Basic Results on Ideals and Varieties in Finite Fields

R. Germundsson
Department of Electrical Engineering
Linköping University
S-581 83 Linköping
SWEDEN

Email: roger@isy.liu.se

1991-09-11

Abstract: The connection between ideals and varieties for polynomial rings over finite fields is investigated. An extension to Hilbert's Nullstellen Satz is given for these ideals. Furthermore projections and embeddings of these is examined. These results basically give ideal theoretic formulations for several algebro-geometric questions. This in turn is translated to Gröbner basis and polynomial remainder calculations. An example implementation in Mathematica is also given.

Keywords: Ideal, Variety, Algebraic Geometry, Gröbner Basis, Nullstellen Satz, Commutative Algebra

1 Introduction

This report basically clarifies the relation between algebro-geometric objects such as variety and homomorphisms and projections thereof to their corresponding ideals.

It might seem strange to have such a report coming from an electrical engineering department, but basically we were following another track, namely finite systems defined by polynomials over finite fields. As the standard algebraic geometry or commutative algebra book seem to start of with the basic assumption that we work in characteristic 0 they are basically useless for our purposes. This report will then serve as the basis for another venture, i.e. finite polynomial dynamical systems rather than exploring this area further. Of course this examination has been a great pleasure. In particular finding connections to classical theorems such as Hilbert's Nullstellen Satz gets you a little excited.

I also owe Michel Le Borgne of IRISA, Rennes France a great many thanks for setting out in this direction before. The main result, i.e. theorem 3.3 was found by him for characteristic 3.

Finally the disposition of the report is:

Notation introduces the basic algebraic objects and notations, e.g. ideal and variety. Furthermore some basic connections between ideals and varieties is presented. Since we want to do explicit computations, Lagrange interpolating polynomials are also presented.

Ideals and Varieties contains the main results of the report such as an extension to Hilbert's Nullstellen Satz and a fairly complete characterization of the ideals in the polynomial rings we study.

Projections and Embeddings translate operations on varieties, such as projection and mapping, to the corresponding operations on ideals.

Computations show how the ideal theoretic formulations can be translated into Gröbner basis and polynomial remainder computations. Several computations are also performed directly on varieties (a luxury we can only afford for very small examples) to illustrate theorems. All computations are done in Mathematica [14].

2 Notation

This section introduces notation and some of the basic concepts such as *ideal* and *variety*. All results can be found in [6, 5, 7, 1, 9, 7, 11].

Let K and R denote a field and ring respectively. And let $R[x]$ denote the ring of polynomials in the variables $x_1, \ldots, x_n$, in particular we may write $K[x]$ to emphasize when R is also a field.

Definition 2.1 *An* ideal *a is a subset of $K[x]$ satisfying:*

- *a is a ring in itself, i.e. closed under addition and multiplication.*
- *If $p \in a$ then $qp \in a$ for all $q \in K[x]$.*

□

The obvious examples of ideals are $\{0\}$ and $K[x]$ (the ring itself), these are usually called the *trivial* ideals. All ideals (except $\{0\}$) are infinite, but by the celebrated Hilbert basis theorem we know that they are finitely generated, i.e. for each ideal a there exist a finite set of polynomials $\{p_1, \ldots, p_N\}$ such

$$a = \{\alpha_1 p_1 + \cdots + \alpha_N p_N : \alpha_1, \ldots, \alpha_N \in K[x]\}$$

and this is denoted $a = (p_1, \ldots, p_N)$ or $a = (\{p_1, \ldots, p_N\})$.

Example 2.1

- *Suppose we have the ring $C[z]$, i.e. polynomials in one variable with complex coefficients. And let $a = (p_1, p_2, \ldots, p_N)$ where then $a = (q = \gcd(p_1, \ldots, p_N))$ since by definition of* gcd *we have $C[z]q = C[z]p_1 + \cdots + C[z]p_N$. This is a case were all ideals are generated by a single polynomial, these are called* principal ideal domains *(PID).*
- *As a more concrete example take*

$$a = (q_1 = -2 + xy, q_2 = x + x^2 y)$$

then we have $-3x \in a$ since $-3x = xq1 - q2$. Generally it is very hard to decide wether or not a polynomial is a member of an ideal or not with general generating sets. By choice of particular generating sets–Gröbner bases–this becomes very simple as we shall see further on.

Definition 2.2 *A* variety *A is a subset of K^n for which there exist some polynomials $p_1, \ldots, p_N$ such that*

$$A = \{x \in K^n : p_1(x) = 0, \ldots, p_N(x) = 0\}$$

□

This is sometimes called *algebraic set* also, but we will stick to variety. A variety is thus the set of common zeros in the field K. In the case all polynomials are linear the variety is commonly called nullspace.

Example 2.2 *Let $K = R$ in all cases below:*

- *$A = \{1, 2, 3\}$ is a variety since $p = (x-1)(x-2)(x-3)$*
- *$A = \{\text{Unit circle}\}$ is a variety since $p = x^2 + y^2 - 1$*
- *$A = \{[t, \exp t] : t \in R\}$ is not a variety since e transcendental, i.e. no polynomial equation has e as zero.*

Notation: We will use small letters at the beginning of the alphabet (a,b, …) to denote ideals and corresponding capital letters (A,B,…) to denote their varieties. Also we will use letters (q,r,s) to denote elements of ideals and letters (u,v,w) to denote elements of varieties. Also let Ideals($K[x]$) denote the set of all ideals in $K[x]$ and let Pow(K) denote the set of all subsets of K.

