Intoducción al álgebra conmutativa computacional

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. Ciclo impar de 2019

> Tout ce qui est beau et noble est le résultat de la raison et du calcul.
>
> Charles Baudelaire, “L’Art romantique”

Una gran parte de estos apuntes esencialmente sigue [CLO2015] y por esto no pretendo ser original. Nuestro enfoque será más práctico: después de aprender cada nuevo concepto, vamos a ver cómo este puede ser o ya está implementado en el programa Macaulay2. La segunda parte es un poco más avanzada y está dedicada a algunos aspectos computacionales de geometría algebraica, y también revisa ciertos conceptos importantes de álgebra conmutativa. Allí las referencias sugeridas son las partes relevantes de [Eis2004], [AM1969] y [Kem2010].

Versión 22/07/2019. Para la última actualización, consulte la página

`http://cadadr.org/san-salvador/2019-groebner/`

¡Todos los comentarios son bienvenidos!

Agradezco al Dr. José Nerys Funes Torres por la oportunidad de dar este curso y a los estudiantes que asistieron a mis lecciones: José Mauricio Calles Ramirez, Jorge Balmore Flores Tejada, César Omar Gómez Juárez, Mario Enrique Hernández Carpio, y Francisco Antonio Mejía Ramos.

Índice

1 Notación

- La letra k siempre denotará el cuerpo base.
- Las variables de polinomios se denotarán por las letras minúsculas $x, y, z, \ldots$
- Los ideales se denotarán por las letras I e J.
- $(f_1, \ldots, f_s)$ denotará el ideal generado por $f_1, \ldots, f_s$.

2 Macaulay2

En este curso vamos a usar el programa Macaulay2. Su nombre conmemora al geómetra algebraico inglés Francis Sowerby Macaulay (1862–1937), y la cifra 2 se refiere a la segunda versión. Para descargarlo y obtener la documentación completa, consulte la página

http://macaulay2.com/

Si el programa está instalado en el sistema, para abrirlo, hay que ejecutar el comando `M2` (con `M` mayúscula). Sino, se puede usar el interfaz web

http://web.macaulay2.com/

Macaulay2 fue desarrollado por especialistas en álgebra y geometría algebraica y la sintaxis de su lenguaje es muy natural, por ejemplo:

- `ZZ` denota el anillo $\mathbb{Z}$,
- `QQ` denota el cuerpo $\mathbb{Q}$,
- `ZZ/`p denota el cuerpo $\mathbb{Z}/p\mathbb{Z}$, donde p debe ser un número primo,
- `GF` q denota el cuerpo finito $\mathbb{F}_q$, donde $q = p^k$ (aquí "GF" viene de "Galois Field"),
- `0_`R y `1_`R denotan el cero y la identidad del anillo R,
- R`[`x`,`y`,`z`]` denota el anillo de polinomios con coeficientes en R en variables x, y, z,
- R`[x_1..x_5]` denota el anillo de polinomios con coeficientes en R en cinco variables `x_1`, `x_2`, `x_3`, `x_4`, `x_5`.
- `(`a`,`b`,`c`)` y `{`a`,`b`,`c`}` denota respectivamente la sucesión y la lista de elementos a, b, c. Los elementos se numeran a partir de `0`.
- `#`X devuelve el número de elementos en X (que puede ser una sucesión, lista, etc.), mientras que X`#`i es el i-ésimo elemento.
- etcétera.

Estos apuntes no son un manual exhaustivo de Macaulay2, así que sus funciones serán ilustradas por ejemplos particulares. El apéndice A contiene una lista de comandos básicos de Macaulay2 que serán relevantes para nuestro curso.

Primera sesión en Macaulay2

He aquí un ejemplo de sesión en Macaulay2 donde vamos a verificar que en el anillo $\mathbb{Q}[a,b,c,d]$ para el ideal

$$I := (a^2 + bc, d^2 + bc, (a+d)\,b, (a+d)\,c)$$

el radical coincide con el ideal

$$J := (ad - bc, a + d).$$

```
alexey@topos:~$ M2
Macaulay2, version 1.13
--loading configuration for package "FourTiTwo" from file .../init-FourTiTwo.m2
--loading configuration for package "Topcom" from file .../init-Topcom.m2
with packages: ConwayPolynomials, Elimination, IntegralClosure, InverseSystems, LLLBases,
               PrimaryDecomposition, ReesAlgebra, TangentCone, Truncations

i1 : R = QQ[a,b,c,d];

i2 : I = ideal (a^2 + b*c, d^2 + b*c, (a+d)*b, (a+d)*c);

o2 : Ideal of R

i3 : radical(I)

                            2
o3 = ideal (a + d, b*c + d )

o3 : Ideal of R

i4 : oo == ideal (a*d - b*c, a+d)

o4 = true

i5 : exit
alexey@topos:~$
```

Notamos que las entradas (*input*) se numeran por `i1`, `i2`, `i3`, ... mientras que las salidas (*output*) se numeran por `o1`, `o2`, `o2`, ... Muy a menudo en una sesión interactiva nos interesa la última salida, y esta se denota por `oo`. La sesión de arriba termina con el comando `exit` que sale del programa.

Note que los comandos en `i1` y `i2` se terminan por el punto y coma (`;`). Esto suprime la salida. He aquí los mismos comandos sin punto y coma:

```
i1 : R = QQ[a,b,c,d]

o1 = R

o1 : PolynomialRing

i2 : I = ideal (a^2 + b*c, d^2 + b*c, (a+d)*b, (a+d)*c)

             2               2
o2 = ideal (a  + b*c, b*c + d , a*b + b*d, a*c + c*d)

o2 : Ideal of R
```

La documentación puede ser obtenida directamente del programa: por ejemplo,

- el comando "`help radical`" mostrará la información sobre la función `radical`;
- el comando "`viewHelp radical`" abre la documentación interactiva en el navegador.

Las teclas ↑ y ↓ pueden ser usadas para ver los comandos digitados previamente, y la tecla Tab completa los comandos. Por ejemplo, se puede digitar "qu" y luego presionar Tab para ver todos los comandos que empiezan por "qu".

Una nota muy importante: todas las expresiones son sensibles a mayúsculas y minúsculas. Por ejemplo, `ideal` es una función que sirve para construir un ideal, mientras que `Ideal` es el tipo de datos que corresponde a los ideales en Macaulay2.

Anillos cociente

Los anillos cociente se definen usando la sintaxis natural. He aquí un ejemplo con el cuerpo ciclotómico

$$\mathbb{Q}(\zeta_5) \cong \mathbb{Q}[x]/\Phi_5, \quad \text{donde } \Phi_5 = x^4 + x^3 + x^2 + x + 1.$$

Calculemos $\frac{1}{1+\zeta_5^3}$ en $\mathbb{Q}(\zeta_5)$:

```
i1 : K = toField (QQ[z_5]/(z_5^4+z_5^3+z_5^2+z_5+1))

o1 = K

o1 : PolynomialRing

i2 : 1/(1+z_5^3)

       2
o2 = z  + z  + 1
       5    5

o2 : K
```

La función `toField` se usa para declarar que un anillo es un cuerpo. Tal vez sería bueno subrayar que el enfoque de Macaulay2 es álgebra conmutativa, y para explorar las propiedades aritméticas de extensiones finitas de $\mathbb{Q}$ existen otros programas como PARI/GP (http://pari.math.u-bordeaux.fr/).

He aquí otro ejemplo con los enteros de Gauss $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$:

```
i3 : R = ZZ[i]/(i^2+1)
o3 = R
o3 : QuotientRing
i4 : (3+2*i)*(3-2*i)
o4 = 13
o4 : R
```

Parte I
Gröbner basics

3 Polinomios en una variable

Revisemos rápidamente la situación con polinomios en una variable. Para un polinomio

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in k[x],$$

donde $a_n \neq 0$, denotemos el **término mayor** por

$$LT(f) := a_n x^n.$$

3.1. Teorema. *Sean $f, g \in k[x]$ dos polinomios, $g \neq 0$. Entonces, existe un algoritmo que obtiene polinomios $q, r \in k[x]$ tales que*

$$f = qg + r$$

y $r = 0$ o bien $\deg r < \deg g$. Además, estos q y r están definidos de modo único.

Demostración. Consideremos el siguiente algoritmo.

Entrada: $f, g \in k[x]$, donde $g \neq 0$

$q := 0$
$r := f$

mientras $r \neq 0$ y $LT(r) \mid LT(g)$ **hacer**
    $q = q + LT(r)/LT(g)$
    $r = r - LT(r)/LT(g) \cdot g$

devolver (q, r)

Aquí la condición $LT(r) \mid LT(g)$ es equivalente a $\deg g < \deg r$. Notamos que a cada paso del algoritmo se cumple la identidad

$$f = qg + r.$$

En efecto, esto es cierto al inicio cuando se pone $q := 0$ y $r := f$. Luego, a cada paso se tiene

$$(q + LT(r)/LT(g))\, g + (r - LT(r)/LT(g) \cdot g) = qg + r = f.$$

El ciclo se termina porque

$$LT(r) = LT(LT(r)/LT(g) \cdot g),$$

así que $r - LT(r)/LT(g) \cdot g = 0$, o bien

$$\deg(r - LT(r)/LT(g) \cdot g) < \deg r,$$

y el grado de r no puede decrecer de manera infinita. Cuando el ciclo termina, tenemos $r = 0$ o bien $\deg r < \deg g$, así que r es el resto de división.

Ahora veremos la unicidad. Asumamos que

$$f = q_1 g + r_1 = q_2 g + r_2.$$

Luego, tenemos

$$(q_1 - q_2) g = r_1 - r_2.$$

Dado que $g \neq 0$, esta expresión nos dice que $q_1 = q_2$ si y solo si $r_1 = r_2$. Ahora si $r_1 \neq r_2$, entonces, puesto que $\deg r_1, \deg r_2 < \deg g$, tenemos

$$0 \leq \deg(r_1 + r_2) < \deg g,$$

pero esto contradice el hecho de que

$$\deg((q_1 - q_2) g) = \deg(q_1 - q_2) + \deg g. \qquad \blacksquare$$

La división con resto implica que $k[x]$ es un dominio de ideales principales.

3.2. Corolario. *Todo ideal $I \subseteq k[x]$ es principal: existe $g \in k[x]$ tal que $I = (g)$.*

Demostración. Si $I = 0$, entonces su generador es 0. Si $I \neq 0$, sea $g \in k[x]$ un polinomio del mínimo grado posible tal que $g \in I$. Ahora para cualquier polinomio $f \in I$, la división con resto nos da

$$f = qg + r,$$

donde $r = 0$ o $\deg r < \deg g$. Pero $r = f - qg \in I$, así que por la elección de g se tiene necesariamente $r = 0$ y por ende $f = qg \in (g)$. $\blacksquare$

3.3. Comentario. El anillo de polinomios en diversas variables $k[x_1, \ldots, x_n]$ no es un dominio de ideales principales para $n > 1$. Por ejemplo, $(x_1, \ldots, x_n)$ es un ideal que no es principal. En particular, la división con resto como tal no existe en $k[x_1, \ldots, x_n]$ (es decir, esto no es un dominio euclidiano).

3.4. Proposición. *En $k[x]$ tenemos para cualesquiera $f_1, \ldots, f_s \in k[x]$*

$$(f_1, \ldots, f_s) = (g),$$
$$(f_1) \cap \cdots \cap (f_s) = (h),$$

donde

$$g = \operatorname{mcd}(f_1, \ldots, f_s), \quad h = \operatorname{mcm}(f_1, \ldots, f_s).$$

Demostración. El ideal $(f_1, \ldots, f_s)$ es el ideal mínimo que contiene a $f_1, \ldots, f_s$. Por el resultado anterior, este puede ser generado por un elemento $g \in k[x]$. Hay que probar que g es el máximo común divisor de $f_1, \ldots, f_s$. Primero, puesto que $f_1, \ldots, f_s \in (g)$, tenemos $g \mid f_1, \ldots, g \mid f_s$. Ahora si $g' \in k[x]$ es otro polinomio tal que $g' \mid f_1, \ldots, g' \mid f_s$, entonces

$$(f_1, \ldots, f_s) = (g) \subseteq (g').$$

La inclusión $(g) \subseteq (g')$ significa que $g' \mid g$.

La parte sobre el mínimo común múltiplo se demuestra de la misma manera y lo dejo como un ejercicio. $\blacksquare$

Ahora, si se tiene un ideal $I = (f_1, \ldots, f_s) \subseteq k[x]$, para encontrar $g \in k[x]$ tal que $I = (g)$, basta saber calcular el máximo común divisor. Recordemos que esto se hace mediante el **algoritmo de Euclides**.

Entrada: $f, g \in k[x]$

mientras $g \neq 0$ **hacer**
  $g' := g$
  $g =$ el resto de división de f por g
  $f = g'$
devolver f

Para justificar el algoritmo, notamos que si

$$f = qg + r,$$

entonces

$$\mathrm{mcd}(f, g) = \mathrm{mcd}(g, r).$$

Esto se sigue de la equivalencia

$$h \mid f,\ h \mid g \iff h \mid g,\ h \mid r.$$

Entonces, a cada paso del algoritmo de arriba, el $\mathrm{mcd}(f, g)$ no cambia. El grado de g siempre decrece, así que en algún momento g se vuelve nulo y el ciclo se termina. Cuando $g = 0$, tenemos $\mathrm{mcd}(f, 0) = f$.

En general, para calcular $\mathrm{mcd}(f_1, \ldots, f_s)$, basta notar que

$$\begin{aligned}
\mathrm{mcd}(f_1, f_2, f_3) &= \mathrm{mcd}(\mathrm{mcd}(f_1, f_2), f_3),\\
\mathrm{mcd}(f_1, f_2, f_3, f_4) &= \mathrm{mcd}(\mathrm{mcd}(\mathrm{mcd}(f_1, f_2), f_3), f_4),\\
\mathrm{mcd}(f_1, f_2, f_3, f_4, f_5) &= \mathrm{mcd}(\mathrm{mcd}(\mathrm{mcd}(\mathrm{mcd}(f_1, f_2), f_3), f_4), f_5),\\
&\ldots
\end{aligned}$$

Todo esto significa que para resolver los problemas básicos sobre los ideales en $k[x]$ hay algoritmos sencillos basados en la división con resto.

3.5. Proposición. *Consideremos dos ideales*

$$I := (f_1, \ldots, f_s), \quad J := (g_1, \ldots, g_t) \subseteq k[x].$$

1) *Se tiene* $f \in I$ *si y solo si* $\mathrm{mcd}(f_1, \ldots, f_s) \mid f$.

2) *Se tiene* $I \subseteq J$ *si y solo* $\mathrm{mcd}(g_1, \ldots, g_t) \mid \mathrm{mcd}(f_1, \ldots, f_s)$.

3) *Se tiene* $I = J$ *si y solo si* $\mathrm{mcd}(f_1, \ldots, f_s) = \mathrm{mcd}(g_1, \ldots, g_t)$[*].

Nuestro objetivo es obtener criterios algorítmicos parecidos para los polinomios en diversas variables.

4 Polinomios en una variable en Macaulay2

El algoritmo de división con resto está implementado en Macaulay2 como `quotientRemainder(f,g)`.

[*] Recordemos que el máximo común divisor está definido salvo un múltiplo invertible, así que la igualdad $\mathrm{mcd}(f_1, \ldots, f_s) = \mathrm{mcd}(g_1, \ldots, g_t)$ se entiende salvo un múltiplo invertible.

```
i1 : R = QQ[x];

i2 : quotientRemainder (x^6, x^2-x+1)

       4    3
o2 = (x  + x  - x - 1, 1)

o2 : Sequence
```

El operador `/` corresponde a la división *exacta*: para dos polinomios $f, g \in k[x_1, \ldots, x_n]$ la expresión f/g es un elemento del cuerpo cociente $\operatorname{Frac} k[x_1, \ldots, x_n]$, incluso en el caso cuando f es divisible por g sin resto. Para la división con resto, hay que usar los operadores `//` (cociente) y `%` (resto).

```
i3 : x^6/(x^2-x+1)

          6
         x
o3 = ----------
      2
     x  - x + 1

o3 : frac R

i4 : x^6//(x^2-x+1)

      4    3
o4 = x  + x  - x - 1

o4 : R

i5 : x^6%(x^2-x+1)

o5 = 1

o5 : R
```

Para aprender a definir nuevas funciones en Macaulay2, podemos implementar el algoritmo de división con resto por nuestra cuenta. Para definir una función, se usa la sintaxis "`f = (x) -> ...`" Veamos un par de ejemplos:

```
i1 : f = (x) -> x^2

o1 = f

o1 : FunctionClosure

i2 : f(23)

o2 = 529

i3 : R = QQ[x];
```

```
i4 : f(x+1)

      2
o4 = x  + 2x + 1

o4 : R

i5 : fib = (n) -> if n==1 or n==2 then 1 else fib(n-1) + fib(n-2)

o5 = fib

o6 : FunctionClosure

i7 : for n from 1 to 10 list fib(n)

o7 = {1, 1, 2, 3, 5, 8, 13, 21, 34, 55}

o7 : List
```

Aquí la expresión

```
for n from 1 to 10 list fib(n)
```

forma una lista de los elementos `fib(`n`)` para $n = 1, \ldots, n$. Es bastante útil en los cálculos. Otra función relacionada es `apply`: por ejemplo,

```
apply (toList (1..10), fib)
```

aplica `fib` a todos los elementos de la lista `{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}` y devuelve el mismo resultado.

Implementemos entonces la división con resto. He aquí algunas funciones útiles para un polinomio $f \in k[x]$:

- el término mayor es `leadTerm(`f`)`,
- el coeficiente mayor es `leadCoefficient(`f`)`,
- el grado respecto a la variable x es `degree(`x`,`f`)`.

El algoritmo de 3.1 se traduce palabra por palabra en el siguiente código:

```
divRem = (f,g) -> (
  q := 0;
  r := f;

  while r != 0 and leadTerm(r)%leadTerm(g) == 0 do (
    q = q + leadTerm(r)//leadTerm(g);
    r = r - leadTerm(r)//leadTerm(g)*g
  );
  (q,r)
);
```

Notamos que la salida de una función es el valor de la última expresión y no hace falta escribir `return (q,r)`.

Este código es un poco tonto porque los operadores `%` y `//` ya corresponden a la división con resto. Si queremos, podemos ajustarlo de la siguiente manera:

```
divRem2 = (f,g) -> (
  q := 0;
  r := f;

  while r != 0 and degree(x,g) <= degree(x,r) do (
    h := x^(degree(x,r)-degree(x,g))*leadCoefficient(r)/leadCoefficient(g);
    q = q + h;
    r = r - h*g
  );
  (q,r)
);
```

Note el uso de dos operadores = y `:=`. El operador `:=` define una variable **local** (que no será visible afuera de la función).

En Macaulay2 el máximo común divisor y mínimo común múltiplo se calculan mediante `gcd(`$f_1,\dots,f_r$`)` y `lcm(`$f_1,\dots,f_r$`)`.

```
i1 : R = QQ[x];

i2 : f = x^5 - 1;

i3 : g = x^3 - 1;

i4 : gcd(f,g)

o4 = x - 1

o4 : R

i5 : lcm(f,g)

      7    6    5    2
o5 = x  + x  + x  - x  - x - 1

o5 : R
```

Como vimos arriba, los ideales en el anillo $k[x]$ son particularmente sencillos, pero sería oportuno mencionar algunas funciones de Macaulay2 relacionadas con ideales, que serán mucho más interesantes en $k[x_1,\dots,x_n]$:

- `ideal(`$f_1,\dots,f_s$`)` — el ideal generado por $f_1,\dots,f_s$;
- `intersect(`I`,`J`)` — la intersección de ideales;
- I`+`J — la suma de ideales;
- I`*`J — el producto de ideales;

- I==J — la igualdad de ideales.

```
i1 : R = QQ[x]

o1 = R

o1 : PolynomialRing

i2 : f = x^6-1;

i3 : g = x^15-1;

i4 : I = ideal(f);

i5 : J = ideal(g);

i6 : intersect(I,J)

             18    15    3
o6 = ideal(x   + x   - x  - 1)

o6 : Ideal of R

i7 : I*J

             21    15    6
o7 = ideal(x   - x   - x  + 1)

o7 : Ideal of R

i8 : I+J

              6       15
o8 = ideal (x  - 1, x   - 1)

o8 : Ideal of R

i9 : ideal(f,g)

              6       15
o9 = ideal (x  - 1, x   - 1)

o9 : Ideal of R

i10 : oo == ideal(x^3-1)

o10 = true
```

5 Órdenes monomiales

Ahora consideremos el anillo de polinomios en n variables $k[x_1,\dots,x_n]$. Vamos a usar la notación para los monomios

$$x^\alpha := x_1^{\alpha_1}\cdots x_n^{\alpha_n}, \quad \text{donde } \alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n.$$

Notamos que hay una biyección entre los monomios y las n-tuplas $\alpha \in \mathbb{N}^n$ y la multiplicación de monomios corresponde a la suma de tuplas:

$$x^\alpha \cdot x^\beta = x^{\alpha+\beta}.$$

5.1. Definición. Un **orden monomial** sobre $k[x_1,\dots,x_n]$ es una relación de orden total[*] $\prec$ sobre los monomios x^α, $\alpha\in\mathbb{N}^n$ que cumple las siguientes propiedades.

1) $\prec$ es compatible con los productos: para cualesquiera $x^\alpha, x^\beta, x^\gamma$ se cumple

$$x^\alpha \prec x^\beta \Longrightarrow x^\alpha\, x^\gamma \prec x^\beta\, x^\gamma.$$

2) $\prec$ es un **buen orden**: en todo conjunto de monomios $\mathscr{S}\neq\emptyset$ existe el elemento mínimo respecto a $\prec$; es decir, $x^\alpha\in\mathscr{S}$ tal que $x^\alpha\preceq x^\beta$ para todo $x^\beta\in\mathscr{S}$.

5.2. Observación. *La condición 2) de la definición es equivalente a la siguiente propiedad: toda sucesión decreciente*

$$x^{\alpha(1)}\succ x^{\alpha(2)}\succ x^{\alpha(3)}\succ\cdots$$

se estabiliza.

Demostración. Vamos a probar la contrapositiva: existe un conjunto $\mathscr{S}\neq\emptyset$ sin elemento mínimo si y solo si existe una sucesión infinita decreciente.

En efecto, si tal $\mathscr{S}$ existe, podemos escoger $x^{\alpha(1)}\in\mathscr{S}$. Luego, ya que en $\mathscr{S}$ no hay elemento mínimo, habrá $x^{\alpha(2)}\in\mathscr{S}$ tal que $x^{\alpha(2)}\prec x^{\alpha(1)}$, etcétera. De esta manera se obtiene una sucesión infinita

$$x^{\alpha(1)}\succ x^{\alpha(2)}\succ x^{\alpha(3)}\succ\cdots$$

Viceversa, si existe tal sucesión infinita, sus términos forman un conjunto sin elemento mínimo. ■

Ejercicio 1. Demuestre que sobre los polinomios en una variable $k[x]$ hay un solo orden monomial que viene dado por

$$1\prec x\prec x^2\prec x^3\prec\cdots$$

Es decir,

$$x^m\prec x^n \iff m<n.$$

Sin embargo, sobre los polinomios en diversas variables, hay muchos diferentes órdenes monomiales. Ahora vamos a introducir algunos de ellos.

5.3. Definición. El **grado total** de un monomio se define mediante

$$\deg(x_1^{\alpha_1}\cdots x_n^{\alpha_n}) := \alpha_1+\cdots+\alpha_n.$$

5.4. Definición. Consideremos el anillo de polinomios $k[x_1,\dots,x_n]$.

1) El **orden lexicográfico** (o **lex**) se define mediante

$$x^\beta \prec_{lex} x^\alpha \iff \text{la primera entrada no nula de } \alpha-\beta\in\mathbb{N}^n \text{ es positiva.}$$

2) El **orden lexicográfico graduado** (o **grlex**) se define mediante

$$x^\beta \prec_{grlex} x^\alpha \iff \begin{cases} \deg(x^\beta)<\deg(x^\alpha), \\ \text{o bien} \\ \deg(x^\beta)=\deg(x^\alpha) \text{ y } x^\beta\prec_{lex} x^\alpha. \end{cases}$$

[*] La palabra "total" significa que para cualesquiera x^α, x^β se cumple una de las siguientes relaciones:

$$x^\alpha\prec x^\beta,\quad x^\alpha=x^\beta,\quad x^\alpha\succ x^\beta.$$

3) El **orden lexicográfico inverso graduado** (o **grevlex**) se define mediante

$$x^\beta \prec_{grevlex} x^\alpha \iff \begin{cases} \deg(x^\beta) < \deg(x^\alpha), \\ \text{o bien} \\ \deg(x^\beta) = \deg(x^\alpha) \text{ y la } \underline{\text{última}} \text{ entrada no nula de } \alpha - \beta \in \mathbb{N}^n \text{ es negativa.} \end{cases}$$

Aquí se asume que las variables están ordenadas como

$$x_1 \succ x_2 \succ \cdots \succ x_n.$$

En práctica, cuando el número de variables es 2 o 3, en lugar de $k[x_1, x_2]$ y $k[x_1, x_2, x_3]$ vamos a usar los anillos $k[x, y]$ y $k[x, y, z]$ respectivamente. En este caso se asume el orden sobre las variables

$$x \succ y \succ z.$$

5.5. Ejemplo. Consideremos el polinomio

$$f = 1 + x^3 + y^3 + xyz + x^2yz + xy^3 \in k[x, y, z].$$

Escribamos sus monómios en el orden decreciente respecto a $\prec_{lex}, \prec_{grlex}, \prec_{grevlex}$.

$$\begin{array}{ll} \prec_{lex}: & x^3 + x^2yz + xy^3 + xyz + y^3 + 1 \\ \prec_{grlex}: & x^2yz + xy^3 + x^3 + xyz + y^3 + 1 \\ \prec_{grevlex}: & xy^3 + x^2yz + x^3 + y^3 + xyz + 1 \end{array}$$

▲

Ejercicio 2. Demuestre que $\prec_{lex}, \prec_{grlex}, \prec_{grevlex}$ son órdenes monomiales.

Ejercicio 3. Consideremos la siguiente propiedad: para cualesquiera α, β existe un número finito de monomios x^γ tales que

$$x^\alpha \prec x^\gamma \prec x^\beta.$$

¿Para cuáles órdenes monomiales entre $\prec_{lex}$, $\prec_{grlex}$ y $\prec_{grevlex}$ esto es cierto?

5.6. Definición. Fijemos un orden monomial $\prec$ sobre $k[x_1, \ldots, x_n]$. Sea $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ un polinomio no nulo.

El **monomio mayor** de f es el monomio mayor respecto a $\prec$ con coeficiente no nulo:

$$LM(f) := \max\{x^\alpha \mid c_\alpha \neq 0\};$$

si el monomio mayor es x^α, entonces el **coeficiente mayor** y el **término mayor** correspondientes son

$$LC(f) := c_\alpha, \quad LT(f) := c_\alpha x^\alpha$$

(del inglés "leading monomial", "leading coefficient" y "leading term" respectivamente).

Ejercicio 4. Fijemos algún orden monomial sobre $k[x_1, \ldots, x_n]$. Sean $f, g \in k[x_1, \ldots, x_n]$ polinomios no nulos. Demuestre las siguientes propiedades.

1) Tenemos
$$LT(fg) = LT(f) \cdot LT(g).$$

2) Si $f + g \neq 0$, entonces
$$LM(f + g) \preceq \max_{\prec}(LM(f), LM(g)).$$

Además, si $LT(f) \neq LT(g)$, entonces

$$LM(f + g) = \max_{\prec}(LM(f), LM(g)).$$

6 Órdenes monomiales en Macaulay2

Por defecto, Macaulay2 usa el orden grevlex que no es tan intuitivo, pero muy útil en los cálculos.

```
i1 : R = QQ [x,y,z];

i2 : 1 + x^3 + y^3 + x*y*z + x^2*y*z + x*y^3

        3    2       3    3
o2 = x*y  + x y*z + x  + y  + x*y*z + 1

o2 : R

i3 : x^2*y*z < x*y^3

o3 = true
```

Para usar otro orden monomial, podemos hacer lo siguiente:

```
i4 : R = QQ [x,y,z, MonomialOrder=>Lex];

i5 : 1 + x^3 + y^3 + x*y*z + x^2*y*z + x*y^3

      3    2         3            3
o5 = x  + x y*z + x*y  + x*y*z + y  + 1

o5 : R

i6 : R = QQ [x,y,z, MonomialOrder=>GLex];

i7 : 1 + x^3 + y^3 + x*y*z + x^2*y*z + x*y^3

      2         3    3            3
o7 = x y*z + x*y  + x  + x*y*z + y  + 1

o7 : R
```

El parámetro `MonomialOrder` puede tomar valores `Lex`, `GLex`, `GRevLex` y varios otros más. El monomio, coeficiente y término mayor en Macaulay2 se calculan mediante

$$\texttt{leadMonomial}(f),\ \texttt{leadCoefficient}(f),\ \texttt{leadTerm}(f).$$

He aquí un ejemplo:

```
i1 : R = QQ[x,y,z, MonomialOrder=>Lex];

i2 : f = 1 + 2*x^3 + 3*y^3 + 4*x*y*z + 5*x^2*y*z + 6*x*y^3

       3     2          3              3
o2 = 2x  + 5x y*z + 6x*y  + 4x*y*z + 3y  + 1
```

```
o2 : R

i3 : leadMonomial(f)

      3
o3 = x

o3 : R

i4 : leadCoefficient(f)

o4 = 2

o4 : QQ

i5 : leadTerm(f)

       3
o5 = 2x

o5 : R
```

7 División con resto para polinomios en diversas variables

7.1. Teorema. *Fijemos un orden monomial sobre $k[x_1,\dots,x_n]$. Sea $(f_1,\dots,f_s)$ una tupla de polinomios. Entonces, todo polinomio $f \in k[x_1,\dots,x_n]$ puede ser escrito como*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

donde $q_1,\dots,q_s, r \in k[x_1,\dots,x_n]$ y se cumplen las siguientes condiciones:

1) *$r = 0$ o r es una combinación k-lineal de monomios no divisibles por $LT(f_1),\dots,LT(f_s)$;*

2) *si $q_i f_i \neq 0$, entonces*
$$LM(q_i f_i) \preceq LM(f).$$

El polinomio r se llama **un resto** de división de f por $(f_1,\dots,f_s)$. En general, las condiciones de arriba no definen a r de modo único.

Demostración. Vamos a describir un algoritmo que calcula $q_1,\dots,q_s$ y r.

Entrada: $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$

$q_1 := 0; \ldots; q_s := 0; r := 0$
$p := f$

mientras $p \neq 0$ **hacer**
  $i := 1$
  $ocurrióDivisión := false$
  mientras $i \leq s$ **y** $ocurrióDivisión = false$ **hacer**
    si $LT(f_i) \mid LT(p)$ **entonces**
      $q_i := q_i + LT(p)/LT(f_i)$
      $p := p - (LT(p)/LT(f_i))\, f_i$
      $ocurrióDivisión = true$
    sino
      $i = i + 1$

  si $ocurrióDivisión = false$ **entonces**
    $r = r + LT(p)$
    $p = p - LT(p)$

devolver $(q_1, \ldots, q_s), r$

Notamos primero que a cada paso del algoritmo se cumple la identidad

$$f = q_1 f_1 + \cdots + q_s f_s + r + p. \tag{7.1}$$

En efecto, esto es obvio al inicio cuando $q_1 = \cdots = q_s = r = 0$ y $p = f$, y luego a cada paso del ciclo más grande se hace precisamente una de las siguientes dos operaciones.

a) Si $LT(f_i) \mid LT(p)$ para algún i, entonces q_i y p se remplazan por

$$q_i' := q_i + LT(p)/LT(f_i), \quad p' := p - (LT(p)/LT(f_i))\, f_i$$

respectivamente. En este caso

$$q_i' f_i + p' = \Big(q_i + LT(p)/LT(f_i)\Big) f_i + \Big(p - (LT(p)/LT(f_i))\, f_i\Big) = q_i f_i + p,$$

así que la identidad (7.1) se preserva.

Notamos que

$$LT\left(\frac{LT(p)}{LT(f_i)}\, f_i\right) = \frac{LT(p)}{LT(f_i)}\, LT(f_i) = LT(p),$$

así que al remplazar p por p' se tiene o bien $p' = 0$, o $LM(p') \prec LM(p)$.

b) Si $LT(f_i) \nmid LT(p)$ para ningún i, entonces r y p se remplazan por

$$r' := r + LT(p), \quad p' := p - LT(p),$$

y de nuevo, $r' + p' = r + p$, y la identidad (7.1) se preserva. Notamos que de nuevo, $p' = 0$ o $LM(p') \prec LM(p)$.

Entonces, después de cada ejecución del ciclo principal, p se vuelve nulo, o su monomio mayor se vuelve más pequeño. Esto significa que el ciclo principal se termina en algún momento, cuando tendremos $p = 0$ y

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

Notamos que en el algoritmo el término $LT(p)$ se suma a r precisamente cuando $LT(f_i) \nmid LT(p)$ para ningún i, así que r cumple la condición 1). Además, durante la ejecución del algoritmo, si $p \neq 0$, entonces se cumple $LM(p) \preceq LM(f)$—al principio $p = f$, y luego el monomio mayor de p decrece. Los términos que se suman a q_i son de la forma $LT(p)/LT(f_i)$, así que

$$LM(q_i f_i) \preceq LM(f).$$

Entonces, la condición 2) también se cumple. ■

Sería un poco tedioso ejecutar cada vez este algoritmo a mano, así que lo implementé en Macaulay2; véase el apéndice B.

7.2. Ejemplo. En el anillo $k[x, y]$ con el orden monomial lexicográfico dividamos

$$f = xy^2 + 1 \text{ por } (f_1, f_2) = (xy + 1, y + 1).$$

```
i1 : load "Division.m2"

i2 : R = QQ[x,y, MonomialOrder=>Lex];

i3 : divRemMultivar (x*y^2 + 1, (x*y+1, y+1))

o3 = ((y, -1), 2)

o3 : Sequence
```

Tenemos entonces

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

Notamos que el resultado del algoritmo depende del orden de los polinomios $f_1, \ldots, f_s$. Por ejemplo, al dividir el mismo polinomio f por (f_2, f_1) se obtiene

$$xy^2 + 1 = (xy - x) \cdot (xy + 1) + 0 \cdot (y + 1) + (x + 1).$$

```
i4 : divRemMultivar (x*y^2 + 1, (y+1, x*y+1))

o4 = ((x*y - x, 0), x + 1)

o4 : Sequence
```

▲

Notamos que si nuestro algoritmo de división devuelve $r = 0$, entonces

$$f = q_1 f_1 + \cdots + q_s f_s \in (f_1, \ldots, f_s).$$

Lamentablemente, lo contrario no está garantizado: si el resto no es nulo, esto *no significa* que $f \notin (f_1, \ldots, f_s)$.

7.3. Ejemplo. De nuevo, consideremos el orden lexicográfico sobre $k[x, y]$ y dividamos

$$f = xy^2 - x \text{ por } (f_1, f_2) = (xy - 1,\ y^2 - 1).$$

El resultado será

$$xy^2 - x = y \cdot (xy - 1) + 0 \cdot (y^2 - 1) + (-x + y).$$

Sin embargo,

$$xy^2 - x \in (xy - 1,\ y^2 - 1).$$

De hecho, la división por (f_2, f_1) nos da

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy - 1) + 0. \qquad \blacktriangle$$

Ejercicio 5. Implemente en Macaulay2 la función `mcd(`f`,`g`)` que calcula el máximo común divisor de $f, g \in k[x]$ usando el algoritmo de Euclides. (Para el resto de división, use el operador `%`.)

División con resto en Macaulay2

Para dividir f con resto por $(f_1, \ldots, f_s)$ en Macaulay2, se pueden usar los operadores habituales `//` (cociente), `%` (resto), y la función `quotientRemainder` (cociente y resto). Sin embargo, lo que calcula Macaulay2 *no es lo mismo que calcula nuestro algoritmo de arriba*. He aquí un ejemplo particular: consideremos el orden lexicográfico graduado sobre $k[x, y]$ y dividamos $f = x^2$ por $f_1 = x^3 - xy$, $f_2 = x^2y - y^2 + x$.

```
i : R = QQ[x,y, MonomialOrder=>GLex];

i : quotientRemainder (matrix {{x^2}}, matrix {{x^3-x*y, x^2*y - y^2 + x}})

o = ({3} | -y |, 0)
     {3} | x  |

o : Sequence
```

Aquí el primer argumento es la matriz (x^2) de 1×1 y el segundo argumento es la matriz fila

$$(x^3 - xy,\ x^2y - y^2 + x)$$

de 1×2. El resultado es

$$(\begin{pmatrix} -y \\ x \end{pmatrix}, 0),$$

lo que significa que

$$x^2 = -y \cdot (x^3 - xy) + x \cdot (x^2y - y^2 + x) + 0.$$

Esto sucede porque cuando f pertenece al ideal $(f_1, \ldots, f_s)$, Macaulay2 siempre da su expresión en términos de estos generadores y el resto nulo. El algoritmo de 7.1 no puede dar la respuesta de arriba porque esta expresión no cumple la condición 2).

Entonces, lo que hace Macaulay2 parece más útil de lo que calcula nuestro algoritmo: allí $r = 0$ sí significa que $f \in (f_1, \ldots, f_s)$. Sin embargo, nuestro algoritmo nos servirá más adelante.

8 Ideales monomiales

Uno de los objetivos de nuestro curso es entender cómo hacer cálculos con los ideales en el anillo de polinomios $k[x_1,\dots,x_n]$. Una clase importante de ideales son los ideales monomiales, y las operaciones con estos son particularmente sencillas.

8.1. Definición. Se dice que un ideal $I \subseteq k[x_1,\dots,x_n]$ es **monomial** si I puede ser generado por monomios:

$$I = (x^\alpha \mid \alpha \in A)$$

para algún subconjunto $A \subseteq \mathbb{N}^n$ (no necesariamente finito)

8.2. Ejemplo. Tenemos los siguientes ideales monomiales en el anillo $k[x,y,z]$:

$$I = (x^2, xy, xz^3), \quad J = (y^2, y^2 - x^3).$$

En efecto, I desde el principio está generado por monomios, mientras que $J = (x^3, y^2)$. Notamos que los elementos de un ideal monomial no son solamente monomios: por ejemplo, $x^2 + xy \in I$ no lo es. ▲

8.3. Lema. *Sea $I = (x^\alpha \mid \alpha \in A)$ un ideal monomial. Entonces, un monomio x^β pertenece a I si y solo si $x^\alpha \mid x^\beta$ para algún $\alpha \in A$.*

Demostración. Está claro que si $x^\alpha \mid x^\beta$, entonces $x^\beta \in I$. Viceversa, si $x^\beta \in I$, entonces

$$x^\beta = f_1\, x^{\alpha(1)} + \cdots + f_s\, x^{\alpha(s)}$$

para algunos polinomios $f_1,\dots,f_s$ y $\alpha(1),\dots,\alpha(s) \in A$. Al despejar esta expresión, nos queda necesariamente

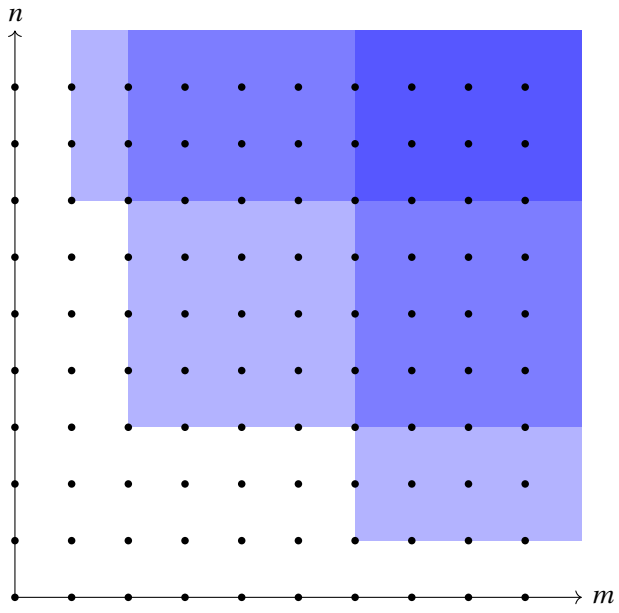
$$x^\beta = x^\gamma\, x^{\alpha(i)}$$

para algún i. ■

Notamos que los múltiplos de x^α son los monomios de la forma $x^{\alpha+\beta}$ para $\beta \in \mathbb{N}^n$. Por ejemplo, para el ideal monomial

$$I = (x^6 y, x^2 y^3, x y^7) \subset k[x,y]$$

los monomios $x^m y^n$ que pertenecen a I pueden ser visualizados mediante el siguiente "diagrama escalonado":



Un polinomio pertenece a un ideal monomial I si y solo si es una combinación lineal de monomios de I. A saber, tenemos el siguiente resultado.

8.4. Proposición. *Un ideal $I \subseteq k[x_1,\dots,x_n]$ es monomial si y solo si se cumple la siguiente propiedad: para cualquier polinomio $f = \sum_\alpha c_\alpha x^\alpha \in I$ se tiene*

$$c_\alpha \neq 0 \Longrightarrow x^\alpha \in I.$$

Demostración. Si I está generado por algunos monomios x^α con $\alpha \in A$, entonces un elemento de f es de la forma

$$f = f_1\, x^{\alpha(1)} + \cdots + f_s\, x^{\alpha(s)}, \quad \text{donde } f_i \in k[x_1,\dots,x_n],\ \alpha(i) \in A.$$

Al despejar esta expresión, tendremos una combinación lineal de monomios de la forma $x^\beta\, x^{\alpha(i)}$, y cada uno de estos monomios pertenece a I.

Viceversa, asumamos que se cumple la propiedad. Entonces, podemos tomar como los generadores de I todos los monomios que aparecen en los polinomios $f \in I$. ■

Para los ideales monomiales I, J es fácil comprobar si $I = J$, o si $f \in I$ para un polinomio f.

8.5. Corolario. *Para $A, B \subseteq \mathbb{N}^n$ consideremos los ideales monomiales*

$$I := (x^\alpha \mid \alpha \in A), \quad J := (x^\beta \mid \beta \in B) \subseteq k[x_1,\dots,x_n].$$

1) *Se tiene $f \in I$ si y solo si f es una combinación k-lineal $\sum_\gamma c_\gamma x^\gamma$ donde cada monomio x^γ es divisible por algún x^α con $\alpha \in A$.*

2) *Se tiene $I = J$ si y solo si en I e J aparecen los mismos monomios.*

3) *Se tiene $I \subseteq J$ si y solo si para cada $\alpha \in A$ existe $\beta \in B$ tal que $x^\beta \mid x^\alpha$.*

Ejercicio 6. Demuestre que para ideales monomiales $I, J \in k[x_1,\dots,x_n]$ los ideales $I + J, IJ, I \cap J$ son también monomiales. Específicamente, si

$$I = (x^\alpha \mid \alpha \in A), \quad J = (x^\beta \mid \beta \in B),$$

entonces

$$\begin{aligned} I + J &= \{x^\gamma \mid \gamma \in A \cup B\}, \\ IJ &= \{x^{\alpha+\beta} \mid \alpha \in A, \beta \in B\}, \\ I \cap J &= \{\operatorname{mcm}(x^\alpha, x^\beta) \mid \alpha \in A, \beta \in B\}. \end{aligned}$$

9 El lema de Dickson

9.1. Teorema (Lema de Dickson). *Sea $I = (x^\alpha \mid \alpha \in A)$ un ideal monomial. Entonces, I puede ser generado por un número finito de monomios de A:*

$$I = (x^{\alpha(1)},\dots,x^{\alpha(s)}) \quad \textit{para algunos } \alpha(1),\dots,\alpha(s) \in A.$$

Demostración. Primero notamos que sería suficiente encontrar un número finito de monomios $x^{\beta(1)},\dots,x^{\beta(s)}$, no necesariamente del conjunto A, que generan a I. En efecto, en este caso cada $x^{\beta(i)} \in I$ es divisible por algún $x^{\alpha(i)}$ para $\alpha(i) \in A$. Luego,

$$I = (x^{\beta(1)},\dots,x^{\beta(s)}) \subseteq (x^{\alpha(1)},\dots,x^{\alpha(s)}) \subseteq I,$$

así que $I = (x^{\alpha(1)},\dots,x^{\alpha(s)})$.

Procedamos por inducción sobre el número de variables n. Si $n = 1$, entonces tenemos un conjunto $A \subseteq \mathbb{N}$ tal que $I = (x^a \mid a \in A)$. Ahora para $b := \min\{a \in A\}$ se tiene $I = (x^b)$.

Para el paso inductivo, asumamos que el resultado es válido para $n-1$ variables. Consideremos un ideal monomial $I \subseteq k[x_1, \ldots, x_{n-1}, y]$. Para $d = 0, 1, 2, 3, \ldots$, consideremos los ideales monomiales

$$I_d := (x^\beta \mid x^\beta y^d \in I) \subset k[x_1, \ldots, x_{n-1}].$$

Estos forman una cadena

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subset k[x_1, \ldots, x_{n-1}],$$

y su unión

$$I_\infty := \bigcup_{d \geq 0} I_d$$

es también un ideal monomial. Por la hipótesis inductiva, el ideal I_∞ está generado por algunos monomios

$$x^{\alpha(1)}, \ldots, x^{\alpha(s)}$$

tales que para cada $i = 1, \ldots, s$ existe d_i que cumple $x^{\alpha(i)} y^{d_i} \in I$. Pongamos ahora $d' := \max\{d_1, \ldots, d_s\}$. Tenemos entonces

$$I_{d'} = I_{d'+1} = I_{d'+2} = \cdots = I_\infty.$$

De nuevo, por la hipótesis inductiva, cada uno de los ideales I_d está generado por algún conjunto finito de monomios G_d. Podemos asumir que

$$G_{d'} = G_{d'+1} = G_{d'+2} = \cdots = G_\infty.$$

Consideremos el conjunto finito de monomios

$$G := \bigcup_{0 \leq d \leq d'} \{x^\alpha y^d \mid x^\alpha \in G_d\}.$$

Este genera a I. En efecto, para todo monomio $x^\alpha y^d \in I$ tenemos $x^\alpha \in I_d$, así que existe $x^\beta \in G_d$ tal que $x^\beta \mid x^\alpha$, y luego $x^\beta y^d \mid x^\alpha y^d$.

