

Constructive ideal theory
(MAS591 Lecture Notes)

Dima Pasechnik

Draft November 14, 2006

Contents

1	Introduction	5
1.1	Elimination and the resultant	5
2	General properties of ideals in R.	9
2.1	Hilbert Basis theorem (Basissatz).	9
2.2	Hilbert Theorems on zeros (Nullstellensetze).	11
2.2.1	Proof of Theorem 2.2.2.	12
3	Algorithmic ideal theory	13
3.1	Gröbner bases.	13
3.1.1	Existence of Gröbner bases.	14
3.1.2	Computing Gröbner bases.	15
4	Appendix I: affine and projective spaces.	17
5	Appendix II: modules.	19
6	Appendix III: finitely generated extensions.	21

Chapter 1

Introduction

The aim of this short course is to give an introduction into algorithmic theory of ideals in polynomial rings, on one hand, and to the corresponding algorithmic problems in algebraic geometry, i.e. algorithms for determining various properties of algebraic sets and polynomial maps.

We consider *ideals* $I \subset R = k[X_1, \dots, X_n] := k[X]$ in *polynomial rings* R in n variables X_1, \dots, X_n (that we abbreviate by X) over (usually) algebraically closed fields k , and the corresponding *algebraic sets* $V(I) = V(\sqrt{I}) \subset k^n$, i.e. the sets of common zeroes (also called *common zero locus*) of $f \in I$. Algebraic sets are also often called *affine varieties*, to emphasise them being subsets of the *affine space* k^n (see Chapter 4 for more on this).

Recall that an ideal I is a closed with respect to addition subset of R satisfying $fI \subseteq I$ for any $f \in R$, and that the *radical* of I is the ideal $\sqrt{I} = \{f \in R \mid f^m \in I \text{ for some } m\}$. An ideal I is said to be generated by f_i 's in I when each $f \in I$ can be written down as $f = \sum_i r_i f_i$, with $r_i \in R$. When the set of f_i 's is finite, of size M , say, we write $I = (f_1, \dots, f_M)$.

In this context the natural topology on k^n is *Zariski topology*, where the closed sets (resp. the open sets) are the algebraic sets (resp. their complements). For any $Y \subset k^n$ we can define $I(Y) = \{f \in R \mid f(p) = 0 \text{ for all } p \in Y\}$. Then in the Zariski topology the closure \bar{Y} is $\bar{Y} = V(I(Y))$. Note that Zariski topology is not Hausdorff, i.e. not any two points have non-intersecting neighbourhoods. Indeed, already in the case $n = 1$ the open sets are the empty set and the complements of finite sets. See Remark 2.1.4 for more on this.

1.1 Elimination and the resultant

One of the simplest nontrivial algorithmic questions involving I is determination of $I \cap k[X_1, \dots, X_{n-1}]$, the *elimination ideal*; the corresponding procedure is called *elimination* of the variable X_n .

When $n > 1$, the geometric counterpart of it is to compute the projection of $V(I)$ from $p = (0, \dots, 0, 1)$ to the subspace $\langle e_1, \dots, e_n \rangle \subset k^n$ generated by the first $n - 1$ standard basis vectors.

In the case $n = 1$ this boils down to determining whether $V(I) = \emptyset$, or, equivalently, whether $I = k[z]$ (denoting $z := X_1$). It suffices to compute the greatest common divisor (GCD) of the generators of I . When $I = (f, g)$, then $f(z) = \sum_k a_k z^k$ and $g(z) = \sum_k b_k z^k$ will have a nontrivial GCD iff there exists a degree $\deg f + \deg g - 1$ polynomial h divisible by both of them, i.e. the vector spaces $\langle f, zf, z^2 f, \dots, z^{\deg g - 1} f \rangle$ and $\langle f, zg, z^2 g, \dots, z^{\deg f - 1} g \rangle$ have a nontrivial intersection. This is equivalent to vanishing of the following determinant, of the matrix of size $(\deg f + \deg g) \times (\deg f + \deg g)$, called the *resultant* $\text{res}_z(f, g)$ of f and g .

$$\text{res}_z(f, g) = \det \begin{pmatrix} a_0 & a_1 & \dots & a_{\deg f} & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{\deg f} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_0 & a_1 & \dots & a_{\deg f} \\ b_0 & b_1 & \dots & b_{\deg g} & 0 & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_{\deg g} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & b_0 & b_1 & \dots & b_{\deg g} \end{pmatrix}.$$

Lemma 1.1.1. *For $f, g \in k[z]$ one has $\text{GCD}(f, g) \neq 1$ iff $\text{res}_z(f, g) = 0$. \square*

Returning to the case $n > 1$, let us restrict attention to the case of I being a *homogeneous ideal*, that is, an ideal generated by homogeneous polynomials (a polynomial $f = \sum_{\alpha} a_{\alpha} X^{\alpha}$ is called *homogeneous* when the degrees $\sum_{i=1}^n \alpha_i$ of the monomials of f are the same for all α such that $a_{\alpha} \neq 0$. Here we abbreviate $X^{\alpha} = \prod_{i=1}^n X_i^{\alpha_i}$.) Note that then $f(x) = 0$ iff and only if $f(cx) = 0$ for all $c \in k$, so we can talk about the set of *projective zeros* of f , i.e. zeros being points of the projective space \mathbb{P}_k^{n-1} , usually denoted by \mathbb{P}^{n-1} (see Chapter 4 for more on projective spaces). The geometry of \mathbb{P}^{n-1} is nicer to deal with, as there, unlike in k^n , the subspaces of complimentary dimension always have a common point.

