Part three

Gauss, Euclid, Buchberger: Elementary Gröbner Bases

And when he had opened the third seal, I heard the third beast say, Come and see. And I beheld, and lo a black horse; and he that sat on him had a pair of balances in his hand.

And I heard a voice in the midst of the four beasts say, A measure of wheat for a penny, and three measures of barley for a penny; and see thou hurt not the oil and the wine.

Revelation (Authorized Version)

The things depending from Mars: choler, iron, diamond, hellebore, horse, vulture, pike.

E. C. Agrippa, *De occulta phylosophia*

The country . . . shopkeepers don't have it!

J.-R. Hèbert, *Père Duchesne*

20

Hilbert

This introductory chapter will discuss how to generalize the notion of 'solving' from the univariate to the multivariate polynomial case introducing the central tools and problems related to multivariate solving.

I will discuss the relation between systems of equations and roots, discussing the duality between affine algebraic varieties and ideals which is implied by Hilbert's Basissatz and Nullstellensatz (Section 20.1); after an *a parte* comment on the ability to perform suitable change of coordinates (Section 20.2), I can prove Hilbert's Nullstellensatz (Section 20.3) and discuss the solver proposed by Kronecker (Section 20.4). I then generalize the duality between varieties and ideals in the projective setting connecting projective varieties and homogeneous ideals (Section 20.5).

In the rest of the chapter I discuss Hilbert's problem of computing 'the number of independent conditions which must be satisfied by the coefficients of a homogeneous polynomial' in order to be a member of a given ideal; this leads to the introduction of the notions of syzygies, free resolutions and the Hilbert function (Section 20.6 and 20.7).

Finally I will present the proofs by Hilbert and Gordan of the Basissatz (Section 20.8).

20.1 Affine Algebraic Varieties and Ideals

Let k be an infinite, perfect field, where, if $p := \mathrm{char}(k) \neq 0$, it is possible to extract pth roots,[1] and let k be an algebraically closed extension of k. Let us

[1] This is the general setting dealt with by the volume, except for Chapters 37 and 38 where moreover $\mathrm{char}(k) = 0$.

These restrictions can be relaxed in most of the volume, but, knowing my absentmindedness, I consider it safer to leave to the reader the responsibility of doing so.

fix an integer value n and let us consider the polynomial ring

$$\mathcal{P} := k[X_1, \ldots, X_n]$$

and the (n-dimensional) *affine space*

$$\mathsf{k}^n := \{(a_1, \ldots, a_n), a_i \in \mathsf{k}\}.$$

On the one hand, we can consider a system of equations

$$f_1(X_1, \ldots, X_n) = \cdots = f_s(X_1, \ldots, X_n) = \cdots = 0,$$

$f_i \in \mathcal{P}$, and look for its roots in k^n; on the other hand we can consider a subset $\mathsf{Z} \subset \mathsf{k}^n$ and wonder which polynomials satisfy them.

Therefore we denote

- for any set $F \subset \mathcal{P}$, by $\mathcal{Z}(F)$ the set of the common roots of all polynomials in F:
$$\mathcal{Z}(F) := \{\mathsf{a} \in \mathsf{k}^n : f(\mathsf{a}) = 0, \quad \text{for all } f \in F\} \subset \mathsf{k}^n;$$
- for any set $\mathsf{Z} \subset \mathsf{k}^n$, by $\mathcal{I}(\mathsf{Z})$ the set of all the polynomials vanishing in Z:
$$\mathcal{I}(\mathsf{Z}) := \{f \in \mathcal{P} : f(\mathsf{a}) = 0, \quad \text{for all } \mathsf{a} \in \mathsf{Z}\} \subset \mathcal{P}.$$

Definition 20.1.1. *Let* A *be a ring; a non-empty subset* $\mathsf{I} \subset \mathsf{A}$ *is an* ideal *if*

- *for each* $a_1, a_2 \in \mathsf{I}$, $a_1 - a_2 \in \mathsf{I}$,
- *for each* $a \in \mathsf{I}$, $b \in \mathsf{A}$, $ab \in \mathsf{I}$.