- Si $d \leq d'$, entonces $x^\beta y^d \in G$.
- Si $d > d'$, entonces $x^\beta \in G_d$ y $x^\beta y^{d'} \mid x^\beta y^d$.

En ambos casos podemos concluir que $x^\alpha y^d \in \langle G \rangle$. ■

Ejercicio 7. Demuestre que el lema de Dickson es equivalente al siguiente resultado: para todo subconjunto $A \subseteq \mathbb{N}^n$ existe un número finito de elementos $\alpha(1), \ldots, \alpha(s) \in A$ tales que para todo $\alpha \in A$ se tiene $\alpha = \alpha(i) + \beta$ para algún $i = 1, \ldots, s$ y $\beta \in \mathbb{N}^n$.

Ejercicio 8. Para un ideal monomial I digamos que un conjunto de generadores $\{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\}$ es **minimal** si $x^{\alpha(i)} \nmid x^{\alpha(j)}$ para $i \neq j$. Demuestre que todo ideal monomial posee un conjunto de generadores minimal y este es único.

Ejercicio 9. Consideremos los ideales monomiales

$$I_j := (x_1, \ldots, \widehat{x_j}, \ldots, x_n) \subset k[x_1, \ldots, x_n], \quad j = 1, \ldots, n,$$

donde $\widehat{x_j}$ significa que x_j se omite de la lista. Encuentre el conjunto de generadores minimal para el ideal

$$I_1 \cap \cdots \cap I_n.$$

Por ejemplo, para $n = 2$ tenemos $(x_2) \cap (x_1) = (x_1 x_2)$; para $n = 3$ tenemos

$$(x_2, x_3) \cap (x_1, x_3) \cap (x_1, x_2) = (x_1 x_2, x_1 x_3, x_2 x_3)$$

(¡demuéstrelo!), etcétera.

El lema de Dickson nos da la siguiente caracterización útil de órdenes monomiales.

9.2. Corolario. *Sea $\prec$ una relación de orden total sobre los monomios de $k[x_1,\dots,x_n]$. Entonces, $\prec$ es un orden monomial si y solo si se cumplen las siguientes condiciones:*

1) $\prec$ es compatible con los productos: para cualesquiera $x^\alpha, x^\beta, x^\gamma$ se cumple

$$x^\alpha \prec x^\beta \Longrightarrow x^\alpha x^\gamma \prec x^\beta x^\gamma.$$

2^*) $x^\alpha \succeq 1$ para todo $\alpha \in \mathbb{N}^n$.

Demostración. En la definición de orden monomial en lugar de 2^*) está la condición de que $\prec$ es un buen orden. Primero, está claro que la propiedad de ser un buen orden implica 2^*): si $x^\alpha \prec 1$ para algún α, entonces por la propiedad 1) tenemos una sucesión infinita

$$x^\alpha \succ x^{2\alpha} \succ x^{3\alpha} \succ \cdots$$

lo que contradice la definición de buen orden.

Viceversa, asumamos que se cumple 2^*). Probemos que $\prec$ es un buen orden. Para cualquier subconjunto $A \subseteq \mathbb{N}^n$ hay que deducir que

$$S := \{x^\alpha \mid \alpha \in A\}$$

tiene un elemento mínimo. Para esto consideremos el ideal monomial

$$I := (S).$$

Por el lema de Dickson, existen

$$\alpha(1),\dots,\alpha(s) \in A$$

tales que

$$I = (x^{\alpha(1)},\dots,x^{\alpha(s)}).$$

Ahora cualquier monomio x^α con $\alpha \in A$ pertenece a $(x^{\alpha(1)},\dots,x^{\alpha(s)})$, así que es divisible por algún $x^{\alpha(i)}$ para $i = 1,\dots,s$; es decir,

$$x^\alpha = x^{\alpha(i)} x^\beta$$

para algún $\beta \in \mathbb{N}^n$. Pero $x^\beta \succeq 1$ por la propiedad 2^*), lo que implica que

$$x^{\alpha(i)} x^\beta \succeq x^{\alpha(i)}.$$

Entonces, el elemento mínimo de S es

$$\text{mín}\{x^{\alpha(1)},\dots,x^{\alpha(s)}\}.$$

■

En práctica es más fácil verificar la condición 2^*) que la condición de buen orden.

Ejercicio 10. Fijemos un vector $u = (u_1,\dots,u_n) \in \mathbb{R}^n$ tal que los números u_i son positivos y linealmente independientes sobre $\mathbb{Q}$. Demuestre que

$$x^\alpha \prec_u x^\beta \iff u\cdot\alpha < u\cdot\beta,$$

donde $\cdot$ denota el producto escalar habitual, define un orden monomial. ¿Qué sucede si los u_i no son linealmente independientes?

10 Ideales monomiales en Macaulay2

Los ideales monomiales están implementados en Macaulay2 como el tipo `MonomialIdeal`. Los algoritmos para ideales monomiales son mucho más fáciles que para los ideales en general. Un ideal monomial se construye mediante

`monomialIdeal (`$x^{\alpha(1)}$`, ..., `$x^{\alpha(s)}$`)`

Para los ideales monomiales Macaulay2 automáticamente calcula el conjunto de generadores minimal.

```
i1 : R = QQ[x,y,z];

i2 : ideal (x*y,x,y,x^2)

                          2
o2 = ideal (x*y, x, y, x )

o2 : Ideal of R

i3 : monomialIdeal (x*y,x,y,x^2)

o3 = monomialIdeal (x, y)

o3 : MonomialIdeal of R
```

Calculemos por ejemplo la intersección de ideales

$$(y,z) \cap (x,z) \cap (x,y)$$

en $\mathbb{Q}[x,y,z]$.

```
i4 : intersect (monomialIdeal (y,z), monomialIdeal (x,z), monomialIdeal (x,y))

o4 = monomialIdeal (x*y, x*z, y*z)

o4 : MonomialIdeal of R
```

Para ver si dos ideales coinciden o no, se pueden usar los operadores `==` y `!=`. Para ver si $I \subseteq J$, se puede usar `isSubset(`I`,`J`)`. En Macaulay2 no existe una función separada que verifica si $f \in I$; en su lugar se puede ejecutar el comando f`%`I `== 0`, pero su verdadero significado será explicado más adelante en el curso.

```
i1 : R = QQ[x,y];

i2 : I = monomialIdeal (x^6*y, x^2*y^3, x*y^7)

                      6    2 3     7
o2 = monomialIdeal (x y, x y , x*y )
o2 : MonomialIdeal of R

i3 : J = monomialIdeal (x^2*y, x*y^3)
```

```
                      2      3
o3 = monomialIdeal (x y, x*y )
o3 : MonomialIdeal of R

i4 : f = 2*x^3*y^3 - 3*x^6*y^2

         6 2     3 3
o4 = - 3x y  + 2x y
o4 : R

i5 : g = x^2*y + x^2*y^7

      2 7    2
o5 = x y  + x y
o5 : R

i6 : f%I == 0
o6 = true

i7 : g%I == 0
o7 = false

i8 : g%J == 0
o8 = true

i9 : isSubset(I,J)
o9 = true
```

Atención: no olvide los paréntesis.

```
i1 : R = QQ[x,y];

i2 : x^2 - y % ideal (x^2-y)

      2
o2 = x  - y

o2 : R

i3 : (x^2 - y) % ideal (x^2-y)

o3 = 0

o3 : R
```

Aquí la expresión "`x^2 - y % ideal (x^2-y)`" no da cero; la expresión deseada es probablemente "`(x^2 - y) % ideal (x^2-y)`".

11 Bases de Gröbner

Escojamos algún orden monomial sobre $k[x_1,\ldots,x_n]$. A partir de ahora todas las definiciones resultados serán relativos a este orden monomial fijo.

11.1. Definición. Sea $I \subseteq k[x_1,\dots,x_n]$ un ideal. Pongamos

$$LT(I) := \{LT(f) \mid f \in I \setminus \{0\}\}.$$

Se dice que un subconjunto finito $G := \{g_1,\dots,g_s\} \subset I$ es una **base de Gröbner** para I (respecto al orden monomial fijo) si el ideal generado por los términos mayores de los polinomios en I coincide con el ideal generado por los términos mayores de $g_1,\dots,g_s$:

$$(LT(I)) = (LT(G)) := (LT(g_1),\dots,LT(g_s)). \tag{11.1}$$

11.2. Comentario. El apellido Gröbner se escribe con la diéresis, el signo diacrítico que consiste en dos puntos. Sin embargo, en los sistemas de álgebra computacional en los comandos relevantes se escribe "`groebner`" con "oe" en lugar de "ö".

Notamos que el ideal $(LT(I))$ es monomial:

$$(LT(f) \mid f \in I \setminus \{0\}) = (LM(f) \mid f \in I \setminus \{0\}).$$

Se ve que la condición (11.1) es equivalente a

$$\text{para todo } f \in I \setminus \{0\} \text{ se tiene } LT(g_i) \mid LT(f) \text{ para algún } i = 1,\dots,s.$$

11.3. Proposición. *Todo ideal no nulo $I \subseteq k[x_1,\dots,x_n]$ tiene una base de Gröbner.*

Demostración. Por el lema de Dickson, hay un número finito de polinomios $g_1,\dots,g_s \in I$ tales que

$$(LT(g_1),\dots,LT(g_s)) = (LM(g_1),\dots,LM(g_s)) = (LM(f) \mid f \in I \setminus \{0\}) = (LT(I)).$$ ■

11.4. Proposición. *Si $\{g_1,\dots,g_s\}$ es una base de Gröbner para I, entonces es una base: se tiene*

$$I = (g_1,\dots,g_s).$$

Demostración. Tenemos $(LT(I)) = (LT(g_1),\dots,LT(g_s))$. Para todo $f \in I$ la división con resto nos da $q_1,\dots,q_s, r \in k[x_1,\dots,x_n]$ tales que

$$f = q_1 g_1 + \cdots + q_s g_s + r,$$

donde los términos que aparecen en r no son divisibles por $LT(g_1),\dots,LT(g_s)$. Pero

$$r = f - (q_1 g_1 + \cdots + q_s g_s) \in I,$$

así que si $r \neq 0$, entonces

$$LT(r) \in (LT(I)) = (LT(g_1),\dots,LT(g_s)),$$

lo que implica $LT(g_i) \mid LT(r)$ para algún i (véase 8.3), pero no es el caso. Entonces, necesariamente $r = 0$ y por lo tanto $f \in (g_1,\dots,g_s)$. ■

Lo que acabamos de probar en particular implica el teorema de la base de Hilbert.

11.5. Corolario. *Todo ideal $I \subseteq k[x_1,\dots,x_n]$ es finitamente generado.*

Aunque hemos establecido la existencia de bases de Gröbner, nuestro argumento usa el lema de Dickson cuya prueba no fue muy constructiva, así que todavía no está claro ni cómo encontrar una base de Gröbner para un ideal I, ni cómo verificar si alguna base es una base de Gröbner.

11.6. Ejemplo. Consideremos el anillo $k[x,y]$ con el orden lexicográfico graduado. Para

$$f_1 := x^3 - xy, \quad f_2 := x^2y - y^2 + x,$$

consideremos el ideal

$$I := (f_1, f_2) \subset k[x,y].$$

Notamos que

$$\begin{aligned} g_1 &:= x^2 = -y\,f_1 + x\,f_2 \in I, \\ g_2 &:= xy = -(xy+1)\,f_1 + x^2\,f_2 \in I, \\ g_3 &:= y^2 - x = -y^2\,f_1 + (xy-1)\,f_2 \in I. \end{aligned}$$

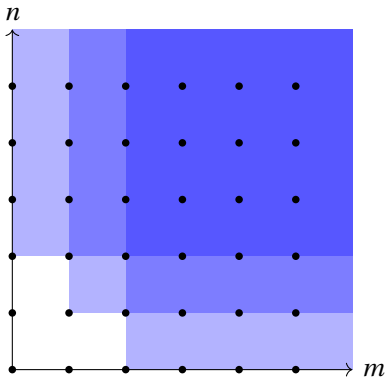
Entonces, los términos mayores de g_1, g_2, g_3 están en el ideal $(LT(I))$:

$$(LT(f_1), LT(f_2)) = (x^3, x^2y) \subsetneq (x^2, xy, y^2) = (LT(g_1), LT(g_2), LT(g_3)) \subsetneq (LT(I)).$$

Esto significa que $\{f_1, f_2\}$ no es una base de Gröbner: el ideal $(LT(f_1), LT(f_2))$ es estrictamente más pequeño que el ideal $(LT(I))$. Un buen candidato para una base de Gröbner es $\{g_1, g_2, g_3\}$. Para esto hay que probar que

$$(LT(I)) = (x^2, xy, y^2).$$

Esto no es tan inmediato como parece. El ideal (x^2, xy, y^2) contiene todos los monomios salvo $1, x, y$:



Entonces, hay que ver que $1, x, y \notin (LT(I))$. Primero, está claro que $1 \notin I$, dado que ni f_1 ni f_2 no tiene término constante. Dejo al lector el placer de verificar que

$$a\,x + b\,y + c \in I \text{ para } a,b,c \in k \iff a = b = c = 0.$$

Esto implica en particular que $x, y \notin (LT(I))$. ▲

11.7. Proposición. *Sea $\{g_1, \ldots, g_s\}$ una base de Gröbner para un ideal $I \subseteq k[x_1, \ldots, x_n]$. Entonces, para cualquier polinomio $f \in k[x_1, \ldots, x_n]$ existe único $r \in k[x_1, \ldots, x_n]$ con las siguientes propiedades:*

1) *los términos que aparecen en r no son divisibles por $LT(g_1), \ldots, LT(g_s)$;*
2) *$f = h + r$ para algún $h \in I$.*

Demostración. El algoritmo de división con resto nos da

$$f = q_1 g_1 + \cdots + q_s g_s + r, \tag{11.2}$$

donde r cumple la propiedad 1) y luego $h := q_1 g_1 + \cdots q_s g_s \in I = (g_1, \ldots, g_s)$ cumple la propiedad 2). Esto establece la existencia. Para la unicidad, supongamos que existen r, r' tales que

$$f = h + r = h' + r'.$$

Luego, $r - r' = h' - h \in I$. Si $r \neq r'$, entonces

$$LT(r - r') \in (LT(I)) = (LT(g_1), \ldots, LT(g_s)),$$

lo que implicaría $LT(g_i) \mid LT(r - r')$ para algún i. Pero en este caso algún término de r o r' tiene que ser divisible por $LT(g_i)$ y no es e caso. Podemos concluir que $r = r'$. ■

11.8. Comentario. En la expresión 11.2 el resto r es único, pero los polinomios $q_1, \ldots, q_s$ no son únicos.

Ejercicio 11. Sea $I \subseteq k[x_1, \ldots, x_n]$ un ideal. Demuestre que para cualquier polinomio $f \in k[x_1, \ldots, x_n]$ existe único $r \in k[x_1, \ldots, x_n]$ con las siguientes propiedades:

1) los términos que aparecen en r no son divisibles por ningún elemento de $LT(I)$;

2) $f = h + r$ para algún $h \in I$.

11.9. Corolario. *Sea $\{g_1, \ldots, g_s\}$ una base de Gröbner para un ideal $I \subseteq k[x_1, \ldots, x_n]$. Entonces, para cualquier polinomio $f \in k[x_1, \ldots, x_n]$ el resto de división de f por $g_1, \ldots, g_s$ está definido de modo único (con cualquier orden de $g_1, \ldots, g_s$). Tenemos $f \in I$ si y solo si este resto es nulo.*

Demostración. La unicidad del resto se sigue inmediatamente de la proposición anterior. Ahora si $f \in I$, podemos tomar $f = g + r$, donde $g = f$ y $r = 0$, así que cualquier resto de división de f por $g_1, \ldots, g_s$ tiene que ser nulo. ■

Notamos que cuando $f \in I$, el algoritmo de división con resto de f por $g_1, \ldots, g_s$ nos dará una expresión particular $f = q_1 g_1 + \cdots + q_s g_s$.

11.10. Ejemplo. Volvamos al ejemplo 11.6. El algoritmo de división con resto de xy por $f_1 := x^3 - xy$ e $f_2 := x^2 y - y^2 + x$ nos da simplemente

$$xy = 0 \cdot f_1 + 0 \cdot f_2 + xy,$$

y el resto no es nulo, aunque $xy \in I$. Esto sucede porque $\{f_1, f_2\}$ no es una base de Gröbner. ▲

11.11. Notación. Fijemos un orden monomial sobre $k[x_1, \ldots, x_n]$. Para una base de Gröbner $G = \{g_1, \ldots, g_s\}$ y $f \in k[x_1, \ldots, x_n]$, el resto de división de f por $(g_1, \ldots, g_s)$ se denotará por $\overline{f}^G$.

Ejercicio 12. Para un ideal $I \subseteq k[x_1, \ldots, x_n]$, sea $\{g_1, \ldots, g_s\}$ un conjunto tal que $I = (g_1, \ldots, g_s)$ y para todo $f \in I$ el resto de división de f por $g_1, \ldots, g_s$ es nulo. Demuestre que $\{g_1, \ldots, g_s\}$ es una base de Gröbner para I.

Ejercicio 13. Sean $\{g_1, \ldots, g_s\}$ y $\{g'_1, \ldots, g'_t\}$ dos bases de Gröbner para un ideal $I \subseteq k[x_1, \ldots, x_n]$. Demuestre que para cualquier polinomio $f \in k[x_1, \ldots, x_n]$ se tiene $\overline{f}^G = \overline{f}^{G'}$.

En Macaulay2, el comando f%I devuelve precisamente $\overline{f}^G$, donde G es una base de Gröbner para I.

Ejercicio 14. Sea $I = (f) \subset k[x_1, \ldots, x_n]$ un ideal principal. Demuestre que cualquier subconjunto finito de I que contiene a f es una base de Gröbner para I.

Entonces, las bases de Gröbner son muy útiles desde el punto de vista computacional, pero el problema es que todavía no sabemos cómo a partir de un ideal construir su base de Gröbner.

12 El criterio de Buchberger

Como antes, trabajamos con un orden monomial fijo sobre $k[x_1,\dots,x_n]$. Notamos que para dos monomios x^α, x^β se tiene

$$\operatorname{mcm}(x^\alpha, x^\beta) = x^\gamma, \text{ donde } \gamma_i = \max\{\alpha_i, \beta_i\}.$$

12.1. Definición. Para $f, g \in k[x_1,\dots,x_n]$ el S-**polinomio** correspondiente viene dado por

$$S(f,g) := \frac{x^\gamma}{LT(f)}\, f - \frac{x^\gamma}{LT(g)}\, g, \quad x^\gamma := \operatorname{mcm}(LT(f), LT(g)).$$

Notamos que $S(g,f) = -S(f,g)$.

Ejercicio 15. Demuestre que

$$LM(S(f,g)) \prec x^\gamma,$$

donde

$$x^\gamma = \operatorname{mcm}(LM(f), LM(g)).$$

Ejercicio 16. Encuentre dos polinomios f, g tales que $S(f,g)$ es diferente respecto a diferentes órdenes monomiales.

12.2. Lema. *Sean $f_1,\dots,f_s$ polinomios que tienen el mismo monomio mayor:*

$$LM(f_i) = x^\delta \text{ para } i = 1,\dots,s.$$

Para algunos $c_1,\dots,c_s \in k$ asumamos que

$$LM(c_1 f_1 + \cdots + c_s f_s) \prec x^\delta.$$

Luego, $c_1 f_1 + \cdots + c_s f_s$ es una combinación k-lineal de polinomios $S(f_i, f_j)$ para $1 \le i < j \le s$. Además, se tiene

$$LM(S(f_i, f_j)) \prec x^\delta.$$

Demostración. Para $i = 1,\dots,s$ pongamos

$$d_i := LC(f_i), \quad p_i := \frac{LT(f_i)}{d_i}.$$

Notamos que

$$LM(p_i) = LM(f_i) = x^\delta, \quad LC(p_i) = 1.$$

Ya que $LM(f_i) = LM(f_j) = \delta$, se tiene

$$S(f_i, f_j) := \frac{x^\delta}{LT(f_i)}\, f_i - \frac{x^\delta}{LT(f_j)}\, f_j = p_i - p_j.$$

Los términos mayores de p_i y p_j se cancelan entre sí y se tiene

$$LM(S(f_i, f_j)) \prec x^\delta.$$

Ahora si

$$LM(c_1 f_1 + \cdots + c_s f_s) \prec x^\delta,$$

entonces los términos mayores de los polinomios $c_i f_i$ necesariamente se cancelan entre sí y se tiene

$$c_1 d_1 + \cdots + c_s d_s = 0.$$

Gracias a esto, podemos escribir

$$\begin{aligned} c_1 f_1 + \cdots + c_s f_s &= c_1 d_1 p_1 + \cdots + c_s d_s p_s \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &+ (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + \underbrace{(c_1 d_1 + \cdots + c_s d_s)}_{=0} p_s \\ &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s). \end{aligned}$$ ■

12.3. Teorema (El criterio de Buchberger). *Sea I un ideal y $\{g_1, \ldots, g_s\} \subset I$ un subconjunto finito tal que $I = (g_1, \ldots, g_s)$. Entonces, $\{g_1, \ldots, g_s\}$ es una base de Gröbner para I si y solo si para todo $i \neq j$ el resto de división de $S(g_i, g_j)$ por $g_1, \ldots, g_s$ (en cualquier orden) es nulo.*

Demostración. Esta condición es necesaria: si $\{g_1, \ldots, g_s\}$ es una base de Gröbner, entonces tenemos

$$S(g_i, g_j) = \frac{x^\gamma}{LT(g_i)} g_i - \frac{x^\gamma}{LT(g_j)} g_j \in (g_1, \ldots, g_s) = I,$$

y como notamos en 11.9, se tiene $f \in I$ si y solo si el resto de división de f por $g_1, \ldots, g_s$ es nulo.

Es más difícil ver que la condición es suficiente para que $g_1, \ldots, g_s$ sea una base de Gröbner. Asumamos entonces que el resto de división de $S(g_i, g_j)$ por $g_1, \ldots, g_s$ es siempre nulo. Luego, para probar que $\{g_1, \ldots, g_s\}$ es una base de Gröbner, bastaría probar que para todo

$$f = h_1 g_1 + \cdots + h_s g_s \in I \tag{12.1}$$

se tiene $LT(f) \in (LT(g_1), \ldots, LT(g_s))$. Pongamos

$$x^{\delta(i)} := LM(h_i f_i), \quad x^\delta := \max_{\prec} \{x^{\delta(1)}, \ldots, x^{\delta(s)}\}.$$

Tenemos entonces

$$LM(f) \preceq x^\delta.$$

Ahora si $LM(f) = x^\delta$, entonces $LT(g_i) \mid LT(f)$ para algún i y por ende $LT(f) \in (LT(g_1), \ldots, LT(g_s))$. Vamos a probar que es siempre posible escribir f como (12.1) tal que $LM(f) = x^\delta$. Ya que cualquier orden monomial es un buen orden, podemos fijar $h_1, \ldots, h_s$ tales que δ es el mínimo posible. Asumamos que

$$LM(f) \prec x^\delta.$$

Nuestro objetivo es obtener una contradicción a la minimalidad de δ. Podemos escribir

$$f = \sum_{1 \leq i \leq s} h_i g_i = \sum_{\delta(i) = \delta} h_i g_i + \sum_{\delta(i) < \delta} h_i g_i = \sum_{\delta(i) = \delta} LT(h_i) g_i + \sum_{\delta(i) = \delta} (h_i - LT(h_i)) g_i + \sum_{\delta(i) < \delta} h_i g_i. \tag{12.2}$$

Escribamos la primera suma como

$$\sum_{\delta(i) = \delta} LT(h_i) g_i = \sum_{\delta(i) = \delta} c_i x^{\alpha(i)} g_i$$

para algunos $c_i \in k$. Notamos que las últimas dos sumas en (12.2) consisten en términos con monomio mayor $\prec x^\delta$, y dado que $LM(f) \prec x^\delta$, para la primera suma se tiene necesariamente

$$LM\left(\sum_{\delta(i) = \delta} c_i x^{\alpha(i)} g_i \right) \prec x^\delta.$$

Además,

$$LM(c_i\, x^{\alpha(i)}\, g_i) = \text{multideg}(h_i\, g_i) = x^\delta.$$

Podemos entonces aplicar el lema anterior y concluir que

$$\sum_{\delta(i)=\delta} c_i\, x^{\alpha(i)}\, g_i = \sum_{j,\ell} c_{j\ell}\, S(x^{\alpha(i)}\, g_i, x^{\alpha(\ell)}\, g_\ell)$$

para algunos $c_{j\ell} \in k$. Calculamos que

$$S(x^{\alpha(i)}\, g_i, x^{\alpha(\ell)}\, g_\ell) = \frac{x^\delta}{LT(x^{\alpha(i)}\, g_i)}\, g_i - \frac{x^\delta}{LT(x^{\alpha(\ell)}\, g_\ell)}\, g_\ell = x^{\delta-\gamma_{j\ell}}\, S(g_j, g_\ell),$$

donde

$$x^{\gamma_{j\ell}} := \text{mcm}(LM(g_j), LM(g_\ell)).$$

Entonces, tenemos

$$\sum_{\delta(i)=\delta} LT(h_i)\, g_i = \sum_{j,\ell} c_{j\ell}\, x^{\delta-\gamma_{j\ell}}\, S(g_j, g_\ell).$$

A este punto podemos aplicar nuestra hipótesis de que el resto de división de $S(g_j, g_\ell)$ por $g_1, \ldots, g_s$ es nulo. Entonces, podemos escribir

$$S(g_j, g_\ell) = \sum_{1\le i\le s} a_{ij\ell}\, g_i$$

para algunos $a_{ij\ell} \in k[x_1, \ldots, x_n]$. Además, el algoritmo de división con resto nos garantiza que

$$LM(a_{ij\ell}\, g_i) \preceq LM(S(g_j, g_k)). \tag{12.3}$$

Entonces, tenemos

$$\sum_{\delta(i)=\delta} LT(h_i)\, g_i = \sum_{j,\ell} c_{j\ell} \sum_{1\le i\le s} b_{ij\ell}\, g_i,$$

donde

$$b_{ij\ell} := x^{\delta-\gamma_{j\ell}}\, a_{ij\ell}.$$

Ahora

$$LM(b_{ij\ell} g_i) = LM(x^{\delta-\gamma_{j\ell}}\, a_{ij\ell}\, g_i) \preceq LM(x^{\delta-\gamma_{j\ell}}\, S(g_j, g_\ell)) \prec x^\delta,$$

donde la primera desigualdad sale de (12.3) y la segunda desigualdad sale del lema anterior. Entonces, hemos logrado escribir

$$\sum_{\delta(i)=\delta} LT(h_i)\, g_i = \sum_i \widetilde{h}_i\, g_i,$$

donde $LM(\widetilde{h}_i g_i) \prec x^\delta$. Pero sustituyendo esta suma en (12.2), se obtiene entonces una expresión de la forma $f = h_1' g_1 + \cdots + h_s' g_s$ con $LM(h_i' g_i) \prec x^\delta$ para todo i, lo que contradice la minimalidad de δ. ■

12.4. Ejemplo. Volviendo al ejemplo 11.6, para

$$f_1 := x^3 - xy, \quad f_2 := x^2 y - y^2 + x$$

se tiene

$$S(f_1, f_2) = -x^2.$$

Para

$$g_1 = x^2, \quad g_2 = xy, \quad g_3 = y^2 - x$$

se tiene

$$S(g_1, g_2) = 0, \quad S(g_1, g_3) = x^3, \quad S(g_2, g_3) = x^2.$$

Notamos que la división con resto de $S(f_1, f_2)$ por f_1 y f_2 nos da

$$-x^2 = 0 \cdot f_1 + 0 \cdot f_2 - x^2,$$

y el resto no es nulo. Esto sucede porque $\{f_1, f_2\}$ no es una base de Gröbner. La división de $S(g_1, g_3)$ y $S(g_2, g_3)$ por g_1, g_2, g_3 nos da

$$x^3 = x \cdot g_1 + 0 \cdot g_2 + 0 \cdot g_3 + 0,$$
$$x^2 = 1 \cdot g_1 + 0 \cdot g_2 + 0 \cdot g_3 + 0,$$

y el resto sí es nulo. ▲

Ejercicio 17. Consideremos el anillo $k[x, y, z]$.

1) Para
$$g_1 := z^2 - x, \quad g_2 := z^3 - y,$$
usando el criterio de Buchberger, determine respecto a cuáles órdenes monomiales entre $\prec_{lex}$, $\prec_{grlex}$, $\prec_{grevlex}$ los polinomios g_1 y g_2 forman una base de Gröbner.

2) La misma pregunta para
$$g_1 := z^2 - x, \quad g_2 := xz - y, \quad g_3 := x^2 - yz.$$

12.5. Comentario. Las bases de Gröbner fueron introducidas en 1965 en la tesis del matemático austriaco Bruno Buchberger quien utilizó el término "base de Gröbner" en homenaje a su director de tesis Wolfgang Gröbner (1899–1980). Resulta que un concepto parecido apareció por primera vez en 1913 en el trabajo del matemático ruso Nikolaï Günther (1871–1941), pero fue olvidado. El matemático japonés Heisuke Hironaka utilizó en 1964 bases parecidas a las de Gröbner, pero para las series de potencias en diversas variables.

13 El algoritmo de Buchberger

El criterio de Buchberger sugiere el siguiente modo de construir una base de Gröbner: para $I = (f_1, \ldots, f_s)$ hay que calcular los polinomios $S(f_i, f_j)$ y sus restos de división por $f_1, \ldots, f_s$. Si todos los restos son nulos, se tiene una base de Gröbner. En el caso contrario, podemos agregar los restos que salen y repetir el proceso. Antes de probar que este método funciona, podemos analizar un ejemplo.

13.1. Ejemplo. Consideremos el anillo $k[x, y]$ con el orden *grlex*. Para los polinomios

$$f_1 := x^3 - xy, \quad f_2 := x^2 y - y^2 + x$$

consideremos el ideal

$$I := (f_1, f_2).$$

Calculamos

$$S(f_1, f_2) = -x^2.$$

Luego, el algoritmo de división con resto nos da

$$S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 - x^2,$$

así que no tenemos una base de Gröbner para I. Podemos agregar el polinomio

$$f_3 := -x^2.$$

Calculamos que

$$S(f_1, f_3) = -xy, \quad S(f_2, f_3) = -y^2 + x.$$

Por nuestra definición de f_3 tenemos

$$S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 + 1 \cdot f_3.$$

Sin embargo, salen nuevos restos de división no nulos:

$$\begin{aligned} S(f_1, f_3) &= 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 - xy, \\ S(f_2, f_3) &= 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 - y^2 + x. \end{aligned}$$

Podemos añadir

$$f_4 := -xy, \quad f_5 := -y^2 + x.$$

Ahora

$$\begin{aligned} S(f_1, f_4) &= -xy^2 = y f_4, \\ S(f_1, f_5) &= x^4 - xy^3 = x f_1 + f_2 + y^4 f_4 - f_5, \\ S(f_2, f_4) &= -y^2 + x = f_5, \\ S(f_2, f_5) &= x^3 - y^3 + xy = f_1 - f_4 + y f_5, \\ S(f_3, f_4) &= 0, \\ S(f_3, f_5) &= x^3 = f_1 - f_4, \\ S(f_4, f_5) &= x^2 = -f_3. \end{aligned}$$

Los restos de división de estos polinomios por f_1, f_2, f_3, f_4, f_5 son nulos, así que no hay que añadir nada y se tiene una base de Gröbner para I

$$f_1 = x^3 - xy, \quad f_2 = x^2 y - y^2 + x, \quad f_3 = -x^2, \quad f_4 = -xy, \quad f_5 = -y^2 + x.$$

Esto significa que

$$(LT(I)) = (LT(f_1), LT(f_2), LT(f_3), LT(f_4), LT(f_5)) = (x^3, x^2 y, x^2, xy, y^2).$$

Aquí hay una redundancia: $x^2 \mid x^3$ y $x^2 \mid x^2 y$. Esto significa que se pueden quitar los polinomios f_1 y f_2 y luego

$$(LT(I)) = (LT(f_3), LT(f_4), LT(f_5)).$$

También podemos normalizar los polinomios f_3, f_4, f_5 para que sus coeficientes mayores sean iguales a 1. De este modo se obtiene una base de Gröbner

$$x^2, \quad xy, \quad y^2 - x. \qquad \blacktriangle$$

13.2. Teorema (Algoritmo de Buchberger). *Sea $I = (f_1, \dots, f_s) \subset k[x_1, \dots, x_n]$ un ideal no nulo. Consideremos el siguiente algoritmo.*

Entrada: $f_1, \dots, f_s \in k[x_1, \dots, x_n]$

$G := \{f_1, \dots, f_s\}$

repetir
  $G' := G$
  para todo $p, q \in G$, $p \neq q$ **hacer**
    $r := \overline{S(p,q)}^G$
    si $r \neq 0$ **entonces** $G' = G' \cup \{r\}$
  $G = G'$
mientras G **se vuelve más grande**
devolver G

Este algoritmo termina en un número finito de pasos y devuelve una base de Gröbner para I.

Demostración. Notamos que si $p, q \in I$, entonces $S(p,q) \in I$. Si además $g_1, \dots, g_t \in I$, entonces el resto de división de $S(p,q)$ por $g_1, \dots, g_t$ también pertenece a I. Esto demuestra por inducción que a cada paso del algoritmo se cumple

$$\{f_1, \dots, f_s\} \subseteq G \subset I,$$

así que G es un conjunto de generadores de I. Cuando el algoritmo termine, se tiene $\overline{S(p,q)}^G = 0$ para cualesquiera $p, q \in G$, lo que significa que G es una base de Gröbner gracias al criterio de Buchberger.

Falta entonces ver que el algoritmo termina en un número finito de pasos. Para esto, asumamos que hemos añadido a $G = \{g_1, \dots, g_t\}$ algún resto $r := \overline{S(p,q)}^G$. Entonces,

$$S(p,q) = a_1 g_1 + \cdots + a_t g_t + r.$$

Aquí r no es divisible por $LT(g_i)$ para ningún i, así que

$$(LT(g_1), \dots, LT(g_t)) \subsetneq (LT(g_1), \dots, LT(g_t), LT(r)).$$

Esto significa que el ideal $(LT(g_1), \dots, LT(g_t))$ se vuelve estrictamente más grande después de cada ejecución del ciclo. Pero el anillo $k[x_1, \dots, x_n]$ es noetheriano, así que puede haber solo un número finito de pasos. ■

Notamos que el argumento de arriba no da una cota específica sobre el número de pasos y de hecho, una base de Gröbner puede ser bastante grande.

13.3. Comentario. El algoritmo de arriba tiene interés pedagógico y puede ser mejorado. En práctica se usan métodos más sofisticados, por ejemplo los algoritmos F4 y F5 desarrollados por el matemático francés Jean-Charles Faugère.

14 Bases de Gröbner reducidas

Las bases de Gröbner están muy lejos de ser únicas. Por ejemplo, consideremos el anillo $\mathbb{Q}[x, y]$ con el orden *grlex*. Tenemos una base de Gröbner

$$g_1 = -3x^2 + xy, \quad g_2 = xy, \quad g_3 = y^2 - x, \quad g_4 = y^3 + x.$$

Pero aquí hay algunas redundancias: se tiene $LT(g_3) \mid LT(g_4)$, así que el polinomio g_4 se puede quitar. Además, del polinomio g_1 se puede quitar el término xy, puesto que $xy = g_2$. El coeficiente mayor de g_1 también se puede normalizar. Al hacerlo, nos queda una base más bonita

$$g_1' = x^2, \quad g_2 = xy, \quad g_3 = y^2 - x.$$

14.1. Definición. Se dice que una base de Gröbner G es **minimal** si se cumplen las siguientes condiciones:

1) para todo $g \in G$ se tiene $LC(g) = 1$;

2) para todo $g \in G$ se tiene $LT(g) \notin (LT(G \setminus \{g\}))$.

Se dice que G es **reducida** si se cumple la condición 1) y en lugar de 2) se cumple la condición más fuerte:

2′) para todo $g \in G$ ningún monomio de g pertenece al ideal $(LT(G \setminus \{g\}))$.

Notamos que toda base reducida es automáticamente minimal. Está claro que todo ideal no nulo $I \subseteq k[x_1, \dots, x_n]$ posee una base de Gröbner minimal: hay que tomar cualquier base de Gröbner G, normalizar sus elementos para que se cumpla la condición 1), y luego quitar uno por uno todos los polinomios innecesarios hasta que se cumpla la condición 2). Es un poco más difícil construir una base reducida.

14.2. Teorema. *Todo ideal no nulo $I \subseteq k[x_1, \dots, x_n]$ posee una base de Gröbner reducida y además esta es única.*

Demostración. Sea G una base de Gröbner para I. En este caso se tiene por la definición $(LT(I)) = (LT(G))$, y si G es una base minimal, entonces $LT(G)$ forma una base minimal para el ideal monomial $(LT(I))$, y esta es única (ejercicio 8). Entonces, todas las bases de Gröbner minimales necesariamente tienen los mismos términos mayores.

Sea G una base minimal para I. Digamos que un elemento $g \in G$ es **reducido** si ningún monomio de g está en el ideal $(LT(G \setminus \{g\}))$. Entonces G es una base reducida si todos sus elementos son reducidos. La observación clave es que si $g \in G$ es reducido, entonces g será reducido respecto a cualquier otra base minimal $G' \ni g$ porque $(LT(G)) = (LT(G'))$.

Ahora para un polinomio $g \in G$ podemos considerar

$$g' := \overline{g}^{G \setminus \{g\}}, \quad G' := (G \setminus \{g\}) \cup \{g'\}.$$

Ya que g' es el resto de división por $G \setminus \{g\}$, los monomios de g' no son divisibles por los términos mayores de $G \setminus \{g\}$, y por lo tanto $g' \notin (G \setminus \{g\})$. Esto significa que g' es reducido. Si la base G era minimal, entonces G' es también una base minimal para I: se tiene $LT(g') = LT(g)$ porque $LT(g)$ no era divisible por los elementos de $LT(G \setminus \{g\})$, y luego al dividir con resto g por $G \setminus \{g\}$, el término mayor $LT(g)$ va al resto de división. Entonces,

$$(LT(G')) = (LT(G)).$$

Puesto que $G' \subset I$, la base G' es una base de Gröbner para I.

Podemos entonces repetir el proceso: a cada paso, al remplazar g por g', este elemento se vuelve reducido. La base de Gröbner minimal G se remplaza por otra base de Gröbner minimal G', pero un elemento reducido se queda reducido respecto a todas las bases minimales.

Para la unicidad de la base reducida, notamos que si G y G' son dos bases reducidas, entonces en particular son minimales y $LT(G) = LT(G')$ (por la unicidad de la base minimal del ideal monomial $(LT(I)) = (LT(G)) = (LT(G'))$). Entonces, para todo $g \in G$ existe $g' \in G'$ tal que $LT(g) = LT(g')$. Ahora $g - g' \in I$, así que $\overline{g - g'}^{G} = 0$, dado que G es una base de Gröbner. Pero $\overline{g - g'}^{G} = g - g'$, puesto que los términos de g y g' no son divisibles por los términos de $LT(G \setminus \{g\}) = LT(G' \setminus \{g'\})$. Entonces, $g = g'$. Podemos concluir que $G = G'$. ∎

Notamos que la prueba nos da un algoritmo que a partir de una base de Gröbner para I produce la base reducida correspondiente.

Ejercicio 18. Analice todos los pasos del algoritmo de Buchberger y el algoritmo de reducción para calcular la base de Gröbner reducida de $I = (f_1, f_2)$, donde

$$f_1 := x^2 + y, \quad f_2 := x^3 + 2x^2y + y^2 + 3,$$

respecto al orden *lex* y *grlex*.

14.3. Corolario. *Sean I, J dos ideales en $k[x_1, \ldots, x_n]$.*

1) *Se tiene $I = J$ si y solamente si las bases de Gröbner reducidas de I e J coinciden.*
2) *En particular, el ideal I es propio si y solamente si su base de Gröbner reducida no coincide con $\{1\}$.*

Demostración. Se sigue de la unicidad de las bases reducidas. ■

Ejercicio 19. Los polinomios de la forma $x^\alpha - x^\beta \in k[x_1, \ldots, x_n]$ se llaman **binomios**. Se dice que un ideal I es **binomial** si I puede ser generado por algunos binomios. En este ejercicio vamos a probar que I es binomial si y solo si su base de Gröbner reducida consiste en binomios.

a) Demuestre que para dos binomios $f_1 = x^{\alpha(1)} - x^{\beta(1)}$ y $f_2 = x^{\alpha(2)} - x^{\beta(2)}$ el polinomio $S(f_1, f_2)$ es también un binomio si $f_1 \neq f_2$.

b) Sean $f = x^\alpha - x^\beta$, $f_1 = x^{\alpha(1)} - x^{\beta(1)}, \ldots, f_s = x^{\alpha(s)} - x^{\beta(s)}$ binomios. Demuestre que el algoritmo de división con resto de f por $(f_1, \ldots, f_s)$ produce

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

donde $r = 0$ o r es también un binomio.

c) Demuestre que todo ideal binomial tiene una base de Gröbner que consiste en binomios.

d) Demuestre que la base de Gröbner reducida de un ideal binomial consiste en binomios.

15 Bases de Gröbner en Macaulay2

Para una implementación básica del algoritmo de Buchberger de 13.2 y el algoritmo de reducción de 14.2, véase el apéndice B. Este código sirve para entender cómo funcionan los algoritmos. Para los cálculos prácticos, hay que usar la función `groebnerBasis(I)` de Macaulay2.

Por ejemplo, calculemos la base de Gröbner para el ideal

$$I = (x^5 + y^4 + z^3 - 1, x^3 + y^3 + z^2 - 1) \subset k[x, y, z]$$

respecto al orden *grlex*.

```
i1 : R = QQ[x,y,z, MonomialOrder=>GLex];

i2 : groebnerBasis (ideal (x^5+y^4+z^3-1, x^3+y^3+z^2-1))

o2 = | x3+y3+z2-1 x2y3+x2z2-y4-z3-x2+1 y6+xy4+2y3z2+xz3+z4-2y3-2z2-x+1 |

             1       3
o2 : Matrix R  <--- R
```

El resultado es una matriz de 1×3 que tiene como sus entradas los elementos de la base de Gröbner reducida correspondiente:

$$x^3 + y^3 + z^2 - 1, \quad x^2y^3 + x^2z^2 - y^4 - z^3 - x^2 + 1, \quad y^6 + xy^4 + 2y^3z^2 + xz^3 + z^4 - 2y^3 - 2z^2 - x + 1.$$

Ahora si cambiamos el orden monomial por el orden lexicográfico especificando

```
R = QQ[x,y,z, MonomialOrder=>Lex]
```

entonces la base de Gröbner correspondiente va a consistir en 8 polinomios de grado mayor y con coeficientes muy grandes. No vamos a reproducir esta base; dejo al lector ejecutar el comando correspondiente. Este ejemplo demuestra que el tamaño de la base de Gröbner puede depender drásticamente del orden monomial.

La salida de `groebnerBasis(`I`)` es precisamente la base de Gröbner reducida para I, solo que la noción de ser reducido es un poco diferente en Macaulay2 de la nuestra: los polinomios con coeficientes en $\mathbb{Q}$ no se van a normalizar como polinomios mónicos, sino como polinomios con coeficientes enteros sin múltiplo común. Por ejemplo, $\frac{1}{2}x^2 + \frac{1}{3}$ se va a normalizar como $3x^2 + 2$.

El lector puede experimentar con Macaulay2 haciendo los ejercicios de abajo.

Algunos ejercicios

Ejercicio 20. Use las bases de Gröbner para determinar si

1) $xy^3 - z^2 + y^5 - z^3 \in (-x^3 + y, x^2y - z)$;
2) $x^3z - 2y^2 \in (xz - y, xy + 2z^2, y - z)$.

Ejercicio 21. Para la función $f : \mathbb{R}^2 \to \mathbb{R}$ definida por

$$f(x, y) := (x^2 + y^2 - 4)(x^2 + y^2 - 1) + (x - 3/2)^2 + (y - 3/2)^2$$

determine sus **puntos críticos** usando las bases de Gröbner; es decir, los puntos donde

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

Sugerencia: para las derivadas en Macaulay2, consulte la documentación sobre la función `diff`.

Ejercicio 22. Calcule la base de Gröbner reducida para

$$I := (f_1, f_2, f_3) \subset k[x, y, z], \quad f_1 = x + 2y + z - 1,\ f_2 := 2x - y + z = 0,\ f_3 := x + 2y - z - 2$$

respecto a los órdenes *lex* y *grlex*.

En general, sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios lineales; es decir, polinomios de la forma

$$a_1x_1 + \cdots + a_nx_n + c, \quad a_1, \ldots, a_n, c \in k.$$

Explique por qué el cálculo de la base de Gröbner reducida para $I = (f_1, \ldots, f_s)$ respecto al orden lexicográfico corresponde al método de Gauss para resolver el sistema de ecuaciones $f_1(x) = \cdots = f_s(x) = 0$.

16 Radical

Otra operación importante es el radical de ideal $\sqrt{I}$. Existen algoritmos que a partir de generadores de I producen generadores de $\sqrt{I}$, pero son demasiado difíciles para nuestro curso. Nos contentamos con el problema más fácil que consiste en determinar si algún elemento pertenece al radical. Primero recordemos un par de resultados sobre la localización.