We now have the following interesting functions:

Definition 2.3

- $I : \mathrm{Pow}(K^n) \to \mathrm{Ideals}(K[x])$ *defined as*

$$I(A) = \{p \in K[x] : \forall u \in A \; p(u) = 0\}$$

- $V : \mathrm{Ideal}(K[x]) \to \mathrm{Pow}(K^n)$ *defined as*

$$V(a) = \{u \in K^n : \forall p \in a \; p(u) = 0\}$$

□

There are some things one has to notice for these functions.

Example 2.3 *Suppose* $a = (x^2 + y^2 - 1)$ *then if*

- $K = C$ *we have* $V(a) = \text{Unit circle}$
- $K = Q$ *we have* $V(a) = \text{Rational points on unit circle}$
- $K = Z_2$ *we have* $V(a) = \{(0,1),(1,0)\}$

Hence the underlying field is important. Suppose $K = Z_p$ *then* $A \subset K^n$ *is finite and we can find a Lagrange polynomial* L *(see below on how to do this) such that* $I(A) = (L)$*, hence this is a PID.*

Although we in the next section more or less explicitly find ways to compute ideals associated with varieties in finite fields, Lagrange interpolating polynomials offer a very direct approach. More generally we will compute a polynomial $q \in Z_p[x]$ such $q(u_1, \ldots, u_n) = f(u_1, \ldots, u_n)$, where $f : Z_p^n \to Z_p$ is a given function. In particular this shows that any such f can be realized as a polynomial.

$$L_i(x) = \frac{x(x-1)\cdots(x-(i-1))(x-(i+1))\cdots(x-(p-1))}{(i-0)(i-1)\cdots(i-(i-1))(i-(i+1))\cdots(i-(p-1))} \in Z_p[x]$$

then

$$L_i(x) = \begin{cases} 1 & , x = i \\ 0 & , x \neq i \end{cases}$$

From this we can define

$$L_\alpha(x_1, \ldots, x_n) = L_{\alpha_1}(x_1) \cdots L_{\alpha_n}(x_n), \;\; \alpha \in Z_p^n$$

with the properties:

$$L_\alpha(x_1, \ldots, x_n) = \begin{cases} 1 & , [x_1, \ldots, x_n] = \alpha \\ 0 & , [x_1, \ldots, x_n] \neq \alpha \end{cases}$$

Then our sought polynomial q is given by:

$$q = \sum_{\alpha \in Z_p^n} L_\alpha(x_1, \ldots, x_n) f(\alpha) \tag{1}$$

Example 2.4 *Perform this in the ring $Z_3[x, y]$, i.e. $p = 3, n = 3$. Let*

$$A = \{(0,0), (1,0), (0,1), (2,2), (1,2), (0,2)\}$$

we then want to find a polynomial q such that

$$q(x,y) = \begin{cases} 0 & (x,y) \in A \\ 1 & (x,y) \notin A \end{cases}$$

By using equation (1) we obtain:

$$q = x + 2x^2 + 2x^2y + 2xy^2$$

We also have $V(q) = A$.

There are some interesting connections between ideals and varieties, these are (more or less) straight forward to show and the proofs can be found in [9].

Theorem 2.1 *Let $a_1, a_2 \in \mathrm{Ideals}(K[x_1, \ldots, x_n])$ then*

$$\begin{aligned} V((0)) &= K^n && (2) \\ V((1)) &= \emptyset && (3) \\ V(a_1 \cap a_2) &= V(a_1) \cup V(a_2) && (4) \\ V(a_1 + a_2) &= V(a_1) \cap V(a_2) && (5) \\ a_1 \subseteq a_2 &\Rightarrow V(a_1) \supseteq V(a_2) && (6) \end{aligned}$$

Let $A_1, A_2 \in \mathrm{Pow}(K^n)$ then

$$\begin{aligned} I(K^n) &= (0) && (7) \\ I(\emptyset) &= K[x_1, \ldots, x_n] && (8) \\ A_1 \subseteq A_2 &\Rightarrow I(A_1) \supseteq I(A_2) && (9) \end{aligned}$$

And combining these we have: ($a \in \mathrm{Ideals}(K[x_1, \ldots, x_n])$, $A \in \mathrm{Pow}(K^n)$)

$$\begin{aligned} I(V(a)) &\supseteq a && (10) \\ V(I(A)) &\supseteq A && (11) \\ I(V(I(A))) &= I(A) && (12) \\ V(I(V(a))) &= V(a) && (13) \end{aligned}$$

□

In general the first inclusions may be proper and we have to assert further conditions in order to get equality.

3 Ideals and Varieties

In this section we will state and prove our main results which were described in the introduction.

From theorem 2.1 we have:

$$I(V(a)) \supseteq a \tag{14}$$

$$V(I(A)) \supseteq A \tag{15}$$

and further conditions are needed to assert equality in these statements.

