FORMALIZED MATHEMATICS
Volume **31**, **2023**, Pages 67–73
DOI: 10.2478/forma-2023-0007
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Introduction to Algebraic Geometry

Yasushige Watase
Suginami-ku Matsunoki 6, 3-21 Tokyo
Japan

Summary. A classical algebraic geometry is study of zero points of system of multivariate polynomials [3], [7] and those zero points would be corresponding to points, lines, curves, surfaces in an affine space. In this article we give some basic definition of the area of affine algebraic geometry such as algebraic set, ideal of set of points, and those properties according to [4] in the Mizar system [5], [2].

We treat an affine space as the n-fold Cartesian product k^n as the same manner appeared in [4]. Points in this space are identified as n-tuples of elements from the set k. The formalization of points, which are n-tuples of numbers, is described in terms of a mapping from n to k, where the domain n corresponds to the set $n = \{0, 1, \ldots, n-1\}$, and the target domain k is the same as the scalar ring or field of polynomials. The same approach has been applied when evaluating multivariate polynomials using n-tuples of numbers [10].

This formalization aims at providing basic notions of the field which enable to formalize geometric objects such as algebraic curves which is used e.g. in coding theory [11] as well as further formalization of the fields [8] in the Mizar system, including the theory of polynomials [6].

MSC: 14-01 14H50 68V20

Keywords: affine algebraic set; multivariate polynomial

MML identifier: ALGGEO_1, version: 8.1.12 5.75.1447

1. Evaluation Functions Revisited

From now on A denotes a non degenerated commutative ring, R denotes a non degenerated integral domain, n denotes a non empty ordinal number, o, o_1, o_2 denote objects, X, Y denote subsets of $(\Omega_R)^n$, S, T denote subsets of

Polynom-Ring(n, R), F, G denote finite sequences of elements of the carrier of Polynom-Ring(n, R), and x denotes a function from n into R.

Let n be an ordinal number, L be a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure, and p be a polynomial of n,L. Note that the functor $\{p\}$ yields a subset of Polynom-Ring(n, L). Let f be an element of Polynom-Ring(n, L) and x be a function from n into L. The functor Eval(f, x) yielding an element of L is defined by

(Def. 1) there exists a polynomial p of n,L such that $p = f$ and $it = \mathrm{eval}(p, x)$.

Let F be a finite sequence of elements of the carrier of Polynom-Ring(n, L). The functor Eval(F, x) yielding a finite sequence of elements of the carrier of L is defined by

(Def. 2) $\mathrm{dom}\, it = \mathrm{dom}\, F$ and for every natural number i such that $i \in \mathrm{dom}\, F$ holds $it(i) = \mathrm{Eval}(F_{/i}, x)$.

Now we state the propositions:

(1) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, and an ordinal number n. Then Support $0_n L = \emptyset$.

(2) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial double loop structure L, elements f, g of Polynom-Ring(n, L), and a function x from n into L. Then $\mathrm{Eval}(f + g, x) = \mathrm{Eval}(f, x) + \mathrm{Eval}(g, x)$.

(3) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial, commutative, associative, non empty double loop structure L, elements f, g of Polynom-Ring(n, L), and a function x from n into L. Then $\mathrm{Eval}(f \cdot g, x) = (\mathrm{Eval}(f, x)) \cdot (\mathrm{Eval}(g, x))$.

(4) Let us consider a natural number N_0, an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial, commutative, associative, non empty double loop structure L, a finite sequence F of elements of the carrier of Polynom-Ring(n, L), and a function x from n into L. Suppose $\mathrm{len}\, F = N_0 + 1$. Then $\mathrm{Eval}(F, x) = \mathrm{Eval}(F \restriction N_0, x) \frown \langle \mathrm{Eval}(F_{/\mathrm{len}\, F}, x)\rangle$.
Proof: For every natural number k such that $1 \leqslant k \leqslant \mathrm{len}\, \mathrm{Eval}(F, x)$ holds $(\mathrm{Eval}(F, x))(k) = (\mathrm{Eval}(F \restriction N_0, x) \frown \langle \mathrm{Eval}(F_{/\mathrm{len}\, F}, x)\rangle)(k)$. □

(5) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial, commutative, associative, non empty double loop structure L, a finite sequence F of elements of the carrier of Polynom-Ring(n, L), and a func-

tion x from n into L. Then $\mathrm{Eval}(\sum F, x) = \sum \mathrm{Eval}(F, x)$. The theorem is a consequence of (2) and (4).