Further, let us assume that $\mathbb{P}^{n-1} \ni p = (0 : 0 : \dots : 1)$ does not belong to $V(I)$ (this can always be achieved by performing a nondegenerate linear transformation of the coordinates). Let $q \in \langle e_1, \dots, e_n \rangle = \mathbb{P}^{n-2} \subset \mathbb{P}^{n-1}$. Then the projective line pq meets $V(I)$ iff every pair $f, g \in I$ has a common zero on pq . Indeed, there always exists homogeneous $f \in I$ with only finitely many zeros on pq , and if pq misses $V(I)$ then by definition of $V(I)$ there will exist homogeneous $g \in I$ that does not vanish on any of the zeros of f on pq . Now we consider f, g as polynomials in X_n with coefficients in $k[X_1, \dots, X_{n-1}]$ and form $\text{res}_{X_n}(f, g)$ as above. Note that $\text{res}_{X_n}(f, g)$ is a homogeneous polynomial in $k[X_1, \dots, X_{n-1}]$.

Theorem 1.1.2. *Let I be homogeneous. Then $I \cap k[X_1, \dots, X_{n-1}]$ is generated by $\text{res}_{X_n}(f, g)$ for all homogeneous $f, g \in I$. \square*

Note that, generally speaking, it is not sufficient to restrict f, g to belong to the generators of I (as we will see later, there are always finite generating sets for I). However, it turns out one can, if necessary, extend the generating set, with finitely many new elements, to ensure that their pairs suffice.

In geometric terms, Theorem 1.1.2 implies the following statement.

Corollary 1.1.3. *The projection of the projective variety $V(I) \subset \mathbb{P}^{n-1}$ from $p \in \mathbb{P}^{n-1} \setminus V(I)$ is a projective variety.* \square

Here by *projective variety* one means the zero locus of a homogeneous ideal in \mathbb{P}^{n-1} .

Algebraic numbers and resultants. Another useful application of resultants is for computing with *algebraic numbers*, or, more generally elements of algebraic field extensions k of a field \mathcal{U} . (We assume that $\text{char } \mathcal{U} = 0$ here, to make things easier.) Such elements α are represented by their *minimal polynomials*: that is, unique \mathcal{U} -irreducible monic polynomials $f_\alpha \in \mathcal{U}[T]$ that satisfy $f_\alpha(\alpha) = 0$.

Proposition 1.1.4. *Let $\alpha, \beta \in k$ and $f_\alpha, f_\beta \in \mathcal{U}[T]$ their minimal polynomials. Then the polynomials $h(Z) = \text{res}_X(f_\alpha(X), f_\beta(Z - X))$ and $g(Z) = \text{res}_X(f_\alpha(X), f_\beta(Z/X)X^{\deg f_\beta})$ satisfy $h(\alpha + \beta) = 0$ and $g(\alpha\beta) = 0$. Thus $f_{\alpha+\beta}$ (resp. $f_{\alpha\beta}$) can be obtained by factoring h (resp. g).* \square

Chapter 2

General properties of ideals in R .

Here we prove few important results on ideals in R .

2.1 Hilbert Basis theorem (Basissatz).

The first important property is that every ideal $I \subseteq R$ is *finitely generated*. There are many different proofs of this result. Here we give a proof based on combinatorics of *monomial ideals*, i.e. ideals generated by monomials. The following result is usually called *Dickson Lemma*, although apparently L.E. Dickson, to whom it is attributed does not hold priority here, as it was already known to XIXth century a classic of invariant theory Gordan.

Proposition 2.1.1. *Let I be a monomial ideal. Then I is finitely generated.*

Proof. Note that the result is essentially about the exponent vectors of the monomials involved. It suffices to prove that a set S of vectors with nonnegative integer coordinates in \mathbb{Z}^n that is closed under addition of arbitrary vectors with nonnegative integer coordinates (the latter is a consequence of ideal property), is finitely generated (as a semi-group¹). The proof is by induction on n . The result is obviously true for $n = 1$.

Suppose that it holds for all $k < n$. Consider the projection $\pi : \mathbb{Z}^n \rightarrow \mathbb{Z}^{n-1}$ that “chops off” the n -th coordinate. Then by induction assumption $\pi(S) \subseteq \mathbb{Z}^{n-1}$ is finitely generated, say, by $\{v'_1, \dots, v'_s\}$. Denote by v_j the element of $\pi^{-1}(v'_j)$ with minimal n -th coordinate v_{jn} . Let

$$\ell = \max_{1 \leq j \leq s} v_{jn}, \quad W_p := \{w \in S \mid w_n = p\}, \quad \text{for } 0 \leq p < \ell.$$

¹a semigroup as an algebraic system that is “just like” a group, except that it does not need to have identity and inverses

Let S_p be the set of exponents of the monomials in the monomial ideal generated by X^w for $w \in W_p$. Then $\pi(S_p)$ is finitely generated, say by $\{v_1^{(p)}, \dots, v_{s_p}^{(p)}\}$. Similarly, denote by $v_j^{(p)}$ the element of $\pi^{-1}(v_j^{(p)})$ with minimal n -th coordinate $v_{jn}^{(p)}$. It is easy to see that without loss of generality $v_{jn}^{(p)} = p$. Indeed, by definition of S_p we have $v_{jn}^{(p)} \geq p$. If $v_{jn}^{(p)} > p$ then $v_{jn}^{(p)}$ is redundant, for by definition of S_p there exists $w \in S_p$ and $r \in \mathbb{Z}^n$ such that $v_{jn}^{(p)} = w + r$, and we can replace $\pi(v_{jn}^{(p)})$ by $\pi(w)$ in the generating set for $\pi(S_p)$.