16.1. Lema. *Sea A un anillo conmutativo. Un elemento $f \in A$ es nilpotente si y solamente si $A[f^{-1}] = 0$.*

Demostración. Recordemos que $A[f^{-1}]$ denota la localización de A respecto al conjunto multiplicativo

$$U := \{1, f, f^2, f^3, \ldots\}.$$

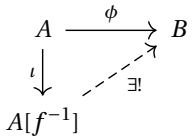
Ahora $A[f^{-1}] = 0$ si y solo si $\frac{1}{1} = \frac{0}{1}$ en $A[f^{-1}]$ lo que sucede si y solo si existe $u \in U$ tal que

$$u(1 \cdot 1 - 0 \cdot 1) = 0,$$

es decir, si y solo si $0 \in U$. ■

16.2. Lema. *Hay un isomorfismo canónico $A[f^{-1}] \cong A[t]/(ft-1)$.*

Demostración. La propiedad universal de la localización $A[f^{-1}]$ consiste en lo siguiente: si $\phi\colon A \to B$ es un homomorfismo tal que $\phi(f) \in B^\times$, entonces ϕ se factoriza de modo único por el homomorfismo canónico de localización $\iota\colon a \mapsto \frac{a}{1}$:



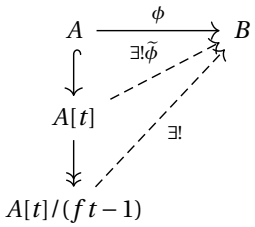
Ahora el anillo de polinomios $A[t]$ tiene la siguiente propiedad universal: para $b \in B$ fijo, un homomorfismo $\phi\colon A \to B$ se levanta de manera única a un homomorfismo $\widetilde{\phi}\colon A[t] \to B$ tal que $\widetilde{\phi}(t) = b$. Luego, la propiedad universal del cociente $A[t]/(ft-1)$ nos dice que todo homomorfismo $\psi\colon A[t] \to B$ tal que $(ft-1) \subseteq \ker\psi$ se factoriza de modo único por $A[t]/(ft-1)$.

Notamos que

$$\widetilde{\phi}(ft-1) = 0 \iff \widetilde{\phi}(f)\widetilde{\phi}(t) = 1 \iff \widetilde{\phi}(t) = \widetilde{\phi}(f)^{-1}.$$

Entonces, si $\phi(f) \in B^\times$, el homomorfismo ϕ se factoriza de modo único por

$$A \hookrightarrow A[t] \twoheadrightarrow A[t]/(ft-1). \tag{16.1}$$



Hemos probado entonces que el homomorfismo canónico (16.1) cumple la misma propiedad universal que el homomorfismo canónico de la localización $\iota\colon A \to A[f^{-1}]$, y por ende hay un isomorfismo canónico entre $A[f^{-1}]$ y $A[t]/(ft-1)$. ■

16.3. Proposición. *Sea $I \subseteq k[x_1,\dots,x_n]$ un ideal. Se tiene $f \in \sqrt{I}$ si y solamente si en el anillo $k[x_1,\dots,x_n,t]$ se cumple*

$$I + (ft-1) = k[x_1,\dots,x_n,t].$$

Demostración. Tenemos $f \in \sqrt{I}$ si y solo si $f^n \in I$ para algún n. Esto significa que f es nilpotente en el anillo cociente $k[x_1,\dots,x_n]/I$, lo que sucede si y solo si la localización

$$(k[x_1,\dots,x_n]/I)[f^{-1}] \cong k[x_1,\dots,x_n,t]/(I + (ft-1))$$

es trivial. ■

16.4. Ejemplo. Consideremos el ideal

$$I := (x^3y - x^2y^2,\ x^3z + z^2yx,\ x^2 - xz) \subseteq \mathbb{Q}[x,y,z].$$

Para ver si $x \in \sqrt{I}$, hay que calcular la base de Gröbner reducida para el ideal

$$\widetilde{I} := (x^3y - x^2y^2,\ x^3z + z^2yx,\ x^2 - xz,\ xt-1) \subseteq \mathbb{Q}[x,y,z,t].$$

Hagámoslo en Macaulay2.

```
i1 : R = QQ[x,y,z];
i2 : I = ideal (x^3*y-x^2*y^2, x^3*z+z^2*y*x, x^2-x*z);
o2 : Ideal of R
i3 : S = R[t];
i4 : groebnerBasis (I + (x*t - 1))
o4 = | 1 |
             1       1
o4 : Matrix S  <--- S
```

La base reducida es $\{1\}$, así que $x \in \sqrt{I}$. Entonces, ¿qué potencia de x pertenece a I? Resulta que es x^5:

```
i5 : for n from 1 to 10 list (x^n%I)

                  2     3
o5 = {x, x*z, x*z , x*z , 0, 0, 0, 0, 0, 0}
```

¿Cómo expresar x^5 en términos de los generadores?

```
i6 : x^5 // gens I

o6 = {4} | -1/2z                |
     {4} | -1/2y+z              |
     {2} | x3+x2z+xyz-1/2y2z+yz2 |

             3       1
o6 : Matrix R  <--- R

i7 : gens I * oo
```

```
o7 = | x5 |

             1       1
o7 : Matrix R  <--- R
```

De hecho, la función `radical` en Macaulay2 calcula de una vez el radical (mediante el **algoritmo de Eisenbud–Huneke–Vasconcelos**[*], que lamentablemente no podemos revisar en este curso introductorio).

```
i8 : radical(I)

o8 = ideal x

o8 : Ideal of R
```

Entonces, tenemos simplemente $\sqrt{I} = (x)$. ▲

16.5. Ejemplo. Consideremos una matriz de 2×2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Un resultado bien conocido de álgebra lineal nos dice que

$$A^2 = 0 \iff \operatorname{tr} A = \det A = 0.$$

Efectivamente, el polinomio característico de A viene dado por

$$\chi_A = X^2 - \operatorname{tr}(A)\, X + \det(A),$$

y el teorema de Cayley–Hamilton nos dice que

$$\chi_A(A) = A^2 - \operatorname{tr}(A)\, A + \det(A)\, I = 0.$$

Si $\operatorname{tr}(A) = \det(A) = 0$, entonces de esta identidad se sigue que $A^2 = 0$. Viceversa, si $A^2 = 0$, entonces $\det(A)^2 = \det(A^2) = 0$, de donde $\det A = 0$, y la identidad de arriba implica que $\operatorname{tr}(A)\, A = 0$, y por lo tanto $\operatorname{tr}(A) = 0$.

Notamos que

$$A^2 = 0 \iff a^2 + bc = ab + bd = ac + cd = bc + d^2 = 0.$$

y

$$\operatorname{tr} A = \det A = 0 \iff a + d = ad - bc = 0.$$

Consideremos los ideales

$$I := (a^2 + bc,\ ab + bd,\ ac + cd,\ bc + d^2), \quad J := (a + d,\ ad - bc)$$

en el anillo de polinomios $k[a, b, c, d]$. Primero, el ideal J es radical: se tiene $\sqrt{J} = J$. Esto se sigue del hecho de que J es un ideal primo:

$$k[a, b, c, d]/(ad - bc,\ a + d) \cong k[a, b, c]/(a^2 + bc),$$

[*] David Eisenbud, Craig Huneke, Wolmer Vasconcelos, *Direct methods for primary decomposition*, Invent. math. 110 (1992), 207–235.

y el polinomio $a^2 + bc$ es irreducible: es un polinomio cuadrático en a y se puede aplicar, por ejemplo, el criterio de Eisenstein. Además, es fácil calcular que

$$(a+d)\,b, (a+d)\,c \in J$$

y que

$$a^2 + bc = (a+d)\,a - (ad - bc) \in J$$

y

$$bc + d^2 = (a+d)\,d - (ad - bc) \in J.$$

Entonces,

$$I \subseteq J.$$

Luego,

$$\sqrt{I} \subseteq \sqrt{J} = J.$$

En efecto, se tiene la igualdad $\sqrt{I} = J$, pero para probarlo necesitamos establecer la inclusión $J \subseteq \sqrt{I}$. Nos puede ayudar Macaulay2.

```
i1 : R = QQ[a,b,c,d];

i2 : I = ideal (a^2 + b*c, a*b + b*d, a*c + c*d, b*c + d^2);

o2 : Ideal of R

i3 : (a+d) % radical(I)

o3 = 0

o3 : R

i4 : (a*d - b*c) % radical(I)

o4 = 0

o4 : R
```

Pero ¿cuáles potencias de $a+d$ y $ad-bc$ están en I? Resulta que para $a+d$ es el cubo y para $ad-bc$ es el cuadrado:

```
i5 : for n from 1 to 10 list ((a+d)^n%I)

                         2
o5 = {a + d, 2a*d + 2d , 0, 0, 0, 0, 0, 0, 0, 0}

o5 : List

i6 : for n from 1 to 10 list ((a*d-b*c)^n%I)

              2
o6 = {a*d + d , 0, 0, 0, 0, 0, 0, 0, 0, 0}

o6 : List
```

Y ¿cómo expresar $(a+d)^3$ y $(ad-bc)^2$ en términos de los generadores de I?

```
i7 : (a+d)^3 // gens I

o7 = {2} | a+3d |
     {2} | 0    |
     {2} | -4b  |
     {2} | 3a+d |

             4       1
o7 : Matrix R  <--- R

i8 : (a*d-b*c)^2 // gens I

o8 = {2} | d2   |
     {2} | 0    |
     {2} | -2bd |
     {2} | bc   |

             4       1
o8 : Matrix R  <--- R
```

Entonces,

$$(a+d)^3 = (a+3d)\cdot(a^2+bc) + (-4b)\cdot(ac+cd) + (3a+d)\cdot(bc+d^2)$$

y

$$(ad-bc)^2 = d^2\cdot(a^2+bc) + (-2bd)\cdot(ac+cd) + bc\cdot(bc+d^2). \qquad \blacktriangle$$

Ejercicio 23. En este ejercicio vamos a calcular el radical de un ideal monomial.

a) Demuestre que un ideal monomial $I \subset k[x_1,\dots,x_n]$ es primo si y solo si $I = (x_{i_1},\dots,x_{i_s})$ es el ideal generado por algunas variables $\{x_{i_1},\dots,x_{i_s}\} \subseteq \{x_1,\dots,x_n\}$.

b) Demuestre que si A es cualquier anillo conmutativo e $I, J \subseteq A$ son ideales, entonces

$$\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}, \quad \sqrt{I\cap J} = \sqrt{I}\cap\sqrt{J}.$$

c) Para un monomio $x^\alpha := x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ demuestre que $\sqrt{(x^\alpha)} = (\sqrt{x^\alpha})$, donde

$$\sqrt{x^\alpha} := x_1^{\min(1,\alpha_1)}\cdots x_n^{\min(1,\alpha_n)} = \text{producto de las variables que están en } x^\alpha.$$

d) Demuestre que el ideal $(\sqrt{x^{\alpha(1)}},\dots,\sqrt{x^{\alpha(s)}})$ es radical.
Sugerencia: note que si $\sqrt{x^\alpha} = x_{i_1}\cdots x_{i_k}$, entonces $\sqrt{(x^\alpha)} = (x_{i_1})\cap\cdots\cap(x_{i_k})$. Usando esta observación, exprese $(\sqrt{x^{\alpha(1)}},\dots,\sqrt{x^{\alpha(s)}}) = \bigcap_i \mathfrak{p}_i$, donde $\mathfrak{p}_i$ son algunos ideales monomiales primos.

e) Demuestre que $\sqrt{(x^{\alpha(1)},\dots,x^{\alpha(s)})} = \sqrt{(\sqrt{x^{\alpha(1)}},\dots,\sqrt{x^{\alpha(s)}})} = (\sqrt{x^{\alpha(1)}},\dots,\sqrt{x^{\alpha(s)}})$.

17 Anillos cociente

Una operación muy importante que nos gustaría algoritmizar es la formación del anillo cociente $k[x_1,\dots,x_n]/I$. Para esto, fijemos un orden monomial sobre $k[x_1,\dots,x_n]$ y una base de Gröbner $G = \{g_1,\dots,g_s\}$ para I. Hemos visto en 11.7 que la división con resto nos permite escribir

$$f = h + \overline{f}^G, \tag{17.1}$$

donde $h \in I$ y los términos de $\overline{f}^G$ no son divisibles por $LT(g_i)$. Esto caracteriza a $\overline{f}^G$ de modo único. Además, el ejercicio 13 nos dice que este $\overline{f}^G$ no depende de una base de Gröbner particular G (pero sí depende del orden monomial).

Notamos que al multiplicar (17.1) por una constante $c \in k$ nos queda

$$cf = ch + c\overline{f}^G,$$

donde $ch \in I$ y los términos de $c\overline{f}^G$ tampoco son divisibles por $LT(g_i)$, así que

$$\overline{cf}^G = c\overline{f}^G. \tag{17.2}$$

Ahora si tenemos la división con resto de f_1 y f_2 por G:

$$f_1 = h_1 + \overline{f_1}^G, \quad f_2 = h_2 + \overline{f_2}^G,$$

entonces al sumar estas dos expresiones nos queda

$$f_1 + f_2 = \underbrace{h_1 + h_2}_{\in I} + \overline{f_1}^G + \overline{f_2}^G,$$

donde los términos de $\overline{f_1}^G + \overline{f_2}^G$ no son divisibles por $LT(g_i)$, así que

$$\overline{f_1 + f_2}^G = \overline{f_1}^G + \overline{f_2}^G. \tag{17.3}$$

Para el producto, vamos a tener

$$f_1 f_2 = \underbrace{h_1 h_2 + \overline{f_1}^G h_2 + \overline{f_2}^G h_1}_{\in I} + \overline{f_1}^G \overline{f_2}^G.$$

Sin embargo, los términos de $\overline{f_1}^G \overline{f_2}^G$ sí pueden ser divisibles por $LT(g_i)$, así que no es necesariamente el resto de división de $f_1 f_2$ por G. Pero usando (17.3) se obtiene

$$\overline{f_1 f_2}^G = \underbrace{\overline{h_1 h_2 + \overline{f_1}^G h_2 + \overline{f_2}^G h_1}^G}_{=0} + \overline{\overline{f_1}^G \overline{f_2}^G}^G = \overline{\overline{f_1}^G \overline{f_2}^G}^G. \tag{17.4}$$

17.1. Ejemplo. Para los polinomios en una variable, si $f = x^2 + x + 1$, entonces la división con resto por $g = x^2$ nos da

$$f = 1 \cdot x^2 + (x + 1).$$

Sin embargo, el resto de división de f^2 por g no es $(x+1)^2$, sino $2x+1$, que es el resto de división de $(x+1)^2$ por g:

$$f^2 = (x^2 + 2x + 3) \cdot x^2 + (2x + 1). \qquad \blacktriangle$$

17.2. Teorema. *Fijemos un orden monomial sobre $k[x_1, \ldots, x_n]$. Sea $I \subseteq k[x_1, \ldots, x_n]$ un ideal y $G = \{g_1, \ldots, g_s\}$ alguna base de Gröbner para I. Sea*

$$k\langle x^\alpha \mid x^\alpha \notin (LT(I))\rangle$$

el espacio vectorial sobre k generado por los monomios x^α que no pertenecen al ideal $(LT(I))$. La aplicación

$$\phi\colon k[x_1, \ldots, x_n]/I \to k\langle x^\alpha \mid x^\alpha \notin (LT(I))\rangle,$$
$$f \mod I \mapsto \overline{f}^G$$

está bien definida y es un isomofismo de espacios vectoriales. En particular,

$$x^\alpha \mod I, \text{ donde } x^\alpha \notin (LT(I))$$

es una base para $k[x_1,\dots,x_n]/I$ como un espacio vectorial sobre k[*].

Además, ϕ es un isomorfismo de k-álgebras, donde la multiplicación sobre $k\langle x^\alpha \mid x^\alpha \notin LT(I)\rangle$ se define mediante

$$\overline{f_1}^G * \overline{f_2}^G := \overline{\overline{f_1}^G \cdot \overline{f_2}^G}^G.$$

Demostración. Notamos primero que la aplicación ϕ está bien definida: si $f_1 \equiv f_2 \pmod I$, entonces $f_1 - f_2 \in I$ y por ende $\overline{f_1 - f_2}^G = 0$, pero gracias a (17.2) y (17.3) esto es equivalente a $\overline{f_1}^G = \overline{f_2}^G$. La aplicación ϕ es k-lineal gracias a las mismas identidades (17.2) y (17.3). La identidad (17.4) nos dice que ϕ preserva productos.

Recordamos que se tiene $\overline{f}^G = 0$ si y solo si $f \in I$ (véase 11.9), y esto demuestra que ϕ es inyectiva. Para ver que es sobreyectiva, basta notar que si

$$\sum_\alpha c_\alpha x^\alpha$$

es una combinación k-lineal de monomios

$$x^\alpha \notin (LT(I)) = (LT(G)) = (LT(g_1),\dots,LT(g_s)),$$

entonces $LT(g_i) \nmid x^\alpha$ para ningún $i = 1,\dots,s$, y x^α es el resto de división de x^α por G. ■

17.3. Ejemplo. Consideremos el ideal

$$I := (x^2 + y - 1, xy - y^2 + y) \subset k[x,y].$$

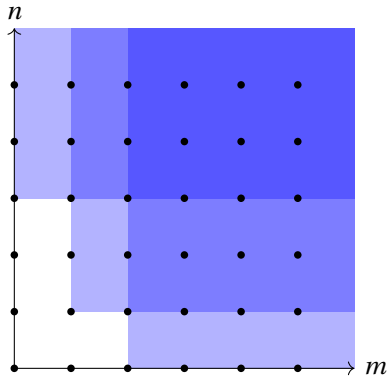
Su base de Gröbner reducida respecto al orden lexicográfico es

$$G = \{y^3 - y^2, xy - y^2 + y, x^2 + y - 1\}.$$

Ahora

$$(LT(I)) = (LT(G)) = (y^3, xy, x^2).$$

Los monomios que no están en $(LT(I))$ son $1, x, y, y^2$:



Esto significa que una base de $\mathbb{Q}[x,y]/I$ como un espacio vectorial sobre $\mathbb{Q}$ viene dada por

$$\overline{1}, \overline{x}, \overline{y}, \overline{y^2}$$

(donde $\overline{f} := f \mod I$). Tenemos la siguiente tabla de multiplicación:

[*] ¡No confundir con una base de k-álgebra!

	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{y^2}$
$\overline{1}$	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{y^2}$
$\overline{x}$	$\overline{x}$	$-\overline{y}+\overline{1}$	$\overline{y^2}-\overline{y}$	$\overline{0}$
$\overline{y}$	$\overline{y}$	$\overline{y^2}-\overline{y}$	$\overline{y^2}$	$\overline{y^2}$
$\overline{y^2}$	$\overline{y^2}$	$\overline{0}$	$\overline{y^2}$	$\overline{y^2}$

Para definir un anillo cociente en Macaulay2, se usa la sintaxis natural: $k[x_1,\dots,x_n]/I$ es el cociente de $k[x_1,\dots,x_n]$ por I. En este caso todos los polinomios en $x_1,\dots,x_n$ automáticamente serán reducidos por una base de Gröbner respecto al orden monomial sobre $k[x_1,\dots,x_n]$.

```
i1 : R = QQ[x,y, MonomialOrder=>Lex]/(x^2 + y - 1, x*y - y^2 + y)

o1 = R

o1 : QuotientRing

i2 : x*y

      2
o2 = y  - y

o2 : R

i3 : y^3

      2
o3 = y

o3 : R
```

▲

El último ejemplo es bastante particular: normalmente la dimensión de $k[x_1,\dots,x_n]/I$ como un espacio vectorial sobre k no es finita.

17.4. Ejemplo. Consideremos el ideal

$$I := (x-z^2,\ y-z^3) \subseteq k[x,y,z].$$

Sus generadores ya forman una base de Gröbner respecto al orden lexicográfico: tenemos

$$S(x-z^2, y-z^3) = xz^3 - yz^2,$$

y luego

$$xz^3 - yz^2 = z^3\cdot(x-z^2) + (-z^2)\cdot(y-z^3) + 0,$$

así que $\{x-z^2, y-z^3\}$ es una base de Gröbner por el criterio de Buchberger. Ahora

$$(LT(I)) = (x,y),$$

y como una base del espacio $k[x,y,z]/I$ se pueden tomar los monomios

$$\overline{1}, \overline{z}, \overline{z^2}, \overline{z^3}, \dots$$

▲

Ejercicio 24. Consideremos el ideal

$$I = (x^3y - z,\ y^2 - z - 1,\ x^2 + 1) \subset k[x, y, z].$$

1) Usando la computadora, encuentre una base de Gröbner para I respecto al orden lexicográfico. Encuentre la base monomial correspondiente para $k[x, y, z]/I$ como un espacio vectorial sobre k.

2) La misma pregunta para el orden lexicográfico graduado.

3) Compile las tablas de multiplicación en $k[x, y, z]/I$ respecto a estas dos bases.

Ejercicio 25. Demuestre que las siguientes condiciones son equivalentes:

a) $\dim_k(k[x_1, \ldots, x_n]/I) < \infty$;

b) $\#\{x^\alpha \mid x^\alpha \notin (LT(I))\} < \infty$;

c) para todo $i = 1, \ldots, n$ existe $\alpha_i \geq 0$ tal que $x_i^{\alpha_i} \in (LT(I))$;

d) si G es una base de Gröbner para I, entonces para todo $i = 1, \ldots, n$ existe $\alpha_i \geq 0$ tal que $x_i^{\alpha_i} = LM(g)$ para algún $g \in G$.

Ejercicio 26. Demuestre que $\dim_k(k[x_1, \ldots, x_n]/I) < \infty$ si y solamente si $I \cap k[x_i] \neq 0$ para todo $i = 1, \ldots, n$. Sugerencia: use el ejercicio anterior y el orden lexicográfico con $x_j \succ x_i$ para todo $j \neq i$.

18 Intersección de ideales y eliminación

Las sumas y productos de ideales especificados por sus generadores se calculan sin ningún problema: si

$$I = (f_1, \ldots, f_r), \quad J = (g_1, \ldots, g_s),$$

entonces

$$I + J = (f_1, \ldots, f_r, g_1, \ldots, g_s)$$

y

$$IJ = (f_i g_j \mid i = 1, \ldots, r,\ j = 1, \ldots, s).$$

La intersección de ideales es una operación más interesante en este sentido. Para calcular las intersecciones en el anillo de polinomios $k[x_1, \ldots, x_n]$, vamos a introducir una variable extra t y trabajar con el anillo de polinomios

$$k[t, x_1, \ldots, x_n] \supset k[x_1, \ldots, x_n].$$

18.1. Lema. *Para un ideal $I \subseteq k[x_1, \ldots, x_n]$ y un polinomio $f(t) \in k[t]$, denotemos por $f(t)\,I$ el ideal en $k[t, x_1, \ldots, x_n]$ generado por los productos $f(t)\,h$ donde $h \in I$.*

1) Si

$$I = (p_1(x), \ldots, p_s(x)),$$

entonces

$$f(t)\,I = (f(t)\,p_1(x), \ldots, f(t)\,p_s(x)).$$

2) Si $g(t, x) \in f(t)\,I$, entonces para todo $c \in k$ se tiene $g(c, x) \in I$.

Demostración. Primero, está claro que

$$(f(t)\,p_1(x),\ldots,f(t)\,p_s(x)) \subseteq f(t)\,I.$$

Para la otra inclusión, notamos que un elemento de $f(t)\,I$ es una suma de polinomios de la forma

$$h(t,x)\,f(t)\,g(x),$$

donde $h(t,x) \in k[t,x_1,\ldots,x_n]$ y $g(x) \in I$. Luego,

$$g(x) = \sum_{1\le i\le s} q_i(x)\,p_i(x)$$

para algunos polinomios $q_i(x) \in k[x_1,\ldots,x_n]$, así que

$$h(t,x)\,f(t)\,g(x) = \sum_{1\le i\le s} h(t,x)\,q_i(x)\,f(t)\,p_i(x).$$

Al sustituir $c \in k$ en lugar de t, se obtiene

$$h(x,c)\,f(c)\,g(x) = \sum_{1\le i\le s} \underbrace{h(x,c)\,q_i(x)\,f(c)}_{\in k[x_1,\ldots,x_n]}\,p_i(x) \in I. \qquad \blacksquare$$

18.2. Teorema. *Para dos ideales $I, J \subseteq k[x_1,\ldots,x_n]$ consideremos los ideales*

$$tI, (1-t)\,J \subseteq k[t,x_1,\ldots,x_n]$$

(definidos como arriba para el caso particular de $f(t) = t$ y $f(t) = 1-t$). Luego,

$$I \cap J = (tI + (1-t)\,J) \cap k[x_1,\ldots,x_n].$$

Demostración. Si $f \in I \cap J$, entonces

$$f = tf + (1-t)f \in (tI + (1-t)\,J) \cap k[x_1,\ldots,x_n].$$

Viceversa, si $f \in (tI + (1-t)\,J) \cap k[x_1,\ldots,x_n]$, entonces

$$f(x) = g(t,x) + h(t,x)$$

para algunos polinomios $g(t,x) \in tI$ y $h(t,x) \in (1-t)\,J$. Ahora notamos que $g(0,x) = 0$ y $h(1,x) = 0$, así que

$$f(x) = h(0,x) = g(1,x) \in I \cap J. \qquad \blacksquare$$

18.1 Eliminación

Para calcular las intersecciones, todavía hay que entender cómo para un ideal $I \subseteq k[t,x_1,\ldots,x_n]$ calcular el ideal $I \cap k[x_1,\ldots,x_n]$. Esto se hace con las bases de Gröbner.

18.3. Proposición (Teorema de eliminación). *Sea $1 \le \ell \le n$. Para un ideal $I \subseteq k[x_1,\ldots,x_n]$ sea G su base de Gröbner respecto al orden lexicográfico con*

$$x_1 \succ \cdots \succ x_n.$$

Entonces, $G \cap k[x_{\ell+1},\ldots,x_n]$ es una base de Gröbner para $I \cap k[x_{\ell+1},\ldots,x_n]$ respecto al orden lexicográfico.

Demostración. Denotemos

$$I' := I \cap k[x_{\ell+1}, \ldots, x_n], \quad G' := G \cap k[x_{\ell+1}, \ldots, x_n].$$

Puesto que $G \subset I$, tenemos $G' \subset I'$. Hay que probar que

$$(LT(I')) = (LT(G')).$$

La inclusión no trivial es $(LT(I')) = (LT(G'))$. Hay que ver entonces que para todo $f \in I'$ existe $g' \in G'$ tal que $LT(g') \mid LT(f)$. Lo que sabemos es que existe $g \in G$ que cumple $LT(g) \mid LT(f)$. En f no aparecen las variables $x_1, \ldots, x_\ell$, y por lo tanto estas tampoco aparecen en $LT(g)$. Ahora, *puesto que el orden es lexicográfico* con $x_1 \succ \cdots \succ x_n$, esto implica que $x_1, \ldots, x_\ell$ no aparecen en ningún término de g, así que $g \in G'$. ■

En Macaulay2, para un ideal $I \subseteq k[x_1, \ldots, x_n]$ el ideal $I \cap k[x_\ell, \ldots, x_n]$ puede ser calculado mediante la función

`eliminate ({`$x_1, \ldots, x_{\ell-1}$`}, I)`

El orden lexicográfico que hemos usado en 18.3 no es muy bueno en práctica. En los siguientes dos ejercicios vamos a investigar otro orden que también funciona y suele ser mejor en los cálculos.

Ejercicio 27. Para $1 \leq \ell \leq n$ consideremos la relación sobre los monomios en $k[x_1, \ldots, x_n]$

$$x^\alpha \prec_\ell x^\beta \iff \left\{ \begin{array}{c} \alpha_1 + \cdots + \alpha_\ell < \beta_1 + \cdots + \beta_\ell \\ \text{o bien} \\ \alpha_1 + \cdots + \alpha_\ell = \beta_1 + \cdots + \beta_\ell \text{ y } \alpha \prec_{grevlex} \beta \end{array} \right\}$$

1) Demuestre que $\prec_\ell$ es un orden monomial.

2) Demuestre que para un ideal $I \subseteq k[x_1, \ldots, x_n]$, si G es una base de Gröbner respecto al orden $\prec_\ell$, entonces, $G \cap k[x_{\ell+1}, \ldots, x_n]$ es una base de Gröbner para $I \cap k[x_{\ell+1}, \ldots, x_n]$ respecto al orden grevlex.

Este orden monomial puede ser especificado en Macaulay2 como

`MonomialOrder=>Eliminate` ℓ

Ejercicio 28. Consideremos el ideal

$$I = (t^2 + x^2 + y^2 + z^2,\ t^2 + 2x^2 - xy - z^2,\ t + y^3 - z^3) \subset \mathbb{Q}[t, x, y, z].$$

1) Calcule en Macaulay2 la base de Gröbner reducida de I respecto al orden lexicográfico. Encuentre la base de Gröbner correspondiente para $I \cap \mathbb{Q}[x, y, z]$.

2) Haga el mismo cálculo para el orden $\prec_1$ del ejercicio anterior (es decir, $\prec_\ell$ con $\ell = 1$). Encuentre la base de Gröbner correspondiente para $I \cap \mathbb{Q}[x, y, z]$.

Ejercicio 29. Consideremos el ideal

$$I = (x^3 y - z,\ y^2 - z - 1,\ x^2 + 1) \subset k[x, y, z].$$

Usando Macaulay2, encuentre generadores de los ideales principales

$$I \cap k[x], \quad I \cap k[y], \quad I \cap k[z].$$

18.2 Cálculo de intersecciones

Ahora para dos ideales

$$I = (f_1, \ldots, f_r), \quad J = (g_1, \ldots, g_s) \subset k[x_1, \ldots, x_n]$$

la intersección puede ser calculada de la siguiente manera.

1) Para el ideal
$$tI + (1-t)J = (t f_1, \ldots, t f_r, (1-t) g_1, \ldots, (1-t) g_s) \subseteq k[t, x_1, \ldots, x_n]$$
se calcula una base de Gröbner G respecto al orden lexicográfico con $t \succ x_1 \succ \cdots \succ x_n$.

2) Luego, $G \cap k[x_1, \ldots, x_n]$ (es decir, los polinomios de G donde no aparece la variable t) será un conjunto de generadores para $I \cap J$.

18.4. Ejemplo. Consideremos los siguientes polinomios en el anillo $\mathbb{Q}[x, y, z]$:

$$\begin{aligned} f &= x^4 + x^3 y + x^3 z^2 - x^2 y^2 + x^2 y z^2 - x y^3 - x y^2 z^2 - y^3 z^2, \\ g &= x^4 + 2x^3 z^2 - x^2 y^2 + x^2 z^4 - 2x y^2 z^2 - y^2 z^4, \\ p &= x^2 + x y + x z + y z, \\ q &= x^2 - x y - x z + y z. \end{aligned}$$

Calculemos la intersección

$$(f, g) \cap (p, q).$$

Primero, tenemos que calcular una base de Gröbner para el ideal

$$(tf, tg, (1-t)\, p, (1-t)\, q)$$

respecto al orden lexicográfico con $t \succ x \succ y \succ z$.

```
i1 : R = QQ[t,x,y,z, MonomialOrder=>Lex];
i2 : f = x^4 + x^3*y + x^3*z^2 - x^2*y^2 + x^2*y*z^2 - x*y^3 - x*y^2*z^2 - y^3*z^2;
i3 : g = x^4 + 2*x^3*z^2 - x^2*y^2 + x^2*z^4 - 2*x*y^2*z^2 - y^2*z^4;
i4 : p = x^2 + x*y + x*z + y*z;
i5 : q = x^2 - x*y - x*z + y*z;

i6 : groebnerBasis (ideal (t*f, t*g, (1-t)*p, (1-t)*q))

o6 = | x3y-x3z2+x2yz2-x2z4-xy3+xy2z2-y3z2+y2z4 x4+2x3z2-x2y2+x2z4-2xy2z2-y2z4
     ---------------------------------------------------------------------------
     ty2z+tyz2-y2z-yz2 txy+txz-xy-xz tx2+tyz-x2-yz |

             1       5
o6 : Matrix R  <--- R
```

Entonces, la base de Gröbner que salió consiste en los polinomios

$$\begin{aligned} g_1 &= x^3 y - x^3 z^2 + x^2 y z^2 - x^2 z^4 - x y^3 + x y^2 z^2 - y^3 z^2 + y^2 z^4, \\ g_2 &= x^4 + 2x^3 z^2 - x^2 y^2 + x^2 z^4 - 2x y^2 z^2 - y^2 z^4, \\ g_3 &= t y^2 z + t y z^2 - y^2 z - y z^2, \\ g_4 &= t x y + t x z - x y - x z, \\ g_5 &= t x^2 + t y z - x^2 - y z. \end{aligned}$$

Quitando los polinomios g_3, g_4, g_5 donde aparece la variable t, podemos concluir que

$$(f,g) \cap (p,q) = (g_1, g_2).$$

En práctica, para calcular la intersección $I \cap J$ en Macaulay2, hay que usar la función `intersect(`I`,`J`)`.

```
i1 : R = QQ[x,y,z, MonomialOrder=>Lex];
i2 : f = x^4 + x^3*y + x^3*z^2 - x^2*y^2 + x^2*y*z^2 - x*y^3 - x*y^2*z^2 - y^3*z^2;
i3 : g = x^4 + 2*x^3*z^2 - x^2*y^2 + x^2*z^4 - 2*x*y^2*z^2 - y^2*z^4;
i4 : p = x^2 + x*y + x*z + y*z;
i5 : q = x^2 - x*y - x*z + y*z;

i6 : intersect (ideal (f,g), ideal (p,q))

               4    3     3 2    2 2    2   2      3      2 2    3 2
o6 = ideal (- x  - x y - x z  + x y  - x y*z  + x*y  + x*y z  + y z ,
     ------------------------------------------------------------------
        4     3 2    2 2    2 4       2 2    2 4
     - x  - 2x z  + x y  - x z  + 2x*y z  + y z )

o6 : Ideal of R
```

▲

Una aplicación curiosa de nuestro algoritmo de arriba es el cálculo del máximo común divisor y mínimo común múltiplo en $k[x_1,\dots,x_n]$. Recordemos que el anillo de polinomios es un dominio de factorización única, así que para cualesquiera $f,g \in k[x_1,\dots,x_n]$ existe el $\operatorname{mcm}(f,g)$, y por ende la intersección de ideales principales es siempre un ideal principal:

$$(f) \cap (g) = (h), \quad \text{donde } h = \operatorname{mcm}(f,g).$$

Luego, se tiene

$$\operatorname{mcd}(f,g) \cdot \operatorname{mcm}(f,g) = fg.$$

Entonces, si sabemos calcular las intersecciones de ideales, sabemos calcular el MCD y MCM, sin factorizar polinomios en $k[x_1,\dots,x_n]$, lo que es un problema mucho más sofisticado.

18.5. Ejemplo. Calculemos el máximo común divisor de los polinomios f y g de 18.4

```
i1 : R = QQ[t,x,y,z, MonomialOrder=>Lex];
i2 : f = x^4 + x^3*y + x^3*z^2 - x^2*y^2 + x^2*y*z^2 - x*y^3 - x*y^2*z^2 - y^3*z^2;
i3 : g = x^4 + 2*x^3*z^2 - x^2*y^2 + x^2*z^4 - 2*x*y^2*z^2 - y^2*z^4;
i4 : groebnerBasis (ideal (t*f, (1-t)*g))

o4 = | x5+x4y+2x4z2-x3y2+2x3yz2+x3z4-x2y3-2x2y2z2+x2yz4-2xy3z2-xy2z4-y3z4
     ------------------------------------------------------------------------
     tx3y-tx3z2+tx2yz2-tx2z4-txy3+txy2z2-ty3z2+ty2z4+x4+2x3z2-x2y2+x2z4-2xy2z2-y2z4
     ------------------------------------------------------------------------
     tx4+2tx3z2-tx2y2+tx2z4-2txy2z2-ty2z4-x4-2x3z2+x2y2-x2z4+2xy2z2+y2z4 |

             1       3
o4 : Matrix R  <--- R

i5 : h = oo_(0,0)
```

```
      5    4      4 2    3 2     3   2    3 4    2 3     2 2 2     2   4       3 2      2 4    3 4
o5 = x  + x y + 2x z  - x y  + 2x y*z  + x z  - x y  - 2x y z  +  x y*z  - 2x*y z  - x*y z  - y z

o5 : R

i6 : f*g//h

      3    2 2      2    2 2
o6 = x  + x z  - x*y  - y z

o6 : R
```

Aquí de nuevo, para calcular $(f)\cap(g)$, hemos calculado una base de Gröbner respecto al orden lexicográfico para $(tf,(1-t)g)\subset\mathbb{Q}[t,x,y,z]$ y tomamos el único polinomio de esta base donde no aparece t. Este es $h=\operatorname{mcm}(f,g)$, y luego $\operatorname{mcd}(f,g)=fg/h$.

En práctica, para calcular el mcd y mcm, hay que usar las funciones `gcd(`f`,`g`)` y `lcm(`f`,`g`)`.

```
i7 : gcd (f,g)

      3    2 2      2    2 2
o7 = x  + x z  - x*y  - y z
```

▲

Nuestro método para calcular el $\operatorname{mcd}(f,g)$ y $\operatorname{mcm}(f,g)$ construyendo bases de Gröbner respecto al orden lexicográfico no es eficaz y sirve solo para demostrar que algún algoritmo existe.

Parte II
Relación con geometría algebraica

Después de ver varios cálculos con ideales de polinomios, no estaría mal entender a qué sirve todo esto. En la segunda parte del curso vamos a revisar la relación entre los ideales en $k[x_1,\dots,x_n]$ y conjuntos algebraicos afines $X \subseteq \mathbb{A}^n(k)$, y luego hablaremos de dos temas importantes: **descomposición primaria** y **dimensión**.

19 Conjuntos algebraicos afines

19.1. Definición. Sea k un cuerpo. El conjunto k^n se llama el **espacio afín sobre** k **de dimensión** n y se denota por $\mathbb{A}^n(k)$.

Por el momento "dimensión n" son solamente palabras que hacen parte de la definición. El concepto de definición será definido en §22 y allí también veremos que $\dim \mathbb{A}^n(k) = n$.

19.2. Definición. Para un subconjunto $S \subseteq k[x_1,\dots,x_n]$ el conjunto de los ceros que tienen en común los polinomios en S se denota por

$$\mathbf{V}(S) := \{\underline{a} = (a_1,\dots,a_n) \in \mathbb{A}^n(k) \mid f(\underline{a}) = 0 \text{ para todo } f \in S\} \subseteq \mathbb{A}^n(k)$$

y se llama un **conjunto algebraico afín sobre** k.

A partir de ahora vamos decir simplemente "conjunto algebraico", omitiendo la palabra "afín" porque en nuestro curso todo será afín (a fin de cuentas, no es un curso de geometría algebraica).

Tenemos las siguientes propiedades.

1) Si $S \subseteq S'$, entonces $\mathbf{V}(S) \supseteq \mathbf{V}(S')$.
2) Si $I \subseteq k[x_1,\dots,x_n]$ es el ideal generado por S, entonces $\mathbf{V}(S) = \mathbf{V}(I)$.
3) Ya que todo ideal en $k[x_1,\dots,x_n]$ es finitamente generado, todo conjunto $\mathbf{V}(S)$ puede ser escrito como $\mathbf{V}(f_1,\dots,f_r)$ para una colección finita de polinomios $f_1,\dots,f_r \in k[x_1,\dots,x_n]$.
4) Se tiene $\mathbf{V}(0) = \mathbb{A}^n(k)$ y $\mathbf{V}(1) = \emptyset$.
5) $\mathbf{V}\left(\bigcup_j I_j\right) = \mathbf{V}\left(\sum_j I_j\right) = \bigcap_j \mathbf{V}(I_j)$.
6) $\mathbf{V}(I \cap J) = \mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

Las pruebas se dejan al lector. Las últimas tres propiedades significan que los conjuntos $\mathbf{V}(I)$ satisfacen los axiomas de conjuntos cerrados en un espacio topológico.

19.3. Definición. La topología sobre $\mathbb{A}^n(k)$ cuyos conjuntos cerrados son $\mathbf{V}(I)$ para ideales $I \subseteq k[x_1,\dots,x_n]$ se llama la **topología de Zariski**.

A partir de ahora $\mathbb{A}^n(k)$ se va a considerar como un espacio dotado de la topología de Zariski. Esta topología puede ser motivada de la siguiente manera: si $k = \mathbb{R}$ o $\mathbb{C}$, todo conjunto de la forma $\mathbf{V}(I)$ es cerrado en la topología analítica. Sin embargo, si tomamos solamente estos conjuntos como los cerrados, también vamos a tener muy pocos abiertos, y la topología de Zariski tiene varias propiedades raras; por ejemplo, casi nunca es Hausdorff. La topología de Zariski no es muy geométrica y su propósito es reflejar ciertos fenómenos algebraicos.

19.4. Ejemplo. Para todo punto $\underline{a} = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$, consideremos el homomorfismo de evaluación de polinomios en $\underline{a}$:

$$\begin{aligned} k[x_1, \dots, x_n] &\twoheadrightarrow k, \\ f &\mapsto f(\underline{a}). \end{aligned}$$

Notamos que el núcleo de este homomorfismo es precisamente el ideal

$$\mathfrak{m}_{\underline{a}} := (x_1 - a_1, \dots, x_n - a_n)$$

—en efecto, está claro que para $\underline{a} = (0, \dots, 0)$ el núcleo es el ideal $(x_1, \dots, x_n)$ formado por los polinomios sin término constante, y en general, se puede considerar el automorfismo

$$k[x_1, \dots, x_n] \xrightarrow{\cong} k[x_1, \dots, x_n], \quad x_i \mapsto x_i + a_i.$$

Además, $k[x_1, \dots, x_n]/\mathfrak{m}_{\underline{a}} \cong k$, así que el ideal $\mathfrak{m}_{\underline{a}}$ es maximal.

Tenemos $\mathbf{V}(\mathfrak{m}_{\underline{a}}) = \{\underline{a}\}$. Esto demuestra que todo punto del espacio afín es cerrado en la topología de Zariski, y por ende todos los subconjuntos finitos de $\mathbb{A}^n(k)$ son también cerrados. En particular, si $k = \mathbb{F}_q$ es un cuerpo finito, la topología sobre $\mathbb{A}^n(\mathbb{F}_q)$ es discreta[*].

Notamos que para todo ideal $I \subseteq k[x_1, \dots, x_n]$ se tiene

$$\underline{a} \in \mathbf{V}(I) \iff \mathfrak{m}_{\underline{a}} \supseteq I.$$

En efecto, $\underline{a} \in \mathbf{V}(I)$ si y solo si $f(\underline{a}) = 0$ para todo $f \in I$, si y solo si $I \subseteq \mathfrak{m}_{\underline{a}}$. ▲

19.5. Ejemplo. El anillo de polinomios $k[x]$ es un dominio de ideales principales, así que los conjuntos cerrados en $\mathbb{A}^1(k)$ son de la forma $\mathbf{V}(f)$ para algún polinomio $f \in k[x]$. Todo polinomio no nulo tiene un número finito de raíces, así que los conjuntos cerrados en $\mathbb{A}^1(k)$ son los subconjuntos finitos y todo $\mathbb{A}^1(k)$.

Notamos que si k es un cuerpo infinito, entonces para cada par de conjuntos abiertos no vacíos $U, V \subseteq \mathbb{A}^1(k)$ se tiene $U \cap V \neq \emptyset$, así que la topología sobre $\mathbb{A}^1(k)$ no es Hausdorff. ▲

Ejercicio 30. Describa la unión de los n ejes de coordenadas en $\mathbb{A}^n(k)$ como un conjunto algebraico.

Ejercicio 31. Demuestre que si k es un cuerpo infinito, entonces la topología de Zariski sobre $\mathbb{A}^2(k)$ es más fina que la topología producto sobre $\mathbb{A}^1(k) \times \mathbb{A}^1(k)$.

19.1 Ideal de polinomios que se anulan en un conjunto

19.6. Definición. Para cualquier subconjunto $X \subseteq \mathbb{A}^n(k)$ pongamos

$$\mathbf{I}(X) := \{f \in k[x_1, \dots, x_n] \mid f(\underline{a}) = 0 \text{ para todo } \underline{a} \in X\}.$$

Es fácil compobar que $\mathbf{I}(X)$ es un ideal en $k[x_1, \dots, x_n]$.

19.7. Proposición. *Los ideales $\mathbf{I}(X)$ satisfacen las siguientes propiedades.*

[*] Esto significa que la topología de Zariski es inútil para la geometría sobre cuerpos finitos.

1) *Si $X \subseteq Y$, entonces $\mathbf{I}(X) \supseteq \mathbf{I}(Y)$.*

2) $\mathbf{I}(X) = \bigcap_{\underline{a} \in X} \mathfrak{m}_{\underline{a}}$.

3) *El conjunto $\mathbf{VI}(X) = \overline{X}$ es la cerradura de X en la topología de Zariski.*

Demostración. La propiedad 1) se ve de la definición. Para 2), notamos que $f(\underline{a}) = 0$ si y solo si $f \in \mathfrak{m}_{\underline{a}}$. Para 3), tenemos claramente $X \subseteq \mathbf{VI}(X)$, donde $\mathbf{VI}(X)$ es un conjunto cerrado. Asumamos que $X \subseteq \mathbf{V}(I)$ para algún conjunto cerrado $\mathbf{V}(I)$. En este caso $f(\underline{a}) = 0$ para todo $f \in I$ y $\underline{a} \in X$, así que $I \subseteq \mathbf{I}(X)$, y luego $\mathbf{VI}(X) \subseteq \mathbf{V}(I)$. Entonces, $\mathbf{VI}(X)$ es el *mínimo* conjunto cerrado que contiene a X. ■

Recordemos la siguiente definición de álgebra conmutativa.

19.8. Definición. Para un ideal $I \subset A$ en un anillo conmutativo A el **radical** viene dado por

$$\sqrt{I} := \{f \in A \mid f^r \in I \text{ para algún } r = 1, 2, 3, \ldots\}.$$

Cuando se cumple $\sqrt{I} = I$, se dice que I es un **ideal radical**.

El radical satisface las siguientes propiedades.

