Herramientas computacionales en álgebra conmutativa

Santiago Laplagne - Mercedes Pérez Millán

Universidad de Buenos Aires

Encuentro RSME-UMA, Diciembre 2017

Polinomios

- $\Bbbk = \mathbb{Q}, \mathbb{C}, \ldots$ cuerpo (en los algoritmos usamos en general $\mathbb{Q}$ y para algunos resultados teóricos usaremos $\mathbb{C}$)
- $R = \Bbbk[X_1, \ldots, X_n]$, el anillo de polinomios en n variables con coeficientes en el cuerpo $\Bbbk$.

Ejemplos:

- $R = \mathbb{Q}[X, Y]$, $f(X, Y) = 3X^2Y - 2X + 1 \in \mathbb{Q}[X, Y]$
- $g(X, Y) = \frac{1}{XY}$, $h(X, Y, Z) = \sqrt{X + Y + Z}$ no son polinomios

Un polinomio es una suma de monomios

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{m} a_i X_1^{d_{i,1}} \cdots X_n^{d_{i,n}}, a_i \in \Bbbk, d_{i,j} \in \mathbb{N}_0$$

Ejemplo: $f(X, Y) = (X + Y)^2 = X^2 + 2XY + Y^2$ es un polinomio

Soluciones de ecuaciones polinomiales

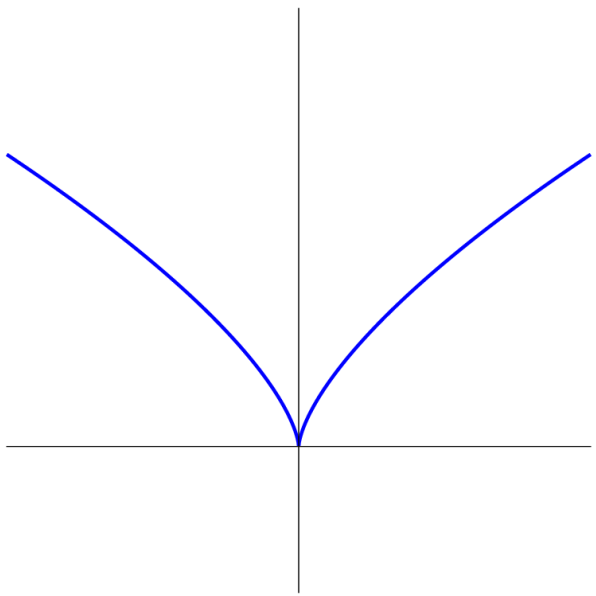
- Si $f \in \mathbb{Q}[X]$ (o $\mathbb{C}[X]$) es un polinomio de grado d, la ecuación $f(X) = 0$ tiene d soluciones en $\mathbb{C}$.

Ejemplo: $X^3 - 1 = (X - 1)(X^2 + X + 1)$ tiene 3 soluciones en $\mathbb{C}$ pero una sola solución en $\mathbb{Q}$.

- Si $f \in \mathbb{Q}[X, Y]$ (o $\mathbb{C}[X, Y]$), las soluciones de $f(X, Y) = 0$ describen una curva en $\mathbb{C}^2$.

Ejemplo:

- $f(X, Y) = Y^3 - X^2$, las soluciones de $Y^3 - X^2 = 0$ definen una cúspide.
- $X^2 + Y^2 + 1 = 0$
  no tiene soluciones en $\mathbb{Q}^2$
  pero tiene infinitas soluciones en $\mathbb{C}^2$.



En Maple:

Factorización de polinomios

```
> f1:=x^3-1
```

```
> factor(f1)
```

Ejercicio: Utilizando `factor`, hallar las raíces de $X^5 - 7X^4 - 2X^3 + 14X^2 - 3X + 21$.

Gráficos de soluciones

```
> f2:=y^3-x^2:
```

```
> with(plots,implicitplot):
```

```
> implicitplot(f2=0, x=-1..1, y=-1..1, gridrefine=2)
```

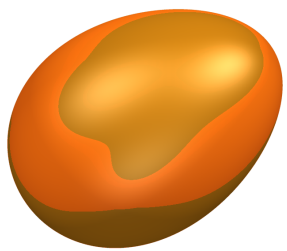
Ejercicio: Graficar las soluciones de $X^2 - Y^2 = 1$.

Soluciones de polinomios en varias variables

- Si $f \in \mathbb{Q}[X_1, \ldots, X_n]$, las soluciones de $f(X_1, \ldots, X_n) = 0$ definen una hiper-superficie (de dimensión $n-1$) en $\mathbb{C}^n$.