The obvious case when the inclusion in equation (15) is proper is when the set $A \subseteq K^n$ is not algebraic. This cannot happend in the case of finite characteristic.

Theorem 3.1 *Let p be prime, then*

$$\forall A \in \mathrm{Pow}(Z_p^n) \quad A = V(I(A))$$

□

Proof 3.1 *We already know $A \subseteq V(I(A))$ from theorem 2.1.*

The key observation needed to obtain $V(I(A)) \subseteq A$ is that each set $A \in \mathrm{Pow}(K^n)$ is algebraic since we can obtain a Lagrange polynomial having that particular set as kernel. From this we know that $I(A) \neq \emptyset$ (if $I(A) = \emptyset$ then $V(I(A)) = K^n$) and from this, the statement is a tautology.

See example 2.4 on how to compute Lagrange interpolating polynomials.

For equation (14) we have a sharper result, but we need the concept of *radical* ideal to state it.

Definition 3.1 *The* radical *ideal associated with $a \in \mathrm{Ideals}(K[x])$ is*

$$\sqrt{a} = \{p \in a : \exists n > 0 \; p^n \in a\}$$

Also an ideal a is radical iff $a = \sqrt{a}$. For later usage we also denote the set of radical ideals in a ring R by $\mathrm{Rad}(R)$. □

We then have Hilbert's Nullstellen Satz:

Theorem 3.2 (Nullstellen Satz)
Let K be algebraically closed (i.e. contains all polynomial roots) and let $a \in \mathrm{Ideals}(K[x])$, then:

- $a \neq (1) \Rightarrow V(a) \neq \emptyset$
- $I(V(a)) = \sqrt{a}$

□

The proof can be found in, e.g. [9]. The first statement says that we have zeros if the ideal is not (1) and this is something we can check using Gröbner bases, see further on. The second statement says that the possible extra elements we get by the I computation are those needed to make the ideal radical.

Unfortunately fields of finite characteristic are not algebraically closed so this theorem does not apply. However we have the following:

Theorem 3.3 *Let p be prime then*

$$\forall a \in \text{Ideals}(Z_p[x])\ I(V(a)) = a + (x_1^p - x_1, \ldots, x_n^p - x_n)$$

$\square$

This is an extension to the second statement of the Hilbert Nullstellen Satz to a certain class of fields which isn't algebraically closed.

We will prove the theorem through a series of lemmas which in themselves should provide some characterization of the ideals in $Z_p[x_1, \ldots, x_n]$.

First we can calculate $I(A)$ for some particular sets $A \subseteq Z_p^n$.

Lemma 3.1

$$I(Z_p^n) = (x_1^p - x_1, \ldots, x_n^p - x_n) = (x^p - x)$$

$\square$

Proof 3.2 *We have*

$$\forall y \in Z\ y^{p-1} = 1 \bmod p$$

by Fermats little theorem and hence

$$\forall y \in Zp\ y^p - y = 0$$

In particular this says

$$y^p - y = y(y-1)\cdots(y-(p-1))$$

This proves $(x^p - x) \subseteq I(Z_p^n)$.

Suppose there exist some element $q \in I(Z_p^n) - (x^p - x)$. We will prove $q = 0$ by induction on the number of variables (n).

$n = 1$ *We know that $\deg(q) < p$, i.e. of the form*

$$q = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_{p-1} x_1^{p-1}$$

Since $q \in I(Z_p)$ we have

$$\begin{aligned} r(0) &= 0 \\ &\vdots \\ r(p-1) &= 0 \end{aligned}$$

Writing these equation using matrices we obtain:

$$\begin{bmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{p-1} \end{bmatrix} \begin{bmatrix} 1 & 1 & \dots & 1 \\ u_0 & u_1 & \dots & u_{p-1} \\ \vdots & \vdots & & \vdots \\ u_0^{p-1} & u_1^{p-1} & \dots & u_{p-1}^{p-1} \end{bmatrix} = 0$$

where $u_0 = 0, u_1 = 1, \dots, u_{p-1} = p-1$. *The matrix in the above equation is a Vandermonde matrix whose determinant equals*

$$\prod_{0 \le i < j < p} (u_i - u_j) \neq 0$$

hence we have $\alpha_0 = \cdots = \alpha_{p-1} = 0$, *i.e.* $q = 0$.

$n = k+1$ *Assume we have proved the statement for* $n \le k$. *Let the* k *first variables be* $x = [x_1, \dots, x_k]$ *and the* $k+1$ *variable be* y. *We can then write*

$$q = \alpha_0 + \alpha_1 y + \cdots + \alpha_{p-1} y^{p-1}$$

with $\alpha_i \in Z_p[x]$ *and of degree less than* p. *Using the same idea as in the case* $n = 1$ *we see that*

$$\forall u \in Z_p^k \ \alpha_i(u) = 0 \ i = 0, \dots, p-1$$

and by induction this means $\alpha_i = 0 \ i = 0, \dots, p-1$.

This proves $I(Z_p^n) - (x^p - x) = 0$, *i.e.* $I(Z_p^n) = (x^p - x)$.

