§ 2 Gröbner bases

2.1 Goals

(1) Hilbert's Nullstellensatz reduces the question whether a system of equations

$$f_1(x_1, \dots, x_n) = 0$$
$$\vdots$$
$$f_r(x_1, \dots, x_n) = 0$$

has a solution $a = (a_1, \dots, a_n) \in \mathbb{A}^n(K)$ for $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ to whether $1 \in I = (f_1, \dots, f_r)$. In principle is a linear algebra question.

We have to find $g_1, \dots, g_r \in K[x_1, \dots, x_n]$ with $1 = g_1 f_1 + \dots + g_r f_r$ and many indeterminant coefficients for the g_i's this linear system of equation in finitely many variables, if we could find an apriori bound on the degree of the g_i

We will use a different approach.

(2) More generally we will solve <u>Ideal membership problem</u>

Given $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ and $f \in K[x_1, \dots, x_n]$

Decide $f \in (f_1, \dots, f_r)$

The solution allows us to compute in the quotient ring $K[x_1, \dots, x_n]/(f_1, \dots, f_r)$

(3) Given a polynomial map $\mathbb{A}^n \xrightarrow{(f_1, \dots, f_m)} \mathbb{A}^m$ and the corresponding ring homomorphism

$$\varphi: K[y_1, \dots, y_m] \to K[x_1, \dots, x_n]$$
$$y_i \mapsto f_i$$

we want to compute (a) $I = \ker \varphi$

Remark $V(I) \subset \mathbb{A}^n$ describes the <u>Zariski closure</u> of $\Phi(\mathbb{A}^n) = B \subset \mathbb{A}^m$

(b) More generally for $\Phi: A \xrightarrow{(f_1, \dots, f_m)} \mathbb{A}^m$ we want to compute the Zariski closure of the image, that is $I = \ker\left(K[y_1, \dots, y_m] \to K[x_1, \dots, x_n]/I(A) = K[A]\right)$

(c) Given a rational map $\Phi: A \dashrightarrow \mathbb{A}^m$ want to compute $f_i \in K(A)$, $\ker\left(K[y_1, \dots, y_m] \to K(A)\right)$

$$y_i \mapsto f_i$$

(d) We would like to compute the

$$\dim A = \operatorname{tr.deg}_{\bar{k}} A$$

via the projection thm
So we would like to compute the k-th elimination ideal of $I \subset k[x_1, \dots, x_n]$ defined by

$$I_k = I \cap k[x_{k+1}, \dots, x_n]$$

which is the ideal obtained by eliminating $x_1, \dots, x_k$

All this is possible with Gröbner bases

2.2 Def: R any ring (commutative with 1)
A monomial in $R[x_1, \dots, x_n]$ is an element

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

where the exponent $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ is a multiindex. A term in $R[x_1, \dots, x_n]$ is element of the form λx^α, $\lambda \in R$.
Then every polynomial $f \in R[x_1, \dots, x_n]$ is finite sum of terms $f = \sum_\alpha f_\alpha x^\alpha$. $f_\alpha \in R$ and all but finitely many are zero

2.3 A polynomial $f \in R[x]$ in a single variable is called monique if

$$f = a_d x^d + \dots + a_1 x + a_0$$

satisfies $a_d = 1$. A degree of $f \in R[x]$ is $\deg f = d$, if $a_d \neq 0$.

2.4 Prop (Euclidean division)
Let $f \in R[x]$ be a monique polynomial.
Then for $g \in R[x]$ there is unique $q, r \in R[x]$ with

$$g = q f + r$$

with $\deg r < \deg f$
r is called the remainder

Proof: Existence by induction on $\deg g$
If $\deg g < \deg f$ we may take $q = 0$, $r = g$

If $m - \deg g \geq \deg S = d$ and b_m is the leading coeff. of g we have for

$$\tilde{g} = g - b_m X^{m-d} S$$

the leading coefficient of the two cancels. Hence $\deg \tilde{g} < \deg g$

$$\tilde{g} = \tilde{q} S + r$$

By ind hypothesis $g = (b_m X^{m-d} + \tilde{q}) S + r$ is the desired expression

Uniqueness: We have to prove that

$$0 = q S + r \Rightarrow q = 0, r = 0$$

If $q \neq 0$. Since S is monique the leading coeff of q and qS coincide and $\deg(q \cdot S) = \deg(q) + \deg(S) > \deg r$ a contradiction. So $q = 0$ and hence $r = 0$.

25 Example $S_1 = X^2 + XY \in K[Y][X] = K[X,Y]$

Any $g \in K[Y][X]$ is congruent to $r \bmod (S_1)$ where no term of r is divisible by X^2.

Similarly $S_2 = Y^2 + XY \in K[X][Y] = K[X,Y]$ can be used to eliminate Y^2 from any g.

Question: Can we use S_1 and S_2 to eliminate any term divisible by X^2 or Y^2?

$$X^2 Y = Y \cdot S_1 - XY^2 \equiv -XY^2 \bmod (S_1, S_2)$$

$$-XY^2 \equiv X S_2 + X^2 Y \equiv X^2 Y \bmod (S_1, S_2)$$

end up with loop.