19.9. Proposición. *Sean A cualquier anillo conmutativo e $I, J \subseteq A$ ideales.*

1) *$\sqrt{I}$ es un ideal que contiene a I.*

2) $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) *Todo ideal primo $\mathfrak{p} \in \operatorname{Spec} A$ es radical: se tiene $\sqrt{\mathfrak{p}} = \mathfrak{p}$.*

4) *El cociente A/I no tiene nilpotentes si y solo si I es un ideal radical.*

5) *Si $I \subseteq J$, entonces $\sqrt{I} \subseteq J$.*

6) $\sqrt{\bigcap_j I_j} = \bigcap_j \sqrt{I_j}$.

7) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

8) $\sqrt{I^n} = I$ *para todo* $n = 1, 2, 3, \ldots$

9) *Se tiene*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq I}} \mathfrak{p}.$$

Es fácil comprobar todas las propiedades. La propiedad menos obvia a partir de la definición 19.8 es 9), y para la prueba se puede consultar cualquier libro de álgebra conmutativa.

19.10. Proposición.

1) *Para cualquier ideal $I \subset k[X_1, \ldots, X_n]$ se tiene $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$.*

2) *Para cualquier subconjunto $X \subseteq \mathbb{A}^n(k)$ el ideal $\mathbf{I}(X)$ es radical: se tiene $\sqrt{\mathbf{I}(X)} = \mathbf{I}(X)$.*

3) *Se tiene $I(\emptyset) = k[x_1, \ldots, x_n]$.*

4) *Si k es un cuerpo infinito, entonces $I(\mathbb{A}^n) = 0$.*

Demostración. 1) y 2) se sigue de

$$f^r(\underline{a}) = 0 \text{ para } r = 1, 2, 3, \ldots \iff f(\underline{a}) = 0.$$

La parte 3) es obvia y 4) se deja como un ejercicio. ■

Ejercicio 32. Demuestre que si k es un cuerpo infinito, entonces $I(\mathbb{A}^n(k)) = 0$. ¿Por qué esto es falso para cuerpos finitos?

19.2 Morfismos de conjuntos algebraicos

Los conjuntos algebraicos están definidos por ecuaciones polinomiales, y es razonable definir morfismos entre conjuntos algebraicos como aplicaciones definidas por polinomios.

19.11. Definición. Sean $X \subseteq \mathbb{A}^m(k)$ e $Y \subseteq \mathbb{A}^n(k)$ conjuntos algebraicos. Un **morfismo** $f\colon X \to Y$ es una aplicación tal que existen polinomios $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$ tal que para todo $\underline{a} \in X$

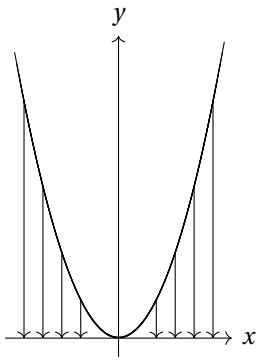
$$f(\underline{a}) = (f_1(\underline{a}), \ldots, f_n(\underline{a})).$$

Para tres conjuntos algebraicos $X \subseteq \mathbb{A}^\ell(k)$, $Y \subseteq \mathbb{A}^m(k)$, $Z \subseteq \mathbb{A}^n(k)$ y morfismos $f\colon X \to Y$, $g\colon X \to Z$ definidos por $f = (f_1, \ldots, f_m)$, $g = (g_1, \ldots, g_n)$, la composición $g \circ f$ es el morfismo $X \to Z$ definido por

$$g(f(\underline{a})) := (g_1(f_1(\underline{a}), \ldots, f_m(\underline{a})), \ldots, g_n(f_1(\underline{a}), \ldots, f_m(\underline{a}))).$$

Respecto a esta composición, los conjuntos algebraicos forman una categoría. Vamos a denotar el conjunto de morfismos $X \to Y$ por $\mathrm{Mor}(X, Y)$.

19.12. Ejemplo. Consideremos la parabola $\mathbf{V}(y - x^2) \subset \mathbb{A}^2(k)$. La proyección al eje x definida por $(x, y) \mapsto x$ define un morfismo $f\colon \mathbf{V}(y - x^2) \to \mathbb{A}^1(k)$. Se ve que este posee una aplicación inversa $f^{-1}\colon x \mapsto (x, x^2)$ que es también un morfismo de conjuntos algebraicos. Entonces, la parábola y la recta son isomorfas en la categoría de conjuntos algebraicos.

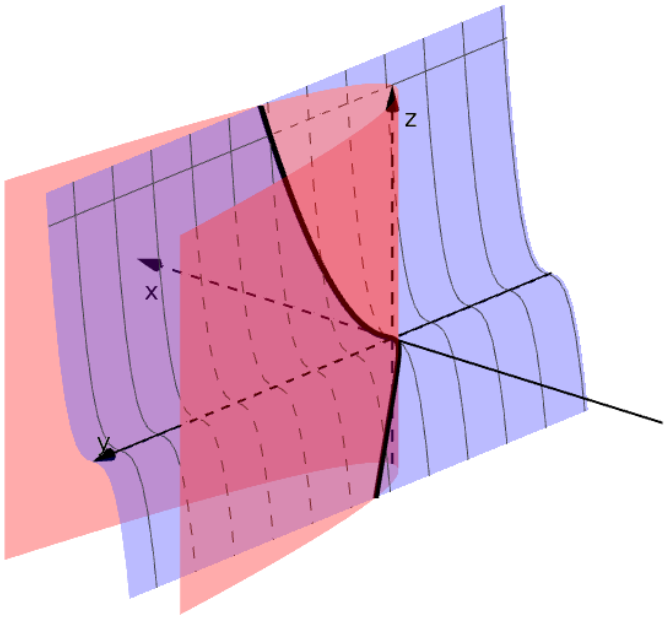


▲

19.13. Ejemplo. Otro ejemplo similar nos da la **cúbica torcida**

$$\mathbf{V}(x^2 - y, x^3 - z) = \mathbf{V}(x^2 - y) \cap \mathbf{V}(x^3 - z) \subset \mathbb{A}^3(k).$$

La aplicación $t \mapsto (t, t^2, t^3)$ es un isomorfismo entre la recta afín $\mathbb{A}^1(k)$ y $\mathbf{V}(x^2 - y, x^3 - z)$. ▲



19.14. Proposición. *Todo morfismo de conjuntos algebraicos $f\colon X \to Y$ es continuo respecto a la topología de Zariski.*

Demostración. Si $X \subseteq \mathbb{A}^m(k)$ e $Y \subseteq \mathbb{A}^n(k)$, entonces f está definido por polinomios $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$. Luego, f define un homomorfismo de k-álgebras

$$f^*\colon k[x_1', \ldots, x_n'] \to k[x_1, \ldots, x_m],$$
$$x_i' \mapsto f_i.$$

Para todo subconjunto cerrado $\mathbf{V}(I) \subseteq Y$ que corresponde a un ideal $I \subseteq k[x_1, \ldots, x_n]$ la preimagen es también cerrada:

$$f^{-1}(\mathbf{V}(I)) = \{\underline{a} \in X \mid f(\underline{a}) \in \mathbf{V}(I)\} = \{\underline{a} \in X \mid g(f(\underline{a})) = f^*(g)(\underline{a}) = 0 \text{ para todo } g \in I\} = \mathbf{V}(f^*(I)). \qquad \blacksquare$$

19.15. Ejemplo. La aplicación $\exp\colon \mathbb{A}^1(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$ no es un morfismo de conjuntos algebraicos: para el punto $1 \in \mathbb{A}^1(\mathbb{C})$ se tiene $\exp^{-1}(1) = \{2\pi i k \mid k \in \mathbb{Z}\}$ que es un subconjunto infinito de $\mathbb{A}^1(\mathbb{C})$ y por ende no es cerrado. ▲

Para un conjunto algebraico $X \subseteq \mathbb{A}^n(k)$ los morfismos $X \to \mathbb{A}^1(k)$ forman una k-álgebra. En efecto, cada uno de estos morfismos está definido por un polinomio $f \in k[x_1, \ldots, x_n]$, y los polinomios pueden ser sumados y multiplicados:

$$(f+g)(\underline{a}) := f(\underline{a}) + g(\underline{a}), \quad (cf)(\underline{a}) := c\, f(\underline{a}), \quad (fg)(\underline{a}) := f(\underline{a})\, g(\underline{a})$$

para $f, g \in k[x_1, \ldots, x_n]$, $c \in k$, $\underline{a} \in X$.

Dos diferentes polinomios $f, g \in k[x_1, \ldots, x_n]$ definen la misma aplicación sobre X si y solo si $f(\underline{a}) = g(\underline{a})$ para todo $\underline{a} \in X$; es decir, si y solo si $f - g \in \mathbf{I}(X)$. Se sigue que hay un isomorfismo natural de k-álgebras

$$\mathrm{Mor}(X, \mathbb{A}^1(k)) \cong k[x_1, \ldots, x_n]/\mathbf{I}(X).$$

19.16. Definición. Para un conjunto algebraico $X \subseteq \mathbb{A}^n(k)$ la k-álgebra

$$\Gamma(X) := \mathrm{Mor}(X, \mathbb{A}^1(k)) \cong k[x_1, \ldots, x_n]/\mathbf{I}(X)$$

se llama el **álgebra de las funciones polinomiales sobre** X, o también el **anillo de coordenadas de** X.

Ejercicio 33. Demuestre que si $X \subset \mathbb{A}^n(k)$ es un conjunto finito, entonces

$$\dim_k \Gamma(X) = |X|.$$

19.17. Proposición. *Para cualquier conjunto algebraico X la k-álgebra $\Gamma(X)$ es finitamente generada y reducida.*

Demostración. Recordemos que A es una **k-álgebra finitamente generada** si y solo si $A \cong k[x_1,\dots,x_n]/I$ para algún n y algún ideal $I \subseteq k[x_1,\dots,x_n]$.

Un anillo A es **reducido** si este no tiene nilpotentes no triviales: si $f^n = 0$ para algún $f \in A$ y $n = 1,2,3,\dots$, entonces $f = 0$. La k-álgebra $\Gamma(X) \cong k[x_1,\dots,x_n]/\mathbf{I}(X)$ es reducida, puesto que el ideal $\mathbf{I}(X)$ es radical. ■

Se ve que un morfismo de conjuntos algebraicos $f\colon X \to Y$ induce un homomorfismo de k-álgebras

$$f^*\colon \Gamma(Y) \to \Gamma(X),$$
$$(Y \xrightarrow{\phi} \mathbb{A}^1(k)) \mapsto (X \xrightarrow{f} Y \xrightarrow{\phi} \mathbb{A}^1(k)),$$

así que se trata de un funtor contravariante entre los conjuntos algebraicos sobre k y k-álgebras finitamente generadas reducidas:

$$(\textbf{conjuntos algebraicos sobre } k)^{\mathrm{op}} \to k\textbf{-álgebras finitamente generadas reducidas}.$$

19.18. Proposición. *El funtor Γ es fielmente pleno: para cualesquiera $X \subseteq \mathbb{A}^m(k)$, $Y \subseteq \mathbb{A}^n(k)$ la aplicación*

$$\mathrm{Mor}(X,Y) \xrightarrow{\cong} \mathrm{Hom}(\Gamma(Y),\Gamma(X)),$$
$$f \mapsto f^*$$

es una biyección entre los morfismos $X \to Y$ y homomorfismos de k-álgebras $\Gamma(Y) \to \Gamma(X)$.

Demostración. Podemos definir una aplicación inversa. Todo homomorfismo de k-álgebras $\phi\colon \Gamma(Y) \to \Gamma(X)$ puede ser levantado a un homomorfismo $\widetilde{\phi}\colon k[x'_1,\dots,x'_n] \to k[x_1,\dots,x_m]$:

$$\begin{array}{ccc} k[x'_1,\dots,x'_n] & \overset{\widetilde{\phi}}{\dashrightarrow} & k[x_1,\dots,x_m] \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ \Gamma(Y) & \xrightarrow{\quad\phi\quad} & \Gamma(X) \end{array}$$

Este $\widetilde{\phi}$ define un morfismo $f\colon X \to Y$ mediante

$$f(\underline{x}) := (\widetilde{\phi}(x'_1)(\underline{x}),\dots,\widetilde{\phi}(x'_n)(\underline{x})).$$

Notamos que diferentes levantamientos de ϕ a $\widetilde{\phi}$ definen el mismo morfismo f. La aplicación $\phi \mapsto f$ es inversa a $f \mapsto f^*$. ■

19.19. Comentario. En general, Γ *no es* una equivalencia de categorías: este funtor no es esencialmente sobreyectivo. Por ejemplo, si $k = \mathbb{R}$, entonces $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$ es una $\mathbb{R}$-álgebra finitamente generada reducida. Sin embargo, si X es un conjunto algebraico sobre $\mathbb{R}$, entonces un morfismo $f\colon X \to \mathbb{A}^1(\mathbb{R})$ no puede cumplir $f^2 = -1$, mientras que en $\mathbb{C}$ hay la unidad imaginaria con esta propiedad.

Ejercicio 34. Demuestre que si k es un cuerpo algebraicamente cerrado y $\mathrm{char}\, k \neq 2$, entonces la hipérbola $\mathbf{V}(xy-1)$ y la parábola $\mathbf{V}(y-x^2)$ son isomorfas. ¿Qué sucede si $\mathrm{char}\, k = 2$?

Ejercicio 35. Sea $k = \overline{\mathbb{F}_p}$, la cerradura algebraica de un cuerpo finito $\mathbb{F}_q$. Demuestre que la aplicación

$$F\colon (x_1, \ldots, x_n) \mapsto (x_1^p, \ldots, x_n^p)$$

es un morfismo biyectivo $\mathbb{A}^n(\overline{\mathbb{F}_p}) \to \mathbb{A}^n(\overline{\mathbb{F}_p})$, pero no es un isomorfismo.

Ejercicio 36. Sea k un cuerpo algebraicamente cerrado.

a) Para $\operatorname{char} k \neq 2$ consideremos los siguientes conjuntos algebraicos en $\mathbb{A}^2(k)$:

$$Z_1 := \mathbf{V}(u(t-1)-1), \quad Z_2 := \mathbf{V}(y^2 - x^2(x+1)).$$

Demuestre que el morfismo $Z_1 \to Z_2$, $(t,u) \mapsto (t^2-1, t(t^2-1))$ es biyectivo, pero no es un isomorfismo. Demuestre que en general, $Z_1 \ncong Z_2$.

b) Demuestre que el morfismo $\mathbb{A}^1(k) \to \mathbf{V}(y^2 - x^3) \subset \mathbb{A}^2(k)$, $t \mapsto (t^2, t^3)$ es biyectivo, pero no es un isomorfismo. Demuestre que en general, $\mathbb{A}^1(k) \ncong \mathbf{V}(y^2 - x^3)$.

Sugerencia: demuestre que $\Gamma(Z_1) \ncong \Gamma(Z_2)$ y $\Gamma(\mathbf{V}(y^2 - x^3)) \ncong k[t]$.

19.3 Teorema de los ceros

En esta sección vamos a recordar brevemente el teorema de los ceros.

19.20. Definición. Se dice que A es un **anillo de Jacobson** si todo ideal primo en A es una intersección de ideales maximales. En otras palabras, para todo $\mathfrak{p} \in \operatorname{Spec} A$ se tiene

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \in \operatorname{Specm} A \\ \mathfrak{m} \supseteq \mathfrak{p}}} \mathfrak{m}.$$

19.21. Ejemplo. Todo cuerpo es trivialmente un anillo de Jacobson: su único ideal propio es (0). ▲

19.22. Ejemplo. Si A es un dominio de ideales principales, entonces los ideales primos en A son de la forma (0) o (p), donde $p \in A$ es primo. Todo ideal primo no nulo es maximal. Ahora si se cumple

$$(0) = \bigcap_{p \in A \text{ primo}} (p),$$

entonces A es un anillo de Jacobson. Esto sucede si y solamente si en A hay un número infinito de primos. Por ejemplo, $\mathbb{Z}$ y el anillo de polinomios en una variable $k[x]$ son anillos de Jacobson. ▲

El resultado principal, que no vamos a probar aquí[*], es el siguiente.

19.23. Teorema. *Sea R un anillo de Jacobson y A una R-álgebra finitamente generada. Entonces,*

1) *A es también un anillo de Jacobson;*
2) *si $\mathfrak{m} \subset A$ es un ideal maximal, entonces $R \cap \mathfrak{m}$ es un ideal maximal en R y el cuerpo $A/\mathfrak{m}$ es una extensión finita de $R/(R \cap \mathfrak{m})$.*

19.24. Corolario. *Si A es una k-álgebra finitamente generada y $\mathfrak{m} \subset A$ es un ideal maximal, entonces $A/\mathfrak{m}$ es una extensión finita de k. En particular, si k es un cuerpo algebraicamente cerrado, entonces $A/\mathfrak{m} \cong k$ para todo ideal maximal $\mathfrak{m} \subset A$.*

[*] Lo probamos en el curso de álgebra conmutativa.

19.25. Corolario. *Sea k un cuerpo y $\phi\colon A \to B$ un homomorfismo de k-álgebras finitamente generadas. Si $\mathfrak{m} \subset B$ es un ideal maximal, entonces $\phi^{-1}(\mathfrak{m}) \subset A$ es también un ideal maximal.*

Demostración. El homomorfismo inducido $A/\phi^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$ nos permite identificar $A/\phi^{-1}(\mathfrak{m})$ con un subanillo del cuerpo $B/\mathfrak{m}$. Tenemos entonces

$$k \subseteq A/\phi^{-1}(\mathfrak{m}) \subseteq B/\mathfrak{m},$$

donde $B/\mathfrak{m}$ es una extensión finita de k. Esto implica que $A/\phi^{-1}(\mathfrak{m})$ es un cuerpo, gracias al lema de abajo. ■

19.26. Lema. *Sea L/k una extensión algebraica de cuerpos. Entonces, toda k-subálgebra $A \subseteq L$ es también un cuerpo.*

Demostración. Todo elemento no nulo $f \in A \subseteq L$ es algebraico sobre k, así que hay una relación algebraica no trivial

$$a_n f^n + a_{n-1} f^{n-1} + \cdots + a_1 f + a_0 = 0$$

para algunos $a_0, a_1, \ldots, a_n \in k$, donde sin pérdida de generalidad $a_0 \neq 0$. Luego,

$$a_0 = -f\,(a_n f^{n-1} + a_{n-1} f^{n-2} + \cdots + a_1),$$

así que

$$f^{-1} = -a_0^{-1}\,(a_n f^{n-1} + a_{n-1} f^{n-2} + \cdots + a_1),$$

y f es invertible en A. ■

Gracias al corolario 19.25, el espectro maximal nos da un funtor contravariante

$$(k\textbf{-álgebras finitamente generadas})^{\mathrm{op}} \to \textbf{conjuntos}.$$

A saber, un homomorfismo $\phi\colon A \to B$ induce de manera funtorial una aplicación

$$\begin{aligned} \phi^*\colon \operatorname{Specm} B &\to \operatorname{Specm} A, \\ \mathfrak{m} &\mapsto \phi^{-1}(\mathfrak{m}). \end{aligned}$$

19.27. Comentario. En general, la preimagen de un ideal maximal es un ideal primo, pero no necesariamente maximal. Considere por ejemplo la inclusión $\mathbb{Z} \hookrightarrow \mathbb{Q}$ y el ideal maximal $(0) \subset \mathbb{Q}$. Por este motivo en general hay que trabajar con el espectro $\operatorname{Spec} A$ y no solamente con el espectro maximal $\operatorname{Specm} A$.

19.28. Corolario. *Sea k un cuerpo algebraicamente cerrado.*

1) *Todo ideal maximal en $k[x_1, \ldots, x_n]$ es de la forma $\mathfrak{m}_{\underline{a}} = (x_1 - a_1, \ldots, x_n - a_n)$ para algún $\underline{x} \in \mathbb{A}^n(k)$, lo que nos da una biyección natural*

$$\begin{aligned} \mathbb{A}^n(k) &\cong \operatorname{Specm} k[x_1, \ldots, x_n], \\ \underline{a} &\mapsto \mathfrak{m}_{\underline{a}}, \\ \mathbf{V}(\mathfrak{m}) &\hookleftarrow \mathfrak{m}. \end{aligned}$$

2) *Para cualquier conjunto algebraico $X \subseteq \mathbb{A}^n(k)$ existe una biyección natural*

$$X \cong \operatorname{Specm} \Gamma(X).$$

Demostración. En la parte 1), ya hemos notado que para todo punto $\underline{a} \in \mathbb{A}^n(k)$ se cumple $\mathbf{V}(\mathfrak{m}_{\underline{a}}) = \underline{a}$. Esto no requiere que el cuerpo base k sea algebraicamente cerrado. Ahora para un ideal maximal $\mathfrak{m} \subset k[x_1,\dots,x_n]$ podemos cpnsiderar el homomorfismo canónico

$$\phi\colon k[x_1,\dots,x_n] \twoheadrightarrow k[x_1,\dots,x_n]/\mathfrak{m} \xrightarrow{\cong} k.$$

Aquí la última flecha es un isomorfismo, *dado que k es algebraicamente cerrado*. Denotemos por $a_i \in k$ la imagen de x_i. Para $\underline{a} = (a_1,\dots,a_n)$ tenemos $\mathfrak{m}_{\underline{a}} \subseteq \ker\phi = \mathfrak{m}$. Luego, por la maximalidad de $\mathfrak{m}_{\underline{a}}$, podemos concluir que $\mathfrak{m} = \mathfrak{m}_{\underline{a}}$.

Ahora si $X \subseteq \mathbb{A}^n(k)$ es un conjunto algebraico, entonces $\underline{a} \in X$ si y solo si $\mathbf{I}(X) \subseteq \mathfrak{m}_{\underline{a}}$. Tales ideales maximales corresponden a los ideales maximales en $k[x_1,\dots,x_n]/\mathbf{I}(X) \cong \Gamma(X)$. Esto nos da la biyección en la parte 2).

Dejo al lector verificar la naturalidad. ■

Los ideales $\mathfrak{m}_{\underline{a}} := (x_1 - a_1,\dots,x_n - a_n)$ son maximales en cualquier caso, pero cuando k no es algebraicamente cerrado, habrá ideales maximales que no tienen esta forma, como por ejemplo el ideal $(x^2+1) \subset \mathbb{R}[x]$.

La biyección $\operatorname{Specm} k[x_1,\dots,x_n]/\mathbf{I}(X) \cong X$ nos sugiere considerar la siguiente topología sobre el espectro maximal: los conjuntos cerrados en X son precisamente $\mathbf{V}(I)$ para los ideales $I \supseteq \mathbf{I}(X)$, así que podemos declarar que los subconjuntos cerrados en $\operatorname{Specm} k[x_1,\dots,x_n]/\mathbf{I}(X)$ son

$$\mathbf{V}(I) := \{\mathfrak{m} \in \operatorname{Specm} k[x_1,\dots,x_n]/\mathbf{I}(X) \mid \mathfrak{m} \supseteq I\} \quad \text{para } I \subseteq k[x_1,\dots,x_n]/\mathbf{I}(X). \tag{19.1}$$

19.29. Proposición. *Sea $I \subseteq k[x_1,\dots,x_n]$ un ideal.*

1) *Se tiene $\sqrt{I} \subseteq \mathbf{IV}(I)$.*
2) *Si k es un cuerpo algebraicamente cerrado, entonces $\mathbf{IV}(I) = \sqrt{I}$.*

Demostración. La parte 1) puede ser vista directamente sin ningún problema. He aquí una explicación complicada: se tiene

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} k[x_1,\dots,x_n] \\ \mathfrak{p} \supseteq I}} \mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \in \operatorname{Specm} k[x_1,\dots,x_n] \\ \mathfrak{m} \supseteq I}} \mathfrak{m} \subseteq \bigcap_{\underline{a} \in \mathbf{V}(I)} \mathfrak{m}_{\underline{a}} = \mathbf{IV}(I).$$

Aquí la segunda igualdad usa el hecho de que $k[x_1,\dots,x_n]$ es un anillo de Jacobson, así que todo ideal primo es una intersección de ideales maximales. Si k es algebraicamente cerrado, entonces todos los ideales maximales en $k[x_1,\dots,x_n]$ son de la forma $\mathfrak{m}_{\underline{a}}$ para $\underline{a} \in \mathbb{A}^n(k)$ y la inclusión "$\subseteq$" de arriba es una igualdad, lo que demuestra la parte 2). ■

Si k no es algebraicamente cerrado, entonces el ideal $\mathbf{IV}(I)$ puede ser más grande que $\sqrt{I}$. Por ejemplo, para $(x^2+1) \subset \mathbb{R}[x]$ se tiene $\mathbf{IV}(x^2+1) = \mathbf{I}(\emptyset) = \mathbb{R}[x]$.

19.30. Corolario. *Si k es un cuerpo algebraicamente cerrado, entonces la categoría de conjuntos algebraicos sobre k es antiequivalente a la categoría de k-álgebras finitamente generadas.*

Demostración. Hemos probado en 19.18 que el funtor contravariante Γ es fielmente pleno. Gracias al teorema de los ceros, es también esencialmente sobreyectivo: una k-álgebra finitamente generada reducida es isomorfa a $k[x_1,\dots,x_n]/I$ para un ideal radical I, y luego

$$\Gamma(\mathbf{V}(I)) \cong k[x_1,\dots,x_n]/\mathbf{IV}(I) \cong k[x_1,\dots,x_n]/I.$$ ■

Ejercicio 37. Para dos conjuntos algebraicos $X \subseteq \mathbb{A}^m(k)$ e $Y \subseteq \mathbb{A}^n(k)$, demuestre que $X \times Y \subseteq \mathbb{A}^{m+n}(k)$ es un conjunto algebraico, y es precisamente el producto de X e Y en el sentido categórico. Demuestre que si k es un cuerpo algebraicamente cerrado, entonces

$$\Gamma(X \times Y) \cong \Gamma(X) \otimes_k \Gamma(Y).$$

19.31. Teorema. *Si k es un cuerpo algebraicamente cerrado, entonces existe una biyección*

$$\begin{array}{ccc} \{\textit{ideales radicales } I \subseteq k[x_1,\dots,x_n]\} & \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} & \{\textit{subconjuntos cerrados } Y \subseteq \mathbb{A}^n(k)\} \\ \uparrow & & \uparrow \\ \operatorname{Specm} k[x_1,\dots,x_n] & \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} & \{\textit{puntos } \underline{a} \in \mathbb{A}^n(k)\} \end{array}$$

Demostración. Si $Y \subseteq \mathbb{A}^n(k)$ es un subconjunto cerrado, entonces

$$\mathbf{VI}(Y) = \overline{Y} = Y.$$

Esto se cumple para cualquier k, no necesariamente algebraicamente cerrado. Ahora si k es algebraicamente cerrado e $I \subseteq k[x_1,\dots,x_n]$ es un ideal radical, entonces

$$\mathbf{IV}(I) = \sqrt{I} = I.$$ ■

20 Ideales primos y componentes irreducibles

Recordemos un par de definiciones de topología general.

20.1. Definición. Se dice que un espacio topológico X es **irreducible** si

1) X no es vacío;
2) X no puede ser representado como una unión $Z_1 \cup Z_2$ donde Z_1, Z_2 son conjuntos cerrados propios.

Un subconjunto $Z \subseteq X$ es **irreducible** si es irreducible como un espacio con la topología inducida.

He aquí otra noción relacionada.

20.2. Definición. Se dice que un espacio topológico X es **conexo** si

1) X no es vacío;
2) X no puede ser representado como una unión $Z_1 \cup Z_2$ donde Z_1, Z_2 son conjuntos cerrados propios y $Z_1 \cap Z_2 = \emptyset$.

(Notamos que en 2) los conjuntos Z_1 y Z_2 son también abiertos.)

En particular, todo espacio irreducible es necesariamente conexo. Sin embargo, la irreducibilidad es una propiedad mucho más fuerte.

20.3. Proposición. *Las siguientes condiciones son equivalentes.*

1) X es irreducible.
2) Si $U, V \subseteq X$ son subconjuntos abiertos no vacíos, entonces $U \cap V \neq \emptyset$.
3) Todo subconjunto abierto no vacío $U \subseteq X$ es denso: se tiene $\overline{U} = X$.
4) Todo subconjunto abierto no vacío $U \subseteq X$ es conexo.
5) Todo subconjunto abierto no vacío $U \subseteq X$ es irreducible.

Demostración. Ejercicio para el lector. ■

20.4. Comentario. Ya que en un espacio irreducible $U \cap V \neq \emptyset$ para cualesquiera $U, V \subseteq X$ abiertos no vacíos, el axioma de Hausdorff nunca se cumple, salvo el caso trivial cuando X consiste en un punto. Por esto el concepto de irreducibilidad no se ve mucho en la geometría habitual.

20.5. Proposición. *Sea X un espacio topológico. Un subconjunto $Y \subseteq X$ es irreducible si y solo si su cerradura $\overline{Y}$ es irreducible.*

Demostración. Asumamos que $\overline{Y}$ es irreducible. En particular, $\overline{Y} \neq \emptyset$ y por lo tanto $Y \neq \emptyset$. Supongamos que $Z_1, Z_2 \subseteq X$ son dos conjuntos cerrados tales que $Y = (Y \cap Z_1) \cup (Y \cap Z_2)$. Luego, tomando las cerraduras en X, se obtiene

$$\overline{Y} = \overline{(Y \cap Z_1)} \cup \overline{(Y \cap Z_2)}.$$

Por la irreducibilidad de $\overline{Y}$, tenemos

$$Y \subseteq \overline{Y} = \overline{Y \cap Z_1} \subseteq Z_1 \quad \text{o} \quad Y \subseteq \overline{Y} = \overline{Y \cap Z_2} \subseteq Z_2,$$

y luego

$$Y \subseteq Y \cap Z_1 \quad \text{o} \quad Y \subseteq Y \cap Z_2.$$

Esto significa que Y es irreducible.

Ahora asumamos que Y es irreducible y $\overline{Y} = Z_1 \cup Z_2$, donde Z_1, Z_2 son cerrados en $\overline{Y}$. Luego,

$$Y = (Y \cap Z_1) \cup (Y \cap Z_1),$$

y por la irreducibilidad de Y se tiene $Y = Y \cap Z_1$ o $Y = Y \cap Z_2$. Entonces, $\overline{Y} \subseteq Z_1$ o $\overline{Y} \subseteq Z_2$. ■

20.6. Definición. Sea X un espacio topológico. Un subconjunto irreducible de X maximal respecto a la inclusión se llama una **componente irreducible** de X.

20.7. Proposición. *Las componentes irreducibles son cerradas.*

Demostración. Si $Y \subseteq X$ es irreducible, entonces $\overline{Y} \supseteq Y$ es también irreducible. Por maximalidad de Y, se tiene $\overline{Y} = Y$. ■

20.8. Proposición. *Sea X un espacio topológico. Todo subconjunto irreducible de X está contenido en una componente irreducible. En particular, todo punto de X está contenido en alguna componente irreducible y X es la unión* [*] *de sus componentes irreducibles.*

Demostración. Se sigue del lema de Zorn. Sea $Z \subseteq X$ un subconjunto irreducible. Para toda cadena

$$Z \subseteq Z_1 \subseteq Z_2 \subseteq Z_3 \subseteq \cdots \subset X$$

de subconjuntos irreducibles la unión $\bigcup_i Z_i$ es también irreducible. Entonces, existe un conjunto irreducible maximal que contiene a Z. ■

20.9. Teorema. *Sea k un cuerpo.*

1) *Si $Z \subseteq \mathbb{A}^n(k)$ es un subconjunto cerrado irreducible, entonces el ideal $\mathbf{I}(Z)$ es primo.*
2) *Si k es algebraicamente cerrado y $\mathfrak{p} \subset k[x_1, \ldots, x_n]$ es un ideal primo, entonces $\mathbf{V}(\mathfrak{p}) \subseteq \mathbb{A}^n(k)$ es irreducible. En particular, $\mathbb{A}^n(k) = \mathbf{V}(0)$ es irreducible.*

[*] ¡No necesariamente disjunta! No confundir con la situación con componentes *conexas* que son disjuntas.

Demostración. Sea $Z = \mathbf{V}(I)$ para algún ideal $I \subset k[x_1, \ldots, x_n]$. Primero, notamos que $\mathbf{V}(I) \neq \emptyset$ implica que $\mathbf{IV}(I) \neq k[x_1, \ldots, x_n]$. Asumamos que $\mathbf{V}(I)$ es irreducible y $fg \in \mathbf{IV}(I)$. Luego,

$$\mathbf{V}(I) = \mathbf{VIV}(I) \subseteq \mathbf{V}(fg) = \mathbf{V}(f) \cup \mathbf{V}(g)$$

y por ende

$$\mathbf{V}(I) = (\mathbf{V}(I) \cap \mathbf{V}(f)) \cup (\mathbf{V}(I) \cap \mathbf{V}(g)).$$

Por la irreducibilidad se tiene $\mathbf{V}(I) \subseteq \mathbf{V}(f)$ o $\mathbf{V}(I) \subseteq \mathbf{V}(g)$. Por ejemplo, en el primer caso,

$$f \in \sqrt{(f)} \subseteq \mathbf{IV}(f) \subseteq \mathbf{IV}(I).$$

De la misma manera, en el segundo caso $g \in \mathbf{IV}(I)$. Esto demuestra que el ideal $\mathbf{IV}(I)$ es primo.

Ahora asumamos que k es algebraicamente cerrado. Sea $\mathfrak{p}$ un ideal primo. Supongamos que

$$\mathbf{V}(\mathfrak{p}) = \mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(IJ),$$

donde $\mathbf{V}(I)$ y $\mathbf{V}(J)$ son dos subconjuntos cerrados de $\mathbf{V}(\mathfrak{p})$. Luego, aplicando la operación $\mathbf{I}$, se obtiene

$$\mathfrak{p} = \mathbf{IV}(\mathfrak{p}) = \mathbf{IV}(IJ) = \sqrt{IJ} \supseteq IJ.$$

Dado que $\mathfrak{p}$ es primo, esto implica $I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$, y por lo tanto $\mathbf{V}(\mathfrak{p}) = \mathbf{V}(I)$ o $\mathbf{V}(\mathfrak{p}) = \mathbf{V}(J)$. ■

Cuando el cuerpo base k no es algebraicamente cerrado, para un ideal primo $\mathfrak{p} \subset k[x_1, \ldots, x_n]$ el conjunto correspondiente $\mathbf{V}(\mathfrak{p})$ no es necesariamente irreducible. He aquí algunos ejemplos.

1) El conjunto $\mathbf{V}(\mathfrak{p})$ puede ser vacío, como en el caso de $(x^2 + 1) \subset \mathbb{R}[x]$.

2) El polinomio $x^2 + y^2\,(y-1)^2$ es irreducible en $\mathbb{R}[x, y]$, y entonces genera un ideal primo, pero

$$\mathbf{V}(x^2 + y^2\,(y-1)^2) = \{(0,0), (0,1)\}.$$

3) Si $k = \mathbb{F}_q$ es un cuerpo finito, al ideal primo $(0) \subset \mathbb{F}_q[x_1, \ldots, x_n]$ corresponde el espacio $\mathbb{A}^n(\mathbb{F}_q)$ que es reducible, siendo la unión de un número finito de puntos.

20.10. Corolario. *Sea k es un cuerpo algebraicamente cerrado.*

1) Existe una biyección natural

$$\begin{array}{ccc} \operatorname{Spec} k[x_1, \ldots, x_n] & \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} & \{\textit{subconjuntos cerrados irreducibles } X \subseteq \mathbb{A}^n(k)\} \\ \uparrow & & \uparrow \\ \operatorname{Specm} k[x_1, \ldots, x_n] & \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} & \{\textit{puntos } \underline{a} \in \mathbb{A}^n(k)\} \end{array}$$

2) Para cualquier conjunto algebraico $X \subseteq \mathbb{A}^n(k)$ existe una biyección natural

$$\begin{array}{ccc} \operatorname{Spec} \Gamma(X) & \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} & \{\textit{subconjuntos cerrados irreducibles } Y \subseteq X\} \\ \uparrow & & \uparrow \\ \operatorname{Specm} \Gamma(X) & \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} & \{\textit{puntos } \underline{a} \in X\} \end{array}$$

Demostración. Se sigue de las identidades $\mathbf{IV}(\mathfrak{p}) = \mathfrak{p}$ y $\mathbf{VI}(X) = X$. ■

Si k no es algebraicamente cerrado, entonces diferentes ideales primos pueden corresponder al mismo subconjunto cerrado irreducible. Por ejemplo, si $k = \mathbb{R}$, entonces

$$\mathbf{V}(x, y) = \mathbf{V}(x^2 + y^2) = \{(0, 0)\}.$$

20.11. Digresión. La topología de (19.1) motiva la siguiente definición general: para cualquier anillo conmutativo A los subconjuntos cerrados de $\operatorname{Spec} A$ son

$$\mathbf{V}(I) := \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supseteq I\} \quad \text{para ideales } I \subseteq A.$$

Esto define una topología sobre $\operatorname{Spec} A$ que también se conoce como la **topología de Zariski**. Este es el punto de partida en la definición del **esquema afín**. Aquí se considera el espectro y no solamente el espectro maximal porque un homomorfismo $\phi\colon A \to B$ induce una aplicación continua

$$\begin{aligned} \phi^*\colon \operatorname{Spec} B &\to \operatorname{Spec} A, \\ \mathfrak{p} &\mapsto \phi^{-1}(\mathfrak{p}). \end{aligned}$$

Para los anillos conmutativos en general, la preimagen de un ideal maximal no tiene por qué ser maximal.

20.12. Corolario. *Sea k es un cuerpo algebraicamente cerrado. Las componentes irreducibles de un conjunto algebraico $\mathbf{V}(I)$ corresponden a los ideales primos **minimales** que contienen al ideal I.*

Demostración. Las operaciones $\mathbf{I}$ y $\mathbf{V}$ invierten las inclusiones, así que los conjuntos irreducibles maximales $\mathbf{V}(\mathfrak{p}) \subseteq \mathbf{V}(I)$ corresponden a los ideales primos minimales $\mathfrak{p} = \mathbf{IV}(\mathfrak{p}) \supseteq \mathbf{IV}(I) = \sqrt{I} \supseteq I$. ■

20.13. Ejemplo. El conjunto algebraico $\mathbf{V}(xy) \subset \mathbb{A}^2(k)$ es reducible: el ideal $\mathbf{IV}(xy) = (xy)$ no es primo, sino es la intersección de dos ideales primos (x) e (y). Tenemos $\mathbf{V}(xy) = \mathbf{V}(x) \cup \mathbf{V}(y)$. Los ideales (x) e (y) son minimales en el siguiente sentido: por ejemplo, si $(xy) \subseteq \mathfrak{p} \subseteq (x)$ para un ideal primo $\mathfrak{p}$, entonces $\mathfrak{p} = (x)$. ▲

Ejercicio 38. Sea k es un cuerpo algebraicamente cerrado. Encuentre las componentes irreducibles de los siguientes conjuntos algebraicos:

1) $\mathbf{V}(x(x+1), y) \subset \mathbb{A}^2(k)$;

2) $\mathbf{V}(xz, yz) \subset \mathbb{A}^3(k)$;

3) $\mathbf{V}(xy^2 - x^2(x^2 - 1)) \subset \mathbb{A}^2(k)$.

20.14. Definición. Se dice que un espacio topológico X es **noetheriano** si toda cadena descendente de subconjuntos cerrados

$$X \supseteq Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \cdots$$

se estabiliza.

20.15. Lema. *Si X es un espacio noetheriano, entonces todo subespacio $Y \subseteq X$ es noetheriano.*

Demostración. Sea

$$Y \supseteq Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \cdots$$

una cadena de subespacios cerrados en Y. Tomando las cerraduras en X se obtiene una cadena

$$X \supseteq \overline{Z_1} \supseteq \overline{Z_2} \supseteq \overline{Z_3} \supseteq \cdots$$

que se estabiliza. Ahora $Z_i = Y \cap \overline{Z_i}$. ■

20.16. Proposición. *Todo subespacio $X \subseteq \mathbb{A}^n(k)$ es noetheriano.*

Demostración. Gracias al lema anterior, bastaría probar que $\mathbb{A}^n(k)$ es un espacio noetheriano. Consideremos una cadena

$$\mathbb{A}^n(k) \supseteq \mathbf{V}(I_1) \supseteq \mathbf{V}(I_2) \supseteq \mathbf{V}(I_3) \supseteq \cdots$$

Esta nos da una cadena de ideales

$$\mathbf{IV}(I_1) \subseteq \mathbf{IV}(I_2) \subseteq \mathbf{IV}(I_3) \subseteq \cdots \subseteq k[x_1, \ldots, x_n]$$

que se estabiliza, puesto que $k[x_1, \ldots, x_n]$ es un anillo noetheriano. Tenemos entonces

$$\mathbf{IV}(I_n) = \mathbf{IV}(I_{n+1}) = \mathbf{IV}(I_{n+2}) = \cdots$$

Luego, dado que $\mathbf{VIV}(I) = \mathbf{V}(I)$,

$$\mathbf{V}(I_n) = \mathbf{V}(I_{n+1}) = \mathbf{V}(I_{n+2}) = \cdots$$ ■

20.17. Digresión. Si A es un anillo noetheriano, entonces el espacio $\operatorname{Spec} A$ con la topología definida en 20.11 es también noetheriano. Sin embargo, si $\operatorname{Spec} A$ es noetheriano, entonces A no es necesariamente noetheriano, sino cumple la condición de cadenas ascendentes *para los ideales radicales*. Por ejemplo, $A = k[x_1, x_2, x_3, \ldots]/(x_1^2, x_2^2, x_3^2, \ldots)$ no es noetheriano, pero $\operatorname{Spec} A$ consiste en un punto.

20.18. Proposición. *Si X es un espacio noetheriano, entonces todo subconjunto cerrado $Z \subseteq X$ tiene un número finito de componentes irreducibles.*

Demostración (inducción noetheriana). Bastaría probar que todo subconjunto cerrado de X puede ser expresado como una unión finita de subconjuntos irreducibles. Asumamos que esto no es cierto y sea $\mathscr{S}$ el conjunto de los subconjuntos cerrados de X que no pueden ser expresados como una unión finita de subconjuntos irreducibles. En este caso, usando que X es noetheriano, podemos concluir que en $\mathscr{S}$ existe un elemento mínimo Z. Este conjunto no es irreducible y por ende $Z = Z_1 \cup Z_2$, donde Z_1 y Z_2 son subconjuntos propios cerrados en Z. Por la minimalidad, $Z_1, Z_2 \notin \mathscr{S}$, y entonces Z_1 y Z_2 sí se expresan como una unión finita de subconjuntos irreducibles. Esto nos lleva a una contradicción. ■

20.19. Comentario. El argumento de arriba puede ser explicado de manera informal pero tal vez más clara. Si Z es irreducible, entonces no hay que hacer nada. Sino, se tiene $Z = Z_1 \cup Z_2$, donde Z_1 y Z_2 son subconjuntos propios cerrados de Z. Ahora el mismo argumento puede ser aplicado a Z_1 y Z_2. Eventualmente este proceso se termina gracias a la noetherianidad del espacio. Como resultado se obtiene una expresión

$$Z = Z_1 \cup \cdots \cup Z_s,$$

donde Z_i son conjuntos cerrados irreducibles. Quitando los términos innecesarios, podemos asumir que la descomposición es minimal en el sentido de que $Z_i \not\subseteq Z_j$ para $i \neq j$.

Tales descomposiciones minimales son únicas. En efecto, asumamos que

$$Z = Z_1 \cup \cdots \cup Z_s = Z_1' \cup \cdots \cup Z_t'.$$

Ahora $Z_1' \subseteq Z_1 \cup \cdots \cup Z_s$ implica por la irreducibilidad de Z_1' que $Z_1' \subseteq Z_i$ para algún i. El mismo argumento aplicado a Z_i nos da $Z_i \subseteq Z_j'$ para algún j. Ahora por la minimalidad de las descomposiciones,

$$Z_1' \subseteq Z_i \subseteq Z_j'$$

implica que $j = 1$ y $Z_1' = Z_i$. Podemos quitar Z_1' y Z_i y por inducción repetir el argumento a los conjuntos de las uniones que nos quedan. Esto nos lleva a la conclusión de que $s = t$ y $Z_i = Z_i'$, salvo alguna permutación de los índices.

Ejercicio 39. Demuestre que X es un espacio Hausdorff noetheriano si y solo si X es finito con la topología discreta.

Ahora si k es un cuerpo algebraicamente cerrado, entonces para todo ideal $I \subseteq k[x_1, \ldots, x_n]$ la descomposición en componentes irreducibles

$$\mathbf{V}(I) = Z_1 \cup \cdots \cup Z_s$$

nos da la descomposición

$$\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s,$$

donde $\mathfrak{p}_i = \mathbf{I}(Z_i)$ son ideales primos. Además, $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ para $i \neq j$ y estos ideales primos están definidos de modo único por $\sqrt{I}$. Esta es una versión muy débil de la **descomposición primaria** en álgebra conmutativa que vamos a investigar en la siguiente sección.

21 Descomposiciones primarias

La descomposición de un conjunto algebraico en componentes irreducibles tiene su análogo en el mundo de álgebra conmutativa que es la descomposición primaria de ideales. Sin embargo, la situación algebraica es más sutil. Nuestra exposición esencialmente sigue [AM1969, Chapter 4].

Para motivar la teoría de esta sección, consideremos un dominio de factorización única A. En este caso todo elemento no nulo $f \in A$ se descompone como

$$f = u\, p_1^{k_1} \cdots p_s^{k_s},$$

donde $u \in A^\times$ es un elemento invertible y $p_1, \ldots, p_s \in A$ son elementos primos no asociados entre sí. En términos de ideales, esta descomposición corresponde a

$$(f) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s,$$

donde $\mathfrak{q}_i = (p_i^{k_i})$. El objetivo de esta sección es generalizar tales expresiones a ideales $I \subseteq A$ en cualquier anillo noetheriano A. Los ideales $\mathfrak{q}_i$ de arriba son un caso particular de ideales primarios.