From this lemma it is natural to consider the ring

$$R_p[x] = Z_p[x_1, \dots, x_n]/(x_1^p - x_1, \dots, x_n^p - x_n) = Z_p[x]/(x^p - x)$$

We also use the notation R_p^n, $R_p[x_1, \dots, x_n]$ and $R_p^n[x]$ to denote this ring. In this ring theorem 3.3 becomes

$$\forall a \in R_p[x] \quad I(V(a)) = a$$

We will continue to characterize the various ideals that can occur in particular we will check the prime ideals:

Definition 3.2 *An ideal* a *is* prime *if*

$$pq \in a \Rightarrow p \in a \text{ or } q \in a$$

We denote the set of prime ideals in the ring R *by* $Spec(R)$. □

In particular one may note that every primeideal is radical, i.e. we have

$$\mathrm{Spec}(R) \subseteq \mathrm{Rad}(R) \subseteq \mathrm{Ideals}(R)$$

We now have:

Lemma 3.2

$$\mathrm{Spec}(R_p[x]) = \{(x_1 - u_1, \ldots, x_n - u_n) : u_i \in Z_p \quad i = 1, \ldots, n\}$$

$\square$

Proof 3.3 *Let $a \in \mathrm{Spec}(R_p[x])$, then*

$$\begin{aligned} a \ni 0 \quad &= x_1^p - x_1 \quad &= x_1(x_1 - 1)\cdots(x_1 - (p-1)) \\ &\cdots &\cdots \\ &= x_n^p - x_n \quad &= x_1(x_n - 1)\cdots(x_n - (p-1)) \end{aligned}$$

Since a is prime we have

$$\forall i \, \exists j \quad x_i - u_j \in a$$

Furthermore a can only hold one such linear factor for each variable x_i, otherwise

$$x_i - k, x_i - l \in a \Rightarrow \frac{1}{l-k}((x_i - k) - (x_i - l)) = 1 \in a$$

which in turn imply $a = R_p[x]$.

Now let $p \in a$ be arbitrary, since $x_i - u_i \in a \quad i = 1, \ldots, n$ we can write

$$p = q_1(x_1 - u_1) + \cdots + q_n(x_n - u_n) + r$$

where r is a constant. If $r \neq 0$ then

$$1 = \frac{1}{r} r(\underbrace{p}_{\in a} - \underbrace{q_1(x_1 - u_1)}_{\in a} - \cdots - \underbrace{q_n(x_n - u_n)}_{\in a}) \in a$$

and again this implies $a = R_p[x]$. Hence $r = 0$. This proves

$$a = (x_1 - u_1, \ldots, x_n - u_n)$$

We save the following result for future use:

Lemma 3.3 *Let $u \in Z_p^n$ then*

$$I(\{u\}) = (x_1 - u_1, \ldots, x_n - u_n)$$

$\square$

Proof 3.4 *Obviously $(x_1 - u_1, \ldots, x_n - u_n) \subseteq I(\{u\})$ and let $q \in I(\{u\})$ we can then write*

$$q = \sum_{1 \leq i \leq n} \alpha_i(x_i - u_i) + r$$

with r constant using the same argument as in lemma 3.2 we have $r = 0$, i.e. $q \in (x_1 - u_1, \ldots, x_n - u_n)$. This proves the lemma.

The following lemma shows that ideals in these rings really have special properties.

Lemma 3.4

$$\mathrm{Ideals}(R_p[x]) = \mathrm{Rad}(R_p[x])$$

$\square$

Proof 3.5 *In $R_p[x]$ we have*

$$(x_1^{i_1} \cdots x_n^{i_n})^p = ((x_1^p)^{j_1} \cdots (x_n^p)^{j_n}) = x_1^{i_1} \cdots x_n^{i_n} \tag{16}$$

and also if we let X_i denote monomials in $R_p[x]$

$$(\sum_{j \in Z_p^n} \alpha_j X_j)^p = \sum_{j \in Z_p^n} \alpha_j^p X_j^p = \sum_{j \in Z_p^n} \alpha_j X_j \tag{17}$$

The last equality in 17 is simply using 16 and Fermats little theorem. The middle equality comes from the fact that using the binomial theorem we get

$$(\alpha + \beta)^p = \sum_{0 \leq m \leq p} \binom{p}{m} \alpha^{p-m} \beta^m$$

and hence p divides every intermediate term, thus we get

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

Using induction on the number of terms we then obtain the middle equality in 17.

To summarize this means

$$\forall q \in R_p[x] \;\; q^p = q \tag{18}$$

Let $a \in \mathrm{Ideals}(R_p[x])$ and suppose $q^m \in a$, by equation 18 we then have

$$q^{p-m} q^m = q^p = q \in a$$

and hence $a \in Rad(R_p[x])$, i.e. $\mathrm{Rad}(R_p[x]) = \mathrm{Ideals}(R_p[x])$.

We are now ready to prove theorem 3.3 through our set of lemmas.