Ejemplo:

Las soluciones de la ecuación $X^2 + Y^2 + 0,6Z^2 + 0,2Z^3 = 0,3$ forman la cáscara de un *huevo* en el espacio.

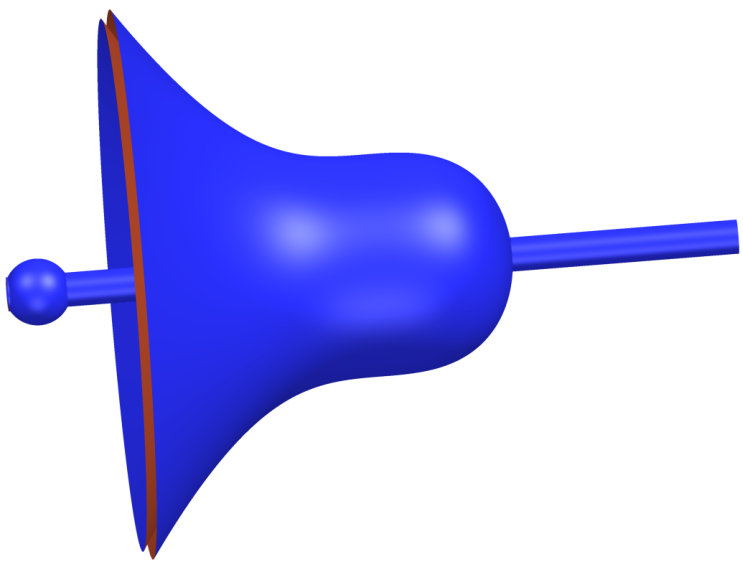


Llamamos $\mathbf{V}(\{f\})$, variedad asociada a f, al conjunto de soluciones de $f = 0$. Cuando sea necesario distinguiremos $\mathbf{V}_{\mathbb{Q}}$ las soluciones en $\mathbb{Q}^n$ y $\mathbf{V}_{\mathbb{C}}$ las soluciones en $\mathbb{C}^n$.

Producto de polinomios $\leftrightarrow$ unión de superficies

- Si $f = gh$, producto de dos polinomios, entonces $\mathbf{V}(\{f\}) = \mathbf{V}(\{g\}) \cup \mathbf{V}(\{h\})$.

Ejemplo. Este gráfico se puede lograr multiplicando las ecuaciones de la campana, un cilindro y una esfera.



En Maple:

Variedad de un producto de polinomios.

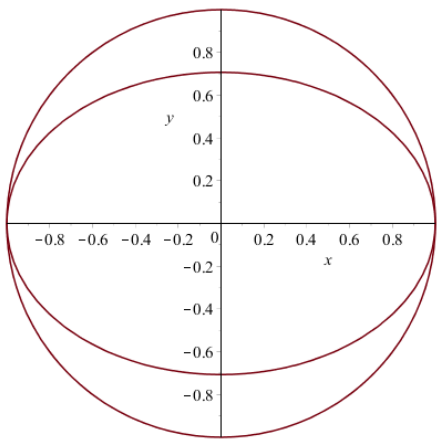
```
> f3:=x-1:
```

```
> f4:=x^2+y^2-2:
```

```
> f5:=f3*f4:
```

```
> implicitplot(f5=0, x=-3..3, y=-2..2, gridrefine=3)
```

Ejercicio: Realizar el siguiente gráfico en Maple.



(no usar `gridrefine` mayor que 10, puede tardar demasiado tiempo)

Ideales de polinomios

Dado un conjunto de polinomios $S = \{f_1, \ldots, f_s\} \subset \Bbbk[X_1, \ldots, X_n]$, definimos el ideal generado por S:

$$\langle f_1, \ldots, f_s \rangle = \{a_1 f_1 + \cdots + a_s f_s : a_i \in \Bbbk[X_1, \ldots, X_n]\} \subset \Bbbk[X_1, \ldots, X_n].$$

Este conjunto cumple las siguientes propiedades:

- $f, g \in I \Rightarrow f + g \in I$
- $f \in I, a \in \Bbbk[X_1, \ldots, X_n] \Rightarrow af \in I$

En general, un conjunto $I \subset R$, R anillo, se llama *ideal* si cumple las dos propiedades.

Proposición

Todos los ideales en $\Bbbk[X_1, \ldots, X_n]$ son generados por un conjunto finito de polinomios (se llaman anillos Noetherianos a tales anillos).