21.1 Ideales primarios

21.1. Definición. Sea A un anillo conmutativo. Se dice que un ideal $\mathfrak{q} \subset A$ es **primario** si el anillo cociente $A/\mathfrak{q}$ tiene las siguientes propiedades:

1) $A/\mathfrak{q} \neq 0$;

2) todo divisor de cero en $A/\mathfrak{q}$ es nilpotente.

De modo equivalente, esto quiere decir que

1) $\mathfrak{q} \neq A$;

2) para cualesquiera $f, g \in A$, si $fg \in \mathfrak{q}$, entonces $f \in \mathfrak{q}$ o $g \in \sqrt{\mathfrak{q}}$ (es decir, $g^r \in \mathfrak{q}$ para algún $r = 1, 2, 3, \ldots$).

Notamos que todo ideal primo es primario: en la definición de ideal primo $\mathfrak{p} \subset A$ se pide que el anillo cociente $A/\mathfrak{p}$ sea un dominio, y la definición de ideal primario impone una condición más débil.

21.2. Observación. *Para todo homomorfismo $\phi\colon A \to B$, si $\mathfrak{q} \subset B$ es un ideal primario, entonces $\phi^{-1}(\mathfrak{q}) \subset A$ es también primario.*

Demostración. Notamos que ϕ induce un homomorfismo inyectivo $A/\phi^{-1}(\mathfrak{q}) \hookrightarrow B/\mathfrak{q}$. ■

21.3. Observación. *Si $\mathfrak{q} \subset A$ es un ideal primario, entonces su radical $\sqrt{\mathfrak{q}}$ es el ideal primo más pequeño que contiene a $\mathfrak{q}$.*

Demostración. Recordemos que en general, para cualquier ideal $I \subseteq A$ se cumple

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq I}} \mathfrak{p},$$

así que sería suficiente comprobar que si $\mathfrak{q} \subset A$ es primario, entonces $\sqrt{\mathfrak{q}}$ es primo. Primero, dado que $\mathfrak{q} \neq A$, se tiene $\sqrt{\mathfrak{q}} \neq A$. Ahora si $fg \in \sqrt{\mathfrak{q}}$, entonces se tiene $(fg)^r \in \mathfrak{q}$ para algún $r = 1, 2, 3, \ldots$ Luego, ya que $\mathfrak{q}$ es primario, tenemos $f^r \in \mathfrak{q}$ o $g^{rs} \in \mathfrak{q}$ para algún $s = 1, 2, 3, \ldots$ Esto significa que $f \in \sqrt{\mathfrak{q}}$ o $g \in \sqrt{\mathfrak{q}}$. ■

21.4. Definición. Si $\mathfrak{q} \subset A$ es un ideal primario y $\sqrt{\mathfrak{q}} = \mathfrak{p}$, entonces se dice que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-**primario**.

21.5. Observación. *Si $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \subset A$ son ideales $\mathfrak{p}$-primarios, entonces su intersección $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ es también un ideal $\mathfrak{p}$-primario.*

Demostración. Es fácil verificar a partir de la definición que la intersección de ideales primarios $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ es un ideal primario si $\sqrt{\mathfrak{q}_1} = \cdots = \sqrt{\mathfrak{q}_s}$. Además,

$$\sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_s} = \mathfrak{p}.$$ ■

21.6. Ejemplo. Si A es un dominio de factorización única y $p \in A$ es un elemento primo, entonces el ideal principal $\mathfrak{q} = (p^k)$ para $k = 1, 2, 3, \ldots$ es primario. ▲

21.7. Ejemplo. Sea A un dominio de ideales principales. En particular, A es un dominio de factorización única y todo elemento no nulo y no ivertible $f \in A$ se factoriza como

$$f = u\, p_1^{k_1} \cdots p_s^{k_s},$$

donde $s \geq 1$, $u \in A^\times$ y $p_1, \ldots, p_s \in A$ son elementos primos. Ahora si el ideal (f) es primario, su radical

$$\sqrt{(f)} = (p_1 \cdots p_s)$$

debe ser un ideal primo, así que necesariamente $s = 1$. Esto nos permite concluir que los ideales primarios no nulos en A son precisamente de la forma $(p^k) = (p)^k$, donde $p \in A$ es un elemento primo y $k = 1, 2, 3, \ldots$ Además, el ideal nulo (0) es también primario. ▲

Notamos que en el último ejemplo los ideales primarios no nulos son precisamente las potencias de ideales maximales. Sin embargo, en general, un ideal primario no debe ser una potencia de un ideal primo, y viceversa, una potencia de un ideal primo no es siempre un ideal primario.

21.8. Ejemplo. En el anillo de polinomios $A := k[x, y]$ consideremos el ideal $\mathfrak{q} = (x, y^2)$. Notamos que

$$A/\mathfrak{q} \cong k[y]/(y^2),$$

y se ve fácilmente que los divisores de cero en este anillo son de la forma $a\overline{y}$, donde $a \in k$, y estos son nilpotentes. Se sigue que $\mathfrak{q}$ es un ideal primario. Ahora si $\mathfrak{q}$ fuera una potencia de algún ideal primo, este ideal sería precisamente su radical: $\sqrt{\mathfrak{p}^k} = \mathfrak{p}$. Sin embargo, en este caso el radical de $\mathfrak{q}$ es el ideal maximal $\mathfrak{p} = \sqrt{\mathfrak{q}} = (x, y)$, y se ve que $\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Entonces, $\mathfrak{q}$ es un ideal primario que no es una potencia de un ideal primo. ▲

21.9. Ejemplo. Consideremos el anillo cociente $A := k[x, y, z]/(xy - z^2)$. El ideal $\mathfrak{p} := (\overline{x}, \overline{z})$ es primo: se tiene $A/\mathfrak{p} \cong k[y]$. Ahora $\overline{x}\,\overline{y} = \overline{z}^2 \in \mathfrak{p}^2$, pero $\overline{x} \notin \mathfrak{p}^2$ e $\overline{y}^r \notin \mathfrak{p}^2$ para ningún $r = 1, 2, 3, \ldots$ Esto significa que el ideal $\mathfrak{p}^2$ no es primario. ▲

De hecho, se puede construir un ejemplo parecido en el anillo $k[x, y, z]$.

21.10. Ejemplo ([Nor1953]). Para los polinomios

$$f = y^2 - xz, \quad g = yz - x^3, \quad h = z^2 - x^2 y$$

el ideal

$$\mathfrak{p} = (f, g, h) \subset k[x, y, z]$$

es primo, pero $\mathfrak{p}^2$ no es primario.

Para ver que $\mathfrak{p}$ es primo, consideremos el homomorfismo

$$\phi\colon k[x, y, z] \to k[t], \quad x \mapsto t^3, y \mapsto t^4, z \mapsto t^5.$$

Primero, está claro que $f, g, h \in \ker\phi$. Luego, todo polinomio en $k[x, y, z]$ puede ser escrito como

$$x^2 A(z) + xy B(z) + x C(z) + y D(z) + E(z) + F(x, y, z),$$

donde $A, B, C, D, E \in k[z]$ y $F(x, y, z) \in (f, g, h)$. La imagen de este polinomio respecto a ϕ es

$$t^6 A(t^5) + t^7 B(t^5) + t^3 C(t^5) + t^4 D(t^5) + E(t^5).$$

Asumamos que este polinomio es igual a 0. Tenemos

$$\sum_i a_i\, t^{5i+6} + \sum_i b_i\, t^{5i+7} + \sum_i c_i\, t^{5i+3} + \sum_i d_i\, t^{5i+4} + \sum_i e_i\, t^{5i} = 0.$$

Los números $6, 7, 3, 4, 0$ dan diferentes restos módulo 5, así que entre los términos no hay cancelaciones y necesariamente $A = B = C = D = E = 0$. Esto demuestra que $\ker\phi \subseteq (f, g, h)$. Entonces,

$$\ker\phi = \mathfrak{p},$$

y podemos concluir que

$$k[x, y, z]/\mathfrak{p} \cong k[t^3, t^4, t^5] \subset k[t],$$

y el ideal $\mathfrak{p}$ es primo.

Ahora tenemos

$$g^2 - fh = (x^5 + xy^3 - 3x^2 yz + z^3)\, x \in \mathfrak{p}^2,$$

pero

$$x^5 + xy^3 - 3x^2 yz + z^3 \notin \mathfrak{p}^2, \quad x \notin \mathfrak{p} = \sqrt{\mathfrak{p}^2}$$

—para verlo, notamos que los polinomios en $\mathfrak{p} = (y^2 - xz,\, yz - x^3,\, z^2 - x^2 y)$ tienen monomios de grado ≥ 2 y los polinomios en $\mathfrak{p}^2$ tienen monomios de grado ≥ 4. Esto significa que el ideal $\mathfrak{p}^2$ no es primario. ▲

Lo que es cierto es que las potencias de ideales *maximales* son ideales primarios.

21.11. Proposición. *Si para un ideal $I \subset A$ su radical $\sqrt{I}$ es un ideal maximal, entonces I es primario. En particular, para cualquier ideal maximal $\mathfrak{m} \subset A$ sus potencias $\mathfrak{m}^k$ son ideales primarios.*

Demostración. Recordemos que los ideales primos en el anillo cociente A/I corresponden a los ideales primos $\mathfrak{p} \subset A$ tales que $\mathfrak{p} \supseteq I$. La última condición es equivalente a $\mathfrak{p} \supseteq \sqrt{I}$. Pero por nuestra hipótesis el ideal $\sqrt{I}$ es maximal, y por ende el único ideal primo en A/I es el ideal $\sqrt{I}/I$, y es también maximal. Ahora los nilpotentes vienen dados por

$$N(A/I) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A/I} \mathfrak{p} = \sqrt{I}/I.$$

Entonces, los elementos de A/I o son nilpotentes, o bien no pertenecen al único ideal maximal $\sqrt{I}/I$, y en este caso son invertibles. Esto nos permite concluir que I es un ideal primario. ■

Ejercicio 40. Demuestre que en el anillo $A = \mathbb{Z}[x]$ el ideal $\mathfrak{m} := (2, x)$ es maximal y el ideal $\mathfrak{q} = (4, x)$ es $\mathfrak{m}$-primario, pero no es una potencia de $\mathfrak{m}$.

Ejercicio 41 (*)**.** Encuentre una caracterización de ideales monomiales primarios. Por ejemplo, el ideal principal $(x^2 y) \subset k[x, y]$ no es primario, mientras que (x^2, y^2) es primario.

21.2 Digresión: el ideal cociente $(I : J)$

Recordemos brevemente la siguiente construcción.

21.12. Definición. Para dos ideales $I, J \subseteq A$ el **ideal cociente** de I por J viene dado por

$$(I : J) := \{f \in A \mid fJ \subseteq I\}.$$

21.13. Observación. *El ideal cociente $(I : J)$ es un ideal. Además, se cumplen las siguientes propiedades:*

1) $I \subseteq (I : J)$*;*

2) si $J_1 \subseteq J_2$*, entonces* $(I : J_1) \supseteq (I : J_2)$*;*

3) $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$*;*

4) si $J = (f)$ *es un ideal principal, entonces* $(I : f) = \{g \in A \mid fg \in I\}$. □

21.14. Comentario. El ideal $(I : J)$ tiene el siguiente significado geométrico: para dos conjuntos algebraicos $X, Y \subseteq \mathbb{A}^n(k)$ se tiene

$$\mathbf{I}(X \setminus Y) = (\mathbf{I}(X) : \mathbf{I}(Y)),$$

donde $X \setminus Y$ denota la diferencia de conjuntos habitual (que normalmente *no es* un conjunto algebraico). Luego,

$$\overline{X \setminus Y} = \mathbf{V}(\mathbf{I}(X) : \mathbf{I}(Y)).$$

En efecto, asumamos que $f \in \mathbf{I}(X \setminus Y)$ y $g \in \mathbf{I}(Y)$. Luego, para todo $x \in X$ se tiene

- si $x \in X \setminus Y$, entonces $f(x) = 0$;
- si $x \in X \cap Y$, entonces $g(x) = 0$.

Esto significa que $fg(x) = 0$ para todo $x \in X$; es decir, que $fg \in \mathbf{I}(X)$. Esto demuestra la inclusión $\mathbf{I}(X \setminus Y) \subseteq (\mathbf{I}(X) : \mathbf{I}(Y))$.

Viceversa, asumamos que $f \in (\mathbf{I}(X) : \mathbf{I}(Y))$. Esto significa que $fg \in \mathbf{I}(X)$ para todo $g \in \mathbf{I}(Y)$. Escribamos $Y = \mathbf{V}(J)$. Ahora para $x \in X \setminus Y$, existe $g \in J \subseteq \mathbf{I}(Y)$ tal que $g(x) \neq 0$. Luego, $fg(x) = 0$ implica que $f(x) = 0$. Esto demuestra la otra inclusión $(\mathbf{I}(X) : \mathbf{I}(Y)) \subseteq \mathbf{I}(X \setminus Y)$. ■

21.15. Comentario. El lector puede verificar que si $J = (f_1, \ldots, f_s)$, entonces

$$(I : J) = \bigcap_{1 \leq i \leq s} (I : f_i),$$

y para $f \neq 0$ se tiene

$$(I : f) = \left\{ \frac{g}{f} \;\middle|\; g \in I \cap (f) \right\}.$$

De este modo el cálculo de $(I : J)$ se reduce al cálculo de intersecciones de ideales que fue estudiado en §18.

21.16. Ejemplo. Para los ideales

$$I = (x^2, xy^2z, yz^2),\ J = (x, y) \subset k[x, y, z],$$

calculemos $(I : J)$. Tenemos

$$(I : J) = (I : x) \cap (I : y).$$

Luego,

$$I \cap (x) = (x^2, xyz^2, xy^2z), \quad I \cap (y) = (x^2y, yz^2, xy^2z),$$

de donde

$$(I : x) = (x, yz^2, y^2z), \quad (I : y) = (x^2, z^2, xyz),$$

así que

$$(I : J) = (x, yz^2, y^2z) \cap (x^2, z^2, xyz) = (x^2, yz^2, xz^2, xyz).$$ ▲

En Macaulay2 el ideal $(I : J)$ se calcula mediante `I : J`.

```
i : R = QQ[x,y];

i : ideal (x^2,x*y) : ideal (x)
o = ideal(y, x)
o : Ideal of R

i : ideal (x^2,x*y) : ideal (y)
o = ideal x
o : Ideal of R
```

21.3 Descomposiciones primarias

21.17. Definición. Para un ideal $I \subseteq A$ una **descomposición primaria** es una expresión

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s,$$

donde s es un número finito y $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \subset A$ son ideales primarios.

Se dice que la descomposición de arriba es **minimal** si se cumplen las siguientes condiciones:

1) $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ para cualesquiera $i \neq j$;

2) $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ para todo $i = 1, \ldots, s$.

Notamos que toda descomposición primaria puede ser reducida a una descomposición minimal: la condición 1) de arriba puede ser satisfecha usando la observación 21.5: si $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}_j}$, podemos reemplazar estos dos ideales por la intersección $\mathfrak{q}_i \cap \mathfrak{q}_j$ que es también un ideal primario. Luego, para que se cumpla la condición 2), basta quitar los ideales innecesarios. Entonces, es fácil obtener descomposiciones minimales; lo que no está claro es si en primer lugar existe *alguna* descomposición primaria. Para esto vamos a asumir que el anillo A es noetheriano.

21.18. Teorema. *En un anillo noetheriano todo ideal posee una descomposición primaria (y por ende una descomposición primaria minimal).*

Demostración. Sea A un anillo noetheriano. Podemos descartar el caso del ideal $I = A$: este puede ser considerado como una intersección vacía de ideales.

Digamos que un ideal $I \subset A$ es **irreducible** si $I = J_1 \cap J_2$ para algunos ideales $J_1, J_2 \subset A$ implica que $J_1 = I$ o $J_2 = I$.

Primero notamos que **en un anillo noetheriano todo ideal es una intersección finita de ideales irreducibles**. En efecto, si esto no fuera cierto, entre los ideales $I \subset A$ que no son intersecciones finitas de ideales irreducibles habría un elemento maximal (gracias a la condición noetheriana). Denotémoslo por I. Luego, el mismo I no es irreducible, así que $I = J_1 \cap J_2$, donde $I \subsetneq J_1$ e $I \subsetneq J_2$. Pero por la maximalidad de I, los ideales J_1 y J_2 son intersecciones finitas de ideales irreducibles, y entonces I lo es. Esto nos lleva a una contradicción. (Compare este argumento con 20.18.)

Ahora probemos que **en un anillo noetheriano todo ideal propio irreducible es primario**. Asumamos que $I \subsetneq A$ es un ideal irreducible y $fg \in I$. Tenemos que probar que $f \in I$ o $g^r \in I$ para algún $r = 1, 2, 3, \ldots$ La cadena decreciente de ideales principales

$$(g) \supseteq (g^2) \supseteq (g^3) \supseteq (g^3) \supseteq \cdots \supset A$$

nos da la cadena creciente de ideales cociente

$$(I : g) \subseteq (I : g^2) \subseteq (I : g^3) \subseteq \cdots \subset A,$$

que se estabiliza por la hipótesis noetheriana: existe $r = 1, 2, 3, \ldots$ tal que

$$(I : g^r) = (I : g^{r+1}).$$

Notamos que en este caso

$$(I + (f)) \cap (I + (g^r)) = I. \tag{21.1}$$

En efecto, la inclusión $I \subseteq (I + (f)) \cap (I + (g^r))$ es obvia. Viceversa, si $h \in (I + (f)) \cap (I + (g^r))$, entonces

$$h = a_1 + b_1 f = a_2 + b_2 g^r$$

para algunos $a_1, a_2 \in I$, $b_1, b_2 \in A$. Luego,

$$b_2 g^{r+1} = \underbrace{(a_1 - a_2) g}_{\in I} + \underbrace{b_1 f g}_{\in I} \in I,$$

así que $b_2 \in (I : g^{r+1}) = (I : g^r)$. Esto nos permite concluir que $b_2 g^r \in I$ y luego $h \in I$.

Por la irreducibilidad de I, la identidad (21.1) implica que $I + (f) = I$ o $I + (g^r) = I$, así que $f \in I$ o $g^r \in I$. ■

21.19. Comentario. El argumento de arriba que expresa un ideal como intersección de irreducibles no es constructivo y no es tan fácil encontrar un *algoritmo* de descomposición primaria.

Las descomposiciones primarias fueron estudiadas por primera vez por Emanuel Lasker, y fue Emmy Noether quien simplificó los argumentos usando la noción de anillo noetheriano.

21.4 El primer teorema de unicidad

En general, las descomposiciones primarias minimales no son únicas.

21.20. Ejemplo. En el anillo de polinomios $A = k[x, y]$ consideremos el ideal $I = (x^2, xy)$. Tenemos dos descomposiciones primarias minimales diferentes:

$$I = \mathfrak{p} \cap \mathfrak{m}^2 = \mathfrak{p} \cap \mathfrak{q},$$

donde

$$\mathfrak{p} = (x), \quad \mathfrak{m} = (x, y), \quad \mathfrak{q} = (x^2, y).$$

El ideal $\mathfrak{p}$ es primo, dado que $A/\mathfrak{p} \cong k[y]$. El ideal $\mathfrak{m}$ es maximal, y por ende $\mathfrak{m}^2$ es primario. El ideal $\mathfrak{q}$ es primario, dado que $A/\mathfrak{q} \cong k[x]/(x^2)$. Notamos que

$$\sqrt{\mathfrak{m}^2} = \sqrt{\mathfrak{q}} = \mathfrak{m}.$$

Entonces, aunque las dos descomposiciones de arriba son diferentes, ambos ideales $\mathfrak{m}^2$ y $\mathfrak{q}$ son $\mathfrak{m}$-primarios. Esto será explicado por el **primer teorema de unicidad** que vamos a probar abajo. El hecho de que el ideal $\mathfrak{p}$ aparece en ambas descomposiciones será explicado por el **segundo teorema de unicidad**. ▲

Antes de formular y probar el primer teorema de unicidad, necesitamos algunos lemas.

21.21. Lema. *Sean $\mathfrak{q} \subset A$ un ideal $\mathfrak{p}$-primario y $f \in A$.*

1) Si $f \in \mathfrak{q}$, entonces $(\mathfrak{q} : f) = A$.

2) Si $f \notin \mathfrak{q}$, entonces $(\mathfrak{q} : f)$ es un ideal $\mathfrak{p}$-primario.

3) Si $f \notin \mathfrak{p}$, entonces $(\mathfrak{q} : f) = \mathfrak{q}$.

Demostración. La parte 1) se sigue inmediatamente de la definición y no usa la hipótesis que $\mathfrak{q}$ es primario.

En la parte 2), si $g \in (\mathfrak{q} : f)$, entonces $fg \in \mathfrak{q}$. Dado que $f \notin \mathfrak{q}$ y $\mathfrak{q}$ es un ideal primario, tenemos $g \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. Esto demuestra la inclusión $(\mathfrak{q} : f) \subseteq \mathfrak{p}$, y entonces $\sqrt{(\mathfrak{q} : f)} \subseteq \mathfrak{p}$. Por otra parte, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ implica la otra inclusión $\mathfrak{p} \subseteq \sqrt{(\mathfrak{q} : f)}$. Ahora si $gh \in (\mathfrak{q} : f)$, entonces $fgh \in \mathfrak{q}$. Si $g \notin \sqrt{(\mathfrak{q} : f)} = \mathfrak{p}$, entonces $fh \in \mathfrak{q}$, de donde $h \in (\mathfrak{q} : f)$. Esto demuestra que $(\mathfrak{q} : f)$ es un ideal primario.

En fin, en la parte 3), si $g \in (\mathfrak{q} : f)$, entonces $gf \in \mathfrak{q}$, lo que implica que $g \in \mathfrak{q}$ o $h \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. Si $f \notin \mathfrak{p}$, esto demuestra la inclusión $(\mathfrak{q} : f) \subseteq \mathfrak{q}$. La otra inclusión $\mathfrak{q} \subseteq (\mathfrak{q} : f)$ es trivial. ■

21.22. Lema. *Si A es un anillo noetheriano, entonces para todo ideal $I \subseteq A$ existe $m = 1, 2, 3, \ldots$ tal que $\sqrt{I}^m \subseteq I \subseteq \sqrt{I}$.*

Demostración. Sean $f_1, \ldots, f_s \in A$ generadores del radical $\sqrt{I}$. En particular, $f_i^{m_i} \in I$ para algunos $m_1, \ldots, m_s$. Pongamos

$$m := \sum_{1 \le i \le s} (m_i - 1) + 1.$$

Ahora

$$\sqrt{I}^m = \left(f_1^{r_1} \cdots f_s^{r_s} \,\middle|\, \sum_i r_i = m \right).$$

Por nuestra elección de m, si $\sum_i r_i = m$, entonces $r_i \ge m_i$ para algún i y luego $f_1^{r_1} \cdots f_s^{r_s} \in I$. ■

21.23. Lema. *Sean $I_1, \ldots, I_s \subseteq A$ ideales y $\mathfrak{p} \subset A$ un ideal primo.*

1) Si $\mathfrak{p} \supseteq I_1 \cap \cdots \cap I_s$, entonces $\mathfrak{p} \supseteq I_i$ para algún i.

2) Si $\mathfrak{p} = I_1 \cap \cdots \cap I_s$, entonces $\mathfrak{p} = I_i$ para algún i.

Demostración. Ejercicio para el lector ■

21.24. Primer teorema de unicidad. *Para una descomposición primaria minimal*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$$

los ideales $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ son precisamente los ideales primos que ocurren entre $\sqrt{(I : f)}$ para $f \in A$. En particular, estos no dependen de una descomposición específica.

Además, si el anillo es noetheriano, entonces los ideales $\mathfrak{p}_i$ son los ideales primos que ocurren entre $(I : f)$ para $f \in A$.

Demostración. Primero, notamos que para todo $f \in A$ se tiene

$$(I : f) = \left(\bigcap_{1 \le i \le s} \mathfrak{q}_i : f \right) = \bigcap_{1 \le i \le s} (\mathfrak{q}_i : f).$$

Luego, tenemos $(\mathfrak{q}_i : f) = A$ para $f \in \mathfrak{q}_i$ y $\sqrt{(\mathfrak{q}_i : f)} = \mathfrak{p}_i$ para $f \notin \mathfrak{q}_i$ según el lema 21.21, así que

$$\sqrt{(I : f)} = \bigcap_{f \notin \mathfrak{q}_i} \mathfrak{p}_i.$$

Asumamos que $\sqrt{(I : f)}$ es un ideal primo. En este caso por el lema 21.23

$$\sqrt{(I : f)} = \mathfrak{p}_i$$

para algún i, donde $f \notin \mathfrak{q}_i$. Esto demuestra que todo ideal primo de la forma $\sqrt{(I:f)}$ es necesariamente uno de los ideales $\mathfrak{p}_i$. De la misma manera, si $(I:f)$ es un ideal primo, entonces

$$(I:f) = \sqrt{(I:f)} = \mathfrak{p}_i$$

para algún i.

Ahora denotemos

$$I_i := \bigcap_{j \neq i} \mathfrak{q}_j.$$

Por la minimalidad de la descomposición, para todo i existe $f_i \in I_i$ tal que $f_i \notin \mathfrak{q}_i$. En este caso

$$\sqrt{(I:f_i)} = \mathfrak{p}_i.$$

Esto demuestra que cada uno de los ideales $\mathfrak{p}_i$ se obtiene como $\sqrt{(I:f)}$ para algún $f \in A$.

En el caso noetheriano, gracias al lema 21.22, sabemos que

$$\mathfrak{p}_i^m \subseteq \mathfrak{q}_i$$

para algún $m = 1, 2, 3, \ldots$ Luego,

$$I_i \mathfrak{p}_i^m \subseteq I_i \cap \mathfrak{p}_i^m \subseteq I_i \cap \mathfrak{q}_i = I,$$

Sea m el mínimo número tal que $I_i \mathfrak{p}_i^m \subseteq I$ (notamos que $I_i \not\subseteq I$, así que $m \geq 1$). Escojamos $f \in I_i \mathfrak{p}_i^{m-1}$ tal que $f \notin I$. Luego, $\mathfrak{p}_i f \subseteq I$ y entonces $\mathfrak{p}_i \subseteq (I:f)$. Por otra parte, dado que $f \in I_i$ y $f \notin I$, tenemos $(I:f) \subseteq \sqrt{(I:f)} = \mathfrak{p}_i$. Podemos concluir que $(I:f) = \mathfrak{p}_i$. ■

El primer teorema de unicidad 21.24 nos lleva a la siguiente definición.

21.25. Definición. Los ideales primos $\mathfrak{p}$ tales que en las descomposiciones primarias minimales de I aparecen ideales $\mathfrak{p}$-primarios se llaman los **ideales asociados con** I. Los ideales primos minimales entre los asociados con I se llaman **minimales**. Los ideales que no son minimales se llaman **encajados**.

21.26. Ejemplo. Volvamos al ejemplo 21.20 con las descomposiciones primarias minimales

$$I = (x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y).$$

Los ideales primos asociados con I son (x) y $(x, y) = \sqrt{(x, y)^2} = \sqrt{(x^2, y)}$. Tenemos

$$(x) = (I:y), \quad (x, y) = (I:x).$$

Puesto que $(x) \subset (x, y)$, el ideal (x) es minimal y (x, y) es encajado. Notamos que el conjunto algebraico $V(I) \subset \mathbb{A}^2(k)$ corresponde a la recta $V(x) = \{(x, y) \mid x = 0\}$, mientras que $V(x, y) = \{(0, 0)\} \subset V(x)$. ▲

En general, para un ideal $I \subset k[x_1, \ldots, x_n]$ y una descomposición primaria

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$$

tenemos

$$V(I) = V(\mathfrak{q}_1) \cup \cdots \cup V(\mathfrak{q}_s) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_s).$$

Ahora si $\mathfrak{p}_i$ es minimal entre los ideales $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, entonces el conjunto algebraico $V(\mathfrak{p}_i)$ no está contenido en ningún otro $V(\mathfrak{p}_j)$. Por otra parte, si $\mathfrak{p}_i$ es encajado, esto significa que $\mathfrak{p}_i \supset \mathfrak{p}_j$ para algún j, y luego $V(\mathfrak{p}_i) \subset V(\mathfrak{p}_j)$.

Entonces, si k es un cuerpo algebraicamente cerrado, los ideales primos minimales corresponden precisamente a las componentes irreducibles $V(\mathfrak{p}) \subseteq V(I) \subseteq \mathbb{A}^n(k)$, mientras que los ideales primos encajados corresponden a subconjuntos algebraicos $V(\mathfrak{p})$ que están incluidos en alguna componente irreducible de $V(I)$. Esto explica el uso del término "encajado".

21.27. Observación. *Los ideales primos minimales asociados a I son precisamente los ideales primos minimales entre $\mathfrak{p} \supseteq I$.*

Demostración. Consideremos una descomposición primaria minimal

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s.$$

Luego,

$$\sqrt{I} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_s} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s.$$

Entonces, para todo ideal primo $\mathfrak{p} \supseteq I$ se tiene $\mathfrak{p} \supseteq \mathfrak{p}_i$ para algún i. ■

Ejercicio 42. Demuestre que si I es un ideal radical, entonces I no tiene ideales asociados encajados.

Ejercicio 43. Para un anillo A y un ideal $I \subseteq A$, denotemos por $I[x] \subseteq A[x]$ el ideal formado por los polinomios con coeficientes en I. Demuestre las siguientes propiedades.

1) Si $\mathfrak{p}$ es un ideal primo en A, entonces $\mathfrak{p}[x]$ es un ideal primo en $A[x]$.
2) Si $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario en A, entonces $\mathfrak{q}[x]$ es un ideal $\mathfrak{p}[x]$-primario en $A[x]$.
3) Si $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ es una descomposición primaria minimal en A, entonces $I[x] = \mathfrak{q}_1[x] \cap \cdots \cap \mathfrak{q}_s[x]$ es una descomposición primaria minimal en $A[x]$.
4) Si $\mathfrak{p}$ es un ideal primo minimal asociado a I, entonces $\mathfrak{p}[x]$ es un ideal primo minimal asociado a $I[x]$.

Ejercicio 44. Demuestre que en el anillo de polinomios $k[x_1, \ldots, x_n]$ para los ideales primos $\mathfrak{p}_i := (x_1, \ldots, x_i)$ (donde $i = 1, \ldots, n$) todas las potencias $\mathfrak{p}_i^m$ son ideales primarios.

21.5 Compatibilidad con la localización y el segundo teorema de unicidad

Recordemos brevemente las propiedades de la localización. Para un anillo conmutativo A y un subconjunto multiplicativo $S \subset A$, denotemos la localización de A respecto a S por $S^{-1}A$. Tenemos el homomorfismo canónico

$$\iota \colon A \to S^{-1}A, \quad f \mapsto \frac{f}{1}.$$

Para un ideal $I \subseteq A$, el ideal en $S^{-1}A$ generado por $\iota(I)$ será denotado por $S^{-1}I$. Para un ideal $J \subseteq S^{-1}A$, el ideal $\iota^{-1}(J)$ será denotado por $J \cap A$.

- En general, para cualquier ideal $J \subseteq S^{-1}A$ se tiene

$$S^{-1}(J \cap A) = J.$$

- Un ideal $I \subseteq A$ es de la forma $J \cap A$ para algún ideal J precisamente cuando los elementos de S no son divisores de cero en A/I; es decir, si $sf \in I$ para algunos $s \in S$, $f \in A$, entonces $f \in I$. Cuando I cumple esta condición, se tiene

$$I = S^{-1}I \cap A.$$

En particular, las operaciones $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ y $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ nos dan una biyección

$$\operatorname{Spec} S^{-1}A \cong \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \emptyset\}. \tag{21.2}$$

En particular, para un ideal primo $\mathfrak{p} \subset A$ el conjunto $S = A \setminus \mathfrak{p}$ es multiplicativo. En este caso la localización respecto a S se denota por $A_{\mathfrak{p}}$. Se tiene

$$\operatorname{Spec} A_{\mathfrak{p}} \cong \{\mathfrak{p}' \in \operatorname{Spec} A \mid \mathfrak{p}' \subseteq \mathfrak{p}\}.$$

Esto explica el significado geométrico de la localización: si k es un cuerpo algebraicamente cerrado y $A = k[x_1,\dots,x_n]/\mathbf{I}(X)$, entonces los ideales primos $\mathfrak{p} \in \operatorname{Spec} A$ corresponden a los subconjuntos cerrados irreducibles $\mathbf{V}(\mathfrak{p}) \subseteq X$. Luego, los ideales primos $\mathfrak{p}' \in \operatorname{Spec} A_{\mathfrak{p}}$ corresponden a los subconjuntos cerrados irreducibles $\mathbf{V}(\mathfrak{p}) \subseteq \mathbf{V}(\mathfrak{p}') \subseteq X$. Entonces, la localización $A_{\mathfrak{p}}$ refleja la geometría de X *localmente*, *alrededor de* $\mathbf{V}(\mathfrak{p})$.

Las pruebas de todos los resultados mencionados es un buen ejercicio para el lector.

La biyección (21.2) se generaliza a una biyección para los ideales primarios.

21.28. Lema. *Sea $S \subset A$ un subconjunto multiplicativo y $\mathfrak{q} \subset A$ un ideal $\mathfrak{p}$-primario.*

1) *Si $\mathfrak{p} \cap S \neq \emptyset$, entonces $S^{-1}\mathfrak{q} = S^{-1}A$.*
2) *Si $\mathfrak{p} \cap S = \emptyset$, entonces $S^{-1}\mathfrak{q}$ es un ideal $S^{-1}\mathfrak{p}$-primario y $S^{-1}\mathfrak{q} \cap A = \mathfrak{q}$.*

Esto nos da una biyección

$$\{\textit{ideales primarios } \mathfrak{q} \subset S^{-1}A\} \cong \{\textit{ideales primarios } \mathfrak{q} \subset A \mid \mathfrak{q} \cap S = \emptyset\}.$$

Demostración. Si $s \in \mathfrak{p} \cap S$, entonces $s^r \in \mathfrak{q} \cap S$ para algún $r = 1,2,3,\dots$ y luego $\frac{s^n}{1} \in S^{-1}\mathfrak{q}$, que es invertible en la localización, así que $S^{-1}\mathfrak{q} = S^{-1}A$.

Ahora si $\mathfrak{p} \cap S = \emptyset$, entonces si $s \in S$, $f \in A$ satisfacen $fs \in \mathfrak{q}$, entonces $s \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$, y por lo tanto $f \in \mathfrak{q}$, dado que $\mathfrak{q}$ es $\mathfrak{p}$-primario. Esto nos permite concluir que

$$S^{-1}\mathfrak{q} \cap A = \mathfrak{q}.$$

Además,

$$\sqrt{S^{-1}\mathfrak{q}} = \bigcap_{\substack{\mathfrak{p}' \in \operatorname{Spec} S^{-1}A \\ \mathfrak{p}' \supseteq S^{-1}\mathfrak{q}}} \mathfrak{p}' = \bigcap_{\substack{\mathfrak{p}' \in \operatorname{Spec} A \\ \mathfrak{p}' \supseteq \mathfrak{q}}} S^{-1}\mathfrak{p}' = S^{-1} \bigcap_{\substack{\mathfrak{p}' \in \operatorname{Spec} A \\ \mathfrak{p}' \supseteq \mathfrak{q}}} \mathfrak{p}' = S^{-1}\sqrt{\mathfrak{q}} = S^{-1}\mathfrak{p}.$$

Aquí hemos usado el hecho de que la localización conmuta con las intersecciones. Luego, es fácil comprobar a partir de las definiciones que si $\mathfrak{q} \subset A$ es primario, entonces $S^{-1}\mathfrak{q} \subset S^{-1}A$ es también primario, y si $\mathfrak{q} \subset S^{-1}A$ es primario, entonces $\mathfrak{q} \cap A \subset A$ es primario. ∎

21.29. Lema. *Sea A un anillo conmutativo y $S \subset A$ un conjunto multiplicativo. Para un ideal $I \subset A$ sea*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$$

una descomposición primaria minimal. Denotemos $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$. Asumamos que $\mathfrak{p}_i \cap S = \emptyset$ para $i = 1,\dots,m$ y $\mathfrak{p}_i \cap S \neq \emptyset$ para $i = m+1,\dots,s$. Entonces,

$$S^{-1}I = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_m$$

es una descomposición primaria minimal para el ideal $S^{-1}I \subseteq S^{-1}A$ y

$$S^{-1}I \cap A = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

es una descomposición primaria minimal para el ideal $S^{-1}I \cap A \subseteq A$.

Demostración. Tenemos por el lema anterior

$$S^{-1}I = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_s = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_m.$$

Luego, dado que $\mathfrak{p}_i \neq \mathfrak{p}_j$ para $i \neq j$, tenemos $S^{-1}\mathfrak{p}_i \neq S^{-1}\mathfrak{p}_j$ para $i \neq j$ (donde $1 \leq i,j \leq m$). Esto demuestra la minimalidad. Luego,

$$S^{-1}I \cap A = S^{-1}\mathfrak{q}_1 \cap A \cap \cdots \cap S^{-1}\mathfrak{q}_m \cap A = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m,$$

usando de nuevo el lema anterior. ∎

Los ideales primos $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ asociados con I son únicos según el primer teorema de unicidad. Los ideales primarios correspondientes $\mathfrak{q}_1,\dots,\mathfrak{q}_s$ no tienen por qué ser únicos, pero entre ellos sí son únicos aquellos $\mathfrak{q}_i$ que corresponden a los primos minimales $\mathfrak{p}_i$ (es decir, estos deben aparecer en cualquier descomposición primaria minimal). Este es el contenido del segundo teorema de unicidad.

21.30. Segundo teorema de unicidad. *Para una descomposición primaria minimal $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ los ideales primarios $\mathfrak{q}_i$ que corresponden a los primos minimales $\mathfrak{p}_i$ están definidos de modo único (no dependen de la descomposición).*

Demostración. Para un primo minimal $\mathfrak{p}_i$ consideremos el conjunto multiplicativo $S := A\setminus\mathfrak{p}_i$. La minimalidad de $\mathfrak{p}_i$ significa que $\mathfrak{p}_j \not\subseteq \mathfrak{p}_i$ para todo $j \neq i$; es decir, que $\mathfrak{p}_j \cap S \neq \emptyset$ para $j \neq i$. Entonces, por el lema anterior se tiene

$$S^{-1}I \cap A = \mathfrak{q}_i.$$

Ya que $\mathfrak{p}_i$ está definido de modo único por I, esto demuestra que $\mathfrak{q}_i$ está definido de modo único. ■

Ejercicio 45. Demuestre que para cualquier $c \in k$ el ideal $(cx+y, x^2)$ es primario y que $(x^2, xy) = (x)\cap(cx+y, x^2)$ es una descomposición primaria minimal.

21.6 Descomposiciones primarias de ideales monomiales

En este breve curso no tenemos tiempo para hablar de los algoritmos de descomposición primaria. El lector interesado puede consultar los artículos [GTZ1988] y [DHV1992]. Solo notamos que una factorización primaria del ideal principal (f) en el anillo de polinomios $k[x_1,\dots,x_n]$ nos da esencialemente los factores irreducibles en f. La misma factorización de polinomios es un problema poco trivial desde el punto de vista algorítmico.

Como siempre, el caso de ideales monomiales es mucho más sencillo, y aquí voy a explicar un método básico de su descomposición.

21.31. Lema. *Si $I \subset k[x_1,\dots,x_n]$ es un ideal monomial generado por las potencias de variables $x_{i_1}^{\alpha_1}$, …, $x_{i_s}^{\alpha_s}$, entonces I es primario.*

Demostración. El ideal $(x_{i_1}^{\alpha_1},\dots,x_{i_s}^{\alpha_s})$ es primario en el anillo $k[x_{i_1},\dots,x_{i_s}]$, dado que su radical[*]

$$\sqrt{(x_{i_1}^{\alpha_1},\dots,x_{i_s}^{\alpha_s})} = (x_{i_1},\dots,x_{i_s})$$

es maximal en $k[x_{i_1},\dots,x_{i_s}]$. Luego, I es la extensión de este ideal al anillo de polinomios $k[x_1,\dots,x_n]$, y entonces es también primario gracias al ejercicio 43. ■

21.32. Lema. *Sea $I = (x^{\alpha(1)},\dots,x^{\alpha(s)})$ un ideal monomial en $k[x_1,\dots,x_n]$, donde los generadores $x^{\alpha(i)}$ son minimales y $x^{\alpha(s)} = x^\beta x^\gamma$ con $\operatorname{mcd}(x^\beta, x^\gamma) = 1$. Luego,*

$$I = (x^{\alpha(1)},\dots,x^{\alpha(s-1)},x^\beta)\cap(x^{\alpha(1)},\dots,x^{\alpha(s-1)},x^\gamma) = (I+(x^\beta))\cap(I+(x^\gamma)).$$

Demostración. Los ideales en cuestión son monomiales, así que bastaría verificar que para un monomio x^α se tiene

$$x^\alpha \in (I+(x^\beta))\cap(I+(x^\gamma)) \iff x^\alpha \in I.$$

En efecto, $x^\alpha \in (I+(x^\beta))\cap(I+(x^\gamma))$ quiere decir que

$$x^\alpha \in I \text{ o } x^\beta \mid x^\alpha,\ x^\gamma \mid x^\alpha.$$

Dado que x^β y x^γ son coprimos, la última condición puede ser escrita como

$$x^\alpha \in I \text{ o } x^\beta x^\gamma \mid x^\alpha \iff x^\alpha \in I.$$ ■

[*] Para los radicales de ideales monomiales, véase el ejercicio 23.

Ahora aplicando recursivamente el último lema a un ideal monomial I, podemos escribirlo como una intersección de ideales monomiales donde ningún generador puede descomponerse como $x^\beta x^\gamma$ con $\mcd(x^\beta, x^\gamma) = 1$. Pero tales ideales son precisamente los ideales generados por potencias de las variables y son primarios según el lema 21.31. Esto nos da un algoritmo bastante tonto de descomposición primaria de ideales monomiales. El problema es que el método produce una descomposición que no es necesariamente minimal, y se necesita más trabajo para simplificarla. Para un método más eficaz, véase [HS2002].

21.33. Ejemplo. Consideremos el ideal monomial $(xz, yz) \subset k[x, y, z]$. Usando el lema 21.32, podemos escribir

$$(xz, yz) = (xz, y) \cap (xz, z) = (xz, y) \cap (z) = (x, y) \cap (z, y) \cap (z) = (x, y) \cap (z).$$

Esta es una descomposición primaria, y es visiblemente minimal. ▲

21.34. Ejemplo. Para ver un ejemplo más trabajoso, tomemos el ideal $(x^2, xy^2z, yz^2) \subset k[x, y, z]$. Primero, escribamos

$$(x^2, xy^2z, yz^2) = (x^2, xy^2z, y) \cap (x^2, xy^2z, z^2) = (x^2, y) \cap (x^2, xy^2z, z^2).$$

Ahora para el segundo ideal en la última intersección,

$$(x^2, xy^2z, z^2) = (x, z^2) \cap (x^2, y^2, z^2) \cap (x^2, z).$$

Esto nos da la descomposición

$$(x^2, xy^2z, yz^2) = (x^2, y) \cap (x, z^2) \cap (x^2, y^2, z^2) \cap (x^2, z),$$

pero no es minimal: tenemos $\sqrt{(x, z^2)} = \sqrt{(x^2, z)} = (x, z)$. Calculamos la intersección correspondiente

$$(x, z^2) \cap (x^2, z) = (x^2, xz, z^2).$$

Tenemos entonces

$$(x^2, xy^2z, yz^2) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3,$$

donde

$$\mathfrak{q}_1 = (x^2, y), \quad \mathfrak{q}_2 = (x^2, xz, z^2) = (x, z)^2, \quad \mathfrak{q}_3 = (x^2, y^2, z^2).$$

Los radicales correspondientes son

$$\mathfrak{p}_1 = (x, y), \quad \mathfrak{p}_2 = (x, z), \quad \mathfrak{p}_3 = (x, y, z).$$

Ahora la descomposición sí es minimal:

$$\begin{aligned} \mathfrak{q}_1 \cap \mathfrak{q}_2 &= (x^2, xyz, yz^2) \not\subseteq \mathfrak{q}_3, \\ \mathfrak{q}_1 \cap \mathfrak{q}_3 &= (x^2, y^2, yz^2) \not\subseteq \mathfrak{q}_2, \\ \mathfrak{q}_2 \cap \mathfrak{q}_3 &= (x^2, xy^2z, z^2) \not\subseteq \mathfrak{q}_1. \end{aligned}$$ ▲

Ejercicio 46. Encuentre una descomposición primaria minimal para el ideal $(x^2yz, y^2z, xz^2) \subset k[x, y, z]$.

21.7 Descomposiciones primarias en Macaulay2

Para trabajar con las descomposiciones primarias, en Macaulay2 existen las siguientes funciones.

- `isPrime(`I`)` verifica si I es un ideal primo.
- `isPrimary(`I`)` verifica si I es un ideal primario.
- `radical(`I`)` calcula el radical $\sqrt{I}$.

- `primaryDecomposition(`I`)` devuelve una descomposición primaria de I.
- `associatedPrimes(`I`)` devuelve los ideales primos asociados con I.
- `minimalPrimes(`I`)` devuelve los ideales primos minimales asociados con I.