Proof 3.6 (of Theorem 3.3)

By the Noether-Lasker decomposition theorem for ideals ([1], pg. 83) any radical ideal a can be written as:

$$a = a_1 \cap \cdots \cap a_k \;\; a_i \in \mathrm{Spec}(R_p[x]) \tag{19}$$

By lemma 3.4 we have $\mathrm{Ideals}(R_p[x]) = \mathrm{Rad}(R_p[x])$ *and hence this also characterizes all ideals in terms or prime ideals. By lemma 3.2 all prime ideals are of the form:*

$$(x_1 - u_1, \ldots, x_n - u_n) \;\; u \in Z_p^n$$

denote this ideal by a_u. *Hence any ideal* $a \in \mathrm{Ideals}(R_p[x])$ *is of the form:*

$$a = a_{u^1} \cap \cdots \cap a_{u^k} \;\; u^i \in Z_p^n$$

Calculating the variety associated with a we get (using theorem 2.1)

$$\begin{aligned} V(a) &= V(a_{u^1} \cap \cdots \cap a_{u^k}) \\ &= V(a_{u^1}) \cup \cdots \cup V(a_{u^k}) \\ &= \{u^1\} \cup \cdots \cup \{u^k\} \\ &= \{u^1, \ldots, u^k\} \end{aligned}$$

On the other hand any $A \in \mathrm{Pow}(Z_p^n)$ *is finite, i.e.*

$$A = \{u^1, \ldots, u^k\} \;\; u^i \in Z_p^n$$

By use of lemma 3.3 we can calculate its ideal through: (again using theorem 2.1)

$$\begin{aligned} I(A) &= I(\{u^1, \ldots, u^k\}) \\ &= I(\{u^1\} \cup \cdots \cup \{u^k\}) \\ &= I(\{u^1\}) \cap \cdots \cap I(\{u^k\}) \\ &= a_{u^1} \cap \cdots \cap a_{u^k} \end{aligned}$$

Summarizing we get $I(V(a)) = a \;\forall a \in \mathrm{Ideals}(R_p[x])$.

This completely clarifies the relation between ideals and varieties. One of the nice things about this is that you may formulate computations in terms of varieties and translate that into computations on ideals. See section 5 for how this gets translated into Gröbner basis and polynomial remainder computations as well as explicit examples.

4 Projections and Embeddings

In this section we investigate operations on varieties such as projections and mappings and translate that to ideal theoretic operations. In a sense this means translating intrinsic operations to coordinate based ones.

Suppose we have a variety and want to only look at certain components of this, i.e. we want to project in the variety. First some notation:

Definition 4.1 *If* $A \subseteq Z_p^n$, *i.e.* $A = \{[u_1^i, \ldots, u_n^i] : i = 1, \ldots, N\}$ *then*

$$P_{[l_1,\ldots,l_k]}(A) = \{[u_{l_1}^i, \ldots, u_{l_k}^i] : [u_1^i, \ldots, u_n^i] \in A \;\; i = 1, \ldots, N\}$$

□

If we have an underlying ring of the form $R_p^{n+m}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ then we may informally write P_x to stand for $P_{[1,\ldots,n]}$.

For projections we have the following nice theorem:

Theorem 4.1 *Suppose*

$$a \in R_p^{n+m}[x, y], \quad x = [x_1, \ldots, x_n], \quad y = [y_1, \ldots, y_m]$$

then

$$a \cap R_p^n[x] = I(P_x(V(a)))$$

□

Another way to state the theorem would be to say that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Ideals}(R_p[x,y]) & \xrightarrow{\cap R_p[x]} & \mathrm{Ideals}(R_p[x]) \\ V \downarrow \uparrow I & & V \downarrow \uparrow I \\ \mathrm{Pow}(Z_p^{m+n}) & \xrightarrow{P_x} & \mathrm{Pow}(Z_p^n) \end{array} \tag{20}$$

Proof 4.1 *Suppose* $a = (x_1 - u_1, \ldots, x_n - u_n, y_1 - v_1, \ldots, y_m - v_m)$ *then* $a \cap R_p^n[x] = (x_1 - u_1, \ldots, x_n - u_n)$ *since obviously* $(x_1 - u_1, \ldots, x_n - u_n) \subseteq a \cap R_p^n[x]$ *and let* q *be any element in* $a \cap R_p^n[x]$ *then*

$$q = \sum_{1 \le i \le n} q_i(x_i - u_i) + r$$

with r *constant. Again this implies* $r = 0$*, i.e. we have*

$$a \cap R_p^n[x] = (x_1 - u_1, \ldots, x_n - u_n)$$

For any $a \in \mathrm{Ideals}(R_p^{n+m}[x, y])$ *we have*

$$a = a_{w^1} \cap \cdots \cap a_{w^m}$$

for some $w^j = [u_1^j, \ldots, u_n^j, v_1^j, \ldots, v_m^j] \in Z_p^{n+m}$*. Hence*

$$a \cap R_p^n[x] = (a_{w^1} \cap R_p^n[x]) \cap \cdots \cap (a_{w^m} \cap R_p^n[x]) = a_{u^1} \cap \cdots \cap a_{u^m}$$

On the other hand we also have

$$I(P_x(V(a))) = I(P_x(\{w^1, \ldots, w^m\})) = I(\{u^1, \ldots, u^m\}) = a_{u^1} \cap \cdots \cap a_{u^m}$$

This proves the theorem.

We will see further on how to use elimination theory to compute $a \cap R_p^n[x]$.

Another important computation is to map your variety onto another variety and the corresponding computation on the ideals defining the variety is the pullback. This is a standard trick used in differential geometry.