For any set $G \subset \mathsf{A}$ *the ideal generated by* G *is the set of all the finite sums*

$$\left\{\sum_{i=1}^{s} h_i f_i : h_i \in \mathsf{A}, \quad f_i \in G\right\}$$

and is denoted by (G).

Lemma 20.1.2. *For any set* $\mathsf{Z} \subset \mathsf{k}^n$, $\mathcal{I}(\mathsf{Z})$ *is an ideal.*

Proof. For each $f_1, f_2 \in \mathcal{I}(\mathsf{Z})$, $g_1, g_2 \in \mathcal{P}$ and each $\mathsf{a} \in \mathsf{Z}$:

$$(g_1 f_1 + g_2 f_2)(\mathsf{a}) = g_1(\mathsf{a}) f_1(\mathsf{a}) + g_2(\mathsf{a}) f_2(\mathsf{a}) = 0.$$

♂

Therefore, when we consider a system of equations

$$f_1(X_1, \ldots, X_n) = \cdots = f_s(X_1, \ldots, X_n) = \cdots = 0$$

we can, on the one hand consider the ideal $\mathsf{I} = (f_1, \ldots, f_s, \ldots)$, and on the other hand restrict ourselves wlog to the case of *finite* systems, because

Fact 20.1.3 (Hilbert's (affine) Basissatz). *For each ideal* $\mathsf{I} \subset \mathcal{P}$ *there is a finite set* $\{f_1, \ldots, f_s\} \subset \mathsf{I}$ *such that* $\mathsf{I} = (f_1, \ldots, f_s)$.

Proof. Compare Section 20.8. ♂

A partial duality between $\mathcal{Z}$ and $\mathcal{I}$ can already be obtained. In fact:

Corollary 20.1.4. *For any ideals* $\mathsf{I}, \mathsf{I}_1, \mathsf{I}_2 \subset \mathcal{P}$ *and any set* $\mathsf{Z}, \mathsf{Z}_1, \mathsf{Z}_2 \subset \mathsf{k}^n$, *we have:*

- $\mathsf{I}_1 \subset \mathsf{I}_2 \implies \mathcal{Z}(\mathsf{I}_1) \supset \mathcal{Z}(\mathsf{I}_2)$;
- $\mathsf{Z}_1 \subset \mathsf{Z}_2 \implies \mathcal{I}(\mathsf{Z}_1) \supset \mathcal{I}(\mathsf{Z}_2)$;
- $\mathcal{Z}(\mathsf{I}_1 + \mathsf{I}_2) = \mathcal{Z}(\mathsf{I}_1) \cap \mathcal{Z}(\mathsf{I}_2)$;
- $\mathcal{I}(\mathsf{Z}_1 \cup \mathsf{Z}_2) = \mathcal{I}(\mathsf{Z}_1) \cap \mathcal{I}(\mathsf{Z}_2)$;
- $\mathcal{Z}(\mathsf{I}_1 \cap \mathsf{I}_2) = \mathcal{Z}(\mathsf{I}_1) \cup \mathcal{Z}(\mathsf{I}_2)$;
- $\mathcal{Z}\mathcal{I}(\mathsf{Z}) \supset \mathsf{Z}$;
- $\mathcal{I}\mathcal{Z}(\mathsf{I}) \supset \mathsf{I}$;
- $\mathcal{I}\mathcal{Z}\mathcal{I}(\mathsf{Z}) = \mathcal{I}(\mathsf{Z})$;
- $\mathcal{Z}\mathcal{I}\mathcal{Z}(\mathsf{I}) = \mathcal{Z}(\mathsf{I})$. ♂

The experience with the univariate case discussed in the first volume should be sufficient to make clear that duality can be obtained only if suitably restricted, since not each subset $\mathsf{Z} \subset \mathsf{k}^n$ can be a set of roots of a polynomial system of equations; not only must Z be closed to k-conjugation, but dealing transcendency cannot be resolved elementarily by extending k to $\mathbb{R}$. Only consider $\mathsf{Z} := \{(a, \exp(a)) : a \in \mathbb{R}\}$.