2. Monic Multivariate Polynomials with Degree 1

Let us consider n and R. Let a be a function from n into R and i be an element of n. The functor deg1Poly(a, i) yielding a polynomial of n,R is defined by the term

(Def. 3) $1\_1(i, R) - (a(i) \restriction (n, R))$.

Let us consider an element a of R and an element i of n. Now we state the propositions:

(6) (i) $(1\_1(i, R))(\mathrm{UnitBag}\, i) = 1_R$, and

(ii) $(a \restriction (n, R))(\mathrm{EmptyBag}\, n) = a$, and

(iii) $(1\_1(i, R))(\mathrm{EmptyBag}\, n) = 0_R$, and

(iv) $(a \restriction (n, R))(\mathrm{UnitBag}\, i) = 0_R$.

Proof: Set $U = \mathrm{UnitBag}\, i$. $U \neq \mathrm{EmptyBag}\, n$. □

(7) (i) $1\_1(i, R)$ is a polynomial of n,R, and

(ii) $a \restriction (n, R)$ is a polynomial of n,R.

(8) Let us consider a non zero element a of R, an element b of R, and an element i of n. Then $(a \restriction (n, R)) * 1\_1(i, R) + (b \restriction (n, R))$ is a polynomial of n,R.

(9) Let us consider an element a of R, and an element i of n. Then $\mathrm{Support}(1\_1(i, R) + (a \restriction (n, R))) \subseteq \{\mathrm{UnitBag}\, i\} \cup \{\mathrm{EmptyBag}\, n\}$.

(10) $\mathrm{degree}(\mathrm{EmptyBag}\, n) = 0$.

(11) Let us consider an element x of n. Then $\mathrm{degree}(\mathrm{UnitBag}\, x) = 1$.

(12) Let us consider an element a of R, and an element i of n. Then $\mathrm{degree}(1\_1(i, R) + (a \restriction (n, R))) = 1$. The theorem is a consequence of (9), (6), (1), (10), and (11).

3. Affine Space and Algebraic Sets from Ideal

Let us consider R and n. Let f be a polynomial of n,R. The functor Roots(f) yielding a subset of $(\Omega_R)^n$ is defined by the term

(Def. 4) $\{x$, where x is a function from n into $R : \mathrm{eval}(f, x) = 0_R\}$.

Now we state the propositions:

(13) $\mathrm{Roots}(0_n R) = (\Omega_R)^n$.

PROOF: If $o \in (\Omega_R)^n$, then $o \in \mathrm{Roots}(0_n R)$. □

(14) $\mathrm{Roots}(1\_(n, R)) = \emptyset_{(\Omega_R)^n}$.

Let us consider R, n, and S. The functor $\mathrm{Roots}(S)$ yielding a subset of $(\Omega_R)^n$ is defined by the term

(Def. 5) $\begin{cases} \{x, \text{ where } x \text{ is a function from } n \text{ into } R: \text{ for every polynomial } p \text{ of } \\ n, R \text{ such that } p \in S \text{ holds } \mathrm{eval}(p, x) = 0_R\}, \textbf{if } S \neq \emptyset, \\ \emptyset, \textbf{otherwise}. \end{cases}$

Now we state the proposition:

(15) Let us consider a polynomial p of n,R. Then $\mathrm{Roots}(\{p\}) = \mathrm{Roots}(p)$.

Let us consider R and n. Let I be a subset of $(\Omega_R)^n$. We say that I is algebraic set from ideal if and only if

(Def. 6) there exists an ideal J of Polynom-Ring(n, R) such that $I = \mathrm{Roots}(J)$.

Let us note that there exists a non empty subset of $(\Omega_R)^n$ which is algebraic set from ideal.

4. Algebraic Sets

Let us consider n and R. An algebraic set of n and R is an algebraic set from ideal subset of $(\Omega_R)^n$. Now we state the propositions:

(16) Let us consider non empty subsets S, T of Polynom-Ring(n, R). If $S \subseteq T$, then $\mathrm{Roots}(T) \subseteq \mathrm{Roots}(S)$.

(17) Let us consider a non empty subset S of Polynom-Ring(n, R). Then $\mathrm{Roots}(S) = \mathrm{Roots}(S\text{–ideal})$.

PROOF: $\mathrm{Roots}(S) \subseteq \mathrm{Roots}(S\text{–ideal})$. □

(18) Let us consider ideals I, J of Polynom-Ring(n, R). Then $\mathrm{Roots}(I \cup J) = \mathrm{Roots}(I) \cap \mathrm{Roots}(J)$. The theorem is a consequence of (16).