21.35. Ejemplo. Calculemos en Macaulay2 una descomposición primaria minimal del ideal

$$I = (x^2 z^2,\, x(x+y^2),\, z(z-y^2)) \subset \mathbb{Q}[x,y,z].$$

```
i1 : R = QQ[x,y,z];

i2 : I = ideal (x^2*z^2, x*(x+y^2), z*(z-y^2));

o2 : Ideal of R

i3 : dec = primaryDecomposition I

                                 2                   2
o3 = {ideal (z, x), ideal (z, y  + x), ideal (x, y  - z),
-------------------------------------------------------------
        2         3   2     2     2         2 2   4    2
ideal (x  + x*z, z , y z - z , x*y  - x*z, x z , y  - z )}

o3 : List

i4 : isPrime dec#3

o4 = false

i5 : isPrimary dec#3

o5 = true

i6 : radical dec#3

o6 = ideal (z, y, x)

o6 : Ideal of R

i7 : associatedPrimes I

                                 2                   2
o7 = {ideal (z, x), ideal (z, y  + x), ideal (x, y  - z), ideal (z, y, x)}

o7 : List

i8 : minimalPrimes I

                                 2                   2
o8 = {ideal (z, x), ideal (z, y  + x), ideal (- y  + z, x)}
```

En este caso Macaulay2 encontró una descomposición primaria minimal

$$I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \cap \mathfrak{q},$$

donde

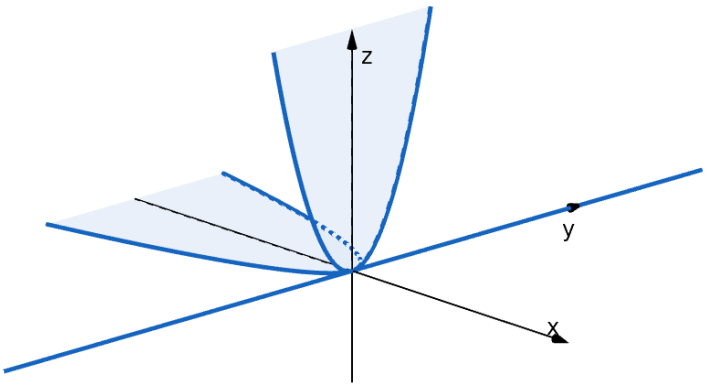
$$\mathfrak{p}_1 = (z, x), \quad \mathfrak{p}_2 = (z, y^2 + x), \quad \mathfrak{p}_3 = (x, y^2 - z)$$

son ideales primos y son minimales, mientras que

$$\mathfrak{q} = (x^2 + xz,\, z^3,\, y^2z - z^2,\, xy^2 - xz,\, x^2z^2,\, y^4 - z^2)$$

es un ideal primario que corresponde al primo encajado

$$\sqrt{\mathfrak{q}} = (x, y, z).$$ ▲



21.36. Ejemplo. Hemos visto en 21.10 que el ideal

$$\mathfrak{p} := (f, g, h) \subset k[x, y, z], \quad f := y^2 - xz, \quad g := yz - x^3, \quad h := z^2 - x^2y$$

es primo, pero $\mathfrak{p}^2$ no es primario. Hagamos estos cálculos en Macaulay2.

```
i1 : R = QQ[x,y,z];

i2 : (f,g,h) = (y^2 - x*z, y*z - x^3, z^2 - x^2*y);

i3 : P = ideal (f,g,h);

o3 : Ideal of R

i4 : isPrime P

o4 = true

i5 : isPrimary P^2

o5 = false

i6 : factor (g^2 - f*h)

          5      3     2       3
o6 = (x)(x  + x*y  - 3x y*z + z )

o6 : Expression of class Product

i7 : x % P == 0

o7 = false
```

```
i8 : pol = value o6#1

      5      3     2       3
o8 = x  + x*y  - 3x y*z + z

o8 : R

i9 : pol % P^2 == 0

o9 = false
```

▲

22 Dimensión de Krull

El concepto correcto de la dimensión en geometría algebraica y álgebra conmutativa es la dimensión de Krull[*]. Para motivar la definición, observemos que para un espacio vectorial V sobre un cuerpo k la dimensión viene dada por

$$\dim_k V = \sup\{n \mid \text{existe una cadena de subespacios } 0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V\}.$$

La dimensión de Krull se define de manera parecida.

22.1. Definición. La **dimensión de Krull** de un espacio topológico X viene dada por

$$\dim X := \sup\{n \mid \text{existe una cadena de subespacios cerrados irreducibles } X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subseteq X\}.$$

Además, se pone

$$\dim \emptyset := -1.$$

Ejercicio 47. Demuestre que si $X \neq \emptyset$ es un espacio noetheriano y $Z_1, \ldots, Z_s$ son sus componentes irreducibles, entonces

$$\dim X = \text{máx}\{\dim Z_1, \ldots, \dim Z_s\}.$$

Ejercicio 48. Demuestre que para un subespacio $Y \subseteq X$ se tiene

$$\dim Y \leq \dim X.$$

22.2. Ejemplo. Para un conjunto algebraico $X \subseteq \mathbb{A}^n(k)$ se tiene $\dim X = 0$ si y solo si X es finito y no vacío. En efecto, si X es un conjunto finito, entonces la topología de Zariski sobre X es discreta y los subconjuntos irreducibles de X son unipuntuales. Entonces, todas las cadenas tienen longitud 0. Viceversa, asumamos que $\dim X = 0$. El espacio X es noetheriano y por ende tiene un número finito de componentes irreducibles, pero estas son unipuntuales, puesto que $\dim X = 0$. ▲

Notamos que si X es Hausdorff, entonces los subespacios irreducibles de X son unipuntuales y la dimensión de X será nula. Vamos a ocupar la definición 22.1 para la topología de Zariski que casi nunca es Hausdorff.

Si k es un cuerpo algebraicamente cerrado y $X \subseteq \mathbb{A}^n(k)$ es un conjunto algebraico, entonces una cadena de subespacios cerrados irreducibles

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subseteq X$$

[*] Wolfgang Krull (1899–1971) — algebrista alemán conocido por sus contribuciones en álgebra conmutativa.

corresponde a una cadena de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset \Gamma(X).$$

Esto motiva la siguiente definición general.

22.3. Definición. La **dimensión de Krull** de un anillo conmutativo A viene dada por

$$\dim A := \sup\{n \mid \text{existe una cadena de ideales primos } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset A\}.$$

Además, por la definición,

$$\dim 0 := -1.$$

En particular, si k es un cuerpo algebraicamente cerrado, entonces para un conjunto algebraico $X \subseteq \mathbb{A}^n(k)$ se tiene

$$\dim X = \dim \Gamma(X).$$

22.4. Comentario. En efecto, la definición 22.3 se obtiene aplicando 22.1 al espacio $\operatorname{Spec} A$ con la topología de Zariski definida en 20.11.

22.5. Ejemplo. Para todo cuerpo k se tiene $\dim k = 0$, dado que $\operatorname{Spec} k = \{(0)\}$. En general, recordemos que un anillo A es **artiniano** si y solo si A es noetheriano y todo ideal primo en A es maximal. En este caso las cadenas de ideales primos tienen longitud 0 y por ende $\dim A = 0$. ▲

22.6. Ejemplo. Si A es un dominio de ideales principales, como por ejemplo $\mathbb{Z}$ o $k[x]$, entonces $\dim A = 1$. Esto se sigue del hecho de que los ideales primos en A son (0) y los ideales maximales (p), donde $p \in A$ es un elemento primo. Entonces, toda cadena de ideales primos de longitud maximal tiene forma

$$(0) \subsetneq (p) \subset A.$$

Esto también demuestra que

$$\dim \mathbb{A}^1(k) = 1, \quad \text{si } k \text{ es infinito.}$$

De hecho, tenemos una cadena de subconjuntos irreducibles

$$\{0\} = \mathbf{V}(x) \subsetneq \mathbf{V}(0) = \mathbb{A}^1(k),$$

y viceversa, toda cadena de subconjuntos cerrados irreducibles en $\mathbb{A}^1(k)$ corresponde a una cadena de ideales primos en $k[x]$ que tiene longitud ≤ 1. ▲

22.7. Ejemplo. En el anillo de polinomios en número finito de variables existe una cadena infinita de ideales primos

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots \subset k[x_1, x_2, x_3, \ldots],$$

así que

$$\dim k[x_1, x_2, x_3, \ldots] = \infty.$$

Este anillo no es noetheriano. En general, existen anillos no noetherianos de dimensión finita y anillos noetherianos de dimensión infinita[*]. Ejemplos específicos de tales anillos fueron descubiertos por el algebrista japonés Masayoshi Nagata. Sin embargo, aquí nos va a interesar el caso de k-álgebras finitamente generadas, donde la dimensión se comporta bien. ▲

Ejercicio 49. Sean A un anillo e $I \subseteq A$ un ideal. Demuestre que $\dim(A/I) \leq \dim A$.

Ejercicio 50. Demuestre que para el producto de dos anillos se tiene

$$\dim(A \times B) = \max\{\dim A, \dim B\}.$$

Ejercicio 51. Sea k un cuerpo. Demuestre que el anillo de las series formales $k[[x]]$ y el anillo de polinomios de Laurent $k[x, x^{-1}]$ tienen dimensión 1.

Ejercicio 52. Demuestre que el anillo $\mathbb{Z}[x]$ tiene dimensión 2.

[*] El hecho de que todas las cadenas de ideales se estabilizan no necesariamente significa que hay una cota para la longitud de cadenas.

22.1 Dimensión y el grado de trascendencia

Intuitivamente, la dimensión del espacio afín $\mathbb{A}^n(k)$ debe ser igual a n. En el anillo $\Gamma(\mathbb{A}^n(k)) = k[x_1,\dots,x_n]$ tenemos la cadena de ideales primos

$$0 \subsetneq (x_1) \subsetneq (x_1,x_2) \subsetneq \cdots \subsetneq (x_1,x_2,\dots,x_n) \subset k[x_1,\dots,x_n]$$

que en el caso de k infinito corresponde a la cadena de subespacios irreducibles

$$\mathbf{V}(x_1,x_2,\dots,x_n) \subsetneq \cdots \subsetneq \mathbf{V}(x_1,x_2) \subsetneq \mathbf{V}(x_1) \subsetneq \mathbb{A}^n(k). \tag{22.1}$$

Notamos que esto demuestra solamente las desigualdades

$$\dim \mathbb{A}^n(k) \geq n, \quad \text{si } k \text{ es infinito}$$

y

$$\dim k[x_1,\dots,x_n] \geq n.$$

—no está claro por qué no existen cadenas más largas. Para resolver este problema, vamos a relacionar la dimensión de Krull con otro invariante: el grado de trascendencia.

22.8. Definición. Sea A un álgebra sobre un cuerpo k. Digamos que $a_1,\dots,a_s \in A$ son **algebraicamente independientes** sobre k si para todo polinomio no nulo $f \in k[x_1,\dots,x_s]$ se tiene

$$f(a_1,\dots,a_s) \neq 0.$$

El **grado de trascendencia** de A se define mediante

$$\operatorname{trdeg}_k A := \sup\{\#S \mid S \subset A \text{ un subconjunto finito, algebraicamente independiente sobre } k\}.$$

Además, se pone

$$\operatorname{trdeg}_k 0 := -1.$$

22.9. Ejemplo. Dejo al lector digerir la definición de arriba y entender que para el anillo de polinomios $k[x_1,\dots,x_n]$ un subconjunto maximal algebraicamente independiente viene dado por $S = \{x_1,\dots,x_n\}$, y por ende

$$\operatorname{trdeg}_k(k[x_1,\dots,x_n]) = n.$$

De la misma manera, para el cuerpo de funciones racionales

$$k(x_1,\dots,x_n) := \operatorname{Frac}(k[x_1,\dots,x_n])$$

se tiene

$$\operatorname{trdeg}_k(k(x_1,\dots,x_n)) = n. \qquad \blacktriangle$$

22.10. Teorema. *Sean A una k-álgebra y $S \subset A$ un conjunto de generadores de A como k-álgebra. Entonces,*

$$\dim A \leq \sup\{\#T \mid T \subseteq S \textit{ subconjunto finito, algebraicamente independiente}\} \leq \operatorname{trdeg}_k A.$$

Además, si A es finitamente generada, entonces se cumplen igualdades

$$\dim A = \sup\{\#T \mid T \subseteq S \textit{ subconjunto finito, algebraicamente independiente}\} = \operatorname{trdeg}_k A.$$

22.11. Comentario. En general, cuando A no es finitamente generada, la desigualdad es estricta: por ejemplo, como todo cuerpo, $k(x_1,\dots,x_n)$ tiene dimensión de Krull 0, aunque $\operatorname{trdeg}_k(k(x_1,\dots,x_n)) = n$.

Antes de probar el teorema, notamos que como un caso particular se obtiene el siguiente resultado.

22.12. Corolario. *Para cualquier cuerpo k se tiene* $\dim k[x_1,\dots,x_n] = n$.

22.13. Corolario. *Para el espacio afín se tiene*

$$\dim \mathbb{A}^n(k) = \begin{cases} n, & \text{si } k \text{ es infinito,} \\ 0, & \text{si } k \text{ es finito.} \end{cases}$$

Demostración. Si $k = \mathbb{F}_q$ es un cuerpo finito, entonces $\dim \mathbb{A}^n(\mathbb{F}_q) = 0$ gracias a la observación en 22.2. Si k es infinito, entonces tenemos una cadena de subconjuntos irreducibles (22.1) de longitud n, así que

$$\dim \mathbb{A}^n(k) \geq n.$$

Viceversa, una cadena de subconjuntos irreducibles

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_m = \mathbb{A}^n(k)$$

nos da una cadena de ideales primos

$$0 = \mathbf{I}(X_m) \subsetneq \cdots \subsetneq \mathbf{I}(X_1) \subsetneq \mathbf{I}(X_0) \subset k[x_1,\dots,x_n],$$

pero su longitud es necesariamente $\leq \dim k[x_1,\dots,x_n] = n$, lo que nos da la otra desigualdad

$$\dim \mathbb{A}^n(k) \leq n.$$ ■

22.14. Comentario. En general, es cierto que para cualquier anillo noetheriano $A \neq 0$ se tiene

$$\dim A[x] = \dim A + 1,$$

pero no lo vamos a probar en nuestro breve curso. Note que esto implica por inducción que

$$\dim k[x_1,\dots,x_n] = n.$$

Demostración del teorema 22.10

Para un conjunto de generadores $S \subset A$ pongamos

$$n := \sup\{\#T \mid T \subseteq S \text{ subconjunto finito, algebraicamente independiente}\}.$$

Tenemos que probar que

$$\dim A \leq n.$$

1) Notamos que es suficiente probar la desigualdad para el caso cuando A es un dominio.
   En efecto, si una cadena de ideales primos de longitud maximal viene dada por

   $$\mathfrak{p} \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset A,$$

   a esta cadena corresponde una cadena en $A/\mathfrak{p}$ de la misma longitud:

   $$(0) \subsetneq \mathfrak{p}_1/\mathfrak{p} \subsetneq \cdots \subsetneq \mathfrak{p}_n/\mathfrak{p} \subset A/\mathfrak{p}.$$

   Además, al remplazar A por $A/\mathfrak{p}$ y el conjunto $S \subset A$ por

   $$S/\mathfrak{p} := \{a + \mathfrak{p} \mid a \in S\} \subset A/\mathfrak{p},$$

   el número n no puede volverse más grande.
   Entonces, a partir de ahora podemos asumir que A es un dominio.

2) Si $n = 0$, entonces todos los elementos de S son algebraicos sobre k, lo que significa que el cuerpo de fracciones $\operatorname{Frac} A$ está generado como k-álgebra por elementos algebraicos sobre k, así que $\operatorname{Frac} A / k$ es una extensión algebraica. En particular, todos los elementos de A son algebraicos sobre k. Ahora, dado que

$$k \subset A \subset \operatorname{Frac} A,$$

donde $\operatorname{Frac} A / k$ es una extensión algebraica, podemos concluir que A es también un cuerpo (véase el lema 19.26), y luego $\dim A = 0$.

3) Ahora asumamos que $n > 0$. Toda una cadena de ideales primos de longitud $m > 0$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m \subset A$$

nos da la cadena correspondiente de longitud $m - 1$ en $A/\mathfrak{p}_1$:

$$0 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1 \subset A/\mathfrak{p}_1.$$

Para el paso inductivo sería suficiente probar que todos los subconjuntos algebraicamente independientes $T \subseteq S/\mathfrak{p}_1$ tienen $< n$ elementos: en este caso

$$m - 1 \leq \dim(A/\mathfrak{p}_1) < n$$

por la hipótesis inductiva, y luego $m \leq n$. Asumamos que existen n elementos $a_1, \ldots, a_n \in S$ tales que

$$a_1 + \mathfrak{p}_1, \ldots, a_n + \mathfrak{p}_1 \in A/\mathfrak{p}_1$$

son n diferentes elementos algebraicamente independientes sobre k. Luego, $a_1, \ldots, a_n \in A$ son también algebraicamente independientes. Ahora por la elección de n, todo elemento de S es algebraico sobre el cuerpo

$$k(a_1, \ldots, a_n) = \operatorname{Frac} k[x_1, \ldots, x_n].$$

Los elementos de S son generadores de A, así que $\operatorname{Frac} A$ es una extensión algebraica de L. En particular, para un elemento no nulo $a \in \mathfrak{p}_1$ existen $f_0, f_1, \ldots, f_s \in k(a_1, \ldots, a_n)$ tales que

$$f_s\, a^s + f_{s-1}\, a^{s-1} + \cdots + f_1\, a + f_0 = 0.$$

Sin pérdida de generalidad, $f_0 \neq 0$. Además, multiplicando los f_i por su común denominador, podemos asumir que $f_0, f_1, \ldots, f_s \in k[a_1, \ldots, a_n]$. Luego,

$$f_0 = -(f_s\, a^{s-1} + f_{s-1}\, a^{s-2} + \cdots + f_1)\, a \in \mathfrak{p}_1.$$

Ahora f_0 corresponde a un polinomio $F_0 \in k[x_1, \ldots, x_n]$ evaluado en $a_1, \ldots, a_n$, pero la expresión de arriba significa que $a_1 + \mathfrak{p}_1, \ldots, a_n + \mathfrak{p}_1$ son algebraicamente dependientes. Contradicción.

Ahora nos gustaría probar que cuando A es un álgebra finitamente generada, entonces se tiene la otra desigualdad

$$\operatorname{trdeg}_k A \leq \dim A.$$

Vamos a probar que si existen n elementos $a_1, \ldots, a_n \in A$ algebraicamente independientes sobre k, entonces en A existe una cadena de ideales primos de longitud n.

1) Como antes, sin pérdida de generalidad, se puede asumir que A es un dominio. En efecto, en este caso A es noetheriano y tiene un número finito de ideales primos minimales $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Su intersección coincide con el nilradical:

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = N(A).$$

Si $a_1, \ldots, a_n \in A$ son algebraicamente independientes sobre k, entonces existe $i = 1, \ldots, s$ tal que los elementos $a_1 + \mathfrak{p}_i, \ldots, a_n + \mathfrak{p}_i \in A/\mathfrak{p}_i$ son algebraicamente independientes. En efecto, si esto no es el caso, entonces para todo i habrá un polinomio no nulo $f_i \in k[x_1, \ldots, x_n]$ tal que $f_i(a_1, \ldots, a_n) \in \mathfrak{p}_i$. Consideremos entonces el polinomio

$$f := f_1 \cdots f_s \neq 0.$$

Tenemos

$$f(a_1, \ldots, a_n) \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = N(A),$$

pero esto implica que existe $r = 1, 2, 3, \ldots$ tal que $f^r(a_1, \ldots, a_n) = 0$, lo que contradice la independencia algebraica de $a_1, \ldots, a_n$.

Ahora si a partir de los elementos algebraicamente independientes $a_1 + \mathfrak{p}_i, \ldots, a_n + \mathfrak{p}_i \in A/\mathfrak{p}_i$ se puede obtener una cadena de ideales primos de longitud n en $A/\mathfrak{p}_i$, esta cadena nos dará una cadena de ideales primos de longitud n en A.

A partir de ahora podemos asumir que A es un dominio.

2) La base de inducción es obvia: en A hay un ideal primo, por ejemplo (0), que nos da una cadena de longitud 0.

3) Consideremos el subcuerpo

$$L := K(a_1) \subseteq \operatorname{Frac} A$$

y la subálgebra

$$A' := L \cdot A \subseteq \operatorname{Frac} A.$$

Notamos que A' es una L-álgebra y $a_2, \ldots, a_n \in A'$ son algebraicamente independientes sobre L. Por la hipótesis inductiva, $\dim A \geq n - 1$ y existe una cadena de ideales primos

$$\mathfrak{p}'_0 \subsetneq \mathfrak{p}'_1 \subsetneq \cdots \subsetneq \mathfrak{p}'_{n-1} \subset A'.$$

Pongamos entonces

$$\mathfrak{p}_i := \mathfrak{p}'_i \cap A.$$

Dado que $L \cdot \mathfrak{p}_i = \mathfrak{p}'_i$, tenemos una cadena de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-1} \subset A.$$

El ideal $\mathfrak{p}_{n-1} \subset A$ no es maximal. En efecto, si $\mathfrak{p}_{n-1}$ fuera maximal, el cuerpo $A/\mathfrak{p}_{n-1}$ sería una extensión finita de k y el elemento $a_1 + \mathfrak{p}_{n-1} \in A/\mathfrak{p}_{n-1}$ sería algebraico sobre k. Luego,

$$c_n a_1^n + c_{n-1} a_1^{n-1} + \cdots + c_1 a_1 + c_0 \in \mathfrak{p}_{n-1}$$

para algunos $c_n, c_{n-1}, \ldots, c_0 \in k$, donde $c_0 \neq 0$. Sin embargo, esto demostraría que

$$c_0 = -(c_n a_1^n + c_{n-1} a_1^{n-1} + \cdots + c_1 a_1) \in \mathfrak{p}'_{n-1},$$

y luego $\mathfrak{p}'_{n-1} = A'$, que no es el caso.

Entonces, el ideal primo $\mathfrak{p}_{n-1}$ no es maximal en A y existe un ideal maximal $\mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n \subset A$. Esto nos da una cadena de longitud n

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n \subset A$$

y concluye la prueba. ■

Este argumento viene de [Kem2010].

22.2 Cálculo de dimensión

22.15. Corolario (Dimensión de álgebras finitamente generadas y eliminación). *La dimensión del álgebra finitamente generada $A = k[x_1, \ldots, x_n]/I$ es el máximo número δ tal que existen variables $\{x_{i_1}, \ldots, x_{i_\delta}\} \subseteq \{x_1, \ldots, x_n\}$ que cumplen*

$$I \cap k[x_{i_1}, \ldots, x_{i_\delta}] = 0. \tag{22.2}$$

Demostración. La condición $I \cap k[x_{i_1}, \ldots, x_{i_\delta}] = 0$ significa precisamente que $\overline{x_{i_1}}, \ldots, \overline{x_{i_\delta}} \in A$ son algebraicamente independientes sobre k. ■

22.16. Corolario. *Sean k un cuerpo algebraicamente cerrado y $X \subseteq \mathbb{A}^n(k)$ un conjunto algebraico. Entonces,* $\dim X$ *es el máximo número δ tal que existen δ variables $\{x_{i_1}, \ldots, x_{i_\delta}\} \subseteq \{x_1, \ldots, x_n\}$ que cumplen*

$$\mathbf{I}(X) \cap k[x_{i_1}, \ldots, x_{i_\delta}] = 0.$$

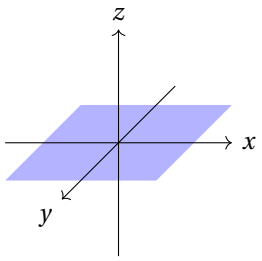
Demostración. Tenemos $\dim X = \dim k[x_1, \ldots, x_n]/\mathbf{I}(X)$. ■

Notamos que la condición (22.2) puede ser verificada usando las bases de Gröbner, como hemos visto en §18.1. Esto nos da un algoritmo para calcular la dimensión de una k-álgebra finitamente generada. Veamos un par de ejemplos.

22.17. Ejemplo. Calculemos la dimensión del álgebra afín $k[x, y, z]/I$ donde $I = (xz, yz)$. Notamos que a este ideal monomial corresponde el conjunto algebraico

$$\mathbf{V}(I) = \mathbf{V}(x, y) \cup \mathbf{V}(z)$$

que es la unión del eje z y el plano xy.



Tenemos $I \neq 0$, y luego

$$I \cap k[y, z] = (yz), \quad I \cap k[x, z] = (xz), \quad I \cap k[x, y] = 0$$

(es fácil verificar estas intersecciones, dado que el ideal en cuestión es monomial). La última intersección nos permite concluir que $\dim k[x, y, z]/I = 2$. ▲

22.18. Ejemplo. Calculemos la dimensión del álgebra afín $k[x, y, z]/I$, donde $I = (x^2 - y, x^3 - z)$. Tenemos

$$I \cap k[x, y] = (x^2 - y), \quad k[x, z] = (x^3 - z), \quad I \cap k[y, z] = (y^3 - z^2).$$

Estos cálculos pueden ser verificados en Macaulay2:

```
i1 : R = QQ[x,y,z];

i2 : I = ideal (x^2-y, x^3-z);
o2 : Ideal of R

i3 : eliminate (x,I)

             3    2
o3 = ideal(y  - z )
o3 : Ideal of R

i4 : eliminate (y,I)

             3
o4 = ideal(x  - z)
o4 : Ideal of R

i5 : eliminate (z,I)

             2
o5 = ideal(x  - y)
o5 : Ideal of R
```

Entonces, la dimensión de $k[x,y,z]/I$ tiene que ser menor que 2. Luego, calculamos que

$$I \cap k[x] = I \cap k[y] = I \cap k[z] = 0,$$

de donde $\dim k[x,y,z]/I = 1$.

```
i6 : eliminate ({x,y},I)
o6 = ideal ()
o6 : Ideal of R

i7 : eliminate ({x,z},I)
o7 = ideal ()
o7 : Ideal of R

i8 : eliminate ({y,z},I)
o8 = ideal ()
o8 : Ideal of R
```

De hecho, tenemos

$$k[x,y,z]/(x^2-y,\, x^3-z) \cong k[x,x^2,x^3] \cong k[x],$$

y ya sabemos que la dimensión de $k[x]$ es igual a 1. Geométricamente, el conjunto algebraico $\mathbf{V}(I)$ es la cúbica torcida que es isomorfa a la recta afín $\mathbb{A}^1(k)$ (véase 19.13). ▲

Ejercicio 53. Encuentre la dimensión de las k-álgebras

$$k[x,y,z]/(xz, xy-1), \quad k[x,y,z,w]/(zw-y^2, xy-z^3)$$

usando el método de arriba.

Ejercicio 54. Demuestre que para toda k-álgebra finitamente generada se cumple

$$\dim A = 0 \iff \dim_k(A) < \infty,$$

donde dim denota la dimensión de Krull y $\dim_k$ denota la dimensión de espacio vectorial sobre k..

Desafortunadamente, para encontrar el número máximo de variables $x_{i_1},\dots,x_{i_s}$ que satisfacen la condición (22.2), en general habrá que calcular un montón de bases de Gröbner (y respecto a órdenes monomiales ineficaces), así que este método no es muy práctico. Más adelante vamos a estudiar las series de Hilbert que es otra herramienta más eficaz para calcular la dimensión a partir de una sola base de Gröbner de I respecto a orden *grlex* o *grevlex*.

Terminemos por una aplicación teórica de 22.16.

22.19. Teorema. *Sean k un cuerpo algebraicamente cerrado y $X \subseteq \mathbb{A}^m(k)$ e $Y \subseteq \mathbb{A}^n(k)$ dos conjuntos algebraicos no vacíos. Entonces, su producto $X \times Y \subseteq \mathbb{A}^{m+n}(k)$ satisface*

$$\dim(X \times Y) = \dim X + \dim Y.$$

Demostración. Tenemos $\mathbf{I}(X) \subseteq k[x_1,\dots,x_m]$ y $\mathbf{I}(Y) \subseteq k[y_1,\dots,y_n]$. Sea

$$d = \dim X = \dim k[x_1,\dots,x_m]/\mathbf{I}(X), \quad e = \dim Y = \dim k[y_1,\dots,y_n]/\mathbf{I}(Y).$$

Según el corolario 22.16, d y e corresponden al máximo número de variables $x_{i_1},\dots,x_{i_d}$ e $y_{j_1},\dots,y_{j_e}$ respectivamente tales que

$$\mathbf{I}(X) \cap k[x_{i_1},\dots,x_{i_d}] = 0, \quad \mathbf{I}(Y) \cap k[y_{j_1},\dots,y_{j_e}] = 0.$$

Ahora un polinomio

$$f \in \mathbf{I}(X \times Y) \cap k[x_{i_1},\dots,x_{i_d},y_{j_1},\dots,y_{j_e}]$$

puede ser escrito como

$$f = \sum_\alpha f_\alpha\, y_{j_1}^{\alpha_1},\dots,y_{j_e}^{\alpha_e},$$

donde $f_\alpha \in k[x_{i_1},\dots,x_{i_d}]$. Luego, para todo punto $(a_1,\dots,a_m) \in X$ se tiene

$$\sum_\alpha f_\alpha(a_1,\dots,a_m)\, y_{j_1}^{\alpha_1} \in \mathbf{I}(Y) \cap k[y_{j_1},\dots,y_{j_e}],$$

así que

$$\sum_\alpha f_\alpha(a_1,\dots,a_m)\, y_{j_1}^{\alpha_1} = 0.$$

Esto implica que $f_\alpha(a_1,\dots,a_m) = 0$ todo $(a_1,\dots,a_m)$. Luego,

$$f_\alpha \in \mathbf{I}(X) \cap k[x_{i_1},\dots,x_{i_d}],$$

así que $f_\alpha = 0$ para todo α y $f = 0$. Esto demuestra que

$$\mathbf{I}(X \times Y) \cap k[x_{i_1},\dots,x_{i_d},y_{j_1},\dots,y_{j_e}] = 0,$$

y por ende

$$\dim(X \times Y) \geq d + e.$$

La otra desigualdad $\dim(X \times Y) \leq d + e$ es más fácil. Si tenemos un subconjunto $T \subseteq \{x_1,\dots,x_m,y_1,\dots,y_n\}$ tal que $\#T > d + e$, entonces

$$\#(T \cap \{x_1,\dots,x_m\}) > d \quad \text{o} \quad \#(T \cap \{y_1,\dots,y_n\}) > d.$$

Asumamos por ejemplo el primer caso. Existen entonces $s > d$ variables $x_{i_1},\dots,x_{i_s} \in T$ tales que

$$\mathbf{I}(X) \cap k[x_{i_1},\dots,x_{i_s}] \neq 0.$$

Esto nos da un polinomio no nulo $f \in k[x_{i_1},\dots,x_{i_s}]$ que se anula en todos los puntos de X. Luego, f se anula en todos los puntos de $X \times Y$ e

$$\mathbf{I}(X \times Y) \cap k[x_{i_1},\dots,x_{i_s}] \neq 0. \qquad \blacksquare$$

22.20. Comentario. El análogo algebraico del último resultado es la identidad

$$\dim(A \otimes_k B) = \dim A + \dim B$$

para k-álgebras finitamente generadas (véase el ejercicio 37). Notamos que en particular,

$$\dim k[x_1, \ldots, x_n] = \dim(k[x_1] \otimes_k \cdots \otimes_k k[x_n]) = \dim k[x_1] + \cdots + \dim k[x_n] = n.$$

En general, afuera del mundo de k-álgebras finitamente generadas, los productos tensoriales no se comportan bien respecto a la dimensión. Por ejemplo, si p y q son diferentes primos, entonces

$$\operatorname{Spec} \mathbb{F}_p = \{(0)\}, \quad \operatorname{Spec} \mathbb{F}_q = \{(0)\}, \quad \operatorname{Spec}(\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{F}_q) = \emptyset.$$

22.3 Dimensión de Krull en Macaulay2

Si A es un cociente del anillo de polinomios $k[x_1, \ldots, x_n]$ (donde $k = \mathbb{Q}$ o $\mathbb{F}_q$), la dimensión de A puede ser calculada en Macaulay2 mediante `dim(`A`)`. Para un ideal $I \subseteq k[x_1, \ldots, x_n]$, el comando `dim(`$I$`)` calcula la dimensión del anillo cociente $k[x_1, \ldots, x_n]/I$.

He aquí un pequeño ejemplo.

```
i1 : R = QQ[x,y,z];

i2 : dim R
o2 = 3

i3 : dim ideal (0_R)
o3 = 3

i4 : dim ideal (x)
o4 = 2

i5 : dim ideal (x,y)
o5 = 1

i6 : dim ideal (x,y,z)
o6 = 0

i7 : dim ideal (x*z,y*z)
o7 = 2

i8 : dim ideal (x^2-y,x^3-z)
o8 = 1
```

23 Digresión sobre las series formales

El **anillo de las series formales** con coeficientes enteros en la variable t se denota por $\mathbb{Z}[\![t]\!]$. Sus elementos son las sumas formales

$$\sum_{d \geq 0} a_d \, t^d = a_0 + a_1 \, t + a_2 \, t^2 + a_3 \, t^3 + \cdots,$$

donde $a_d \in \mathbb{Z}$. A diferencia de los polinomios, *no se pide* que $a_d = 0$ para d suficientemente grande. Las sumas y productos se definen de la manera habitual:

$$\sum_{d \geq 0} a_d \, t^d + \sum_{d \geq 0} b_d \, t^d := \sum_{d \geq 0} (a_d + b_d) \, t^d$$

y

$$\left(\sum_{p\geq 0} a_p\, t^p\right)\cdot\left(\sum_{q\geq 0} b_q\, t^q\right) := \sum_{d\geq 0}\left(\sum_{p+q=d} a_p b_q\right) t^d.$$

Ejercicio 55. Demuestre que una serie formal $\sum_{d\geq 0} a_d\, t^d \in \mathbb{Z}[[t]]$ es invertible si y solamente si $a_0 = \pm 1$.

23.1. Definición. Las **derivadas formales** vienen dadas por

$$\left(\sum_{d\geq 0} a_d\, t^d\right)' := \sum_{d\geq 1} d\, a_d\, t^{d-1}.$$

Ejercicio 56. Demuestre que para cualesquiera $f, g \in \mathbb{Z}[[t]]$ se cumple

$$(f+g)' = f' + g'$$

y la regla de Leibniz

$$(fg)' = f'g + fg'.$$

Demuestre que para $f = a_0 + a_1\, t + a_2\, t^2 + \cdots$ se tiene

$$d!\, a_d = f^{(d)}(0),$$

donde $f^{(d)}(0)$ denota el término constante de la d-ésima derivada formal de f.

23.2. Lema. *Para todo $n \in \mathbb{Z}$ se tiene*

$$((1-t)^n)' = -n\,(1-t)^{n-1}.$$

Demostración. Si $n \geq 0$, podemos proceder por inducción usando la regla de Leibniz. La base de inducción sería $n = 0, 1$, y luego para $n \geq 2$

$$\begin{aligned}((1-t)^n)' = ((1-t)\,(1-t)^{n-1})' = (1-t)'\,(1-t)^{n-1} + (1-t)\,((1-t)^{n-1})' \\ = -(1-t)^{n-1} - (1-t)\,(n-1)\,(1-t)^{n-2} = -n\,(1-t)^{n-1}.\end{aligned}$$

Para exponentes negativos, podemos calcular usando la regla de Leibniz que en general, para cualquier serie invertible f se tiene

$$0 = (f\, f^{-1})' = f'\, f^{-1} + f\,(f^{-1})',$$

de donde

$$(f^{-1})' = -f'\, f^{-2}.$$

En particular, para $n \geq 0$

$$((1-t)^{-n})' = -((1-t)^n)'\,(1-t)^{-2n} = n\,(1-t)^{-n-1}.$$ ■

23.3. Corolario. *Consideremos la serie $f := (1-t)^n$ para $n \in \mathbb{Z}$. Luego, para cualquier $d \in \mathbb{N}$ se cumple*

$$f^{(d)} = (-1)^d\, n\,(n-1)\cdots(n-d+1)\,(1-t)^{n-d}.$$

Demostración. Inducción usando el cálculo anterior. ■

23.4. Definición. Para $n \in \mathbb{Z}$ y $d \in \mathbb{N}$, el coeficiente binomial $\binom{n}{d}$ viene dado por

$$\binom{n}{0} := 1, \quad \binom{n}{d} := \frac{n\,(n-1)\,(n-2)\cdots(n-d+1)}{d!} \text{ para } d > 0. \tag{23.1}$$

Cuando $0 \le n \le d$, la expresión (23.1) viene de la fórmula conocida

$$\binom{n}{d} = \frac{n!}{d!\,(n-d)!} \in \mathbb{Z}.$$

Además, la definición de arriba nos da

$$\binom{n}{d} = 0, \text{ si } n > d.$$

23.5. Lema. *Para $n \in \mathbb{Z}$ y $d \in \mathbb{N}$ se cumple*

$$\binom{-n}{d} = (-1)^d \binom{n+d-1}{d}. \tag{23.2}$$

Demostración. Cálculo directo:

$$\binom{-n}{d} = \frac{-n\,(-n-1)\,(-n-2)\cdots(-n-d+1)}{d!} = (-1)^d\,\frac{n\,(n+1)\,(n+2)\cdots(n+d-1)}{d!} = (-1)^d \binom{n+d-1}{d}. \qquad \blacksquare$$

23.6. Proposición (Serie binomial). *Para todo $n \in \mathbb{Z}$ se cumple*

$$(1-t)^n = \sum_{d \ge 0} (-1)^d \binom{n}{d} t^d.$$

Demostración. Los coeficientes de la serie $f = (1-t)^n$ cumplen

$$d!\,a_d = f^{(d)}(0) = (-1)^d\,n\,(n-1)\cdots(n-d+1),$$

y luego

$$a_d = \frac{(-1)^d\,n\,(n-1)\cdots(n-d+1)}{d!} = (-1)^d \binom{n}{d}. \qquad \blacksquare$$

Notamos que para $n > 0$ esta es la fórmula del binomio de toda la vida, mientras que para $n < 0$ esta es una serie infinita.

23.7. Ejemplo. Si $n = -1$, tenemos gracias a la fórmula (23.2)

$$\binom{-1}{d} = (-1)^d,$$

así que

$$\frac{1}{1-t} = 1 + t + t^2 + t^3 + \cdots$$

Si $n = -2$, entonces

$$\binom{-2}{d} = (-1)^d \binom{d+1}{d} = (-1)^d\,(d+1),$$

así que

$$\frac{1}{(1-t)^2} = 1 + 2t + 3t^2 + 4t^3 + \cdots \qquad \blacktriangle$$

23.8. Corolario (Identidad de Vandermonde). *Para cualesquiera $m, n \in \mathbb{Z}$ se tiene*

$$\sum_{p+q=d} \binom{m}{p}\binom{n}{q} = \binom{m+n}{d}.$$

Demostración. Compare los coeficientes de las series $(1-t)^m \cdot (1-t)^n$ y $(1-t)^{m+n}$. ■

Para hacer cálculos con las series formales, recomiendo el programa PARI/GP. Para indicar que una expresión en t es una serie con precisión hasta el n-ésimo término, hay que añadir "`+ O(t^n)`". He aquí algunos ejemplos.

```
? 1/(1-t) + O (t^10)
% = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + O(t^10)
? 1/(1-t)^2 + O (t^10)
% = 1 + 2*t + 3*t^2 + 4*t^3 + 5*t^4 + 6*t^5 + 7*t^6 + 8*t^7 + 9*t^8 + 10*t^9 + O(t^10)
? (-t^2+t+1)/(1-t)^2 + O (t^10)
% = 1 + 3*t + 4*t^2 + 5*t^3 + 6*t^4 + 7*t^5 + 8*t^6 + 9*t^7 + 10*t^8 + 11*t^9 + O(t^10)
? (1+t)/(1-t) + O (t^10)
% = 1 + 2*t + 2*t^2 + 2*t^3 + 2*t^4 + 2*t^5 + 2*t^6 + 2*t^7 + 2*t^8 + 2*t^9 + O(t^10)
```

Ejercicio 57. Para $d \in \mathbb{N}$ consideremos los polinomios

$$\binom{x}{d} := \frac{x(x-1)\cdots(x-d+1)}{d!} \in \mathbb{Q}[x].$$

a) Demuestre que

$$\binom{x}{0} = 1, \binom{x}{1}, \binom{x}{2}, \ \ldots, \binom{x}{d}$$

forman una base del $\mathbb{Q}$-espacio vectorial formado por los polinomios racionales de grado $\leq d$.

b) Demuestre que todo polinomio $f \in \mathbb{Q}[x]$ tal que $f(n) \in \mathbb{Z}$ para todo $n \in \mathbb{Z}$ puede ser escrito como

$$f = a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_d \binom{x}{d},$$

donde $a_0, a_1, \ldots, a_d \in \mathbb{Z}$.

23.9. Comentario. En Macaulay2 la función `binomial (`α`,`n`)` calcula el coeficiente binomial

$$\binom{\alpha}{n} := \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$

He aquí un ejemplo:

```
i : for i in 0..10 list binomial (i,2)

o = {0, 0, 1, 3, 6, 10, 15, 21, 28, 36, 45}
o : List

i : binomial (-2,5)
o = -6

i : R = QQ[x];

i : binomial (x,2)
```

```
     1 2   1
o = -x  - -x
     2     2

o : R

i : binomial (x+2,2) - 2*binomial (x,2) + binomial (x-1,2)

o = x + 2
o : R
```

24 Series de Hilbert

24.1. Definición. Para un monomio $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in k[x_1, \ldots, x_n]$, su **grado (total)** viene dado por

$$\deg(x^\alpha) := \alpha_1 + \cdots + \alpha_n.$$

Para un polinomio no nulo $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ el grado viene dado por

$$\deg f := \text{máx}\{\deg x^\alpha \mid c_\alpha \neq 0\}.$$

Además, pongamos

$$\deg 0 := -1.$$

24.2. Definición. Para un ideal $I \subseteq k[x_1, \ldots, x_n]$ y el álgebra $A := k[x_1, \ldots, x_n]/I$, para $d = 0, 1, 2, \ldots$ consideremos los k-espacios vectoriales

$$k[x_1, \ldots, x_n]_{\leq d} := \{f \in k[x_1, \ldots, x_n] \mid \deg f \leq d\},$$
$$I_{\leq d} := I \cap k[x_1, \ldots, x_n]_{\leq d}.$$

Pongamos entonces

$$A_{\leq d} := k[x_1, \ldots, x_n]_{\leq d} / I_{\leq d} \cong \{\overline{f} \in A \mid f \in k[x_1, \ldots, x_n],\ \deg f \leq d\}.$$

Además, sea

$$A_d := A_{\leq d} / A_{\leq d-1}.$$

La **función de Hilbert de** I viene dada por

$$h_I \colon d \mapsto \dim_k(A_d)$$

y la **serie de Hilbert de** I es la serie formal

$$H_I(t) := \sum_{d \geq 0} h_I(d)\, t^d \in \mathbb{Z}[[t]].$$

24.3. Comentario. En algunas fuentes como [CLO2015] y [Kem2010] por una muy buena razón se considera otra definición

$$\widetilde{h}(d) := \dim_k(A_{\leq d}), \quad \widetilde{H}_I(t) := \sum_{d \geq 0} \widetilde{h}_I(d)\, t^d.$$

Notamos que

$$h(d) = \widetilde{h}(d) - \widetilde{h}(d-1),$$

y luego

$$H_I(t) = \sum_{d\geq 0} h_I(d)\, t^d = \sum_{d\geq 0} \widetilde{h}_I(d)\, t^d - t \sum_{d\geq 0} \widetilde{h}_I(d)\, t^d = (1-t)\, \widetilde{H}_I(t).$$

De hecho, el lector notará que para nuestros propósitos será más razonable hacer cálculos con $\widetilde{H}_I$, pero no hemos tomado $\widetilde{H}_I$ como la definición principal de la serie de Hilbert para seguir la convención adoptada por Macaulay2 que usa H_I[*].

Ejercicio 58. Demuestre que si $I \subseteq J$, entonces $H_I(t) = H_J(t)$ implica que $I = J$.

24.1 Primeros ejemplos

24.4. Ejemplo. Consideremos el ideal nulo $I = (0) \subset k[x_1, \ldots, x_n]$. En este caso

$$A_d \cong k[x_1, \ldots, x_n]_d \cong k\langle x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_1 + \cdots + \alpha_n = d\rangle.$$

Necesitamos entonces contar los monomios de grado total d. Por ejemplo, para dos variables x, y se tiene

$$\begin{aligned} &d = 0\colon 1,\\ &d = 1\colon x, y,\\ &d = 2\colon x^2, xy, y^2,\\ &d = 3\colon x^3, x^2y, xy^2, y^3,\\ &\qquad \cdots \end{aligned}$$

El número de monomios de grado total d es $d+1$. La serie de Hilbert será

$$1 + 2\,t + 3\,t^3 + 4\,t^3 + \cdots = \frac{1}{(1-t)^2}.$$

Para tres variables x, y, z se tiene

$$\begin{aligned} &d = 0\colon 1,\\ &d = 1\colon x, y, z,\\ &d = 2\colon x^2, xy, xz, y^2, yz, z^2,\\ &d = 3\colon x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^3, y^2z, yz^2, z^3,\\ &\qquad \cdots \end{aligned}$$

El número de monomios de grado total d es $\binom{d+2}{2}$. En general, en $k[x_1, \ldots, x_n]$ el número de monomios de grado total d es

$$\binom{n+d-1}{d} = (-1)^d \binom{-n}{d}.$$

Usando la serie binomial, calculamos que la serie de Hilbert viene dada por

$$H_{(0)}(t) = \sum_{d\geq 0} \binom{n+d-1}{d} t^d = \sum_{d\geq 0} (-1)^d \binom{-n}{d} t^d = \sum_{d\geq 0} \binom{-n}{d} (-t)^d = \frac{1}{(1-t)^n}. \qquad \blacktriangle$$

[*] La serie $\widetilde{H}_I$ es un caso particular de la serie de Hilbert de un **álgebra filtrada**

$$\{0\} \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq A,$$

mientras que H_I es un caso particular de la serie de Hilbert de un **álgebra graduada**

$$A = \bigoplus_{d\geq 0} A_d.$$

A toda álgebra filtrada se asocia un álgebra graduada con $A_d := F_d / F_{d-1}$.

Ejercicio 59. Demuestre que el número de monomios $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ con $\alpha_1 + \cdots + \alpha_n = d$ es igual a $\binom{n+d-1}{d}$.