This leads to

Definition 20.1.5. *A set* $\mathsf{Z} \subset \mathsf{k}^n$ *is called an* affine algebraic variety *if there is an ideal* $\mathsf{I} \subset \mathcal{P}$ *such that* $\mathsf{Z} = \mathcal{Z}(\mathsf{I})$,

which gives one side of the required duality:

Lemma 20.1.6. *For each affine algebraic variety* Z,

$$\mathcal{Z}(\mathcal{I}(\mathsf{Z})) = \mathsf{Z}.$$

Proof. By assumption we have $\mathsf{Z} = \mathcal{Z}(\mathsf{I})$ for an ideal I, therefore

$$\mathsf{Z} = \mathcal{Z}(\mathsf{I}) = \mathcal{Z}\mathcal{I}\mathcal{Z}(\mathsf{I}) = \mathcal{Z}(\mathcal{I}(\mathsf{Z})).$$

♂

Of course this lemma holds only for affine algebraic varieties, the obvious examples being

- $k := \mathbb{Q}$, $\mathsf{k} = \mathbb{C}$, $\mathsf{Z} := \{(\sqrt{2}, -\sqrt{2})\} \subset \mathsf{k}^2$, $\mathcal{I}(\mathsf{Z}) = (X_1^2 - 2, X_2 + X_1)$, $\mathcal{Z}(\mathcal{I}(\mathsf{Z})) = \{(\sqrt{2}, -\sqrt{2}), (-\sqrt{2}, \sqrt{2})\}$;
- $k := \mathbb{R}$, $\mathsf{k} = \mathbb{C}$, $\mathsf{Z} := \{(a, \exp(a)) : a \in \mathbb{R}\}$, $\mathcal{I}(\mathsf{Z}) = \{0\}$, $\mathcal{Z}(\mathcal{I}(\mathsf{Z})) = \mathbb{C}^2$.

Once our restriction to affine algebraic varieties guarantees one side of duality, in order to obtain the other one we must at least query whether each ideal has such a set of roots; again the univariate case gives us the hint: the only ideal with no roots is the polynomial ring itself, generated by the polynomial 1.

Fact 20.1.7 (Weak Hilbert's Nullstellensatz). *For each finite set*

$$F := \{f_1, \ldots, f_s\} \subset \mathcal{P},$$

we have

$$\mathcal{Z}(F) = \emptyset \iff \text{there exist } g_1, \ldots, g_s \in \mathcal{P} : 1 = \sum_{i=1}^{s} g_i f_i.$$

Proof. Compare Sections 20.3 and 20.4. ♂

Corollary 20.1.8. *For each ideal* $\mathsf{I} \subset \mathcal{P}$ *we have* $\mathcal{Z}(\mathsf{I}) = \emptyset \iff 1 \in \mathsf{I}$. ♂

Once we have restricted, via Hilbert's Basissatz, the systems of equations that will be considered to finite ones and/or to ideals, and the Weak Hilbert's Nullstellensatz gives that each non-trivial such ideal has a set of roots, we have to deal with duality, querying which ideals $\mathsf{I} \subset \mathcal{P}$ satisfy

$$\mathcal{I}(\mathcal{Z}(\mathsf{I})) = \mathsf{I},$$

or at least whether different ideals necessarily have different sets of roots.

Again, the univariate case gives us the clue:

- different polynomials can share a set of roots and the only way to distinguish them is to consider also the multiplicity of the roots;
- in other words, in order to be able to distinguish polynomials by their sets of roots, we must restrict ourselves to squarefree polynomials;
- and, if we are looking for the ideal of all the polynomials vanishing at the roots of a given polynomial $f \in k[X]$, we obtain the ideal generated by the squarefree associate of f.

