RLVECT_1, ALGSTR_0, GROUP_2, TARSKI, STRUCT_0, VECTSP_1, GROUP_1, XBOOLE_0, ZFMISC_1, GROUP_6, INT_1;

theorems TARSKI, FUNCT_1, CARD_1, NAT_1, ZFMISC_1, XREAL_1, FINSEQ_3, FINSEQ_1, FINSEQ_5, FINSEQ_2, ORDINAL1, HILB10_3, XBOOLE_0, RELAT_1, PRE_POLY, FUNCT_2, POLYNOM1, POLYNOM2, FUNCOP_1, PARTFUN1, XBOOLE_1, RLVECT_1, POLYNOM7, SUBSET_1, IDEAL_1, ALGSTR_1, RING_1, SETFAM_1, BINOM, GROUP_1, XCMPLX_1, FVSUM_1, VECTSP_2, TARSKI_0, HILBASIS, XXREAL_0, TOPZARI1;

schemes FINSEQ_2, NAT_1;

begin *:: Preliminaries*

reserve K **for** Field;
reserve R **for non** degenerated comRing;
reserve o,o1,x,x1,y,y1 **for** object;
reserve q,I **for** Ideal **of** R;
reserve n **for non** zero Nat;
reserve m,d,i,j **for** Nat;
reserve S,T **for non** empty Subset **of** Polynom−Ring(n,R);
reserve F,G **for** FinSequence **of the** carrier **of** Polynom−Ring(n,R);
reserve X **for non** empty **set**;
reserve A **for non** empty **set**;
reserve x1,x2,z **for set**;
reserve A,B **for non** empty **set**;

:: Affine Space (X,V)
definition *::numerical space*
  let R, n;
  func NumSp(R,n) −> **non** empty **set equals**
:: ALGGEO_1:def 1
  Funcs(n,[#]R);
end;

reserve t **for** Element **of** n−tuples_on [#]R;
reserve t1 **for** FinSequence **of** [#]R;

definition
  let n **be** Nat;
  let K **be** Field;
  let p **be** n−element [#]K−valued XFinSequence;
  func @p −> Function **of** n,K **equals**
:: ALGGEO_1:def 2
      p;
end;