Notamos que si el ideal I es monomial, entonces $I_{\leq d}$ como espacio vectorial sobre k tiene una base que consiste en los monomios

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in I, \quad \alpha_1 + \cdots + \alpha_n \leq d.$$

Luego,

$$A_d \cong k\langle x^\alpha \mid x^\alpha \notin I,\ \alpha_1 + \cdots + \alpha_n = d \rangle.$$

24.5. Ejemplo. Consideremos el ideal monomial $I = (xz, yz) \subset k[x, y, z]$. Para el álgebra $A := k[x, y, z]/I$, la dimensión del espacio A_d corresponde al número de monomios de grado total d que no son divisibles por xz o yz, y son los siguientes:

$$\begin{aligned}
&d = 0\colon 1,\\
&d = 1\colon x, y, z,\\
&d = 2\colon x^2, xz, y^2, z^2,\\
&d = 3\colon x^3, x^2z, xz^2, y^3, z^3,\\
&d = 4\colon x^4, x^3z, x^2z^2, xz^3, y^4, z^4,\\
&\qquad \cdots
\end{aligned}$$

En general, para $d > 0$ habrá $d + 1$ monomios de la forma $x^a y^b$, donde $a + b = d$, más el monomio z^d. Esto significa que la función de Hilbert viene dada por

$$h_I(d) = \begin{cases} 1, & d = 0, \\ d + 2, & d > 0, \end{cases}$$

y la serie de Hilbert correspondiente es

$$H_I(t) = 1 + 3t + 4t^2 + 5t^3 + 6t^4 + \cdots = \frac{1}{t(1-t)^2} - \frac{1}{t} - 1 = \frac{-t^2 + t + 1}{(1-t)^2}. \qquad \blacktriangle$$

Ejercicio 60. Calcule las series de Hilbert de los siguientes ideales monomiales en $k[x, y, z]$:

$$(x^2, y^2, z^2), \quad (xy, xz^3), \quad (xy, xz, yz)$$

de manera directa, contando los monomios.

Cuando el ideal no es monomial, el problema se vuelve más sutil.

24.6. Ejemplo. Consideremos el ideal $I = (x^2 - y) \subset k[x, y]$. El álgebra $A := k[x, y]/I$ tiene como una base sobre k los monomios xy^m e y^m para $m \geq 0$. Además, notamos que si un polinomio $f \in k[x, y]$ tiene grado $\leq d$, entonces reescribiéndolo en esta base, se obtiene un polinomio de grado $\leq d$: en efecto,

$$x^a y^b \equiv \begin{cases} y^{b + a/2}, & \text{si } a \text{ es par}, \\ x\, y^{b + (a-1)/2}, & \text{si } a \text{ es impar}, \end{cases}$$

así que el grado no se vuelve más grande. Esto significa que

$$\dim_k(A_{\leq d}) = \#\{xy^b \mid 0 \leq b \leq d - 1\} \cup \#\{y^b \mid 0 \leq b \leq d\} = 2d + 1.$$

Luego, para $d > 0$

$$\dim_k(A_d) = \dim_k(A_{\leq d}) - \dim_k(A_{\leq d-1}) = 2,$$

y la serie de Hilbert es

$$H_I(t) = 1 + 2t + 2t^2 + 2t^3 + \cdots = 1 + \frac{2t}{1-t} = \frac{1+t}{1-t}.$$

Hay que tener cuidado: otra base de monomios de A viene dada por $1, x, x^2, x^3, \ldots$, y uno podría pensar que la serie de Hilbert es más bien $1 + t + t^2 + t^3 + \cdots$ Sin embargo, el pasaje a esta base remplaza el monomio $x^a y^b$ por x^{a+2b} y el grado se sube si $b \neq 0$. ▲

24.7. Advertencia. La serie de Hilbert es un invariante de un ideal $I \subset k[x_1, \ldots, x_n]$, pero no del álgebra correspondiente $k[x_1, \ldots, x_n]/I$. Por ejemplo, se tiene $k[x, y]/(x^2 - y) \cong k[x]$, y sin embargo, al ideal $(x^2 - y) \subset k[x, y]$ corresponde la serie de Hilbert $\frac{1+t}{1-t}$, mientras que al ideal $(0) \subset k[x]$ corresponde la serie $\frac{1}{1-t}$.

Resumamos nuestros cálculos de arriba.

I	$H_I(t)$	$\mathbf{V}(I)$	$\dim A$
$(0) \subset k[x_1, \ldots, x_n]$	$\frac{1}{(1-t)^n}$	$\mathbb{A}^n(k)$	n
$(xz, yz) \subset k[x, y, z]$	$\frac{-t^2+t+1}{(1-t)^2}$	$\mathbf{V}(z) \cup \mathbf{V}(x, y)$	2
$(x^2 - y) \subset k[x, y]$	$\frac{1+t}{1-t}$	parábola	1

Notamos que en el denominador de $H_I(t)$ está precisamente $(1-t)^{\dim A}$. Más adelante vamos a probar que esto se cumple en cualquier caso, y de esta manera la serie de Hilbert permite calcular la dimensión de Krull de $k[x_1, \ldots, x_n]/I$.

24.2 Reducción al caso de ideales monomiales

Hemos visto en §17 cómo encontrar una base monomial de $k[x_1, \ldots, x_n]/I$ a partir de una base de Gröbner G para I: a saber, se tiene un isomorfismo de espacios vectoriales

$$\phi\colon k[x_1, \ldots, x_n]/I \to k\langle x^\alpha \mid x^\alpha \notin (LT(I))\rangle,$$
$$f \mod I \mapsto \overline{f}^G$$

Para que el isomorfismo ϕ sea útil en cálculos de las series de Hilbert, este debe respetar el grado en cierto sentido.

24.8. Definición. Se dice que un orden monomial $\preceq$ sobre $k[x_1, \ldots, x_n]$ **respeta el grado** si $x^\alpha \preceq x^\beta$ implica que $\deg x^\alpha \leq \deg x^\beta$.

En particular, el orden lexicográfico graduado (*grlex*) y el orden lexicográfico inverso graduado (*grevlex*) respetan el grado, mientras que el orden lexicografico sobre $k[x_1, \ldots, x_n]$ con $n > 1$ no lo respeta.

24.9. Lema. *Fijemos algún orden monomial $\preceq$ sobre $k[x_1, \ldots, x_n]$ que respete el grado. Para cualquier ideal $I \subseteq k[x_1, \ldots, x_n]$, el isomorfismo*

$$\phi\colon k[x_1, \ldots, x_n]/I \to k\langle x^\alpha \mid x^\alpha \notin (LT(I))\rangle$$

induce isomorfismos

$$\phi_d\colon (k[x_1, \ldots, x_n]/I)_{\leq d} \to k\langle x^\alpha \mid \deg x^\alpha \leq d,\ x^\alpha \notin (LT(I))\rangle.$$

Demostración. Sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de I. Notamos que si $x^\alpha \notin (LT(I)) = (LT(G))$, entonces $\overline{x^\alpha}^G = x^\alpha$, así que la aplicación ϕ restringida a $(k[x_1, \ldots, x_n]/I)_{\leq d}$ contiene en su imagen el espacio

$$k\langle x^\alpha \mid \deg x^\alpha \leq d,\ x^\alpha \notin (LT(I))\rangle.$$

Necesitamos verificar que este espacio coincide con la imagen, y para esto sería suficiente ver que

$$\deg \overline{f}^G \leq \deg f.$$

Recordemos que para un polinomio $f \in k[x_1, \ldots, x_n]$ el resto $\overline{f}^G$ puede ser obtenido del algoritmo de división que nos da

$$f = q_1 g_1 + \cdots + q_s g_s + \overline{f}^G,$$

donde

1) los monomios de $\overline{f}^G$ no son divisibles por $LT(g_i)$,

2) $LM(q_i g_i) \preceq LM(f)$ si $q_i g_i \neq 0$.

Estas condiciones definen a $\overline{f}^G$ de modo único. Ahora

$$LM(\overline{f}^G) \preceq LM(f - (q_1 g_1 + \cdots + q_s g_s)) \preceq LM(f),$$

y nuestra hipótesis sobre el orden monomial implica que

$$\deg \overline{f}^G \leq \deg f.$$ ■

24.10. Teorema. *Fijemos algún orden monomial $\preceq$ sobre $k[x_1, \ldots, x_n]$ que respete el grado. Para cualquier ideal $I \subseteq k[x_1, \ldots, x_n]$ se tiene*

$$H_I(t) = H_{(LT(I))}(t).$$

Demostración. Según el lema anterior,

$$\widetilde{h}(d) := \dim_k (k[x_1, \ldots, x_n]/I)_{\leq d}$$

depende solamente de $(LT(I))$. Esto quiere decir que si $(LT(I)) = (LT(J))$, entonces $\widetilde{H}_I(t) = \widetilde{H}_J(t)$, y luego $H_I(t) = H_J(t)$. En particular, tenemos $(LT(LT(I))) = (LT(I))$. ■

Ejercicio 61. Encuentre un ideal particular $I \subset k[x_1, \ldots, x_n]$ y orden monomial $\preceq$ que no respeta el grado tales que $H_I(t) \neq H_{(LT(I))}(t)$.

24.11. Ejemplo. Consideremos el ideal $I = (x^2 - y, x^3 - z) \subset k[x, y, z]$. La base de Gröbner reducida de I respecto al orden *grevlex* viene dada por

$$G = \{y^2 - xz,\ xy - z,\ x^2 - y\}.$$

Necesitamos entonces contar los monomios que no pertenecen al ideal (y^2, xy, x^2).

- para $d = 0$ tenemos el monomio 1,
- para $d > 0$ tenemos tres monomios xz^{d-1}, yz^{d-1}, z^d.

Entonces,

$$H_I(t) = 1 + 3t + 3t^2 + 3t^3 + \cdots = 1 + \frac{3t}{1-t} = \frac{2t+1}{1-t}.$$

Recordemos que el conjunto algebraico $\mathbf{V}(I)$ es la cúbica torcida (véase 19.13 y 22.18). ▲

24.3 Algoritmo recursivo

Acabamos de reducir el cálculo de la serie de Hilbert al caso de ideal monomial. Ahora vamos a obtener un algoritmo recursivo para los ideales monomiales.

24.12. Lema. *Para el ideal principal $I = (x^\alpha) \subseteq k[x_1, \dots, x_n]$ generado por un monomio x^α se tiene*

$$H_I(t) = \frac{1 - t^{\deg x^\alpha}}{(1-t)^n}.$$

Demostración. La multiplicación por x^α es una aplicación k-lineal inyectiva sobre $k[x_1, \dots, x_n]$ que nos da sucesiones exactas cortas de espacios vectoriales sobre k

$$0 \to k[x_1, \dots, x_n]_{d-\deg x^\alpha} \xrightarrow{\times x^\alpha} k[x_1, \dots, x_n]_d \to \frac{k[x_1, \dots, x_n]_d}{x^\alpha \cdot k[x_1, \dots, x_n]_{d-\deg x^\alpha}} = A_d \to 0$$

donde

$$k[x_1, \dots, x_n]_{d-\deg x^\alpha} = 0 \text{ si } d < \deg x^\alpha.$$

Entonces,

$$\dim_k(k[x_1, \dots, x_n]_{d-\deg x^\alpha}) + \dim_k(A_d) = \dim_k(k[x_1, \dots, x_n]_d),$$

lo que nos lleva a la identidad de series formales

$$t^{\deg x^\alpha} \sum_{d \geq 0} \dim_k(k[x_1, \dots, x_n]_d)\, t^d + \sum_{d \geq 0} \dim_k(A_d)\, t^d = \sum_{d \geq 0} \dim_k(k[x_1, \dots, x_n]_d)\, t^d,$$

de donde

$$H_I(t) = \sum_{d \geq 0} \dim_k(A_d)\, t^d = (1 - t^{\deg x^\alpha})\, H_{(0)}(t) = \frac{1 - t^{\deg x^\alpha}}{(1-t)^n}.$$ ■

Ejercicio 62. Demuestre que en general, para un polinomio no nulo $f \in k[x_1, \dots, x_n]$, el ideal principal correspondiente $I = (f) \subseteq k[x_1, \dots, x_n]$ tiene la serie de Hilbert

$$H_I(t) = \frac{1 - t^{\deg f}}{(1-t)^n}.$$

(Use el argumento de arriba, remplazando los espacios V_d por $V_{\leq d}$.)

24.13. Lema (Inclusión-exclusión). *Para dos ideales monomiales $I, J \subseteq k[x_1, \dots, x_n]$ se tiene*

$$H_{I+J}(t) = H_I(t) + H_J(t) - H_{I \cap J}(t).$$

Demostración. Consideremos los espacios vectoriales

$$I_{\leq d} := \{f \in I \mid \deg f \leq d\}, \quad J_{\leq d} := \{f \in J \mid \deg f \leq d\}.$$

Notamos que

$$I_{\leq d} \cap J_{\leq d} = (I \cap J)_{\leq d} := \{h \in I \cap J \mid \deg h \leq d\}.$$

Dado que los ideales en cuestión son monomiales, tenemos

$$I_{\leq d} = k\langle x^\alpha \in I \mid \deg x^\alpha \leq d\rangle, \quad J_{\leq d} = k\langle x^\beta \in J \mid \deg x^\beta \leq d\rangle.$$

De aquí se ve que

$$I_{\leq d} + J_{\leq d} = (I + J)_{\leq d} := \{f + g \mid f \in I,\, g \in J,\, \deg f, \deg g \leq d\}.$$

El segundo teorema de isomorfía nos da entonces

$$\frac{(I+J)_{\leq d}}{J_{\leq d}} \cong \frac{I_{\leq d}}{(I\cap J)_{\leq d}},$$

de donde

$$\dim_k((I+J)_{\leq d}) - \dim_k(J_{\leq d}) = \dim_k(I_{\leq d}) - \dim_k((I\cap J)_{\leq d}).$$

Entonces,

$$\begin{aligned}\Big(\dim_k(k[x_1,\ldots,x_n]_{\leq d}) - \dim_k((I+J)_{\leq d})\Big) - \Big(\dim_k(k[x_1,\ldots,x_n]_{\leq d}) - \dim_k(J_{\leq d})\Big)\\ = \Big(\dim_k(k[x_1,\ldots,x_n]_{\leq d}) - \dim_k(I_{\leq d})\Big) - \Big(\dim_k(k[x_1,\ldots,x_n]_{\leq d}) - \dim_k((I\cap J)_{\leq d})\Big),\end{aligned}$$

así que

$$\widetilde{h}_{I+J}(d) - \widetilde{h}_J(d) = \widetilde{h}_I(d) - \widetilde{h}_{I\cap J}(d).$$

Esto nos da la identidad

$$\widetilde{H}_{I+J}(t) = \widetilde{H}_I(t) + \widetilde{H}_J(t) - \widetilde{H}_{I\cap J}(t),$$

y luego

$$H_{I+J}(t) = H_I(t) + H_J(t) - H_{I\cap J}(t).$$ ■

El siguiente ejercicio representa una generalización del resultado que acabamos de probar.

Ejercicio 63. Se dice que un ideal $I \subseteq k[x_1,\ldots,x_n]$ es **homogéneo** si I está generado por **polinomios homogéneos**

$$f = c_{\alpha(1)}\, x^{\alpha(1)} + \cdots + c_{\alpha(s)}\, x^{\alpha(s)},$$

donde

$$\deg x^{\alpha(1)} = \cdots = \deg x^{\alpha(s)}.$$

Por ejemplo, $(x^3 - xz^2 - y^2z,\ x+y)$ es un ideal homogéneo.

Demuestre que si $I, J \subseteq k[x_1,\ldots,x_n]$ son homogéneos, entonces

$$H_{I+J}(t) = H_I(t) + H_J(t) - H_{I\cap J}(t).$$

Encuentre un contraejemplo para el caso no-homogéneo.

Los dos lemas de arriba nos llevan al siguiente método recursivo de calcular la serie de Hilbert $H_I(t)$ para un ideal monomial

$$I = (x^{\alpha(1)},\ldots,x^{\alpha(s)}) \subseteq k[x_1,\ldots,x_n].$$

Primero, si $I = (x^\alpha)$ está generado por un monomio, entonces

$$H_I(t) = \frac{1 - t^{\deg x^\alpha}}{(1-t)^n}$$

según 24.12. Si I está generado por más de un monomio, entonces podemos escribir

$$I = (x^{\alpha(1)}) + J, \quad J := (x^{\alpha(2)},\ldots,x^{\alpha(s)}).$$

Ahora

$$(x^{\alpha(1)}) \cap J = (\operatorname{mcm}(x^{\alpha(1)}, x^{\alpha(2)}),\ldots,\operatorname{mcm}(x^{\alpha(1)}, x^{\alpha(s)})).$$

(véase el ejercicio) y

$$H_I(t) = \frac{1 - t^{\deg x^\alpha}}{(1-t)^n} + H_J(t) - H_{(x^{\alpha(1)})\cap J}(t). \tag{24.1}$$

Notamos que los ideales monomiales J y $(x^{\alpha(1)}) \cap J$ tienen un generador menos, así que sus series de Hilbert pueden ser calculadas recursivamente.

En fin, si I no es un ideal monomial, podemos calcular su base de Gröbner $G = \{g_1, \dots, g_s\}$ respecto a un orden que respeta el grado, y luego

$$H_I(t) = H_{(LT(g_1),\dots,LT(g_s))}(t).$$

Notamos que el método descrito no se ve muy eficaz: si la base de Gröbner de I tiene s elementos, entonces la fórmula (24.1) tendrá que ser aplicada un número exponencial en s de veces. (Y no es muy sorprendente: esta fórmula esconde todas las dificultades combinatorias del conteo de monomios.) Sin embargo, en práctica el cálculo de la misma base de Gröbner suele ser mucho más pesado, y nuestro algoritmo la calcula una sola vez, usando un orden monomial eficaz como *grevlex*.

24.14. Ejemplo. Asumamos que $\operatorname{char} k \neq 2$. Consideremos el ideal

$$I = (x^2 + y^2 - z^2,\ x + y) \subset k[x, y, z],$$

Su base de Gröbner respecto al orden lexicográfico graduado viene dada por

$$(x + y,\ 2y^2 - z^2).$$

Luego,

$$(LT(I)) = (x, y^2).$$

Calculamos

$$H_I(t) = H_{(x,y^2)}(t) = H_{(x)}(t) + H_{(y^2)}(t) - H_{xy^2}(t) = \frac{1-t}{(1-t)^3} + \frac{1-t^2}{(1-t)^3} - \frac{1-t^3}{(1-t)^3} = \frac{t^3 - t^2 - t + 1}{(1-t)^3} = \frac{1+t}{1-t}.$$

Geométricamente, $\mathbf{V}(I)$ es la intersección del cono $x^2 + y^2 = z^2$ con el hiperplano $x + y = 0$. La dimensión de Krull correspondiente es igual a 1, como uno puede ver desde las intersecciones

$$I \cap k[x, y] = (x + y), \quad I \cap k[x, z] = I \cap k[y, z] = (2x^2 - z^2), \quad I \cap k[x] = I \cap k[y] = 0. \qquad \blacktriangle$$

Entonces, hemos obtenido un algoritmo bastante eficaz para calcular la serie de Hilbert. Aunque en general este requiere muchas aplicaciones de la fórmula $H_{I+J}(t) = H_I(t) + H_J(t) - H_{I\cap J}(t)$, el cálculo más pesado suele ser el de la base de Gröbner de I, y esta se calcula solo una vez, respecto al orden *grlex* o *grevlex*.

Ejercicio 64. Comprueba sus cálculos del ejercicio 60 usando el algoritmo recursivo.

Ejercicio 65. Calcule la serie de Hilbert del ideal $(xy + z,\ xy^3) \subset k[x, y, z]$ mediante una base de Gröbner y el algoritmo recursivo.

Ejercicio 66. Consideremos un ideal $I \subseteq k[x_1, \dots, x_m]$. Sea $\widetilde{I}$ el ideal generado por los elementos de I en $k[x_1, \dots, x_m, y_1, \dots, y_n]$. Describa la relación entre las series de Hilbert $H_I(t)$ y $H_{\widetilde{I}}(t)$.

24.4 Polinomio de Hilbert

El algoritmo descrito arriba nos da el siguiente resultado teórico.

24.15. Teorema. *Para cualquier ideal $I \subseteq k[x_1, \dots, x_n]$ la serie de Hilbert de I tiene forma*

$$H_I(t) = \frac{a_m t^m + \dots + a_1 t + a_0}{(1-t)^n}, \quad \textit{donde } a_i \in \mathbb{Z}.$$

Este resultado implica que la función de Hilbert $h_I(d)$ coincide con valores de algún polinomio racional $p_I \in \mathbb{Q}[x]$ para d suficientemente grande.

24.16. Corolario. *Existe un polinomio $p_I(x) \in \mathbb{Q}[x]$ cuyos valores en los números naturales coinciden con los valores de la función de Hilbert $h_I(d)$ para d suficientemente grande:*

$$p_I(d) = h_I(d) \text{ para } d \gg 0. \tag{24.2}$$

Demostración. El polinomio en cuestión viene dado por

$$p_I := \sum_{0 \le i \le m} a_i \binom{x-i+n-1}{n-1} \in \mathbb{Q}[x].$$

Recordemos que

$$\frac{1}{(1-t)^n} = \sum_{d \ge 0} \binom{n+d-1}{d} t^d = \sum_{d \ge 0} \binom{d+n-1}{n-1} t^d.$$

Ahora

$$\frac{t^i}{(1-t)^n} = \sum_{d \ge i} \binom{d-i+n-1}{d} t^d,$$

así que

$$H_I(t) = \sum_{0 \le i \le m} \sum_{d \ge i} a_i \binom{d-i+n-1}{d} t^d = \sum_{d \ge 0} \left(\sum_{0 \le i \le \min\{d,m\}} a_i \binom{d-i+n-1}{d} \right) t^d.$$

En particular, si $d \ge m$, el coeficiente de t^d coincide con $p_I(d)$. ■

24.17. Definición. El polinomio $p_I \in \mathbb{Q}[x]$ de arriba se llama el **polinomio de Hilbert** de I.

Notamos que la identidad (24.2) caracteriza a p_I de modo único: un polinomio $p_I \in \mathbb{Q}[x]$ se determina por un número finito de sus valores $p_I(d)$.

24.18. Ejemplo. Volvamos al ejemplo 24.14, donde hemos calculado que para el ideal

$$(x^2 + y^2 - z^2,\ x + y) \subset k[x, y, z]$$

la serie de Hilbert viene dada por

$$H_I(t) = \frac{t+1}{1-t} = 1 + 2t + 2t^2 + 2t^3 + \cdots.$$

El polinomio de Hilbert correspondiente es

$$p_I(x) = \binom{x-0}{0} + \binom{x-1}{0} = 2.$$

Y en efecto,

$$h_I(d) = 2 \quad \text{para } d > 0.$$ ▲

24.19. Ejemplo. En el ejemplo 24.5 hemos calculado que para el ideal monomial $I = (xz, yz) \subset k[x, y, z]$ la serie de Hilbert viene dada por

$$H_I(t) = \frac{-t^2 + t + 1}{(1-t)^2} = 1 + 3t + 4t^2 + 5t^3 + 6t^4 + \cdots$$

El polinomio de Hilbert correspondiente será

$$p_I(x) = \binom{x+1}{1} + \binom{x}{1} - \binom{x-1}{1} = (x+1) + x - (x-1) = x + 2.$$ ▲

24.20. Ejemplo. Para dar un ejemplo más interesante, consideremos el ideal

$$I = (x^4 + y^4 + z^4 + w^4) \subset k[x, y, z, w].$$

Es fácil calcular la serie de Hilbert correspondiente (la base de Gröbner reducida respecto a cualquier orden monomial es $G = \{x^4 + y^4 + z^4 + w^4\}$):

$$H_I(t) = \frac{1 - t^4}{(1-t)^4} = \frac{t^3 + t^2 + t + 1}{(1-t)^3} = 1 + 4t + 10t^2 + 20t^3 + 34t^4 + 52t^5 + 74t^6 + 100t^7 + \cdots$$

Luego, el polinomio de Hilbert correspondiente viene dado por

$$p_I(x) = \binom{x+2}{2} + \binom{x+1}{2} + \binom{x}{2} + \binom{x-1}{2} = \frac{1}{2!}\Big((x+2)(x+1) + (x+1)x + x(x-1) + (x-1)(x-2)\Big) = 2x^2 + 2.$$

También podríamos escribir usando la expresión $\frac{1-t^4}{(1-t)^4}$

$$p_I(x) = \binom{x+3}{3} - \binom{x-1}{3} = \frac{1}{3!}\Big((x+3)(x+2)(x+1) - (x-1)(x-2)(x-3)\Big) = 2x^2 + 2. \qquad \blacktriangle$$

Ejercicio 67. Calcule el polinomio de Hilbert para los ideales del ejercicio 60. ¿Para cuáles valores de d se cumple $h_I(d) = p_I(d)$?

Ejercicio 68. Hemos probado en clase que para la serie de Hilbert

$$H_I(t) = \sum_{d \geq 0} h_I(d)\, t^d = \frac{a_m\, t^m + \cdots + a_1\, t + a_0}{(1-t)^n}$$

el polinomio de Hilbert $p_I \in \mathbb{Q}[x]$ cumple

$$p_I(d) = h_I(d) \quad \text{para } d \gg 0.$$

Demuestre que esto sucede precisamente para $d > m - n$.

24.5 Series de Hilbert en Macaulay2

He aquí algunas de las funciones de Macaulay2 relacionadas con series de Hilbert. Sea I un ideal en algún anillo de polinomios $k[x_1, \ldots, x_n]$.

- `hilbertFunction (`d`,`I`)` — devuelve la función de Hilbert $h_I(d)$.

```
i : R = QQ[x,y];

i : for d in 0..10 list hilbertFunction (d, ideal (x^2-y))

o = {1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2}

o : List
```

- `hilbertSeries (`I`)` — devuelve la serie de Hilbert $H_I(t)$ como una expresión de la forma

$$\frac{a_k\, t^k + \cdots + a_1\, t + a_0}{(1-t)^n}.$$

  Si queremos reducir esta fracción y escribirla como $\frac{f}{(1-t)^m}$, donde $(1-t) \nmid f$, se puede usar la función `reduceHilbert`.

```
i : R = QQ[x,y];

i : hilbertSeries ideal (x^2-y)

          2
     1 - T
o = --------
           2
    (1 - T)

o : Expression of class Divide

i : reduceHilbert (oo)

     1 + T
o = -------
    (1 - T)

o : Expression of class Divide
```

25 Digresión: subálgebras de k-álgebras finitamente generadas

Sean

$$A := k[x_1, \dots, x_n]/I$$

una k-álgebra finitamente generada y $a_1, \dots, a_m \in A$ algunos de sus elementos. La subálgebra

$$k[a_1, \dots, a_m] \subseteq A$$

generada por $a_1, \dots, a_m$ es también finitamente generada. Para los cálculos sería útil expresar $k[a_1, \dots, a_m]$ como un cociente de anillo de polinomios. Notamos que los elementos $a_1, \dots, a_m$ se representan por algunos polinomios

$$g_1, \dots, g_m \in k[x_1, \dots, x_n].$$

Luego, $k[a_1, \dots, a_m]$ es precisamente la imagen del homomorfismo

$$\begin{aligned} \phi\colon k[t_1, \dots, t_m] &\to k[x_1, \dots, x_n]/I, \\ t_i &\mapsto \overline{g_i}. \end{aligned}$$

Entonces, por el primer teorema de isomorfía,

$$k[a_1, \dots, a_m] \cong k[t_1, \dots, t_m]/\ker\phi.$$

Necesitamos un algoritmo* para calcular el núcleo de ϕ.

25.1. Proposición. *Si $I = (h_1, \dots, h_s)$ para algunos polinomios $h_1, \dots, h_s \in k[x_1, \dots, x_n]$, consideremos el ideal*

$$J := (h_1, \dots, h_s, g_1 - t_1, \dots, g_m - t_m) \subseteq k[t_1, \dots, t_m, x_1, \dots, x_n].$$

Luego,

$$\ker\phi = J \cap k[t_1, \dots, t_m].$$

*Esta sección probablemente debe aparecer antes, con la discusión de k-algebras finitamente generadas y eliminación.

Demostración. Para todo polinomio $f \in k[t_1, \ldots, t_m]$ se tiene por la definición de J

$$f(g_1, \ldots, g_m) - f(t_1, \ldots, t_m) \in J.$$

Ahora si $f \in \ker \phi$, entonces $f(g_1, \ldots, g_m) \in I$, y por la ecuación de arriba $f(t_1, \ldots, t_m) \in J$. Viceversa, asumamos que $f \in J \cap k[t_1, \ldots, t_m]$. Esto quiere decir que

$$f(t_1, \ldots, t_m) = \sum_{1 \le i \le s} p_i h_i + \sum_{1 \le j \le m} q_j (g_j - t_j)$$

para algunos polinomios $p_i, q_j \in k[t_1, \ldots, t_m, x_1, \ldots, x_n]$. Al sustituir g_j en lugar de t_j en la identidad de arriba, nos queda

$$f(g_1, \ldots, g_m) = \sum_{1 \le i \le s} \underbrace{p_i(g_1, \ldots, g_m, x_1, \ldots, x_n)}_{\in k[x_1, \ldots, x_n]} \underbrace{h_i(x_1, \ldots, x_n)}_{\in I} \in I.$$

Esto quiere decir que $f \in \ker \phi$. ∎

25.2. Ejemplo. Asumamos que $\operatorname{char} k \neq 2$ y consideremos la k-álgebra

$$A := \frac{k[x, y, z]}{(x^2 + y^2 + z^2 - 1, x + y + z)}.$$

Calculemos la subálgebra $k[\overline{x}, \overline{y}]$. Según la proposición de arriba, el núcleo del homomorfismo

$$\begin{aligned} \phi \colon k[t, u] &\to \frac{k[x, y, z]}{(x^2 + y^2 + z^2 - 1, x + y + z)}, \\ t &\mapsto \overline{x}, \\ u &\mapsto \overline{y} \end{aligned}$$

viene dado por

$$(x^2 + y^2 + z^2 - 1, x + y + z, x - t, y - u) \cap k[t, u].$$

Hemos aprendido a calcular estos ideales en §18.1: basta calcular una base de Gröbner respecto al orden lexicográfico con $x \succ y \succ z \succ t \succ u$ y quitar los elementos donde aparecen x, y, z.

```
i : R = QQ[x,y,z,t,u, MonomialOrder => Lex];

i : groebnerBasis ideal (x^2 + y^2 + z^2 - 1, x+y+z, x-t, y-u)

o = | 2t2+2tu+2u2-1 z+t+u y-u x-t |

             1       4
o : Matrix R  <--- R
```

O de una vez,

```
i : eliminate ({x,y,z}, ideal (x^2 + y^2 + z^2 - 1, x+y+z, x-t, y-u))

             2            2
o = ideal(2t  + 2t*u + 2u  - 1)

o : Ideal of R
```

Entonces,

$$\ker\phi = (2t^2 + 2tu + 2u^2 - 1).$$

De hecho, en Macaulay2 se puede definir un homomorfismo de k-álgebras y calcular su núcleo usando la función `kernel (`ϕ`)`.

```
i : f = map (QQ[x,y,z]/(x^2+y^2+z^2-1, x+y+z), QQ[t,u], {x,y});

                      QQ[x, y, z]
o : RingMap ---------------------------- <--- QQ[t, u]
              2    2    2
            (x  + y  + z  - 1, x + y + z)

i : kernel (f)

             2             2
o = ideal(2t  + 2t*u + 2u  - 1)

o : Ideal of QQ[t, u]
```

La sintaxis para definir un homomorfismo

$$k[t_1,\dots,t_m]/J \to k[x_1,\dots,x_n]/I$$

es la siguiente:

$$\texttt{map (}k[x_1,\dots,x_n]/I\texttt{, }\ k[t_1,\dots,t_m]/J\texttt{, \{ }g_1,\dots,g_m\texttt{ \})}$$

donde el tercer argumento es la lista de imágenes de los generadores $t_1,\dots,t_m$. Note que aquí el primer argumento es el *codominio* del homomorfismo y el segundo es el *dominio*. Para más información, consulte la documentación de Macaulay2 sobre el tipo `RingMap` (por ejemplo, escriba "`help RingMap`" en la sesión interactiva).

Entonces, tenemos la subálgebra

$$\frac{k[x,y]}{(2x^2+2xy+2y^2-1)} \hookrightarrow \frac{k[x,y,z]}{(x^2+y^2+z^2-1,\, x+y+z)}.$$

Geométricamente, esta inclusión corresponde a la proyección

$$\begin{aligned}\mathbf{V}(x^2+y^2+z^2-1,\, x+y+z) &\to \mathbf{V}(2x^2+2xy+2y^2-1),\\ (x,y,z) &\mapsto (x,y).\end{aligned}$$

Notamos que $\mathbf{V}(x^2+y^2+z^2-1,\, x+y+z)$ es la intersección de la esfera unitaria $\mathbf{V}(x^2+y^2+z^2-1)$ con el plano $\mathbf{V}(x+y+z)$, y su proyección al plano xy es precisamente el elipse $\mathbf{V}(2x^2+2xy+2y^2-1)$. ▲

Ejercicio 69. Calcule la subálgebra

$$k[\overline{x},\overline{y}] \subset k[x,y,z]/(x^2+y^2-z^2,\, x+y+z).$$

Ejercicio 70. Usando los métodos de arriba calcule que para el homomorfismo

$$\phi\colon k[x,y,z] \to k[t], \quad x \mapsto t^3, y \mapsto t^4, z \mapsto t^5$$

se tiene

$$\ker\phi = (y^2 - xz,\, yz - x^3,\, z^2 - x^2y).$$

26 Normalización de Noether

Recordemos algunas definiciones y resultados relacionados con extensiones integrales de anillos. Hemos visto este material en el curso de álgebra conmutativa, pero voy a dar también las referencias correspondientes en los libros de Eisenbud y Atiyah–Macdonald.

26.1. Definición. Sea $A \subseteq B$ una extensión de anillos. Se dice que un elemento $b \in B$ es **integral** sobre A si existe un polinomio mónico

$$f = x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0 \in A[x]$$

tal que $f(b) = 0$. Se dice que $A \subseteq B$ es una extensión **intergral** si todo elemento de B es integral sobre A.

Recordemos la siguiente caracterización de integridad.

26.2. Lema. *Un elemento $b \in B$ es integral sobre A si y solamente si $A[b]$ es un A-módulo finitamente generado.*

Demostración. Véase [Eis2004, Corollary 4.6] o [AM1969, Proposition 5.1]. ■

26.3. Teorema. *Para una extensión de anillos $A \subseteq B$, los elementos de B que son integrales sobre A forman una A-subálgebra de B. En particular, si B está generado como A-álgebra por elementos integrales sobre A, entonces B es integral sobre A.*

Demostración. Véase [Eis2004, Theorem 4.2] o [AM1969, Corollary 5.3]. ■

26.4. Lema. *Para extensiones de anillos $A \subseteq B \subseteq C$, si B es integral sobre A y C es integral sobre B, entonces C es integral sobre A.*

Demostración. Véase [AM1969, Corollary 5.4] ■

Recordemos el siguiente resultado importante.

26.5. Teorema de Cohen–Seidenberg ("going up"). *Sea $A \subseteq B$ una extensión integral de anillos.*

1) *Para todo ideal primo $\mathfrak{p} \subset A$ existe un ideal primo $\mathfrak{q} \subset B$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$.*
2) *Si para dos ideales primos $\mathfrak{q} \subseteq \mathfrak{q}' \subset B$ se cumple $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$, entonces $\mathfrak{q} = \mathfrak{q}'$.*

Demostración. Véase por ejemplo [Eis2004, Proposition 4.15, Corollary 4.18] o [AM1969, Theorem 5.10, Corollary 5.9]. ■

El teorema de Cohen–Seidenberg nos permite concluir que las extensiones integrales preservan la dimensión.

26.6. Lema. *Si $A \subseteq B$ una extensión integral de anillos, entonces*

$$\dim A = \dim B.$$

Demostración. Una cadena de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset A$$

se levanta gracias a la primera parte de 26.5 a una cadena de ideales primos

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n \subset B,$$

tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, y en particular las inclusiones de arriba son propias. Viceversa, dada una cadena de ideales primos

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n \subset B,$$

se obtiene una cadena de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset A,$$

donde $\mathfrak{p}_i := \mathfrak{q}_i \cap A$ y las inclusiones son estrictas por la segunda parte de 26.5. ■

26.7. Comentario. Para k-álgebras finitamente generadas el último resultado puede ser deducido de 22.10 sin recurrir a 26.5.

26.8. Ejemplo. Consideremos la k-álgebra $A := k[x,y]/(x^3 - y^2)$ y la subálgebra $k[\overline{y}]$. Notamos que $k[\overline{y}]$ es precisamente la imagen del homomorfismo inyectivo

$$k[t] \to k[x,y]/(x^3 - y^2), \quad t \mapsto \overline{y},$$

así que $k[\overline{y}] \cong k[t]$. El elemento $\overline{x} \in A$ satisface la relación mónica $\overline{x}^3 - \overline{y}^3 = 0$, así que es integral sobre $k[\overline{y}]$. Podemos concluir que $k[\overline{y}] \subset A$ es una extensión integral. De la misma manera se demuestra que $k[\overline{x}] \subset A$ es una extensión integral.

Consideremos ahora la k-álgebra $B := k[x,y,z]/(x - z^2, y - z^3)$. El homomorfismo natural

$$k[x,y] \hookrightarrow k[x,y,z] \twoheadrightarrow k[x,y,z]/(x - z^2, y - z^3)$$

induce un homomorfismo inyectivo

$$k[x,y]/(x^3 - y^2) \hookrightarrow k[x,y,z]/(x - z^2, y - z^3).$$

El elemento $\overline{z} \in B$ satisface las relaciones

$$\overline{z}^2 - \overline{x}, \quad \overline{z}^3 - \overline{y}$$

que significan que $\overline{z}$ es integral sobre A. Entonces, $B = A[\overline{z}]$ es integral sobre A. Tenemos entonces una cadena de extensiones integrales

$$k[t] \cong k[\overline{y}] \subset A \subset B,$$

y de hecho

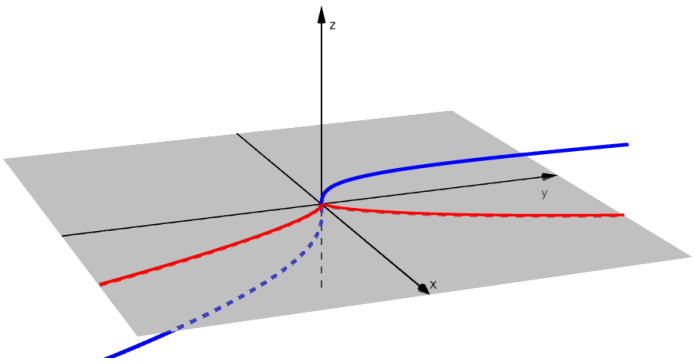
$$\dim k[t] = \dim A = \dim B = 1,$$

lo que coincide con el resultado de 26.6.

Geométricamente, el homomorfismo inyectivo $A \hookrightarrow B$ corresponde a la proyección natural

$$\begin{aligned} \mathbf{V}(x - z^2, y - z^3) &\to \mathbf{V}(x^3 - y^2), \\ (x,y,z) &\mapsto (x,y), \end{aligned}$$

donde $\mathbf{V}(x - z^2, y - z^3)$ es la cúbica torcida. ▲



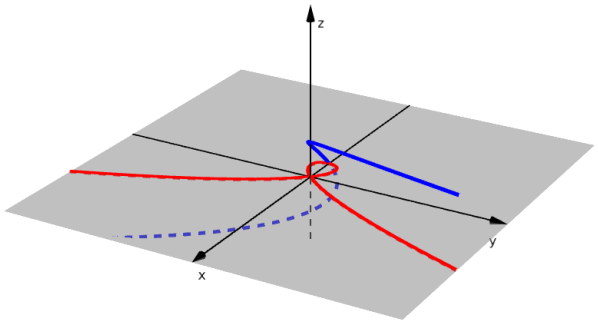
Ejercicio 71. Consideremos las k-álgebras

$$A := k[x,y]/(x^2(x+1)-y^2), \quad B := k[x,y,z]/(x-z^2+1, y-z^3+z).$$

Demuestre que se tiene un homomorfismo inyectivo natural $A \hookrightarrow B$, y B es integral sobre A.

Al homomorfismo $A \hookrightarrow B$ del ejercicio anterior corresponde la proyección natural entre los conjuntos algebraicos

$$\mathbf{V}(x-z^2+1, y-z^3+z) \subset \mathbb{A}^3(k) \quad \text{y} \quad \mathbf{V}(x^2(x+1)-y^2) \subset \mathbb{A}^2(k).$$



26.1 Normalización de Noether

Como hemos visto en el teorema 22.10, si A es una k-álgebra finitamente generada de dimensión d, entonces existen elementos algebraicamente independientes $a_1,\ldots,a_d \in A$. El siguiente resultado nos dice que estos elementos pueden ser escogidos de tal manera que $k[a_1,\ldots,a_d] \subseteq A$ es una extensión integral.

26.9. Teorema de normalización de Noether. *Sea $A = k[x_1,\ldots,x_n]/I$ una k-álgebra finitamente generada no nula. Entonces, existen elementos*

$$a_1,\ldots,a_d \in A$$

tales que

1) *$a_1,\ldots,a_d$ son algebraicamente independientes sobre k;*
2) *A es una extensión integral de $k[a_1,\ldots,a_d]$;*
3) *A es finitamente generado como un módulo sobre $k[a_1,\ldots,a_d]$;*
4) *$d = \dim A$.*

Antes de lanzarnos en la prueba, expliquemos cuál es el punto de lo que vamos a hacer. En el ejemplo 26.8 de arriba teníamos $A = k[x,y]/(x^3-y^2)$, y allí es fácil ver que A es integral sobre $k[\overline{x}]$ y también sobre $k[\overline{y}]$: tenemos una relación integral de $\overline{y}$ sobre $k[\overline{x}]$ dada por $\overline{y}^2 - \overline{x}^3 = 0$, y de la misma manera una relación integral de $\overline{x}$ sobre $k[\overline{y}]$. Sin embargo, no es siempre posible obtener una dependencia integral directamente. Por ejemplo, en el caso de $A = k[x_1,x_2]/(x_1x_2-1)$, el polinomio $f = x_1x_2-1$ no nos da una dependencia integral de $\overline{x_2}$ sobre $k[\overline{x_1}]$, ni de $\overline{x_1}$ sobre $k[\overline{x_2}]$ (de hecho, tales dependencias integrales simplemente no existen). La siguiente prueba consiste en un truco que permite sustituir x_2 por otra expresión y_2 en x_1x_2-1 para poder sacar una dependencia integral de x_1 sobre $k[\overline{y_2}] \subseteq A$.

Demostración. Procedamos por inducción sobre n. La base de inducción es el caso cuando $n = 0$. Para el paso inductivo, notamos que si $I = 0$, entonces bastaría tomar $a_i = x_i$ para $i = 1, \dots, n$. Asumamos entonces que $0 \neq I \subsetneq A$. Todo polinomio no nulo $f \in I$ puede ser escrito como

$$f = \sum_{(i_1,\dots,i_n)\in S} c_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

donde $S \subseteq \mathbb{N}^n$ es un conjunto finito no vacío. Escojamos $\delta > \deg f$ y pongamos

$$y_i := x_i - x_1^{\delta^{i-1}}, \quad i = 2, \dots, n.$$

Ahora

$$f = f(x_1, y_2 + x_1^{\delta}, y_3 + x_1^{\delta^2}, \dots, y_n + x_1^{\delta^{n-1}}) = \sum_{(i_1,\dots,i_n)\in S} c_{i_1,\dots,i_n} \left(x_1^{s(i_1,\dots,i_n)} + g_{i_1,\dots,i_n}(x_1, y_2, \dots, y_n) \right),$$

donde

$$s(i_1, \dots, i_n) := i_1 + i_2\,\delta + i_3\,\delta^2 + \cdots + i_n\,\delta^{n-1},$$

y los polinomios $g_{i_1,\dots,i_n}$ cumplen

$$\deg_{x_1}(g_{i_1,\dots,i_n}) < s(i_1, \dots, i_n).$$

Notamos que la función

$$(i_1, \dots, i_n) \mapsto s(i_1, \dots, i_n)$$

es inyectiva sobre S por nuestra elección de δ, y por ende existe único $(i_1, \dots, i_n) \in S$ tal que el valor $N := s(i_1, \dots, i_n)$ es el máximo posible. El polinomio f no es constante, así que $N > 0$. Podemos escribir

$$f = c_{i_1,\dots,i_n} x_1^N + h(x_1, y_2, \dots, y_n),$$

donde $\deg_{x_1}(h) < N$. Luego,

$$x_1^N + c_{i_1,\dots,i_n}^{-1} h(x_1, y_2, \dots, y_n) \in I. \tag{26.1}$$

Consideremos la k-álgebra

$$C := k[\overline{y_2}, \dots, \overline{y_n}] \subseteq A.$$

Tenemos

$$A = C[\overline{x_1}],$$

donde $\overline{x_1}$ es un elemento integral sobre A gracias a la relación (26.1). Esto implica también que A es un módulo finitamente generado sobre C (véase el lema 26.2). Entonces, A es integral sobre C. Ahora por inducción, existen elementos $b_1, \dots, b_d \in C$ algebraicamente independientes sobre k tales que C es integral sobre $k[b_1, \dots, b_d]$ y es un módulo finitamente generado sobre $k[b_1, \dots, b_d]$. Luego, A cumple las mismas propiedades sobre $k[b_1, \dots, b_d]$ (véase el lema 26.4).

Notamos que si $a_1, \dots, a_d$ son algebraicamente independientes, entonces

$$\dim k[a_1, \dots, a_d] = \dim k[x_1, \dots, x_d] = d.$$

Ahora si A es integral sobre $k[a_1, \dots, a_d]$, entonces

$$\dim A = \dim k[a_1, \dots, a_d] = d$$

gracias al lema 26.6. ∎

La prueba de arriba es constructiva y contiene un algoritmo para obtener los elementos $a_1, \dots, a_d \in A$.