The same process happens in the multivariate case:

Definition 20.1.9. *An ideal* $\mathsf{I} \subset \mathcal{P}$ *is called* radical *(or* squarefree*) if*

$$\text{for each } f \in \mathcal{P}, r \in \mathbb{N} : f^r \in \mathsf{I} \implies f \in \mathsf{I}.$$

The radical $\sqrt{\mathsf{I}}$ *of an ideal* I *is the ideal consisting of all the elements some power of which belongs to* I*:*

$$\sqrt{\mathsf{I}} := \{f \in \mathcal{P} : \text{ there exists } r \in \mathbb{N} : f^r \in \mathsf{I}\}.$$

Lemma 20.1.10 (Strong Hilbert's Nullstellensatz). *Let* $\mathsf{I} := (f_1, \ldots, f_s)$ *be an ideal and let* $f \in \mathcal{P}$*. Then*

$$f \in \mathcal{I}(\mathcal{Z}(\mathsf{I})) \iff \text{there exists } r \in \mathbb{N}, g_1, \ldots, g_s \in \mathcal{P} : f^r = \sum_{i=1}^{s} g_i f_i.$$

Proof (Rabinowitch). Let $f \in \mathcal{I}(\mathcal{Z}(\mathsf{I}))$ and let us consider the ideal

$$\mathsf{J} := \mathsf{I} + (fT - 1) = (f_1, \ldots, f_s, fT - 1) \subset k[X_1, \ldots, X_n, T]$$

and the affine algebraic variety $\mathcal{Z}(\mathsf{J}) \in \mathsf{k}^{n+1}$.

For any $(a_1, \ldots, a_n, t) \in \mathcal{Z}(\mathsf{J})$ we have:

- for each $g \in \mathsf{I} \subset \mathsf{J}$, $g(a_1, \ldots, a_n) = 0$ so that $(a_1, \ldots, a_n) \in \mathcal{Z}(\mathsf{I})$;
- therefore, $f(a_1, \ldots, a_n) = 0$, since $f \in \mathcal{I}(\mathcal{Z}(\mathsf{I}))$;
- as a consequence, since $fT - 1 \in \mathsf{J}$,

$$-1 = f(a_1, \ldots, a_n)t - 1 = 0,$$

giving a contradiction. We can therefore deduce that $\mathcal{Z}(\mathsf{J}) = \emptyset$ and the existence of $\mathsf{g}_1, \ldots, \mathsf{g}_s, \mathsf{g}_0 \in k[X_1, \ldots, X_n, T]$ such that

$$1 = \sum_{i=1}^{s} \mathsf{g}_i f_i + \mathsf{g}_0(1 - fT).$$

If we set $r := \max\{\deg(\mathsf{g}_i), 0 \le i \le s\}$, then

$$g_i := f^r \mathsf{g}_i \left(X_1, \ldots, X_n, \frac{1}{f}\right) \in k[X_1, \ldots, X_n],$$

so that, if we replace T with $1/f$ in the equality

$$f^r = \sum_{i=1}^{s} f^r \mathsf{g}_i f_i + f^r \mathsf{g}_0(1 - fT),$$

we obtain the required representation $f^r = \sum_{i=1}^{s} g_i f_i$.

The converse statement,

$$f^r(a_1, \ldots, a_n) = 0 \implies f(a_1, \ldots, a_n) = 0, \quad \text{for each } (a_1, \ldots, a_n) \in \mathcal{Z}(\mathsf{I}),$$

is trivial. ♂

Corollary 20.1.11. *Let* $\mathsf{I} := (f_1, \ldots, f_s)$ *be an ideal. Then* $\mathcal{I}(\mathcal{Z}(\mathsf{I})) = \sqrt{\mathsf{I}}$.