definition
  let n **be** Nat;
  let K **be** Field;

```
  let p be n−element [#]K−valued XFinSequence;
  func @p −> Function of n,K equals
:: ALGGEO_1:def 3
      p;
end;


definition
  let n be Ordinal, L be right_zeroed add−associative right_complementable
  well−unital distributive non trivial doubleLoopStr,
  p be Polynomial of n,L;
  redefine func {p} −> Subset of Polynom−Ring(n,L);
end;

definition
  let n be Ordinal, L be right_zeroed add−associative right_complementable
  well−unital distributive non trivial doubleLoopStr;
  let f be Element of Polynom−Ring (n,L),x be Function of n,L;
  func E_eval(f,x) −> Element of L means
:: ALGGEO_1:def 4

  ex p be Polynomial of n,L st p = f & it = eval(p,x);
end;

::new Function for FinSeq of Polynomial is introduced
reserve x for Function of n,R;
definition
   let R,n,F,x;
   func E_eval(F,x) −> FinSequence of the carrier of R means
:: ALGGEO_1:def 5
   dom it = dom F & for i be Nat st i in dom F holds it.i = E_eval(F/.i,x);
 end;

theorem :: ALGGEO_1:1
    for N0 be Nat for x,F st len F = N0+1 holds
    E_eval(F,x) = (E_eval(F|N0,x))^<*E_eval(F/.(len F),x)*>;

theorem :: ALGGEO_1:2
    for x,F st len F = 0 holds E_eval(Sum F,x) = Sum E_eval(F,x);

theorem :: ALGGEO_1:3
    for x,F st len F <> 0 holds E_eval(Sum F,x) = Sum E_eval(F,x);

theorem :: ALGGEO_1:4
    for F be FinSequence of the carrier of Polynom−Ring(n,R),
    x be Function of n,R holds E_eval(Sum F,x) = Sum E_eval(F,x);

theorem :: ALGGEO_1:5
    for G be FinSequence of the carrier of R holds
    G = (len G)|−> 0.R iff (for i be Nat st i in dom G holds G.i = 0.R);

theorem :: ALGGEO_1:6
    for n be Nat holds
    Sum (n|−>0.R) = 0.R;

definition ::Zero set of f
  let R,n;
  let f be Polynomial of n,R;
  func Roots(f) −> Subset of Funcs(n,[#]R) equals
:: ALGGEO_1:def 6
  {x where x is Function of n,R : eval(f,x) = 0.R};
end;

theorem :: ALGGEO_1:7
    Roots(0_(n,R)) = Funcs(n,[#]R);

theorem :: ALGGEO_1:8
    Roots(1_(n,R)) = {};
```

```
::1.2 Affine Space and Algebraic Sets

::reserve S,T for non empty Subset of Polynom−Ring(n,R);
definition ::Zero set of S ={F1,F2,...Fn}
  let R,n,S;
  func Zero_(S) −> Subset of Funcs(n,[#]R) equals
:: ALGGEO_1:def 7

  meet {Roots(f) where f is Polynomial of n,R : f in S};
end;

theorem :: ALGGEO_1:9
    for n,R,S holds
    {Roots(f) where f is Polynomial of n,R : f in S} <> {};

theorem :: ALGGEO_1:10
    Zero_(S) = {} implies
    {x where x is Function of n,R : for f be Element of Polynom−Ring(n,R)
    st f in S holds E_eval(f,x) = 0.R} ={};

theorem :: ALGGEO_1:11
    Zero_(S) <> {} implies
    Zero_(S) =
    {x where x is Function of n,R : for f be Element of Polynom−Ring(n,R)
    st f in S holds E_eval(f,x) = 0.R};

theorem :: ALGGEO_1:12
    Zero_(S) =
    {x where x is Function of n,R : for f be Element of Polynom−Ring(n,R)
     st f in S holds E_eval(f,x) = 0.R};

theorem :: ALGGEO_1:13
    for p be Polynomial of n,R holds Zero_({p}) = Roots(p);

theorem :: ALGGEO_1:14
    for o be Function of n,R holds (not o in Zero_(S)) implies
    (ex f be Polynomial of n,R st f in S & not o in Roots(f));

theorem :: ALGGEO_1:15
    Zero_({0_(n,R)}) = Funcs(n,[#]R);

theorem :: ALGGEO_1:16
    S c= T implies Zero_(T) c= Zero_(S);

theorem :: ALGGEO_1:17
    Zero_(S\/T) = Zero_(S)/\Zero_(T);

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::2.10.2021
theorem :: ALGGEO_1:18
    Zero_(S) = Zero_(S−Ideal);

definition
  let R,n;
  let IT be Subset of Funcs(n,[#]R);
  attr IT is zero_points_derived means
:: ALGGEO_1:def 8
  ex S be non empty Subset of Polynom−Ring(n,R) st IT = Zero_(S);
end;

theorem :: ALGGEO_1:19
    [#]Funcs(n,[#]R) is zero_points_derived;

registration
  let R,n;
  cluster zero_points_derived for non empty Subset of Funcs(n,[#]R);
end;

definition
```

```
  let n,R;
  mode Algebraic_Set of n,R is