We claim that S (resp. I) is generated by the vectors (resp. by monomials with exponent vectors)

$$v_1, \dots, v_s, v_1^{(0)}, \dots, v_{s_0}^{(0)}, \dots, v_1^{(p)}, \dots, v_{s_p}^{(p)}, \dots, v_{s_{\ell-1}}^{(\ell-1)}.$$

To see this, let $w \in S$. If $w_n \geq \ell$ then consider the decomposition $\pi(w) = v_j' + r'$, for some $r' \in \mathbb{Z}^{n-1}$ and $1 \leq j \leq s$. Then $w = \pi(w) + w_n e_n = v_j' + r' + w_n e_n = v_j + r$, for some $r \in \mathbb{Z}^n$. Otherwise, $w_n = p < \ell$. Consider the decomposition $\pi(w) = v_j^{(p)} + r'$, for some $r' \in \mathbb{Z}^{n-1}$ and $1 \leq j \leq s_p$. Then $w = \pi(w) + w_n e_n = v_j^{(p)} + r' + p e_n = v_j^{(p)} + r$, for some $r \in \mathbb{Z}^n$. \square

Now we can prove the result for general I . To do this, we introduce an order \succ , so-called *lexicographic order*, also known as *pure lexicographic order*, on the monomials, as follows: $X^\alpha \succ X^\beta$ iff the first $0 \leq k < n$ coordinates of α and β are equal, i.e. $\alpha_k = \beta_k$, and $\alpha_{k+1} > \beta_{k+1}$. A proof of the following is left to the reader.

Lemma 2.1.2. *There is no infinite decreasing chain $X^{\alpha_1} \succ X^{\alpha_2} \succ \dots$* \square

Given $f = \sum_{\alpha} a_{\alpha} X^{\alpha} \in R$, the *leading term* of f is the monomial $a_{\gamma} X^{\gamma}$ (with $a_{\gamma} \neq 0$, certainly) that is biggest among all the monomials of f , w.r.t. \succ . It is denoted by $\text{LT}(f)$.

Theorem 2.1.3. (Hilbert's Basissatz) *Let I be an ideal in R . Then I is finitely generated.*

Proof. Let $\text{LT}(I)$ be the ideal generated by the leading terms of $f \in I$. By Prop. 2.1.1 it is finitely generated, say $\text{LT}(I) = (m_1, \dots, m_s)$. For each m_j let us pick up, arbitrarily, $f_j \in R$ such that $\text{LT}(f_j) = m_j$.

We claim that $I = (f_1, \dots, f_s)$. To see this, let $f \in I$. Then $\text{LT}(f) = m_j m$, for m an arbitrary monomial in R . Then $\text{LT}(f) \succ \text{LT}(f - f_j m)$. Replacing f by $f - f_j m$ and repeating the procedure, we obtain a zero polynomial, after finitely many iterations, due to Lemma 2.1.2. \square

Remark 2.1.4. It is interesting to remark that Theorem 2.1.3 implies that Zariski topology is indeed a topology, i.e. that the intersection of an arbitrary collection of closed sets is closed, i.e. equal to $V(I)$. Indeed, it is equal to the intersection of a finite number s of sets $V((f_i))$, where $I = (f_1, \dots, f_s)$. This is

drastically different from more usual topologies, such as the natural topology of \mathbb{R}^n .

Another important implication of Theorem 2.1.3 is the following

Lemma 2.1.5. *R is Noetherian, that is, every ascending chain of ideals $I \subset I_1 \subset_2 \subset \dots$ terminates.*

Proof. $J = \bigcup_{i \geq 0} I_i$ is an ideal, finitely generated by Theorem 2.1.3. Thus $J = (f_1, \dots, f_s)$. Each f_j belongs to a I_{i_j} from the chain, so $J = I_\ell$, where $\ell = \max_{1 \leq j \leq s} i_j$. \square

2.2 Hilbert Theorems on zeros (Nullstellensatz).

The second important property relates ideal $I \subseteq R$ and the variety $V(I)$.

Theorem 2.2.1. (*Hilbert's Strong Nullstellensatz*) $I(V(I)) = \sqrt{I}$, i.e. $f^s \in I$ for some $s = s_f$ and every $f \in R$ vanishing on $V(I)$.