26.10. Ejemplo. Consideremos $A = k[x_1, x_2]/(x_1x_2 - 1)$. La prueba del teorema de arriba nos sugiere considerar el polinomio

$$f = x_1x_2 - 1.$$

Este tiene grado 2, así que podemos poner $\delta = 3$ y

$$y_2 := x_2 - x_1^3.$$

Ahora

$$f = x_1(x_1^3 + y_2) = x_1^4 + x_1y_2.$$

Esto demuestra que $\overline{x_1} \in A$ es integral sobre $C := k[\overline{y_2}] \cong k[t]$. Entonces, nuestra prueba de la normalización de Noether nos dice que A es integral sobre $k[a]$, donde $a = \overline{x_2} - \overline{x_1}^4$. Luego,

$$k[\overline{x_2} - \overline{x_1}^4] \cong k[t]/\ker\phi,$$

donde

$$\phi\colon k[t] \to k[x_1, x_2]/(x_1x_2 - 1), \quad t \mapsto \overline{x_2 - x_1^4}.$$

Uno puede comprobar que este homomorfismo es inyectivo:

$$\ker\phi = (x_1x_2 - 1,\, x_2 - x_1^4 - t) \cap k[t] = (0),$$

así que

$$k[\overline{x_2} - \overline{x_1}^4] \cong k[t]. \qquad \blacktriangle$$

El elemento $x_2 - x_1^4$ que surgió en el último ejemplo es algo aleatorio, y de hecho la normalización de Noether tiene otra prueba más natural que vamos a ver a continuación.

26.2 Normalización de Noether: forma lineal

26.11. Ejemplo. Continuando el ejemplo de $A = k[x_1, x_2]/(x_1x_2 - 1)$, notamos que las extensiones $k[\overline{x_1}] \subset A$ y $k[\overline{x_2}] \subset A$ *no son* integrales. He aquí un modo geométrico de verlo. Por ejemplo, si la extensión $k[\overline{x_1}] \subset A$ fuera integral, entonces por el teorema de Cohen–Seidenberg habría un ideal primo $\mathfrak{p} \subset A$ tal que $\mathfrak{p} \cap k[\overline{x_1}] = (\overline{x_1})$. Pero $\overline{x_1}$ es invertible en A, su inverso siendo $\overline{x_2}$, así que sobre el ideal primo $(\overline{x_1}) \subset k[\overline{x_1}]$ no puede haber ningún primo en A.

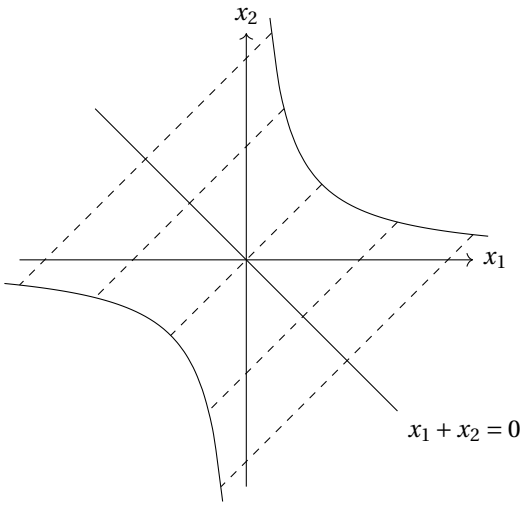
De hecho, la inclusión $k[\overline{x_1}] \subset A$ corresponde a la proyección

$$\begin{aligned} \phi\colon \mathbf{V}(x_1x_2 - 1) &\to \mathbb{A}^1(k), \\ (t, t^{-1}) &\mapsto t, \end{aligned}$$

y el problema es que el punto 0 no está en la imagen de ϕ.

Podemos tomar la proyección ortogonal sobre la recta $x_1 + x_2 = 0$. Cuando $\operatorname{char} k \neq 2$, tal proyección se define mediante el morfismo

$$\begin{aligned} \mathbf{V}(x_1x_2 - 1) &\to \mathbb{A}^2(k)/(x_1 + x_2), \\ (x_1, x_2) &\mapsto \Big(\frac{x_1 - x_2}{2}, \frac{x_2 - x_1}{2}\Big). \end{aligned}$$



Si nos preocupa la característica 2, podemos tomar el morfismo

$$(x, y) \mapsto (x_1 - x_2, x_2 - x_1)\,.$$

Tenemos el homomorfismo correspondiente

$$k[t] \xrightarrow{\cong} k[x_1, x_2]/(x_1 + x_2) \to k[x_1, x_2]/(x_1\,x_2 - 1),$$

donde $t \mapsto x_1$. La imagen de este homomorfismo es $k[\overline{x_1} - \overline{x_2}] \subset A$. Notamos que A es integral sobre $k[\overline{x_1} - \overline{x_2}]$ gracias a las relaciones

$$\overline{x_1}^2 - (\overline{x_1} - \overline{x_2})\,\overline{x_1} - 1 = \overline{x_2}^2 + (\overline{x_1} - \overline{x_2})\,\overline{x_2} - 1 = 0. \qquad \blacktriangle$$

El último ejemplo sugiere que la normalización de Noether puede ser mejorada de la siguiente manera.

26.12. Teorema. *Asumamos que el cuerpo base k es infinito. Sea $A = k[x_1, \ldots, x_n]/I$ una k-álgebra finitamente generada no nula. Entonces, existen n elementos*

$$a_1, \ldots, a_d \in A$$

que cumplen las condiciones del teorema de normalización de Noether y que pueden ser elegidos como combinaciones lineales

$$a_i = x_i + \sum_{d+1 \le j \le n} c_{i,j}\,x_j$$

para algunos $c_{i,j} \in k$.

Demostración. Vamos a seguir la prueba de 26.9, solo necesitamos modificar un poco el paso inductivo. Consideremos un polinomio no nulo

$$f = \sum_{(i_1,\ldots,i_n)\in S} c_{i_1,\ldots,i_n}\,x_1^{i_1} \cdots x_n^{i_n} \in I.$$

Pongamos

$$y_i := x_i - c_i\,x_n \quad \text{para } i = 1, \ldots, n-1$$

para algunos $c_i \in k$ (que vamos a escoger más adelante). Ahora

$$f = f(y_1 + c_1\,x_n, y_2 + c_2\,x_n, \ldots, x_n) = \sum_{(i_1,\ldots,i_n)\in S} c_{i_1,\ldots,i_n}\left(c_1^{i_1} \cdots c_{n-1}^{i_{n-1}}\,x_n^{s(i_1,\ldots,i_n)} + g_{i_1,\ldots,i_n}(y_1, y_2, \ldots, x_n)\right),$$

donde

$$s(i_1,\dots,i_n) := i_1 + i_2 + \cdots + i_n,$$

y los polinomios $g_{i_1,\dots,i_n}$ cumplen

$$\deg_{x_n}(g_{i_1,\dots,i_n}) < s(i_1,\dots,i_n).$$

Sea $f_d \in k[x_1,\dots,x_n]$ la parte homogénea de f de grado $d := \deg f$. Tenemos entonces

$$f = f_d(c_1,\dots,c_{n-1},1)\cdot x_n^d + h(y_1,\dots,y_{n-1},x_n),$$

donde $\deg_{x_n}(h) < d$. Ahora dado que el cuerpo k es infinito (!), podemos escoger algunos elementos $c_1,\dots,c_{n-1} \in k$ de tal manera que $f_d(c_1,\dots,c_{n-1},1) \neq 0$. En este caso la identidad de arriba nos dirá que $\overline{x_n}$ es integral sobre la subálgebra

$$C := k[\overline{y_1},\dots,\overline{y_{n-1}}].$$

Luego, $A = C[\overline{x_n}]$ es integral sobre C. ■

26.13. Ejemplo. Volvamos al álgebra $A = k[x_1,x_2]/(x_1x_2-1)$ para entender cómo funciona el argumento de arriba. Podemos considerar el polinomio

$$f = x_1x_2 - 1$$

y hacer una sustitución lineal $y_1 = x_1 - cx_2$. Luego,

$$f(x_1,x_2) = f(y_1+cx_2,x_2) = (y_1+cx_2)\,x_2 - 1 = cx_2^2 + y_1x_2 - 1.$$

Entonces, para obtener una dependencia integral de $\overline{x_2}$ sobre $k[\overline{y}_1]$, basta tomar cualquier $c \neq 0$. En particular, podemos considerar $c = -1$, lo que nos dirá que A es integral sobre $k[\overline{y}_1] = k[\overline{x_1}+\overline{x_2}]$. ▲

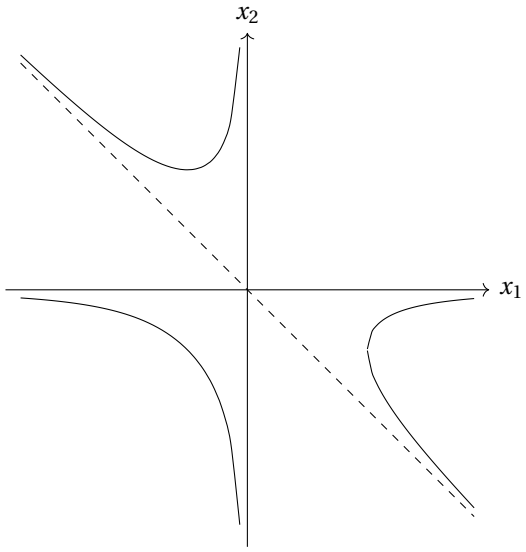
26.14. Ejemplo. La hipótesis que el cuerpo k es infinito es importante. Consideremos por ejemplo

$$A = k[x_1,x_2]/(x_1^2x_2 + x_1x_2^2 + 1).$$

En este caso $\overline{x_1}$, $\overline{x_2}$, $\overline{x_1}+\overline{x_2}$ son invertibles en A:

$$\overline{x_1}^{-1} = -(\overline{x_1}\,\overline{x_2} + \overline{x_2}^2),$$
$$\overline{x_2}^{-1} = -(\overline{x_1}\,\overline{x_2} + \overline{x_1}^2),$$
$$(\overline{x_1}+\overline{x_2})^{-1} = -\overline{x_1}\,\overline{x_2}.$$

Esto significa que A no puede ser integral sobre las subálgebras $k[\overline{x_1}]$, $k[\overline{x_2}]$, $k[\overline{x_1}+\overline{x_2}]$. Ahora si $k = \mathbb{F}_2$, entonces las únicas combinaciones lineales no triviales de $\overline{x_1}$ y $\overline{x_2}$ son estas tres, y la normalización de Noether en la forma lineal no existe.



Nuestra prueba de arriba no va a funcionar porque para

$$f = x_1^2 x_2 + x_1 x_2^2 + 1$$

la parte homogénea de grado mayor será

$$f_2 = x_1^2 x_2 + x_1 x_2^2,$$

y este polinomio se anula en todo $x_1, x_2 \in \mathbb{F}_2$. ▲

Sin entrar en los detalles (*lamentablemente*, este no es precisamente un curso de geometría algebraica), la normalización de Noether en la forma establecida arriba significa que para k algebraicamente cerrado, un conjunto algebraico $\mathbf{V}(f) \subset \mathbb{A}^n(k)$ puede ser proyectado a algún hiperplano $H \subset \mathbb{A}^n(k)$ de tal manera que para todo punto $x \in H$ la preimagen $p^{-1}(x)$ es finita y no vacía.

Ejercicio 72. Consideremos la k-álgebra $A := k[x_1, x_2]/(x_1 x_2^2 + x_1^2 x_2 + 1)$. Encuentre

a) una normalización de Noether para $k = \mathbb{F}_2$ (recuerde que esta no puede ser lineal),

b) una normalización de Noether para $k = \mathbb{Q}$ de la forma $a = c_1 x_1 + c_2 x_2$ para $c_1, c_2 \in \mathbb{Q}$.

Ejercicio 73. Encuentre una normalización de Noether en la forma lineal para la k-álgebra

$$A := k[x_1, x_2, x_3]/(x_1^2 x_2^2, x_1^2 x_3^2).$$

26.3 Normalización de Noether en Macaulay2

Para calcular la normalización de Noether en Macaulay2, existe el paquete `NoetherNormalization`. Para usarlo, primero hay que ejecutar el comando

```
loadPackage "NoetherNormalization";
```

Este paquete provee la función `noetherNormalization(I)` o `noetherNormalization(k[x_1,...,x_n]/I)` que calcula una normalización de Noether para $k[x_1, \ldots, x_n]/I$. A saber, para encontrarla, se busca un *automorfismo lineal*

$$\begin{aligned} \phi\colon k[x_1, \ldots, x_n] &\to k[x_1, \ldots, x_n], \\ x_i &\mapsto \sum_j c_{ij}\, x_j \end{aligned}$$

y variables $x_{i_1}, \ldots, x_{i_d}$ tales que son algebraicamente independientes y $k[x_1, \ldots, x_n]/\phi(I)$ es integral sobre la subálgebra $k[\overline{x_{i_1}}, \ldots, \overline{x_{i_d}}]$. Los coeficientes c_{ij} se buscan de modo aleatorio, y como hemos visto arriba, esto en general no funciona si k es un cuerpo finito.

26.15. Ejemplo. Calculemos una normalización de Noether de $\mathbb{Q}[x, y]/(x^3 - y^2)$ (ejemplo 26.8).

```
i : noetherNormalization (QQ[x,y]/(x^3-y^2))

                                          3    2
o = (map(QQ[x, y],QQ[x, y],{x, y}), ideal(x  - y ), {y})

o : Sequence
```

Notamos que el automorfismo ϕ en este caso es la aplicación identidad. ▲

26.16. Ejemplo. Tratemos de calcular una normalización de Noether de $k[x,y]/(x^2y+xy^2+1)$ (ejemplo 26.14) para $k=\mathbb{F}_2$ y $\mathbb{F}_3$.

```
i : noetherNormalization (ZZ/2[x,y]/(x^2*y + x*y^2 + 1))
--warning: no good linear transformation found by noetherNormalization

          ZZ       ZZ                                2       2
o = (map(--[x, y],--[x, y],{x + y, x}), ideal(x y + x*y  + 1), {y})
          2        2

o : Sequence

i : noetherNormalization (ZZ/3[x,y]/(x^2*y + x*y^2 + 1))

          ZZ       ZZ                                  3      2
o = (map(--[x, y],--[x, y],{x + y, x}), ideal(- x  + x*y  + 1), {y})
          3        3

o : Sequence
```

Aquí primero Macaulay2 nos avisa que una normalización no fue encontrada en el caso de $k=\mathbb{F}_2$. Esto sucede porque `noetherNormalization` analiza combinaciones lineales de las variables, lo que no puede funcionar en este caso particular (véase el ejemplo 26.14).

Para $k=\mathbb{F}_3$ fue encontrado el automorfismo

$$\phi\colon x\mapsto x+y,\quad y\mapsto x$$

y una normalización de Noether de

$$k[x,y]/I\cong k[x,y]/\phi(I)=k[x,y]/(x^3-xy^2-1)\,:$$

la salida significa que el álgebra $k[x,y]/(x^3-xy^2-1)$ es integral sobre $k[\overline{y}]$. En efecto, se tiene la relación

$$\overline{x}^3-\overline{x}\,\overline{y}^2-1=0 \text{ en } k[x,y]/(x^3-xy^2-1).$$

Notamos que $\phi^{-1}(x)=y$, $\phi^{-1}(y)=x-y$, así que en términos de $k[x,y]/I$, lo que fue calculado significa que $k[\overline{x},\overline{y}]=k[\overline{y},\overline{x}-\overline{y}]$ es integral sobre la subálgebra $k[\overline{x}-\overline{y}]$, puesto que

$$\overline{y}^3-\overline{y}(\overline{x}-\overline{y})^2-1=0 \text{ en } k[x,y]/(x^2y+xy^2+1). \qquad \blacktriangle$$

26.17. Comentario. No hay que confundir **una normalización de Noether** de A con la noción de **la cerradura integral**[*], que a veces también se conoce como **la normalización**. Para una R-álgebra A que es un dominio, se pueden considerar los elementos de $\operatorname{Frac}A$ integrales sobre A. Estos forman una R-subálgebra $\widetilde{A}\subset\operatorname{Frac}A$ que se llama la **cerradura integral** de A. Cuando $A=\widetilde{A}$, se dice que A es **integralmente cerrada** o **normal**.

Por ejemplo, el álgebra $A=k[x,y]/(x^3-y^2)$ no es integralmente cerrada, y su cerradura integral fue descrita en 26.8. La importancia geométrica de este concepto se refleja en el hecho de que para una curva C, el álgebra $\Gamma(C)$ es integralmente cerrada si y solo si C no tiene singularidades. La curva $y^2=x^3$ tiene una cúspide en el origen, mientras que la cúbica torcida "resuleve" esta singularidad.

Para calcular la cerradura integral en Macaulay2, existe la función `integralClosure`. He aquí un pequeño ejemplo:

[*] Si tuviera más tiempo, definitivamente hablaría de la cerradura integral y su cálculo.

```
i : integralClosure (QQ[x,y]/(x^3-y^2))

              QQ[w   , x, y]
                  0,0
o = --------------------------------
              2               2
    (w   y - x , w   x - y, w    - x)
      0,0         0,0         0,0

o : QuotientRing
```

Aquí la salida es la $\mathbb{Q}$-álgebra

$$\mathbb{Q}[w,x,y]/(wy-x^2,\, wx-y,\, w^2-x).$$

Notamos que

$$(wy-x^2,\, wx-y,\, w^2-x) = (x-w^2,\, y-w^3),$$

así que Macaulay2 encontró la cúbica torcida (véase el ejemplo 26.8).

27 Series de Hilbert y dimensión

Volvamos al estudio de la serie y polinomio de Hilbert. He aquí una pequeña tabla de ideales y sus series y polinomios de Hilbert.

I	$H_I(t)$	$p_I(x)$	$\dim A$
$(0) \subset k[x_1,\ldots,x_n]$	$\frac{1}{(1-t)^n} = \sum_{d\geq 0} \binom{d+n-1}{n-1} t^d$	$\binom{x+n-1}{n-1}$	n
$(x^4+y^4+z^4+w^4) \subset k[x,y,z,w]$	$\frac{1-t^4}{(1-t)^4} = \frac{t^3+t^2+t+1}{(1-t)^3}$ $= 1+4t+10t^2+20t^3+34t^4+\cdots$	$2x^2+2$	3
$(xz,yz) \subset k[x,y,z]$	$\frac{t^3-2t^2+1}{(1-t)^3} = \frac{-t^2+t+1}{(1-t)^2}$ $= 1+3t+4t^2+5t^3+6t^4+\cdots$	$x+2$	2
$(x^2+y^2-z^2) \subset k[x,y,z]$	$\frac{-t^2+1}{(1-t)^3} = \frac{1+t}{(1-t)^2}$ $= 1+3t+5t^2+7t^3+9t^4+\cdots$	$2x+1$	2
$(x^2-y) \subset k[x,y]$	$\frac{-t^2+1}{(1-t)^2} = \frac{1+t}{1-t}$ $= 1+2t+2t^2+2t^3+2t^4+\cdots$	2	1
$(x^2-y,\, x^3-z) \subset k[x,y,z]$	$\frac{2t^3-3t^2+1}{(1-t)^3} = \frac{2t+1}{1-t}$ $= 1+3t+3t^2+3t^3+3t^4+\cdots$	3	1

Se nota que

$$\dim(k[x_1,\ldots,x_n]/I) = \deg p_I + 1,$$

y que la dimensión es el mínimo número δ tal que la serie de Hilbert puede ser escrita como

$$H_I(t) = \frac{f(t)}{(1-t)^\delta},$$

donde $f(t) \in \mathbb{Z}[t]$. La minimalidad de δ significa que $f(1) \neq 0$ (sino, $f(t)$ tendría un factor $(1-t)$). Primero aclaramos la relación entre δ y el grado del polinomio de Hilbert.

27.1. Proposición. *Para un ideal $I \subset k[x_1,\dots,x_n]$, sea δ el número tal que la serie de Hilbert puede ser escrita como*

$$H_I(t) = \frac{f(t)}{(1-t)^\delta},$$

donde $f(1) \neq 0$. Entonces,

$$\delta = \deg p_I + 1.$$

Demostración. Escribamos

$$H_I(t) = \frac{f(t)}{(1-t)^\delta} = \frac{a_m\, t^m + \cdots + a_1\, t + a_0}{(1-t)^\delta},$$

donde $f(1) \neq 0$. Ahora como en la prueba de 24.16, podemos expresar el polinomio de Hilbert mediante

$$p_I = \sum_{0 \leq i \leq m} a_i \binom{x-i+\delta-1}{\delta-1}.$$

Notamos que

$$\binom{x-i+\delta-1}{\delta-1} = \frac{x^{\delta-1}}{(\delta-1)!} + \cdots.$$

Esto significa que $\deg p_I \leq \delta - 1$. Por otra parte, el coeficiente de $x^{\delta-1}$ del polinomio p_I es igual a

$$\sum_{0 \leq i \leq m} \frac{a_i}{(\delta-1)!} = \frac{f(1)}{(\delta-1)!} \neq 0.$$

Podemos concluir que $\deg p_I = \delta - 1$. ∎

Recordemos que el polinomio de Hilbert se caracteriza por

$$p_I(d) = h_I(d) \quad \text{para } d \gg 0.$$

En algunos cálculos ya hemos ocupado la función de Hilbert alternativa

$$\widetilde{h}_I(d) := \dim_k(k[x_1,\dots,x_n]/I)_{\leq d} = \{\overline{f} \mid f \in k[x_1,\dots,x_n], \deg f \leq d\}.$$

Tenemos

$$h_I(d) = \widetilde{h}_I(d) - \widetilde{h}_I(d-1).$$

Sería conveniente trabajar con otro polinomio de Hilbert caracterizado por

$$\widetilde{p}_I(d) = \widetilde{h}_I(d) \quad \text{para } d \gg 0.$$

Tenemos entonces

$$p_I(x) = \widetilde{p}_I(x) - \widetilde{p}_I(x-1).$$

Notamos que si $\widetilde{p}_I(x) = c_m\, x^m + \cdots$, entonces

$$\widetilde{p}_I(x) - \widetilde{p}_I(x-1) = m\, c_m\, x^{m-1} + \cdots,$$

así que

$$\deg \widetilde{p}_I(x) = \deg p_I(x) + 1.$$

A partir de ahora nuestro objetivo será probar que

$$\delta = \deg p_I(x) + 1 = \deg \widetilde{p}_I(x) \overset{???}{=} \dim(k[x_1,\dots,x_n]/I).$$

27.2. Lema. *Supongamos que para dos ideales*

$$I \subseteq k[x_1,\dots,x_m] \quad \text{y} \quad J \subseteq k[y_1,\dots,y_n]$$

se tiene

$$k[x_1,\dots,x_m]/I \cong k[y_1,\dots,y_n]/J.$$

Luego,

$$\deg \widetilde{p}_I = \deg \widetilde{p}_J.$$

Demostración. Consideremos un isomorfismo de k-álgebras

$$\phi\colon k[x_1,\dots,x_m]/I \xrightarrow{\cong} k[y_1,\dots,y_n]/J.$$

Entonces, existen polinomios $f_1,\dots,f_n \in k[x_1,\dots,x_m]$ tales que $\phi(\overline{f_i}) = \overline{y_i}$. Pongamos

$$N := \text{máx}\{\deg f_1,\dots,\deg f_n\}.$$

Luego, para todo d se tiene

$$(k[y_1,\dots,y_n]/J)_{\le d} \subseteq \phi\Big((k[x_1,\dots,x_m]/I)_{\le Nd}\Big).$$

Esto nos da la desigualdad $\widetilde{h}_J(d) \le \widetilde{h}_I(Nd)$, y luego

$$\widetilde{p}_J(d) \le \widetilde{p}_I(Nd) \quad \text{para } d \gg 0.$$

Esto implica que $\deg \widetilde{p}_J \le \deg \widetilde{p}_I$. De la misma manera se obtiene la otra desigualdad $\deg \widetilde{p}_I \le \deg \widetilde{p}_J$. ■

27.3. Teorema. *Para toda k-álgebra finitamente generada $A := k[x_1,\dots,x_n]/I$ se tiene*

$$\dim A = \deg \widetilde{p}_I.$$

Demostración. Podemos asumir que $A \neq 0$; en el caso contrario la identidad se cumple por las convenciones sobre $\dim 0$ y $\deg 0$. La normalización de Noether nos da elementos $a_1,\dots,a_\delta \in A$ tales que la extensión

$$C := k[a_1,\dots,a_\delta] \subseteq A$$

es integral, $\delta = \dim A$, y además A es un C-módulo finitamente generado. Lo último significa que existen elementos $b_1,\dots,b_r \in A$ tales que

$$A = C\cdot b_1 + \cdots + C\cdot b_r.$$

Podemos asumir que $b_1 = 1$ y otros elementos $b_2,\dots,b_r$ están representados por polinomios de grado > 0. Consideremos el homomorfismo de k-álgebras

$$\begin{aligned} \phi\colon k[y_1,\dots,y_\delta, z_1,\dots,z_r] &\to A,\\ y_i &\mapsto a_i,\\ z_j &\mapsto b_j. \end{aligned}$$

Puesto que ϕ es sobreyectivo,

$$A = k[x_1,\dots,x_n]/I \cong k[y_1,\dots,y_\delta, z_1,\dots,z_r]/J, \quad \text{donde } J = \ker\phi.$$

Por el lema anterior, tenemos entonces $\deg \widetilde{p}_I = \deg \widetilde{p}_J$, y nuestro objetivo será probar que $\deg \widetilde{p}_J = \delta$.

Recordemos que $\widetilde{h}_J(d)$ es la dimensión del espacio k-vectorial

$$B_{\le d} := \{f + J \mid f \in k[y_1,\dots,y_\delta, z_1,\dots,z_r], \deg f \le d\}.$$

Allí se tiene un subespacio más pequeño

$$C_{\leq d} := \{f + J \mid f \in k[y_1, \ldots, y_\delta], \deg f \leq d\}.$$

Recordemos que $J = \ker\phi$ y $\phi(y_i) = a_i$, donde los elementos a_i son algebraicamente independientes, así que en este caso

$$C_{\leq d} \cong \{f \mid f \in k[y_1, \ldots, y_\delta], \deg f \leq d\} \cong k\langle y_1^{\alpha_1} \cdots y_\delta^{\alpha_\delta} \mid \alpha_1 + \cdots + \alpha_\delta \leq d\rangle.$$

Ya hemos usado muchas veces que el número de monomios en δ variables de grado total δ es igual a $\binom{\delta+d-1}{\delta-1}$, y la función generatriz de estos números es

$$H_{(0)\subset k[y_1,\ldots,y_\delta]}(t) = \frac{1}{(1-t)^\delta}.$$

El cálculo de los monomios de grado total $\leq d$ es parecido, pero también bastaría notar que la función generatriz será

$$\widetilde{H}_{(0)\subset k[y_1,\ldots,y_\delta]}(t) = \frac{1}{(1-t)^{\delta+1}},$$

así que el número de estos monomios es $\binom{d+\delta}{\delta}$.

Ahora de la relación $C_{\leq d} \subseteq B_{\leq d}$ sale la desigualdad

$$\widetilde{h}_J(d) = \dim_k(B_{\leq d}) \geq \dim_k(C_{\leq d}) = \binom{d+\delta}{\delta}.$$

Para los polinomios de Hilbert, esto significa que

$$\widetilde{p}_J(d) \geq \binom{d+\delta}{\delta} \text{ para } d \gg 0,$$

y luego

$$\deg \widetilde{p}_J(x) \geq \deg \binom{x+\delta}{\delta} = \delta.$$

Nos falta establecer la otra desigualdad.

Los elementos $b_1, \ldots, b_r$ son generadores de A como un C-módulo, y en particular tenemos

$$b_i b_j = \sum_{1\leq \ell \leq r} a_{ij\ell}\, b_k$$

para algunos $a_{ij\ell} \in C$. Sea $e > 0$ un número tal que $a_{ij\ell} \in C_{\leq e}$ para todo $1 \leq i, j, \ell \leq r$. Tenemos en particular

$$b_i b_j \in \sum_{1\leq \ell \leq r} C_{\leq e} \cdot b_k.$$

Por inducción se sigue que para todo $s = 1, 2, 3, \ldots$ se cumple

$$b_{i_1} \cdots b_{i_s} \in \sum_{1\leq \ell \leq r} C_{\leq (s-1)\,e} \cdot b_k.$$

Ahora se tiene

$$B_{\leq d} \subseteq C_{\leq d} \cdot b_1 + \sum_{1\leq s\leq d} \sum_{1\leq \ell \leq r} C_{\leq d-s} \cdot C_{\leq (s-1)\cdot e} \cdot b_k.$$

Notamos que

$$d - s + (s-1)\,e \leq ed \quad \text{para todo } 1 \leq s \leq d.$$

Tenemos entonces

$$B_{\leq d} \subseteq \sum_{1 \leq \ell \leq r} C_{\leq ed} \cdot b_k.$$

Esto nos da la desigualdad

$$\widetilde{h}_J(d) = \dim_k(B_{\leq d}) \leq \sum \Big(\sum_{1 \leq \ell \leq r} C_{\leq ed} \cdot b_k \Big) \leq r \cdot \dim_k(C_{\leq d}) = r \cdot \binom{ed+\delta}{\delta}.$$

De nuevo, podemos pasar a la desigualdad para el grado de los polinomios de Hilbert correspondientes

$$\deg \widetilde{p}_J \leq \deg \binom{ex+\delta}{\delta} = \delta.$$

Esta es la otra desigualdad deseada. ■

27.1 Cálculo de dimensión (bis)

Recordamos que la serie de Hilbert depende solamente de $(LT(I))$, si el orden monomial respeta el grado (véase 24.10). Entonces, el último teorema implica el siguiente resultado importante.

27.4. Corolario. *Fijemos algún orden monomial $\preceq$ sobre $k[x_1, \ldots, x_n]$ que respete el grado*[*]*. Luego, para cualquier ideal $I \subseteq k[x_1, \ldots, x_n]$ se tiene*

$$\dim(k[x_1, \ldots, x_n]/I) = \dim(k[x_1, \ldots, x_n]/(LT(I))).$$

Ahora recordemos que en 22.15 hemos probado que la dimensión de $k[x_1, \ldots, x_n]/I$ es el máximo número δ tal que existen variables $\{x_{i_1}, \ldots, x_{i_\delta}\} \subseteq \{x_1, \ldots, x_n\}$ que cumplen

$$I \cap k[x_{i_1}, \ldots, x_{i_\delta}] = 0.$$

En general, el cálculo de estas eliminaciones es bastante pesado, pero gracias al último corolario, el problema se reduce al caso de ideales *monomiales* $J = (LT(I))$, para cuales $J \cap k[x_{i_1}, \ldots, x_{i_\delta}] = 0$ significa nada más que en cada uno de los generadores monomiales de J aparecen variables distintas de $x_{i_1}, \ldots, x_{i_\delta}$.

27.5. Ejemplo. Consideremos nuestra k-álgebra preferida

$$k[x, y, z]/(x^2 - y, x^3 - z).$$

La base de Gröbner reducida respecto al orden *grevlex* es

$$G = \{x^2 - y, xy - z, y^2 - xz\}.$$

Luego,

$$J := (LT(I)) = (x^2, xy, y^2).$$

De aquí se ve que

$$J \cap k[x] = J \cap k[x, z] = (x^2), \quad J \cap k[y] = J \cap k[y, z] = (y^2), \quad J \cap k[z] = 0, \quad J \cap k[x, y] = J.$$

Entonces, la dimensión es igual a 1. ▲

[*] De hecho, el resultado es válido para cualquier orden monomial $\preceq$.

A Algunas funciones de Macaulay2

oo	La última salida en la sesión interactiva
==	Igualdad
!=	Desigualdad

```
i : R = QQ[x,y];
i : ideal(y^2,y^2-x^3) == ideal (y^2,x^3)
o = true
i : ideal(y^2,x^3) != ideal (y^2,x^2)
o = true
```

x+y	Suma (en particular, de ideales)
x*y	Producto (en particular, de ideales)
f // g	División exacta (en el cuerpo de fracciones)

```
i : R = QQ[x];
i : x^6//(x^2-x+1)

         6
        x
o = ----------
     2
    x  - x + 1

o : frac R
```

ZZ	Anillo $\mathbb{Z}$
QQ	Cuerpo $\mathbb{Q}$
ZZ/p	Cuerpo $\mathbb{Z}/p\mathbb{Z}$ (donde p debe ser primo)
GF q	Cuerpo finito $\mathbb{F}_q$

`toField(`R`)`	Declara que R es un cuerpo
	`i : R = QQ[i]/(i^2+1);`
	`i : 1/(1+i)`
	`  1`
	`o = -----`
	`  i + 1`
	`o : frac R`
	`i : R = toField (QQ[i]/(i^2+1));`
	`i : 1/(1+i)`
	`  1  1`
	`o = - -i + -`
	`  2  2`
	`o : R`

`matrix {{`$a_{00},\ldots,a_{0n}$`}, ..., {`$a_{m0},\ldots,a_{mn}$`}}`	Matriz (a_{ij})
	`i : matrix {{1,2},{3,4}}`
	`o = | 1 2 |`
	`  | 3 4 |`
	`  2  2`
	`o : Matrix ZZ  <--- ZZ`

M`_(`i`,`j`)`	Entrada (i,j) de la matriz M. Las filas y columnas se numeran a partir de 0.
	`i : M = matrix {{1,2},{3,4}};`
	`  2  2`
	`o : Matrix ZZ  <--- ZZ`
	`i : M_(0,0)`
	`o = 1`

R`[`x`,`y`,`z`]`	Anillo de polinomios con coeficientes en R en x,y,z

R/I	Anillo cociente R/I.
	`i : R = ZZ[i]/(i^2+1);`
	`i : (3+2*i)*(3-2*i)`
	`o = 13`
	`o : R`
	
	`i : S = QQ[x,y,z]/(x^2-y,x^3-z);`
	`i : (x+y)^2`
	`o = x*z + y + 2z`
	`o : S`
	
	`i : S = QQ[x,y,z,MonomialOrder=>GLex]/(x^2-y,x^3-z);`
	`i : (x+y)^2`
	
	`     2`
	`o = y  + y + 2z`
	
	`o : S`

`degree(`x`,`f`)`	Grado de f respecto a la variable x

`Lex`
`GLex`
`GRevLex`
	Orden lexicográfico
	Orden lexicográfico graduado
	Orden lexicográfico inverso graduado
	`i : R = QQ [x,y,z,MonomialOrder=>GLex];`
	
	`i : x^2*y > z^3`
	`o = true`
	
	`i : x^2*y > z^4`
	`o = false`

`<, <=, >, >=`	Comparación (en particular, de monomios)

`leadMonomial(`f`)`
`leadCoefficient(`f`)`
`leadTerm(`f`)`
	Monomio mayor de f
	Coeficiente mayor de f
	Término mayor de f
	
	`i : R = QQ[x,y, MonomialOrder=>GLex];`
	`i : f = 5*x^2*y^2 + 3*x*y^2 + 2*y + 1;`
	`i : leadMonomial(f)`
	
	`     2 2`
	`o = x y`
	`o : R`
	
	`i : leadCoefficient(f)`
	
	`o = 5`
	`o : QQ`
	
	`i : leadTerm(f)`
	
	`      2 2`
	`o = 5x y`
	`o : R`

`quotientRemainder(`f`,`g`)`	Cociente y el resto de división de f por g
f`//`g	Cociente de la división con resto
f`%`g	Resto de división
`gcd(`a,b`)` `lcm(`a,b`)`	mcd(a,b) mcm(a,b)
`diff(`x`,`f`)`	Derivada parcial $\frac{\partial f}{\partial x}$
`ideal(`$f_1,\ldots,f_s$`)`	Ideal generado por $f_1,\ldots,f_s$
`monomialIdeal(`$x^{\alpha(1)},\ldots,x^{\alpha(s)}$`)`	Ideal monomial generado por $x^{\alpha(1)},\ldots,x^{\alpha(s)}$ (se calculan automáticamente los generadores minimales).

`gens(`I`)` — Matriz fila de los generadores del ideal I

`I_*` — Lista de los generadores de I

`I_i` — El i-ésimo generador de I

```
i : R = QQ[x,y,z];
i : I = ideal (x^2-y,x^3-z);
o : Ideal of R

i : gens I

o = | x2-y x3-z |

             1       2
o : Matrix R  <--- R

i : I_*

      2       3
o = {x  - y, x  - z}

o : List

i : I_0

     2
o = x  - y

o : R
```

`groebnerBasis(`I`)` — La base de Gröbner reducida para I

`intersect(`$I_1,\ldots,I_s$`)` — Intersección de ideales $I_1 \cap \cdots \cap I_s$

```
i : R = QQ[x,y,z];
i : intersect (ideal(x,y), ideal(x,z), ideal(y,z))
o = ideal (y*z, x*z, x*y)
o : Ideal of R
```

`radical(`I`)` — Radical de un ideal I

```
i : R = QQ[a,b,c,d];
i : radical (ideal (a^2 + b*c, d^2 + b*c, (a+d)*b, (a+d)*c))

                                2
o = ideal (a + d, b*c + d )

o : Ideal of R
```

$I : J$ — Ideal cociente $(I : J)$

```
i : R = QQ[x,y];
i : ideal (x^2 - x*y) : ideal (x)
o = ideal(x - y)
o : Ideal of R
```

`dim(`R`)` — Dimensión de Krull de R

`dim(`I`)` — Dimensión de Krull de R/I

```
i : R = QQ[x,y,z];
i : dim R
o = 3

i : dim ideal (x^2-y, x^3-z)
o = 1
```

`hilbertFunction(`d`,`I`)` — Función de Hilbert $h_I(d)$

`hilbertSeries(`I`)` — Serie de Hilbert $H_I(t)$

`reduceHilbert(`$H(t)$`)` — Serie de Hilbert $H(t)$ en la forma reducida

```
i : R = QQ[x,y,z];
i : for d in 0..10 list hilbertFunction (d,ideal(x*z,y*z))
o = {1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}
i : hilbertSeries ideal(x*z,y*z)

          2    3
    1 - 2T  + T
o = ------------
             3
      (1 - T)

i : reduceHilbert oo

              2
    1 + T - T
o = ----------
             2
     (1 - T)
```

`isPrime(`I`)` — Verifica si I es un ideal primo

`isPrimary(`I`)` — Verifica si I es un ideal primario

```
i : R = QQ[x,y];
i : isPrime (ideal(x^2,y))
o = false
i : isPrimary (ideal(x^2,y))
o = true
```

---

primaryDecomposition(I)
associatedPrimes(I)
minimalPrimes(I)
	Una descomposición primaria de I
	Primos asociados con I
	Primos minimales asociados con I
	
	`i : R = QQ[x,y];`
	`i : I = ideal (x^2, x*y);`
	`i : primaryDecomposition (I)`
	
	`                      2`
	`o = {ideal x, ideal (x , y)}`
	`o : List`
	
	`i : associatedPrimes (I)`
	`o = {ideal x, ideal (x, y)}`
	`o : List`
	
	`i : minimalPrimes (I)`
	`o = {ideal x}`
	`o : List`

map(B, A, { $g_1,\ldots,g_m$ })	Homomorfismo $A \to B$ definido por $t_i \mapsto g_i$, donde $t_1,\ldots,t_m$ son generadores de A

kernel(ϕ)	Núcleo de ϕ
	
	`i : f = map (QQ[x,y,z]/(x^2+y^2+z^2-1,x+y+z), QQ[t,u], {x,y});`
	`i : kernel (f)`
	`            2             2`
	`o = ideal(2t  + 2t*u + 2u  - 1)`
	`o : Ideal of QQ[t, u]`

{a, b, c}	Lista con elementos a, b, c
(a, b, c)	Sucesión con elementos a, b, c
#L	El número de elementos en L
L#i	El i-ésimo elemento de L

(a..z)	Sucesión de elementos de a a z
	
	`i : (1..10)`
	`o = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)`

`remove(`L`,`i`)`	Quitar el i-ésimo elemento de la lista/sucesión L
`append(`L`,`x`)`	Añadir x a la lista/sucesión L.

	`i : L = {1,2,3};`
	`i : remove(L,1)`
	`o = {1, 3}`
	`o : List`
	`i : append(L,4)`
	`o = {1, 2, 3, 4}`
	`o : List`

`for` i `from` a `to` b `do ..`
`for` x `in` L `do ..`
`while .. do ..`
	Ciclos

`for` i `in` I `list` a_i	La lista $\{a_i\}$ para $i \in I$
	`i : for i in 0..10 list i^2` `o = {0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100}`
`if .. then ..` `if .. then .. else ..`	Expresiones condicionales

B Algunos algoritmos básicos implementados en Macaulay2

El código de este apéndice sirve solo para entender los algoritmos básicos y aprender a programar. Normalmente todo lo necesario ya está implementado en Macaulay2.

B.1 Division.m2: división con resto en $k[x_1,\ldots,x_n]$

```
-- divRemMultivar
-- Entrada: f, (f_1, ..., f_s)
-- Salida:  (q_1, ..., q_s), r

divRemMultivar = (f,fs) -> (
  -- pongamos q_1 := 0, ..., q_s := 0:
  q := new MutableList from (#fs : 0);

  r := 0;
  p := f;

  while p != 0 do (
    i := 0;
    divisionoccured := false;

    while i < #fs and divisionoccured == false do (
      if leadTerm(p)%leadTerm(fs#i) == 0 then (
        q#i = q#i + leadTerm(p)//leadTerm(fs#i);
        p   = p - leadTerm(p)//leadTerm(fs#i) * fs#i;
        divisionoccured = true
      )
      else
        i = i+1
    );

    if divisionoccured == false then (
      r = r + leadTerm(p);
      p = p - leadTerm(p)
    )
  );

  (toSequence q, r)
);

-- Ejemplo:
-- R = QQ[x,y, MonomialOrder=>Lex];
-- divRemMultivar (x*y^2 + 1, (x*y + 1, y+1))
-- divRemMultivar (x^2*y + x*y^2 + y^2, (x*y-1, y^2-1))
-- divRemMultivar (x^2*y + x*y^2 + y^2, (y^2-1, x*y-1))
```

B.2 Buchberger.m2: algoritmo de Buchberger

```
load "Division.m2";


-----------------
-- S-polinomio --
-----------------

S = (f,g) -> (
  xg := lcm (leadMonomial(f),leadMonomial(g));
  xg//leadTerm(f)*f - xg//leadTerm(g)*g
);


-------------------------------------------
-- Algoritmo de Buchberger, versión básica --
-------------------------------------------

buchberger = fs -> (
  gs := fs;
  changed := true;

  while changed do (
    changed = false;
    gs' := gs;

    for i from 0 to #gs-1 do (
      for j from i+1 to #gs-1 do (
        r := (divRemMultivar (S(gs#i,gs#j), gs))#1;
        if r != 0 and not member(r,gs') then (
          gs' = append(gs',r);
          changed = true
        )
      )
    );

    gs = gs'
  );

  gs
);
```

```
-------------------------------------------------------------
-- Una base mínima a partir de una base de Gröbner cualquiera --
-------------------------------------------------------------

minimalizeBasis = gs -> (
  gs = apply (gs, f->f//leadCoefficient(f));
  minimal = false;

  while not minimal do (
    minimal = true;

    for i from 0 when i<#gs and minimal do (
      for j from 0 when j<#gs and minimal do (
        if i != j and leadTerm(gs#i)%leadTerm(gs#j) == 0 then (
          gs = remove(gs,i);
          minimal = false
        )
      )
    )
  );

  gs
);

-------------------------------------------------------------
-- La base reducida a partir de una base de Gröbner cualquiera --
-------------------------------------------------------------

reduceBasis = gs -> (
  gsm := new MutableList from minimalizeBasis(gs);
  for i from 0 to #gsm-1 do
    gsm#i = (divRemMultivar (gsm#i, remove(gsm,i)))#1;
  toList gsm
);

-----------------------------------------------------
-- La base de Gröbner reducida para I = (f_1,...,f_s) --
-----------------------------------------------------

myGroebner = fs -> matrix {sort reduceBasis buchberger fs};

-- Ejemplo:
-- R = QQ[x,y,z,MonomialOrder=>GLex];
-- myGroebner (x^5+y^4+z^3-1, x^3+y^3+z^2-1)
-- Para comparar con los cálculos de Macaulay2:
-- groebnerBasis (ideal(x^5+y^4+z^3-1, x^3+y^3+z^2-1))
```

Referencias

[AM1969] Michael Francis Atiyah and I. G. MacDonald, *Introduction to commutative algebra.*, Addison-Wesley-Longman, 1969.

[CLO2015] David A. Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*, fourth ed., Undergraduate Texts in Mathematics, Springer, 2015.
http://doi.org/10.1007/978-3-319-16721-3

[DHV1992] Eisenbud David, Craig Huneke, and Wolmer Vasconcelos, *Direct methods for primary decomposition*, Inventiones Mathematicae **110** (1992), 207–235.
https://www.msri.org/~de/papers/pdfs/1992-001.pdf

[Eis2004] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 2004.
http://doi.org/10.1007/978-1-4612-5350-1

[GTZ1988] Patrizia Gianni, Barry Trager, and Gail Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, Journal of Symbolic Computation **6** (1988), 149–167.
http://doi.org/10.1016/S0747-7171(88)80040-3

[HS2002] Serkan Hoşten and Gregory Smith, *Monomial ideals*, Computations in algebraic geometry with Macaulay2 (D. Eisenbud, D. Grayson, M. Stillman, and B. Sturmfels, eds.), Algorithms and Computation in Mathematics, vol. 8, Springer-Verlag, 2002, pp. 73–100.
http://faculty.math.illinois.edu/Macaulay2/Book/

[Kem2010] Gregor Kemper, *A course in commutative algebra*, Graduate Texts in Mathematics, vol. 256, Springer, 2010.
http://doi.org/10.1007/978-3-642-03545-6

[Nor1953] Douglas Geoffrey Northcott, *Ideal theory*, Cambridge Tracts in Mathematics, Cambridge University Press, 1953.
http://doi.org/10.1017/CBO9780511565908