♂

To conclude this discussion we can deduce that:

Corollary 20.1.12. *The maps $\mathcal{Z}$ and $\mathcal{I}$ induce a duality between affine algebraic varieties in k^n and radical ideals in $\mathcal{P} = k[X_1, \ldots, X_n]$.*

In particular:

- $\mathcal{Z}\mathcal{I}(\mathsf{Z}) = \mathsf{Z} \iff \mathsf{Z}$ *is an affine variety;*
- $\mathcal{I}\mathcal{Z}(\mathsf{I}) = \mathsf{I} \iff \mathsf{I} = \sqrt{\mathsf{I}}$.

♂

20.2 Linear Change of Coordinates

The proof of Hilbert's Nullstellensatz requires the ability, given any polynomial $f \in k[X_1, \ldots, X_n] \setminus k$, to prove the existence of a change of coordinates

$$L : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$$

such that

$$L(f) = cX_n^{\deg(f)} + \sum_{j=0}^{\deg(f)-1} h_j(X_1, \ldots, X_{n-1})X_n^j, \qquad c \neq 0.$$

In order to prove this, let us begin by stating the following:

Lemma 20.2.1. *Let $S \subset k$ be any infinite set.*[2]

For each $g \in k[X_1, \ldots, X_n] \setminus \{0\}$, there are $c_1, \ldots, c_n \in S$ such that $g(c_1, \ldots, c_n) \neq 0$.

Proof. By induction on the number of variables: if $n = 1$ then g only has a finite number of roots, and there is $c \in S : g(c) \neq 0$.

If $n > 1$ we can express g as

$$g(X_1, \ldots, X_n) = \sum_{j=0}^{d} g_j(X_1, \ldots, X_{n-1})X_n^j, \qquad g_d \neq 0,$$

and, by induction, we can deduce the existence of $c_1, \ldots, c_{n-1} \in S$ such that $g_d(c_1, \ldots, c_{n-1}) \neq 0$, so that $g(c_1, \ldots, c_{n-1}, X_n) = 0$ has only a finite number of roots, guaranteeing the existence of some $c_n \in S$ such that $g(c_1, \ldots, c_{n-1}, c_n) \neq 0$. ♂

Corollary 20.2.2. *Given any infinite set $S \subset k$ and any finite set of polynomials $g_1, \ldots, g_s \in k[X_1, \ldots, X_n] \setminus \{0\}$, there are $c_1, \ldots, c_n \in S$ such that*

$$g_i(c_1, \ldots, c_n) \neq 0, \quad \text{for all } i, 1 \leq i \leq s.$$

[2] Remember that we are assuming k to be infinite.

Proof. Apply the lemma above to $g := \prod_i g_i$. ♂

We denote, for any field k and any $n \in \mathbb{N}$, by $C(n,k)$ the n-tuples of non-zero elements in k:

$$C(n,k) := \{(c_1,\ldots,c_n) \in k^n,\ c_i \neq 0,\ \text{for each } i\},$$

and, for each, $\mathsf{c} := (c_1,\ldots,c_n) \in C(n,k)$,

$$L_{\mathsf{c}} : k[X_1,\ldots,X_n] \to k[X_1,\ldots,X_n]$$

the map defined by

$$L_{\mathsf{c}}(X_i) := \begin{cases} X_i + c_i X_n & \text{if } i < n, \\ c_n X_n & \text{if } i = n. \end{cases}$$

Theorem 20.2.3. *For each $f \in k[X_1,\ldots,X_n]\backslash k$ there is $\mathsf{c} := (c_1,\ldots,c_n) \in C(n,k)$:*

- $L_{\mathsf{c}}(f) = cX_n^{\deg(f)} + \sum_{j=0}^{\deg(f)-1} h_j(X_1,\ldots,X_{n-1})X_n^j, \quad c \neq 0$;
- *for each $(b_1,\ldots,b_{n-1}) \in \mathsf{k}^{n-1}$ there is at least one value $b \in \mathsf{k}$ such that*

$$L_{\mathsf{c}}(f)(b_1,\ldots,b_{n-1},b) = 0;$$

- *for each $(b_1,\ldots,b_{n-1}) \in \mathsf{k}^{n-1}$, and each $b \in \mathsf{k}$ such that*

$$L_{\mathsf{c}}(f)(b_1,\ldots,b_{n-1},b) = 0,$$

writing

$$a_i := \begin{cases} b_i + c_i b & \text{if } i < n, \\ c_n b & \text{if } i = n, \end{cases}$$

we have $f(a_1,\ldots,a_n) = 0$.