This theorem² can be easily derived from the case $V(I) = \emptyset$, that is, from the following

Theorem 2.2.2. (*Hilbert's Weak Nullstellensatz*) $I(\emptyset) = R$, i.e. for any $I = (f_1, \dots, f_m)$ such that $V(I) = \emptyset$ there exist $g_1, \dots, g_m \in R$ such that

$$1 = g_1 f_1 + g_2 f_2 + \dots + g_m f_m.$$

Note that we have made use of Hilbert's Basissatz in the statement of Theorem 2.2.2 when we wrote $I = (f_1, \dots, f_m)$. As well, note the importance of k being algebraically closed for this result to hold. We postpone the proof of Theorem 2.2.2 to Subsection 2.2.1. Assuming it holds true, we prove Theorem 2.2.1.

Proof of Theorem 2.2.1. Introduce one more variable $Z = X_{n+1}$ and consider the ideal $J = (f_1, \dots, f_m, 1 - Zf) \subseteq k[X_1, \dots, X_n, Z]$. Note that $V(J) = \emptyset$. Indeed, the $J' = (f_1, \dots, f_m) \subseteq k[X_1, \dots, X_n, Z]$ satisfies $V(J') = V(I) \times k \subseteq k^{n+1}$. By the choice of f , it vanishes on $V(I)$, implying that $Zf(v) = 0$ for any $v \in V(J')$, implying that $1 - Zf$ does not vanish on any $v \in V(J')$, showing that $V(J) = \emptyset$.

By Theorem 2.2.1, there exist $g_1, \dots, g_m, g \in k[X_1, \dots, X_n, Z]$ satisfying

$$1 = g_1 f_1 + g_2 f_2 + \dots + g_m f_m + (1 - Zf)g. \quad (2.1)$$

²*Nullstellensatz* is a German word meaning Theorem (= Satz) on zeros of polynomials (= Nullstellen); and *Setze* is plural form of Satz.

Substituting $Z = \frac{1}{f}$ in (2.1) we obtain the following expression, where the right-hand side is a rational function $\frac{h}{f^s} \in k(X_1, \dots, X_n)$ for some s depending on the maximal degree of g_j 's.

$$1 = g_1(X_1, \dots, X_n, \frac{1}{f})f_1 + \dots + g_m(X_1, \dots, X_n, \frac{1}{f})f_m. \quad (2.2)$$

By multiplying both parts of (2.2) by f^s we obtain

$$f^s = r_1 f_1 + r_2 f_2 + \dots + r_m f_m \in I, \quad \text{for } r_j \in R,$$

as required. \square

2.2.1 Proof of Theorem 2.2.2.

First, we show how to derive Theorem 2.2.2 from the following natural looking

Proposition 2.2.3. *Every maximal (proper, i.e. not equal to R) ideal I of R is of the form $I_p = (X_1 - p_1, \dots, X_n - p_n)$ for some $p \in k^n$.*

Indeed, if $I \neq R$ then by Lemma 2.1.5 there exists a maximal ideal $J \subset R$ such that $I \subseteq J$. By Proposition 2.2.3 we have $J = I_p$, implying $p \in V(I)$ and proving Theorem 2.2.2.

It remains to prove Proposition 2.2.3. Observe that the ring $A = R/I = \phi(R)$, where $\phi : R \rightarrow R/I$ is the ring homomorphism sending $f \in R$ to $f + I$, is a field. Indeed, all we need to check that each $\phi(f) \in R/I$ has an inverse, i.e. $g \in R$ such that $fg \in 1 + I$. By maximality of I the ideal generated by I and f equals R , in particular

$$1 = -gf + \sum_{i=1}^s g_i f_i, \quad \text{where } I = (f_1, \dots, f_s),$$

as required. Thus A is a field, and it is generated by $\phi(X_j)$, for $1 \leq j \leq n$.

At this point we make use of Theorem 6.0.12 in Appendix III, that asserts that a finitely generated field extension of k is *algebraic*, that is, obtained from k by attaching roots of polynomials from $k[T]$. But k is algebraically closed, thus $A \cong k$. This means that $\phi(X_j) = b_j \in k$, for $1 \leq j \leq n$. Note that each b_j has a preimage p_j in k , i.e. ϕ is an isomorphism when restricted to the degree 0 polynomials $k \subset R$ (indeed, a nonzero constant polynomial cannot be in the kernel of ϕ , i.e. in I). Therefore $J = (X_1 - p_1, \dots, X_n - p_n) \subseteq I$. As J is maximal, $J = I$, proving Proposition 2.2.3.

Chapter 3

Algorithmic ideal theory

Here we discuss techniques allowing one to solve problems like ideal membership in R algorithmically; these procedures are implemented in several computer algebra systems, such as *Singular*, *CoCoA*, etc.

3.1 Gröbner bases.

There exist other orders on the monomials, that share similar properties with the lexicographic order. (The latter is denoted \succ_{lex} when one wants to emphasise that we talk about the lexicographic order, and not about some other order). Formally, a (total) order \succ on the monomials (with coefficient 1) of R is called a *term order* when the following holds.

1. $1 = X^0$ is (unique) minimal element w.r.t. \succ .
2. $X^\alpha \succ X^\beta$ implies $X^\alpha X^\gamma \succ X^\beta X^\gamma$ for all $X^\gamma \in R$.

Most of the theory explained here works for an arbitrary term order. E.g. the following holds.

Lemma 3.1.1. $LT(fg) = LT(f)LT(g)$ for any $f, g \in R$. □

Similarly, Lemma 2.1.2 holds for any term order.