(19) Let us consider algebraic sets S, T of n and R. Then $S \cap T$ is an algebraic set of n and R. The theorem is a consequence of (18) and (17).

Let us consider A. Let F be a non empty subset of Ideals A. One can verify that the functor $\bigcup F$ yields a non empty subset of A. Now we state the propositions:

(20) Let us consider a non empty subset F of Ideals Polynom-Ring(n, R). Then $\mathrm{Roots}(\bigcup F) = \bigcap \{\mathrm{Roots}(I)$, where I is an ideal of Polynom-Ring$(n, R) : I \in F\}$.

PROOF: Set P_1 = Polynom-Ring(n, R). Set $M = \{\mathrm{Roots}(I)$, where I is an ideal of $P_1 : I \in F\}$. Consider I being an object such that $I \in F$. Consider I_1 being an ideal of P_1 such that $I = I_1$. For every o such that

$o \in \mathrm{Roots}(\bigcup F)$ holds $o \in \bigcap M$. For every o such that $o \in \bigcap M$ holds $o \in \mathrm{Roots}(\bigcup F)$. □

(21) Let us consider polynomials f, g of n,R.
Then $\mathrm{Roots}(\{f * g\}) = \mathrm{Roots}(\{f\}) \cup \mathrm{Roots}(\{g\})$.
PROOF: If $o \in \mathrm{Roots}(\{f * g\})$, then $o \in \mathrm{Roots}(\{f\}) \cup \mathrm{Roots}(\{g\})$. If $o \in \mathrm{Roots}(\{f\}) \cup \mathrm{Roots}(\{g\})$, then $o \in \mathrm{Roots}(\{f * g\})$. □

Let us consider ideals I, J of Polynom-Ring(n, R). Now we state the propositions:

(22) $\mathrm{Roots}(I \cap J) = \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$.
PROOF: $\mathrm{Roots}(I) \subseteq \mathrm{Roots}(I \cap J)$ and $\mathrm{Roots}(J) \subseteq \mathrm{Roots}(I \cap J)$. For every o such that $o \in \mathrm{Roots}(I \cap J)$ holds $o \in \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$. □

(23) $\mathrm{Roots}(I * J) = \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$.
PROOF: $\mathrm{Roots}(I \cap J) \subseteq \mathrm{Roots}(I * J)$. For every o such that $o \in \mathrm{Roots}(I * J)$ holds $o \in \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$. □

5. The Collection of Algebraic Sets

Let us consider n and R. The functor AlgSets(n, R) yielding a set is defined by the term

(Def. 7) $\{S$, where S is a subset of $(\Omega_R)^n$: S is an algebraic set of n and $R\}$.

Now we state the proposition:

(24) Let us consider a non zero natural number m, and a subset F of AlgSets(n, R). Suppose $\overline{\overline{F}} = m$. Then $\bigcup F$ is an algebraic set of n and R.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every subset G of AlgSets(n, R) such that $\overline{\overline{G}} = \$_1$ holds $\bigcup G$ is an algebraic set of n and R. For every non zero natural number m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m+1]$ by [9, (1)]. $\mathcal{P}[1]$. For every non zero natural number n, $\mathcal{P}[n]$. □

Let us consider n and R. Let a be a function from n into R. The functor polyset(a) yielding a non empty subset of Polynom-Ring(n, R) is defined by the term

(Def. 8) $\{f$, where f is a polynomial of n,R : there exists an element i of n such that $f = \mathrm{deg1Poly}(a, i)\}$.

Now we state the propositions:

(25) Let us consider a function a from n into R. Then $\mathrm{Roots}(\mathrm{polyset}(a)) = \{a\}$.
PROOF: If $o \in \mathrm{Roots}(\mathrm{polyset}(a))$, then $o \in \{a\}$ by [10, (24)], [1, (1)]. If $o \in \{a\}$, then $o \in \mathrm{Roots}(\mathrm{polyset}(a))$ by [10, (24)], [1, (1)]. □

(26) Let us consider an element x of $(\Omega_R)^n$. Then $\{x\}$ is an algebraic set of n and R. The theorem is a consequence of (25) and (17).