Proof. The polynomial $f \in k[X_1,\ldots,X_n]$ is a linear combination

$$f = \sum_{t\in\mathcal{T}} c(f,t)t$$

of terms

$$t \in \mathcal{T} := \left\{X_1^{a_1}\ldots X_n^{a_n} : (a_1,\ldots,a_n) \in \mathbb{N}^n\right\}$$

with coefficients $c(f,t)$ in k; if we write $d := \deg(f)$ and

$$f_d := \sum_{t\in\mathcal{T}_d} c(f,t)t$$

where

$$\mathcal{T}_d := \{t \in \mathcal{T} : \deg(t) = d\},$$

then each $\mathsf{c} := (c_1, \ldots, c_n) \in k^n$ satisfies

$$L_{\mathsf{c}}(f) = f_d(c_1, \ldots, c_n)X_n^d + \sum_{j=0}^{d-1} h_j(X_1, \ldots, X_{n-1})X_n^j$$

provided that $c_i \neq 0$, for each i.

By Lemma 20.2.1 above, we can deduce the existence of $\mathsf{c} := (c_1, \ldots, c_n) \in C(n, k)$ such that $c := f_d(c_1, \ldots, c_n) \neq 0$, so that

$$L_{\mathsf{c}}(f) = cX_n^{\deg(f)} + \sum_{j=0}^{\deg(f)-1} h_j(X_1, \ldots, X_{n-1})X_n^j, \qquad c \neq 0.$$

Therefore, for each $(b_1, \ldots, b_{n-1}) \in \mathsf{k}^{n-1}$ the polynomial

$$L_{\mathsf{c}}(f)(b_1, \ldots, b_{n-1}, X_n) = cX_n^d + \sum_{j=0}^{d-1} h_j(b_1, \ldots, b_{n-1})X_n^j \in \mathsf{k}[X_n]$$

has exactly $d = \deg(f)$ roots counted with the proper multiplicity, and for each such root $b \in \mathsf{k}$ we have

$$f(a_1, \ldots, a_n) = L_{\mathsf{c}}(f)(b_1, \ldots, b_{n-1}, b) = 0.$$

Corollary 20.2.4. *For each $f \in k[X_1, \ldots, X_n] \setminus k$ there is $(a_1, \ldots, a_n) \in \mathsf{k}^n$ such that $f(a_1, \ldots, a_n) = 0$.*

Proof. It is sufficient to choose any arbitrary tuple $(b_1, \ldots, b_{n-1}) \in \mathsf{k}^{n-1}$ and any tuple $\mathsf{c} := (c_1, \ldots, c_n) \in C(n, k)$ satisfying Lemma 20.2.1, in order to deduce the result from Theorem 20.2.3. 

Note that almost all choices c satisfy the above results.

20.3 Hilbert's Nullstellensatz

We give here an old-fashioned proof of the Nullstellensatz combining those reported by van der Waerden and Gröbner.

Let us therefore assume we have a finite set

$$F_n := \{f_1, \ldots, f_s\} \subset \mathcal{P} := k[X_1, \ldots, X_n]$$

generating the ideal $\mathsf{I} := \mathsf{I}_n$. Our aim is to show that either

- $1 \in \mathsf{I}$, or
- there is $(a_1, \ldots, a_n) \in \mathsf{k}^n$ such that $(a_1, \ldots, a_n) \in \mathcal{Z}(\mathsf{I})$.