Formally this is how it goes:

Definition 4.2 *Let* $P : Z_p^n \rightarrow Z_p^m$ *then the pullback* $P^* : R_p^m[y] \rightarrow R_p^n[x]$ *is defined by*

$$\forall q \in R_p^m[y] \;\; P^*(q(y)) = q(P(x)) \in R_p^n[x]$$

□

Note that every function $P : Z_p^n \rightarrow Z_p^m$ is a polynomial so this P^* is well defined. In commutative algebra P^* is commonly called a *ringmap* or a *ringhomomorphism.*

This theorem will clarify the relation to ideals and varieties.

Theorem 4.2 *Let* $a \in \mathrm{Ideals}(R_p^m[y])$*,* $A \in \mathrm{Pow}(Z_p^n)$ *and* $P : Z_p^n \rightarrow Z_p^m$*, then*

$$\begin{aligned} I(P(A)) &= P^{*-1}(I(A)) &(21)\\ V(P^*(a)) &= P^{-1}(V(a)) &(22) \end{aligned}$$

□

Proof 4.2 *Let us start with the first item. Firs we have*

$$\begin{array}{lll} q \in P^{*-1}(I(A)) & & \\ & \Rightarrow & P^* \in I(A) \\ & \Leftrightarrow & \forall u \in Z_p^n \;\; q(P(u)) = 0 \\ & & \Rightarrow q \in I(P(A)) \\ & P^{*-1}(I(A)) \subseteq I(P(A)) & \end{array}$$

The other way around

$$\begin{array}{lll} r \in I(P(A)) & & \\ & \Leftrightarrow & \forall u \in A \;\; r(P(u)) = 0 \\ & \Leftrightarrow & P^* r \in I(A) \\ & \Rightarrow & r \in P^{*-1}(\{P^* r\}) \subseteq P^{*-1}(I(A)) \\ & I(P(A)) \subseteq P^{*-1}(I(A)) & \end{array}$$

This proves the first item. For the second one:

$$\begin{array}{lll} u \in P^{-1}(V(a)) \subseteq Z_p^n & & \\ & \Rightarrow & P(u) \in V(a) \subseteq Z_p^m \\ & \Rightarrow & \exists q \in a \;\; q(P(u)) = P^* q(u) = 0 \\ & \Rightarrow & u \in V((P * (a))) \\ & P^{-1}(V(a)) \subseteq V((P^*(a))) & \end{array}$$

The other way we have

$$
\begin{array}{llll}
u \in V((P^*(a))) \subseteq Z_p^n & & & \\
 & \Rightarrow & & \forall q \in a \;\; P^* q(u) = 0 \\
\text{Let } v = P(u) \in Z_p^m & \Rightarrow & & \forall q \in a \;\; q(v) = 0 \\
 & \Rightarrow & & v \in V(a) \\
 & \Rightarrow & & u \in P^{-1}(v) \subseteq P^{-1}(V(a)) \\
 & & V((P^*(a))) \subseteq P^{-1}(V(a)) &
\end{array}
$$

And this proves the theorem.

Restating the theorem in terms of commutative diagrams:

$$
\begin{array}{ccc}
\text{Ideals}(R^m[y]) & \xrightarrow{P^*} & \text{Ideals}(R^n[x]) \\
V \downarrow \uparrow I & & V \downarrow \uparrow I \\
\text{Pow}(Z_p^m) & \xleftarrow{P} & \text{Pow}(Z_p^n)
\end{array}
\tag{23}
$$

5 Computations

This section will show how one can perform the computations associated with the last two sections. In particular we will use Gröbner bases, see [2, 10, 8] for more on this.

Since the prime tool will be Gröbner bases any of the major computer algebra packages, e.g. Mathematica [14], Macsyma [13], Reduce [4] or Maple [3] is a candidate. In this case Maple though, is not appropriate since it doesn't support modular arithmetic in connection with Gröbner basis computations. Also some more algebraic packages such as Macaulay [12] and CoCoA are candidates. Since we however want to perform much more computations than the purely algebraic ones its better to choose one of the larger computer algebra packages. In this particular case we chose Mathematica. In most examples the code is self explanatory and comments before and after an example will cover most other cases.

We will initially do a series of computations to illustrate theorems 3.1 and 3.3.

$V(a)$ We assume that a is given in the form $a = (q_1, \ldots, q_m)$. To compute the variety is the same as solving the set of equations

$$q_1(x_1, \ldots, x_n) = 0, \ldots, q_m(x_1, \ldots, x_n) = 0$$

There exist several methods for this. In our small example its enough to use the stupendous method of trying all possible solutions in Z_p^n.

As a specific example, take:

$$a = (F) = (\{1 + x_1 x_2, x_1 + x_2\}), \;\; a \in \text{Ideals}(R_p[x_1, x_2])$$

```
In[1]:= <<Variety.m

In[2]:= F = {1 + x1 x2, x1 + x2};

In[3]:= X = {x1,x2};

In[4]:= FunctionTable[ F, X, 5 ]//Short

Out[4]//Short=

>   {{{0, 0}, {1, 0}}, {{0, 1}, {1, 1}}, <<22>>, {{4, 4}, {2, 3}}}

In[5]:= A = Variety[ F, X, 5 ]

Out[5]= {{1, 4}, {4, 1}}
```

where `FunctionTable[]` computes a list of the form: $\{[u, f(u)] : u \in Z_p^n\}$ and `Variety[]` picks out the elements of this list where $f(u) = 0$. Hence we have $V(a) = \{[1,4],[4,1]\}$.