(27) Let us consider a non zero natural number m, and a subset P of $S_{((\Omega_R)^n)}$. Suppose $\overline{\overline{P}} = m$. Then $\bigcup P$ is an algebraic set of n and R.
PROOF: $S_{((\Omega_R)^n)} \subseteq \mathrm{AlgSets}(n, R)$. □

6. The Ideal of a Set of Points

Let us consider R, n, and X. The functor Ideal(X) yielding a non empty subset of Polynom-Ring(n, R) is defined by the term

(Def. 9) $\{f$, where f is a polynomial of n,R : $X \subseteq \mathrm{Roots}(f)\}$.

Now we state the proposition:

(28) Ideal(X) is an ideal of Polynom-Ring(n, R).

Let us consider R, n, and X. One can check that Ideal(X) is closed under addition as a subset of Polynom-Ring(n, R) and Ideal(X) is right ideal as a subset of Polynom-Ring(n, R). Now we state the propositions:

(29) If $X \subseteq Y$, then $\mathrm{Ideal}(Y) \subseteq \mathrm{Ideal}(X)$.

(30) $X = \emptyset$ if and only if $\mathrm{Ideal}(X) = \Omega_{\text{Polynom-Ring}(n,R)}$.
PROOF: If $X = \emptyset$, then $\mathrm{Ideal}(X) = \Omega_{\text{Polynom-Ring}(n,R)}$. If $\mathrm{Ideal}(X) = \Omega_{\text{Polynom-Ring}(n,R)}$, then $X = \emptyset_{(\Omega_R)^n}$. □

(31) $\{0_{\text{Polynom-Ring}(n,R)}\} \subseteq \mathrm{Ideal}(\Omega_{(\Omega_R)^n})$. The theorem is a consequence of (13).

(32) $S \subseteq \mathrm{Ideal}(\mathrm{Roots}(S))$.

(33) $X \subseteq \mathrm{Roots}(\mathrm{Ideal}(X))$.
PROOF: For every o such that $o \in X$ holds $o \in \mathrm{Roots}(\mathrm{Ideal}(X))$. □

(34) $\mathrm{Roots}(\mathrm{Ideal}(\mathrm{Roots}(S))) = \mathrm{Roots}(S)$. The theorem is a consequence of (33), (16), (32), and (30).

(35) $\mathrm{Ideal}(\mathrm{Roots}(\mathrm{Ideal}(X))) = \mathrm{Ideal}(X)$.

(36) Let us consider an algebraic set X of n and R. Then $X = \mathrm{Roots}(\mathrm{Ideal}(X))$. The theorem is a consequence of (34).

(37) Let us consider algebraic sets V, W of n and R. Then $V = W$ if and only if $\mathrm{Ideal}(V) = \mathrm{Ideal}(W)$. The theorem is a consequence of (36).

(38) Let us consider algebraic sets X, Y of n and R. If $X \subset Y$, then $\mathrm{Ideal}(Y) \subset \mathrm{Ideal}(X)$. The theorem is a consequence of (36) and (29).

(39) $\sqrt{\mathrm{Ideal}(X)} = \mathrm{Ideal}(X)$. The theorem is a consequence of (30) and (15).

7. Reducible Algebraic Sets

Let us consider R and n. Let I be an algebraic set of n and R. We say that I is reducible if and only if

(Def. 10) there exist algebraic sets V_1, V_2 of n and R such that $I = V_1 \cup V_2$ and $V_1 \subset I$ and $V_2 \subset I$.

Let V be an algebraic set of n and R. We introduce the notation V is irreducible as an antonym for V is reducible. Now we state the proposition:

(40) Let us consider a non empty algebraic set V of n and R. Then V is irreducible if and only if Ideal(V) is a prime ideal of Polynom-Ring(n, R).
Proof: If Ideal(V) is a prime ideal of Polynom-Ring(n, R), then V is irreducible. If V is irreducible, then Ideal(V) is a prime ideal of Polynom-Ring (n, R). □

References

[1] Marcin Acewicz and Karol Pąk. Basic Diophantine relations. *Formalized Mathematics*, 26(**2**):175–181, 2018. doi:10.2478/forma-2018-0015.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Edward J. Barbeau. *Polynomials.* Springer, 2003.

[4] William Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry.* The Benjamin/Cummings Publishing Company, 1969.

[5] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[6] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[7] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[8] Christoph Schwarzweller. Existence and uniqueness of algebraic closures. *Formalized Mathematics*, 30(**4**):281–294, 2022. doi:10.2478/forma-2022-0022.

[9] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

[10] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.

[11] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer, 2008.

Accepted June 30, 2023