Let us fix a term order \succ , and talk about $LT(f)$ for $f \in R$ w.r.t. this order. Let $I = (f_1, \dots, f_s)$ be an ideal in R . Its generating set f_1, \dots, f_s is called a *Gröbner basis* with respect to a term order \succ if $LT(I) = (LT(f_1), \dots, LT(f_s))$. (Sometimes you see “Gröbner” written as “Groebner”. This is in principle a correct spelling for the devices that cannot depict characters like “ä”, “ö”, etc, so called German *umlauts* properly.)

As a matter of fact, any ideal admits a finite *universal* Gröbner basis, i.e. a finite generating set that is a Gröbner basis w.r.t. any term order.

Example 3.1.2. Let $I = (X_1^2 - X_2, X_1^2 - X_3) \subset k[X_1, X_2, X_3]$. Then the difference of the generators $X_3 - X_2 \in I$. Using the lexicographic order, we see that $\text{LT}(X_3 - X_2) = -X_2$ is not in $(\text{LT}(X_1^2 - X_2), \text{LT}(X_1^2 - X_3)) = (X_1^2)$, thus our basis is not a Gröbner basis (in this order). We will see below that appending $X_3 - X_2$ to the basis makes it Gröbner.

Using essentially the same argument as in the proof of Theorem 2.1.3, we can show the following two results.

Ideal membership

Theorem 3.1.3. *Let $I = (f_1, \dots, f_s)$ be an ideal in R generated by the Gröbner basis $\{f_1, \dots, f_s\}$ with respect to a term order \succ . Then there is an algorithmic procedure to decide in a finitely many arithmetic operations in R whether $f \in I$ belongs to R .*

Proof. If $f \in I$ then $\text{LT}(f) = \text{LT}(f_j)r$ for a monomial $r \in R$ and $1 \leq j \leq s$. Otherwise, if no such decomposition of $\text{LT}(f)$ exists, we conclude that $f \notin I$.

Then we replace f by $f' = f - f_j r$. Note that $\text{LT}(f) \succ \text{LT}(f')$. Now, repeat the step in the beginning of the proof. The procedure terminates in finitely many steps, according to Lemma 2.1.2, when either $f = 0$, meaning that $f \in I$, or with $f \neq 0$ without a decomposition $\text{LT}(f) = \text{LT}(f_j)r$, meaning that $f \notin I$. \square

3.1.1 Existence of Gröbner bases.

Gröbner bases are ideal bases that have certain extra properties, so it is *a priori* unclear whether they always exist, and whether they are finite. The following clears this up.

Theorem 3.1.4. *Let I be an ideal in R and \succ a term order. Then a finite Gröbner basis, w.r.t. to \succ , for I exists.*

Proof. Let $\text{LT}(I)$ be the monomial ideal generated by the leading terms $\text{LT}(f)$ of $f \in I$. It has a finite basis (m_1, \dots, m_s) . Choose for each m_j a polynomial $f_j \in I$ satisfying $m_j = \text{LT}(f_j)$. Then $\{f_1, \dots, f_s\}$ is a Gröbner basis for I (that it is a basis can be shown as in the proof of Theorem 2.1.3, and that it is Gröbner basis holds by construction). \square

Elimination

Here we show how to, given an ideal $I \subset R$, compute $I \cap S$, for $S = k[X_1, \dots, X_s]$, with $1 \leq s < n$, using Gröbner bases. We have to choose a monomial order \succ such that $X_j \succ X_i$ for all $1 \leq i \leq s$ and all $s < j \leq n$. Such an order is called an *elimination order* w.r.t. X_{s+1}, \dots, X_n . (Note that the usual lexicographic order with appropriately chosen ordering of variables will do, although it might not be the best to use in practice.)

Proposition 3.1.5. *Let \succ be an elimination order w.r.t. X_{s+1}, \dots, X_n , and $I = (g_1, \dots, g_t)$ a Gröbner basis for I w.r.t. \succ . Then a Gröbner basis for $I \cap S$ is given by the $g_i \in \{g_1, \dots, g_t\}$ that do not involve any X_{s+1}, \dots, X_n , i.e. $g_i \in S$.*

Proof. Let $J = I \cap S$. Clearly $\text{LT}(J) \subset \text{LT}(I) \cap S$. It suffices to show that the $\text{LT}(g_i)$, for $g_i \in S$, generate $\text{LT}(I) \cap S$.

Let $m \in \text{LT}(I) \cap S$ be a monomial. Since g_1, \dots, g_t form a Gröbner basis, m is divisible by $\text{LT}(g_j)$ for some j . As $m \in S$, we must have $\text{LT}(g_j) \in S$, so $g_j \in S$, as \succ is an elimination order. \square

3.1.2 Computing Gröbner bases.

Here we present a naive procedure to compute Gröbner bases, with respect to a given term order \succ . (Actual algorithms implemented in computer algebra systems are more refined.)

Let $f, g \in R$, and X^γ the least common multiple of $\text{LT}(f)$ and $\text{LT}(g)$. The S -polynomial of f and g is the polynomial

$$S(f, g) = X^\gamma \left(\frac{f}{\text{LT}(f)} - \frac{g}{\text{LT}(g)} \right) \in R.$$

Given an ideal $I = (f_1, \dots, f_s)$, a Gröbner basis for I can be computed by the following procedure.