$I(A)$ There are really several possibilities on how to do this. From the proof of theorem 3.3 we see that $I(A)$ is described as:

$$I(A) = I(\{u^1, \ldots, u^m\}) = a_{u^1} \cap \cdots \cap a_{u^m}$$

where $a_u = (x_1 - u_1, \ldots, x_n - u_n)$.
Another way would be to consider a function $f : Z_p^n \to Z_p$ such that:

$$f(u) = \begin{cases} 1, & u \in A \\ 0, & u \notin A \end{cases}$$

and then realize this function as a polynomial through, e.g. Lagrange interpolation as was shown in section 2. This is what the function `Ideal[]` does. Continuing on the previous example we get:

```
In[6]:= <<Ideal.m

In[7]:= G = Ideal[ A, X, 5 ]

                          3           2   2        4   2          3
Out[7]= {1 + 2 x1 x2 + 2 x1  x2 + 3 x1  x2  + 3 x1  x2  + 2 x1 x2  +

           3   3        2   4       4   4
>     2 x1  x2  + 3 x1  x2  + 3 x1  x2 }
```

As can be seen from this, the ideal, $b = (G)$, that is produced in this manner is generated by a single polynomial, i.e. principal. If our proof of theorem 3.3 is correct then we have $(F) = a = b = (G)$ although it is far from obvious right now. See below for a proof of this.

$V(I(A))$ Theorem 3.1 states that $V(I(A)) = A$ and we can check it on this example:

```
In[8]:= Variety[ G, X, 5 ]

Out[8]= {{1, 4}, {4, 1}}
```

So $V((G)) = V((F)) = \{[1,4],[4,1]\}$.

$I(V(a))$ As was seen above $(G) = I(V((F)))$, but $G \neq F$ so we cannot immediately conclude this equality. Ideal equality can be checked by use of Gröbner basis computation, see [2]. The criterion is that you should get the same autoreduced Gröbner basis. Another criterion is of course to check subideal inclusion which also done with Gröbner bases.

```
In[9]:= SubidealQ[G,F,X,5]

Out[9]= True

In[10]:= SubidealQ[F,G,X,5]

Out[10]= True
```

So indeed the ideals are the same as stated

Gröbner basis computations is of course the tool to use in order to check ideal equality, but in this case we can even do it explicitly. Of course this can only be carried out for toy examples, since:

$$R_p[x_1, \ldots, x_{n-1}, x_n] = \sum_{0 \leq i < p} R_p[x_1, \ldots, x_{n-1}] x_n^i$$

and the sum on the right hand side is disjoint. Hence if we let $l(n,p) = |R_p[x_1, \ldots, x_n]|$ then we get the following difference equation:

$$l(n,p) = l(n-1,p)^p, \quad l(1,p) = p^p$$

Solving this we get $l(n,p) = p^{p^n}$. In the example used above we had $p = 5,\ n = 2$ so the ring contains $5^{5^2} = 298023223876953125 \approx 2.98 10^{17}$ terms. Noticing that the estimated lifespan of the solarsystem is on the order of 10^{17} seconds we abandon this project. Instead we study the case $n = 2,\ p = 2$ and use the example:

$$F_1 = \{1 + x_1 x_2, x_1 + x_2\}, \quad F_2 = I(V(F_2))$$

```
In[1]:= <<Ideal.m

In[2]:= <<Variety.m
```

```
In[3]:= F1 = {q1 = 1 + x1 x2, q2 = x1 + x2};

In[4]:= F2 = Ideal[ Variety[F1,X,2], X, 2 ]

Out[4]= {1 + x1 x2}
```

The ideal a generated by a finite set $F = \{f_1, \ldots, f_m\}$, is:

$$a = (F) = \{\alpha_1 f_1 + \cdots + \alpha_m f_m : \alpha_i \in R[x]\} = R[x]f_1 + \cdots + R[x]f_n$$

where $R[x] = R_p[x_1, \ldots, x_n]$ in our case. One slight complication is that

$$R_p[x_1, \ldots, x_n] = Z_p[x_1, \ldots, x_n]/(x_1^p - x_1, \ldots, x_n^p - x_n)$$