En Maple:

En Maple los ideales de definen por una lista de polinomios generadores.

```
> f6 := 5*x^3*y+x^2:

> f7 := x^2+y^2:

> f8 := z+7:

> F1 := [f6, f7, f8]

> F2 := [x^3*y+x^2, x^2*y^3+y^2]
```

Sistemas de ecuaciones polinomiales

Queremos estudiar las soluciones de un conjunto de ecuaciones polinomiales

$$\begin{cases} f_1(X_1, \ldots, X_n) = 0 \\ \qquad\qquad\qquad\qquad \ldots \\ f_s(X_1, \ldots, X_n) = 0 \end{cases}$$

- Definimos
  $\mathbf{V}(F) = \{(x_1, \ldots, x_n) \in \Bbbk^n : f(x_1, \ldots, x_n) = 0 \ \forall f \in F\}$, la variedad del conjunto $F \subset \Bbbk[X_1, \ldots, X_n]$.

Proposición

Para $\{f_1, \ldots, f_s\} \subset \Bbbk[X_1, \ldots, X_n]$,

$$\mathbf{V}(\{f_1, \ldots, f_s\}) = \mathbf{V}(\langle f_1, \ldots, f_s \rangle).$$

Hallar las soluciones de un sistema de ecuaciones polinomiales equivale a encontrar la variedad asociada al ideal generado.

- Un conjunto $V \subset \Bbbk^n$ es una variedad si existe un ideal I tal que $V = \mathbf{V}(I)$.

Casos simples

Polinomios en una variable

- Si $I = \langle f_1, \ldots, f_s \rangle \subset \Bbbk[X]$ y $g = \mathrm{mcd}(f_1, \ldots, f_s)$ entoces

$$I = \langle g \rangle$$

  (en $\Bbbk[X]$ todos los ideales son *principales*, están generados por un solo polinomio)

- Para encontrar las soluciones de $\{X^6 - 1 = 0, X^8 - 1 = 0\}$, tenemos

$$\mathbf{V}(\{X^6 - 1, X^8 - 1\}) = \mathbf{V}(\langle X^6 - 1, X^8 - 1 \rangle) = \mathbf{V}(\langle X^2 - 1 \rangle),$$

  por lo tanto, las únicas soluciones son $X = 1$ y $X = -1$.

Casos simples

Ecuaciones lineales en varias variables

- Para resolver el sistema de ecuaciones

$$\begin{cases} a_{1,1}X_1 + \cdots + a_{1,n}X_n = b_1 \\ \cdots \\ a_{n,1}X_1 + \cdots + a_{n,n}X_n = b_n \end{cases} \tag{1}$$

podemos usar eliminación de Gauss para obtener un sistema más simple:

$$\begin{cases} a_{1,1}X_1 + \cdots + a_{1,n-1}X_{n-1} + a_{1,n}X_n = b_1 \\ \cdots \\ a_{n-1,n-1}X_{n-1} + a_{n-1,n}X_n = b_{n-1} \\ a_{n,n}X_n = b_n \end{cases}$$

Triangulando obtenemos un sistema de generadores del ideal más simple que el sistema original.

Bases de Groebner

Las bases de Groebner generalizan los ejemplos anteriores al caso general de polinomios de cualquier grado en cualquier cantidad de variables.

Antes de introducir las bases de Groebner, necesitamos algunos preliminares para generalizar la división de polinomios en una variable a varias variables.

Órden monomial lexicográfico

Definimos un orden en los monomios análogo al orden del diccionario:

$$X_1^{d_1} X_2^{d_2} \dots X_n^{d_n} \leq X_1^{e_1} X_2^{e_2} \dots X_n^{e_n}$$

si se cumple alguna de las siguientes condiciones

- $d_1 \leq e_1$
- $d_1 = e_1,\ d_2 \leq e_2$
- $d_1 = e_1,\ d_2 = e_2,\ d_3 \leq e_3$

  $\dots$
- $d_1 = e_1, \dots, d_{n-1} = e_{n-1}, d_n \leq e_n$

Ejemplos

- $Y^{10} < XY^2,\ XY < XYZ.$

Coeficiente principal y monomio de cabeza

Dado $f(X_1, \ldots, X_n) = \sum_{i=1}^{m} a_i X_1^{d_{i,1}} \cdots X_n^{d_{i,n}} \in \Bbbk[X_1, \ldots, X_n]$, con

$$X_1^{d_{1,1}} \cdots X_n^{d_{1,n}} > \cdots > X_1^{d_{m,1}} \cdots X_n^{d_{m,n}},$$

llamamos

$$\operatorname{lm}(f) = a_1 X_1^{d_{1,1}} \cdots X_n^{d_{1,n}}$$

monomio de cabeza de f.