1. For each pair f_i, f_j of basis elements, compute $S(f_i, f_j)$, and reduce it as in the proof of Theorem 3.1.3 by the basis elements. Call the result of this reduction F_{ij} .
2. If all the $F_{ij} = 0$, terminate. Add all the nonzero F_{ij} to the basis. Repeat the step 1 with the new basis $(f_1, \dots, f_{s'})$.

Note that in step 1 it suffices to choose only these f_i, f_j such that $\text{LT}(f_j)$ and $\text{LT}(f_i)$ have nontrivial GCD. This is due to the following.

Lemma 3.1.6. *Let $f, g \in R$ with trivial $\text{GCD}(\text{LT}(f), \text{LT}(g))$. Then $S(f, g)$ reduces to 0 w.r.t. (f, g) , i.e. (f, g) form a Gröbner basis for the ideal (f, g) .*

Proof. It suffices to show that for any $u, v \in R$ we have that $\text{LT}(fu + gv)$ is divisible either by $\text{LT}(f)$, or by $\text{LT}(g)$.

Suppose false, and that $\text{LT}(u)$ is minimal w.r.t. \succ over all the representations of $F = fu + gv$. Then $\text{LT}(fu) = -\text{LT}(gv)$, so $\text{LT}(u) = w \text{LT}(g)$ and $\text{LT}(v) = -w \text{LT}(f)$ for a monomial w . But then $F = (gw + u_1)f + (-wf + v_1)g = fu_1 + gv_1$, and $u \succ u_1$, a contradiction. \square

Now let us *prove* that this procedure indeed terminates and gives what is claimed. We will need the following technical result.

Lemma 3.1.7. *Let f, f_1, \dots, f_s satisfy $\text{LT}(f_1) = \dots = \text{LT}(f_s) \succ \text{LT}(f)$. Then $f = \sum_{i < j} \nu_{ij} S(f_i, f_j)$, with $\nu_{ij} \in k$. \square*

Theorem 3.1.8. (*Buchberger Criterion*) *Let $I = (f_1, \dots, f_s)$ be an ideal in R and \succ a term order. Then I is a Gröbner basis of I w.r.t. \succ if and only if $S(f_i, f_j)$ reduces to 0 w.r.t. the basis.*

Proof. If f_1, \dots, f_s form a Gröbner basis then $\text{LT}(I)$ is generated by $\text{LT}(f_j)$'s and $S(f_i, f_j)$ reduces to 0.

To the ‘if’ part of the statement, by the way of contradiction we assume that $f = \sum_u g_u f_u$ with $\text{LT}(f) \notin (\text{LT}(f_1), \dots, \text{LT}(f_s))$. Let $m = \max_u \text{LT}(g_u f_u)$, where max is understood w.r.t. \succ , and the expansion $f = \sum_u g_u f_u$ chosen so that m is as small as possible. Let

$$h = \sum_{v \in V} g_v f_v, \quad V = \{v \mid \text{LT}(g_v f_v) = c_v m, c_v \in k\}.$$

We can write $\text{LT}(g_v f_v) = n_v \text{LT}(g_v)$ for a term n_v of f_v . If $q = \sum_{v \in V} n_v \text{LT}(g_v) \neq 0$ then $q = \text{LT}(f)$, contradicting the choice of f . Thus $q = 0$. By Lemma 3.1.7 we have a representation of the polynomial

$$Q := \sum_{v \in V} f_v \text{LT}(g_v) = \sum_{i < j} \nu_{ij} S(\text{LT}(g_i) f_i, \text{LT}(g_j) f_j).$$

As $\text{LT}(g_i)$ are monomials, $S(f_i, f_j)$ divides $S(\text{LT}(g_i) f_i, \text{LT}(g_j) f_j)$. Using representations $S(f_i, f_j) = \sum_\ell g_{i,j,\ell} f_\ell$, where $\text{LT}(S(f_i, f_j))$ coincides with the LT of some $g_{i,j,\ell} f_\ell$, we obtain representations of $Q = \sum_\ell d_{Q,\ell} f_\ell$, and of $f = \sum_\ell d_\ell f_\ell$. As the biggest of the LT's of $d_\ell f_\ell$ is smaller than m , we obtain a contradiction. \square

Finally, we remark that Theorem 3.1.8 provides finiteness of the algorithm, as we cannot keep generating new non-reducible $S(f_i, f_j)$ forever, for we can use the Basissatz to select a finite basis from their LT's, and for each ‘new’ $S(f_i, f_j)$, its LT will be divisible by one of these basis elements, a contradiction.

Chapter 4

Appendix I: affine and projective spaces.

Here we summarise basic information on affine and projective spaces over an arbitrary field F . They can be viewed as “incidence systems”. There are axiomatic characterisations of these objects known, but we will not go into this here.

Affine spaces

The affine n -dimensional space \mathbb{A}^n over F consists of the vectors of F^n as *points*, and shifts (also called translations) $W + s$ by $v \in F^n$ of the subspaces W of F^n , as *subspaces*, i.e. lines, planes, etc. Informally, we say we “forget where $0 \in F^n$ is”.