However this is also a simplification because otherwise we wouldn't have a finite computation[1]. Anyway as far as computation goes, we only need to enumerate all polynomials in $R_2[x_1, x_2]q_1 + R_2[x_1, x_2]q_2$ and then compute their remainder w.r.t. the Gröbner basis of $(x_1^2 - x_1, x_2^2 - x_2)$. This results in a unique representative in $R_2[x_1, x_2]$. In this example:

```
In[5]:= (Rpx = R[X,2]) //Short

Out[5]//Short=

>   {0, 1, x1, <<11>>, x1 + <<1>> + x1 x2, 1 + x1 + x2 + x1 x2}

In[6]:= ring = GB[{},X,2]

                        2            2
Out[6]= {-2 -> 0, x2  -> -x2, x1  -> -x1}

In[7]:= a1 = Union[ Rem[SetPlus[ q1 Rpx, q2 Rpx ], ring] ]

Out[7]= {0, 1 + x1, 1 + x2, x1 + x2, 1 + x1 x2, x1 + x1 x2,

>    x2 + x1 x2, 1 + x1 + x2 + x1 x2}

In[8]:= a2 = Union[ Rem[ F2[[1]] Rpx, ring ] ]

Out[8]= {0, 1 + x1, 1 + x2, x1 + x2, 1 + x1 x2, x1 + x1 x2,

>    x2 + x1 x2, 1 + x1 + x2 + x1 x2}
```

where **Rpx** $= R_2[x_1, x_2]$, **ring** $= GB(\{x_1^2 + x_1, x_2^2 + x_2\})$, **SetPlus[s1,s2]** is set addition and **Rem[F, G]** computes the remainders of **F** w.r.t. the Gröbner basis **G**.

As can be seen from this computation the theorem is indeed valid[2].

Now to illustrate theorem 4.1, assume we have

$$a \in \text{Ideals}(R_p[x1, x2, y1, y2]) \quad a = (x_1 + x_2 y_1, x_1 y_1 y_2 + x_2)$$

[1] This would be somewhat complicated ...

[2] Well at least in this case ...

we want to do show that

$$a \cap R_p[x1, x2] = I(P_x(V(a)))$$

Computing the left hand side we obtain:

```
In[1]:= a = {x1 + x2 y1, x1 y1 y2 + x2};

In[2]:= r = {x1^2 + x1, x2^2 + x2, y1^2 + y1, y2^2 + y2, Modulus - 2};

In[3]:= gb = GroebnerBasis[ Join[ a, r ], {y1, y2, x1, x2} ]

                       2                                            2
Out[3]= {-2, x2 + x2 , x1 + x2, x2 + x2 y2, y2 + y2 , x2 + x2 y1,

               2
>      y1 + y1 }

In[4]:= G1 = gb[[{3}]]

Out[4]= {x1 + x2}
```

Where we need the polynomials in **r** in order to do computations in $R_2[x, y]$ and the **GroebnerBasis[]** command computes the Gröbner basis w.r.t. to a ranking such that $\{y_1, y_2\} \gg \{x_1, x_2\}$. We then obtain $a \cap R_2[x_1, x_2]$ by extracting the polynomials containing only polynomials in $\{x_1, x_2\}$ from this Gröbner basis. (The -2 is a Mathematica bug.)

So $a \cap R_2[x_1, x_2] = (x_1 + x_2)$. Similarly computing the right hand side we get:

```
In[5]:= <<Variety.m

In[6]:= A = Variety[ a, {x1,x2, y1, y2}, 2 ]

Out[6]= {{0, 0, 0, 0}, {0, 0, 0, 1}, {0, 0, 1, 0}, {0, 0, 1, 1},

>      {1, 1, 1, 1}}

In[7]:= Ax = Union[ Project[ A, {1,2} ] ]

Out[7]= {{0, 0}, {1, 1}}

In[8]:= <<Ideal.m

In[9]:= G2 = Ideal[ Ax, {x1,x2}, 2 ]

Out[9]= {x1 + x2}
```

Where `Project[ A, {1,2} ]` projects onto the first two coordinates.

So $I(P_x(V(a))) = (x_1 + x_2)$ and hence we have $a \cap R_2[x1, x2] = I(P_x(V(a)))$.

References

[1] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[2] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. Dordrecht Reidel, 1985.

[3] B. Char, K.O. Geddes, G.H. Gonnet, M.B. Monagan, and S.M. Watt. *Maple Reference Manual.* Symbolic Computation Group, Univ. of Waterloo, fifth edition, March 1988.

[4] A.C. Hearn. *Reduce User's Manual.* Rand Corp., Santa Monica, 1987.

[5] S. Lang. *Algebra.* Addison-Wesley, 1984.

[6] H. Matsumura. *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics 8. Cambridge University Press, 1986.

[7] D. Mumford. *The Red Book of Varieties and Schemes*, volume 1388 of *Lect. Notes in Math.* Springer, 1988.

[8] F. Pauer and M. Pfeifhofer. The theory of Gröbner bases. *L'Enseignement Mathématique*, 34:215–232, 1988.

[9] M. Reid. *Undergraduate Algebraic Geometry*, volume 12 of *London Mathematical Society Student Texts.* Cambridge University Press, 1988.

[10] L. Robbiano. Gröbner bases: a foundation for commutative algebra. Internal. Email: robbiano@igecuniv (bitnet).

[11] I.R. Shafarevich. *Basic Algebraic Geometry.* Springer, 1974.

[12] Maureen Stillman, Michael Stillman, and Dave Bayer. *Macaulay User Manual.* bayer@zariski.harvard.edu, first edition, October 1989. A TEX document available with the software.

[13] Symbolics Inc. *Macsyma Reference Manual*, November 1988. Version 13.

[14] S. Wolfram. *Mathematica. A System for Doing Mathematics by Computer.* Addison-Wesley, second edition, 1991.