Dado un conjunto $F \subset \Bbbk[X_1, \ldots, X_n]$, definimos

$$\operatorname{Lm}(F) = \langle \operatorname{lm}(f) : f \in F \rangle,$$

el ideal de monomios de cabeza de F.

En Maple:

Monomios y términos de cabeza.

```
> with(Groebner):

> LeadingTerm(f6, plex(x, y))

> LeadingMonomial(f6, plex(x, y))

> LeadingTerm(F2[1], plex(x, y))

> LeadingMonomial(F2[1], plex(x, y))
```

Reducción (división en varias variables)

- Decimos que f es *reducible* por g si $\mathrm{lm}(f)$ es múltiplo de $\mathrm{lm}(g)$. Ejemplo: $X^2Y^3 + 1$ es reducible por $XY^2 - 3X + 1$.
- Si f es reducible por g llamamos

$$\mathrm{red}(f, g) = f - \frac{\mathrm{lm}(f)}{\mathrm{lm}(g)} g$$

la reducción de f por g.

Proposición

Si f es reducible por g, $\mathrm{red}(f, g)$ tiene "menor grado" que f. Es decir,

$$\mathrm{lm}(\mathrm{red}(f, g)) < \mathrm{lm}(f)$$

Reducción por un conjunto

Un polinomio f es reducible por un conjunto $G \subset \Bbbk[X_1, \ldots, X_n]$ si existe $g \in G$ tal que f es reducible por g.

Decimos que $\tilde{f}$ es un reducido de f por G si es resultado de reducir a f sucesivamente por polinomios de G hasta obtener un polinomio irreducible por G.

Ejercicio (en Maple). Reducir el polinomio $f = X^3Y^2 + 1$ por el conjunto $G = \{X^2 + Y, Y^3 + 2Z\}$.

Observación: dependiendo del orden en el que se realiza la reducción, se pueden obtener distintos reducidos.

Bases de Groebner

Dado un ideal I, un conjunto $G = \{g_1, \ldots, g_m\} \subset I$ es una *base de Groebner* de I si

$$\mathrm{Lm}(I) = \mathrm{Lm}(G)$$

Propiedades

1. Si f es reducible por I entonces f es reducible por algún polinomio de G.
2. El resultado de reducir un polinomio f por G es único, no depende del orden en que se reduce.
3. Si $f \in I$, entonces el reducido de f por G es 0.

Ejercicio: Ver que (1) y (2) implican (3).

¡Esto nos permite decidir si un polinomio $f \in I$!

En Maple:

Bases de Groebner

```
> G2 := Basis(F2, plex(x, y))

> G1 := Basis(F1, plex(x, y, z))

> f9 := x^3*y^4-y^2:

> Reduce(f9, F1, plex(x, y, z))

> Reduce(f9, F2, plex(x, y, z))
```

Eliminación de variables

Si $G = \{g_1, \ldots, g_s\}$ es una base de Groebner de I en el orden lexicográfico $X_1 > X_2 > \cdots > X_n$, entonces $I \cap \Bbbk[X_i, \ldots, X_n]$ está generado por los polinomios de G en las variables $X_i, \ldots, X_n$.

Esto nos permite triangular un sistema de polinomios en varias variables.

Ejemplo. Para $I = \langle YX^3 + X^2, Y^3X^2 + Y^2 \rangle$, una base de Groebner en el orden lexicográfico $X > Y$ es $G = \{X^2 - Y^2, XY^2 - Y^2, Y^3 + Y^2\}$. El sistema

$$\begin{cases} X^2 - Y^2 = 0 \\ XY^2 - Y^2 = 0 \\ Y^3 + Y^2 = 0 \end{cases}$$

está *triangulado*. De la última ecuación obtenemos $Y = 0$ o $Y = -1$, y reemplazando en las otras ecuaciones obtenemos que las únicas soluciones del sistema son $(0, 0)$ y $(1, -1)$.

Eliminación de variables

Ejercicio.

Hallar todas las soluciones racionales del siguiente sistema de ecuaciones.

$$\begin{cases} x - y - z = 10 \\ w^2 - y = 7 \\ 4yz + 2z^2 + 2w^2 + 39y + 39z = -179 \\ 2y^2 + y + z = -1 \\ 8z^3 + 238z^2 - 27y + 2239z = -6533 \end{cases}$$