Obviously, subspaces of the form $W + s$ and $W + p$ either coincide, or are disjoint, as they are just cosets of the subgroup W in the additive group of F^n . The automorphism group of \mathbb{A}^n is the semidirect product of F^n and $\Gamma L_n(F)$, the semi-linear automorphism group of F^n .

The set of $W + s$, as s ranges through F^n , is called the *parallel class* of W .

Projective spaces

The projective $(n-1)$ -dimensional space \mathbb{P}^{n-1} over F consists of the 1-dimensional subspaces of F^n as *points*, and 2, 3, \dots , $(n-1)$ -dimensional subspaces of F^n as *subspaces*, of dimension 1, 2, \dots , $n-2$. That is, the dimension “drops by 1”. As well, \mathbb{P}^{n-1} can be identified with the “geometry of parallel classes”, or “geometry at infinity”, of \mathbb{A}^n .

An important and elementary property of \mathbb{P}^{n-1} is that whenever two subspaces

U, W satisfy $\dim U + \dim W \geq n - 1$ they have a nonempty intersection. This is not true in \mathbb{A}^n , due to presence of parallel classes there.

Chapter 5

Appendix II: modules.

Modules are natural generalisations of vectorspaces: the main difference is that the field is replaced by a ring R . The ring does not even need to be a commutative ring. Formally speaking, an R -module is an abelian group M with R -action defined on it, namely, a map $R \times M \rightarrow M$, written $(r, m) \mapsto rm$, satisfying for all $r, s \in R$ and all $m \in M$ the following properties.

$$\begin{aligned} r(sm) &= (rs)m && \text{associativity} \\ r(m+n) &= rm + rn \\ (r+s)m &= rm + sm && \text{distributivity, or bilinearity} \\ 1m &= m && \text{identity.} \end{aligned}$$

In particular an ideal $I \subset R$, and the quotient ring R/I are R -modules. When the ring R used is clear from the context, we often just say *module* instead of *R -module*.

A natural construction of new modules from old ones is the *direct sum of modules*: given two modules M and N we define their direct sum $M \oplus N := \{(m, n) \mid m \in M, n \in N\}$ with the R -action given by $r(m, n) = (rm, rn)$.

Modules, that are direct sums of copies of R , are called *free modules*. Unlike in the vector space case, not all the R -modules are free.

Chapter 6

Appendix III: finitely generated extensions.

Here we assume that k is a not necessarily algebraically closed, although infinite, field¹, and $R = k[X_1, \dots, X_n]$ and an ideal $I \subset R$ as above. Further, denote $A = k[a_1, \dots, a_n] = R/I$, with $\phi : R \rightarrow A$ the natural ring homomorphism with kernel I and $a_j = \phi(X_j)$, for $1 \leq j \leq n$.

First we prove the *Noether normalisation lemma*, a classical result that appears throughout commutative algebra in seemingly different forms. We need to introduce the following notion. Let B a ring and A a subring of B . Then B is called a *finite A -algebra* if there exist finitely many $b_j \in B$ such that

$$B = b_1A + b_2A + \dots + b_sA, \quad (6.1)$$

i.e. B is a finitely generated A -module. Note that this is stronger than B being *finitely generated over A* , where we only require that B be generated as a ring by A and b_1, \dots, b_s .

Lemma 6.0.9. *If B is finite A -algebra and C is a finite B -algebra then C is a finite A -algebra.*

Proof. Let B satisfy (6.1). Then

$$C = c_1B + \dots + c_mB = c_1 \sum_{i=1}^s b_iA + \dots + c_m \sum_{i=1}^s b_iA = c'_1A + \dots + c'_\ell A,$$

as claimed. □

Finiteness of B as A -algebra admits the following characterisation.

¹Note that every algebraically closed field is infinite.

Proposition 6.0.10. *If B is a finite A -algebra then each $x \in B$ is integral over A , i.e. is a root of a monic polynomial of degree $m \leq s$ (where s is a constant) with coefficients in A , i.e. (6.2) holds:*

$$x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0, \quad a_0, \dots, a_{m-1} \in A. \quad (6.2)$$

If $x \in B$ is integral over A then $A[x]$ is a finite A -algebra.

Proof. As any $x \in A$ satisfies the linear relation $x - a = 0$, with $x = a \in A$, we can assume $x \in B \setminus A$. Suppose $B = b_1A + \cdots + b_sA$. As $xb_i \in B$, there exist $a_{ij} \in A$ such that $xb_i = \sum_{j=1}^s a_{ij}b_j$. Consider the $s \times s$ matrix M with the entries $M_{ij} = x\delta_{ij} - a_{ij}$.

Writing $b = (b_1, \dots, b_s)$, we get $Mb = 0$. so by the usual lineal algebra line of thought we would expect $\det M = 0$.

We should be more careful of course, as we work over a ring. Take the *adjugate* (also called *classical adjoint*) M^* of M , that is the matrix with the entries $M_{ij}^* = (-1)^{i+j} \det M^{ji}$, where M^{ij} denotes the submatrix of M obtained by removing i -th row and j -th column. Then $MM^* = M^*M = \Delta I_s$, where we use I_s to denote the $s \times s$ identity matrix. This implies that $\Delta I_s b = 0$, so in particular polynomial identities $\Delta b_j = 0$ hold for $1 \leq j \leq s$. As $1_B = 1 = b_1 a'_1 + \cdots + b_s a'_s$ for some $a'_j \in A$, we also get $\Delta 1_B = 0$, so indeed we have $\Delta = 0$, that is obviously a monic relation of degree s in x . The first part is proved.