  zero_points_derived non empty Subset of Funcs(n,[#]R);
end;

definition
  let R,n;
  let IT be Subset of Funcs(n,[#]R);
  attr IT is Alg_Set means
:: ALGGEO_1:def 9
  ex S be non empty Subset of Polynom-Ring(n,R) st IT = Zero_(S);
end;

theorem :: ALGGEO_1:20
    for Z be Algebraic_Set of n,R holds
    ex I be Ideal of Polynom-Ring(n,R) st Z = Zero_(I);


theorem :: ALGGEO_1:21
    for R be non degenerated domRing, f,g be Polynomial of n,R holds
    Zero_({f*'g}) = Zero_({f}) \/ Zero_({g});

  theorem :: ALGGEO_1:22 :::Integral Domain requires
    for R be non degenerated domRing, I,J be Ideal of Polynom-Ring(n,R),
    M be non empty Subset of Polynom-Ring(n,R) st
    M = rng ((the multF of Polynom-Ring(n,R))|[:I,J:]) holds
    Zero_(I) \/ Zero_(J) = Zero_(M);

 theorem :: ALGGEO_1:23
    for a be Element of R,x,i be Element of n holds
    1_1(i,R) is Polynomial of n,R & a|(n,R) is Polynomial of n,R;

definition
  let n,R;
  let a be Function of n,R, i be Element of n;
  func wpoly(a,i) -> Element of Polynom-Ring(n,R) equals
:: ALGGEO_1:def 10
  1_1(i,R) - (a.i)*1_(n,R);
end;

definition
  let n,R;
  let a be Function of n,R;
  func polyset(a) -> non empty Subset of Polynom-Ring(n,R) equals
:: ALGGEO_1:def 11
  { f where f is Element of Polynom-Ring(n,R):
    ex i be Element of n st f = wpoly(a,i)};
end;

theorem :: ALGGEO_1:24
    for a be Function of n,R holds Zero_(polyset(a)) = {a};

definition let X be non empty set;
 mode Point of X is 1-element Subset of X;
end;

::1.3 The Ideal of a Set of Points
reserve X,Y for Subset of Funcs(n,[#]R);
reserve a for Function of n,R;

definition ::Ideal of X c= Funcs(n,R);
  let R, n, X;
  func Ideal_X -> non empty Subset of Polynom-Ring(n,R) equals
:: ALGGEO_1:def 12

  {f where f is Polynomial of n,R : X c= Roots(f)};
end;

theorem :: ALGGEO_1:25
```

```
    for p, q being Element of Polynom−Ring(n,R) st p in Ideal_X & q in Ideal_X
    holds p + q in Ideal_X;

theorem :: ALGGEO_1:26
    for a, p being Element of Polynom−Ring(n,R) st p in Ideal_X holds
    a∗p in Ideal_X;

theorem :: ALGGEO_1:27
    for a, p being Element of Polynom−Ring(n,R) st p in Ideal_X holds
    p∗a in Ideal_X;

theorem :: ALGGEO_1:28
    for X holds Ideal_X is Ideal of Polynom−Ring(n,R);

registration
  let R, n, X;
  cluster Ideal_X −> add−closed for Subset of Polynom−Ring(n,R);
  cluster Ideal_X −> right−ideal for Subset of Polynom−Ring(n,R);
end;



::(6) If X c= Y , then I(Y) c= I(X).
::(7) I({}) = k[X1,...,Xn]; I(An) = (0) if k is an infinite field;
::I({(a1,...,an)}) = (X1 − a1,...,Xn − an) for a1,...,an \in k.
::(8) S c= I(V(S))for any set S of polynomials; X c= V (I(X))for any set X of
::points.
::(9) V (I(V (S))) = V (S) for any set S of polynomials, and I(V (I(X))) = I(X) ::for any set X of points. So if V is
      an algebraic set, V = V (I(V )), and
::if I is the ideal of an algebraic set, I = I(V (I)).

theorem :: ALGGEO_1:29 ::(6)
     X c= Y implies Ideal_Y c= Ideal_X;

theorem :: ALGGEO_1:30 ::(7)
     X = {} implies Ideal_X = [#]Polynom−Ring(n,R);

theorem :: ALGGEO_1:31 ::(7)
    X = Funcs(n,[#]R) implies {0.Polynom−Ring(n,R)} c= Ideal_(X);

theorem :: ALGGEO_1:32
    for S be non empty Subset of Polynom−Ring(n,R) holds S c= Ideal_(Zero_(S));

theorem :: ALGGEO_1:33
    S c= Ideal_(Zero_(S));

theorem :: ALGGEO_1:34 ::(8)
       X c= Zero_(Ideal_X);

theorem :: ALGGEO_1:35 ::(9)
    Zero_(Ideal_(Zero_S)) = Zero_S;

theorem :: ALGGEO_1:36 ::(9)
    Ideal_(Zero_(Ideal_X)) = Ideal_X;

theorem :: ALGGEO_1:37 ::(9)
    for X be Algebraic_Set of n,R holds X = Zero_(Ideal_X);

definition
 let R,n;
 let IT be Algebraic_Set of n,R;
 attr IT is reducible
 means
:: ALGGEO_1:def 13
 ex V1,V2 be Algebraic_Set of n,R st IT = V1 \/ V2 & V1 <> V2;
end;

notation
```

```
 let R,n;
 let V be Algebraic_Set of n,R;
  antonym V is irreducible for V is reducible;
end;
```