Answer No

Assume yes. Then $1, \bar{X}, \bar{Y}, \bar{X}\bar{Y}$ would represent generators of $K[X,Y]/(S_1, S_2)$ as a K-Vectorspace

But then $|V(S_1, S_2)| < \infty$. But. $V(S_1, S_2) \supset V(X+Y)$

4.2 Exercise $S_1, \dots, S_r \in K[X_1, \dots, X_n]$

Suppose $d = \dim_{K\text{-VS}} K[X_1, \dots, X_n]/(S_1, \dots, S_r) < \infty$

then $V(S_1, \dots, S_r) \subset \mathbb{A}^n = \mathbb{A}^n(\bar{K})$ is finite as well and $|V(S_1, \dots, S_r)| \leq d$

What went wrong?

We picked the initial term X^2 of $X^2 + XY$ and Y^2 of $Y^2 + XY$ without respecting the multiplicative structure on the set of monomials

2.6 Def: A monomial order on a polynomial ring over field K is a complete order $"<"$ on the set of monomials $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ satisfying

$$x^\alpha < x^\beta \Rightarrow x^\alpha x^\delta < x^\beta x^\delta$$

$"<"$ is called global if in addition we have $x_i > 1 = x^0$

Given a monomial order $"<"$ we define the initial term

$$f = \sum_\alpha f_\alpha x^\alpha \in K[x_1, \dots, x_n]$$

$in(f) = f_\beta x^\beta$ where $x^\beta = \max_{"<"} \{x^\alpha \mid f_\alpha \neq 0\}$, β leading exponent, f_β leading coefficient and $in(0) = 0$ by convention

Back to the example:

$in(x^2 + xy) = 2$. $x^2 > xy \Rightarrow x > y \Rightarrow xy = in(y^2 + xy)$

2.7 Examples: There are many global maximal orders

(1) Lexicographic order $"<_{lex}"$:

$x^\alpha <_{lex} x^\beta$ if the first nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is positive i.e. if there is k

$\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}, \alpha_k > \beta_k$

(2) degree reverse lexicographic, $drlex$ ($rlex$)

$x^\alpha <_{drlex} x^\beta$, if $|\alpha| = \sum \alpha_i < |\beta| = \sum \beta_i$

or $"="$ and the last nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is $"$negative$"$

Remark: The difference between lex and $drlex$ is subtle but as we will see important

$K[x, y, z]$, $x > y > z$

lex: $x^2 > xy > xz > x > y^2 > yz > y > z^2 > z > 1$

$drlex$: $x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1$

(3) Let $\omega = (\omega_1, \dots, \omega_n) \in \mathbb{R}^n_{>0}$

we define $x^\alpha <_\omega x^\beta$ if

$\omega_1 \alpha_1 + \dots + \omega_n \alpha_n < \omega_1 \beta_1 + \dots + \omega_n \beta_n$

or $\omega_1 \alpha_1 + \dots + \omega_n \alpha_n = \omega_1 \beta_1 + \dots + \omega_n \beta_n$ and $x^\alpha <_t x^\beta$

where $<_t$ is any (tie break) monomial order

4.2 Exercise

Let $M \subset K[x_1, \dots, x_n]$ be a finite set of monomials and $>$ any global monomial order.

Proove that there are weights such that $>_w$ induces the same order on M, then there is a weight $(w_1, \dots, w_n) \in \mathbb{N}^n_{>0}$

2.6. Thm (Division with remainder)

Let $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ and $>$ a global monomial order. For any $f \in K[x_1, \dots, x_n]$ there exists unique $g_1, \dots, g_r \in K[x_1, \dots, x_n]$ and remainder $h \in K[x_1, \dots, x_n]$ such that

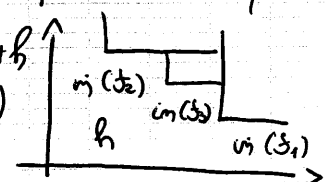
(1) $f = g_1 f_1 + \dots + g_r f_r + h$

(2a) No term of $g_i \operatorname{in}(f_i)$ is divisible by any $\operatorname{in}(f_j)$ for a $j < i$

(2b) No term of h is divisible by an $\operatorname{in}(f_i)$ for any $i = 1, \dots, r$

Example If $f_1, \dots, f_r$ are monomials then the statement is obvious identifying monomials with points in $\mathbb{N}^n$ we obtain by (2) a partition of $\mathbb{N}^n$:

So $f = \tilde{g}_1 \operatorname{in}(f_1) + \dots + \tilde{g}_r \operatorname{in}(f_r) + h$ satisfying (2a) and (2b)



In the general case we will apply $\mathbb{N}^n$ induction.

2.7 Lemma (Dixon) Let $>$ be a global monomial order on $K[x_1, \dots, x_n]$ and $M \subset K[x_1, \dots, x_n]$ a non empty set of monomials

Then M contains a minimal element w.r. to $>$

Proof: Consider the maximal ideal I generated by M

I is finitely generated. $I = (m_1, \dots, m_r)$ by monomials and the minimal generators (these we can not omit) are elements of M.

Since $m\, m_i > m_i$ for any monomial $m > 1$ the minimal of I is one of the generators and exists since there are finitely many ∎

Ex 4.3 Dixon proved for orders on $\mathbb{N}^n$