To prove the second part, let us assume, without loss in generality, that $B = A[x]$ and (6.2) holds. Set $b_1 = x$, $b_2 = x^2$, \dots , $b_{m-1} = x^{m-1}$, $b_m = 1$. We claim that (6.1) holds, with $s = m$. In view of (6.2) every power of x belongs to B . B is closed w.r.t. multiplication by $\alpha \in A$ and w.r.t. addition, completing the proof. \square

Another important notion we use is that of *algebraic independence* of a finite subset $Y = \{y_1, \dots, y_m\} \subset B$. We say that the y_j 's are algebraically independent if there is no nontrivial polynomial relation between them, or, in other words, the natural surjection of the polynomial ring $k[Y_1, \dots, Y_m] \rightarrow k[y_1, \dots, y_m] \subseteq B$ is injective.

Theorem 6.0.11. (*Noether normalisation lemma*) *There exist algebraically independent $y_1, \dots, y_m \in A$, with $m \leq n$, such that A is a finite $k[y_1, \dots, y_m]$ -algebra.*

Proof. Suppose there exists $0 \neq f \in I$, otherwise we just take $m = n$ and $y_j = a_j$, for $1 \leq j \leq n$. Then $f(a_1, \dots, a_n) = 0$ is an equation satisfied by a_n . The idea is to replace each X_j , for $1 \leq j < n$, by certain X'_j so that f becomes monic in a_n .

Set $a'_1 = a_1 - \alpha_1 a_n$, \dots , $a'_{n-1} = a_{n-1} - \alpha_{n-1} a_n$, with $\alpha_j \in k$ to be specified later. Then

$$f(a'_1 + \alpha_1 a_n, \dots, a'_{n-1} + \alpha_{n-1} a_n, a_n) = 0.$$

We claim that for a suitable choice of α_j 's the polynomial

$$h(X'_1, \dots, X'_{n-1}, X_n) := f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n) = 0$$

is monic in X_n . Let $d = \deg f = \deg h$, and set $h = h_d + g$, with h_d homogeneous of degree d and $\deg g < d$. Then

$$(X_1, \dots, X_n) = h(X'_1, \dots, X'_{n-1}, X_n) = h_d(\alpha_1, \dots, \alpha_{n-1}, 1)X_n^d + \\ + (\text{terms of degree } < d \text{ in } X_n). \quad (6.3)$$

So as soon as $h_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$ we have our claim; in fact, for almost all the choices of α this will be true. We have now a monic equation for a_n with coefficients in $A' = k[a'_1, \dots, a'_{n-1}]$.

Now we can complete the proof by induction on n . The result is obvious for $n = 1$, as we can just divide by the coefficient of the highest power of X_n . By inductive assumption, there are $y_1, \dots, y_m \in A'$ that are algebraically independent in A' and so that A' is a finite k -algebra over $K = k[y_1, \dots, y_m]$. On the other hand A is a finite k -algebra over A' by Proposition 6.0.10. By Lemma 6.0.9 a finite k -algebra over K . \square

Theorem 6.0.12. *A finitely generated field extension $B = k[a_1, \dots, a_n]$ of k , that is, a field $B = R/I$, is algebraic, that is, obtained from k by attaching roots of polynomials.*

Proof. By Theorem 6.0.11 there exist algebraically independent y_1, \dots, y_m such that B is a finite A -algebra, where $A = k[y_1, \dots, y_m]$, and $m \leq n$. If A is a field then $m = 0$ and B is an algebraic extension of $A = k$.

It remains to show that A is a field. Let $a \in A$. Then $b^{-1} \in B$ and, as B is a finite A -algebra, satisfies (6.2). Multiplying both parts of (6.2) by b^{m-1} we obtain

$$b^{-1} = -a_{m-1} - a_{m-2}b - \dots - a_0b^{m-1} \in A,$$

as required for A to be a field. \square

Index

- R -module, 19
- S -polynomial, 15
- Hilbert's Basissatz, 10

- adjugate, 22
- affine varieties, 5
- algebraic, 12, 23
- algebraic independence, 22
- algebraic numbers, 7
- algebraic sets, 5

- Buchberger Criterion, 16

- classical adjoint, 22
- CoCoA, 13

- Dickson Lemma, 9
- direct sum of modules, 19

- elimination, 5
- elimination ideal, 5
- elimination order, 14

- finite A -algebra, 21
- finitely generated, 9
- finitely generated over A , 21
- free modules, 19

- Gröbner basis, 13

- Hilbert's Strong Nullstellensatz, 11
- Hilbert's Weak Nullstellensatz, 11
- homogeneous, 6
- homogenous ideal, 6

- ideals, 5
- integral over A , 22

- leading term, 10

- lexicographic order, 10

- minimal polynomials, 7
- monomial ideals, 9

- Noether normalisation lemma, 21
- Noetherian, 11

- polynomial rings, 5
- projective variety, 7
- projective zeros, 6
- pure lexicographic order, 10

- radical, 5
- resultant, 6

- Singural, 13

- term order, 13

- Zariski topology, 5
- zero locus, 5