Álgebra computacional

Álgebra conmutativa y geometría algebraica afín desde el punto de vista algorítmico

Curso 2020

Alvaro Rittatore

Índice general

Introducción

Descripción somera del curso

El objetivo del curso es introducir temas básicos del álgebra conmutativa y de la geometría algebraica, a través de la perspectiva del álgebra computacional.

En los años 60, Buchberger desarrolló algoritmos para la manipulación de ecuaciones polinomiales en varias variables. Desde la óptica del álgebra conmutative (o de la geometría algebraica afín), su trabajo peude resumirse diciendo que Buchberger creó un algoritmo que permite, dado un ideal I del álgebra de polinomios $\Bbbk[x_1, \ldots, x_n]$, encontrar un conjunto finito de generadores de I, con buenas propiedades — las por él llamadas *base de Gröbner*.

En este curso estudiaremos, junto con el algoritmo mencionado, las propiedades básicas de las bases de Gröbner, así como las primeras aplicaciones de estas técnicas: resolución de sistemas polinomiales, parametrización de variedades afines, el problema de la implicitación. Aprovecharemos para dar los primerísimos pasos en el estudio de la geometría algebraica afín.

Estudiaremos algunas implementaciones de los algoritmos presentados en el curso en clases de discusión práctica (usando SAGE).

Carga horaria: Se darán dos clases teóricas y una clase práctica (de discusión de ejercicios e implementación de los algoritmos).

Prerrequisitos: Un curso de que cubra las nociones básicas de la teoría de anillos conmutativos.

Programa – cronograma tentativo

(1) *Repaso de anillos de polinomios.* Anillos, ideales, definiciones básicas, ideales primos y maximales. Polinomios en una variable. Algoritmo de división para polinomios en una variable. Teorema de la base de Hilbert. Polinomios en varias variables. (*4 clases*)

(2) *Primeras nociones de geometría algebraica.* Topología de Zariski, subvariedades de k^n (variedades algebraicas afines). Parametrizaciones de variedades afines. (*3 clases*)

(3) *División de polinomios en variaas variables.* Bases de Gröbner; pesentación de los problemas que motivan la construcción. Anillos graduados. Órdenes en los monomios de $k[x_1, \ldots, x_n]$. Algoritmo de división en $k[x_1, \ldots, x_n]$. Ideales monomiales, lema de Dickson. (*4 clases*)

(4) *Bases de Gröbner* propiedades. Teorema de la base de Hilbert revisitado. Bases de Gröbner y generación finita de ideales. El algoritmo de Buchberger. Bases de Gröbner minimales y reducidas. (*4 clases*)

(5) Primeras aplicaciones de bases de Gröbner. Pertenencia a ideales. Resolución de ecuaciones polinomiales. Descripción del ideal asociado a una subvariedad de k^n descrita paramétricamente. (*3 clases*)

(6) Mejoras al algoritmo de Buchberger. (*1 clase*)

(7) Conceptos básicos de la geometría algebraica afín. Nullstellensatz débil. Anillos noëtherianos, anillos artinianos. Suma, intersección y producto de ideales, su interpretación geométrica. Ideales radicales, radical de Jacobson. Ideales primarios, Nullstellenstaz fuerte. La correspondencia ideales–variedades. (*4 clases*)

(8) Descomposici'on primaria. Descomposici'on de variedades en componentes irreducibles. Producto tensorial. Producto de variedades afines. Morfismos entre variedades afines. (*3 clases*)

(9) Teoría de la eliminación. Teoremas de eliminación y extensión. Geometría de la eliminación. Implicitación. Puntos singulares. Factorización única y resultantes. resultantes yel teorema de extensión. (*4 clases*)

Capítulo 1

Anillos de polinomios

1. Anillos

En este curso trabajaremos con *anillos conmutativos con unidad*

Definición 1.1. Un *anillo* es un quíntuple $(A, s, m, \mathrm{op}, 0)$, donde A es un conjunto, $s, m : A \times A \to A$, $\mathrm{op} : A \to A$ tres funciones y $0 \in A$ un elemento, tales que

(1) $(A, s, \mathrm{op}, 0)$ es un *grupo conmutativo*, es decir

(I) la *suma* s es asociativa: si notamos la suma como $+$, tenemos que $(a+b)+c = a+(b+c)$ para todo $a, b, c \in A$, lo que puede resumirse en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} (A \times A) \times A & \xrightarrow{s \times \mathrm{id}_A} & A \times A \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle s} \\ A \times (A \times A) & \xrightarrow[\mathrm{id}_A \times s]{} & A \end{array}$$

donde $r : (A \times A) \times A \to A \times (A \times A)$ es el isomorfismo canónico $r\big((a, b), c\big) = \big(a, (b, c)\big)$.

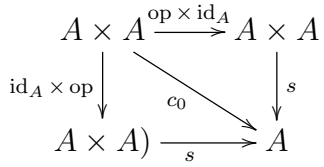
(II) el elemento 0 es el *neutro para la suma*, lo que se expresa en los siguientes diagramas conmutativos:

$$\begin{array}{ccc} A & \xrightarrow{c_0 \times \mathrm{id}_A} & A \times A \\ & \searrow^{\mathrm{id}_A} & \downarrow{\scriptstyle s} \\ & & A \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\mathrm{id}_A \times c_0} & A \times A \\ & \searrow^{\mathrm{id}_A} & \downarrow{\scriptstyle s} \\ & & A \end{array}$$

donde $c_0 : A \to A$ es el morfismo constante igual a 0.

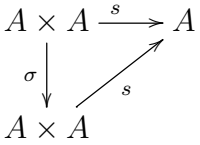
(III) el *opuesto de un elemento para la suma* existe y está dado por la función $\mathrm{op} : A \to A$.[1] En otras palabras, el siguiente diagrama es conmutativo:

[1] Es fácil ver que si el opuesto a izquierda y derecha existe, entonces tiene que ser único.



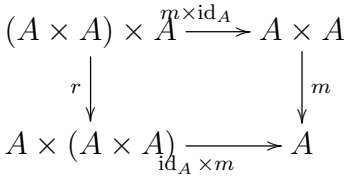
donde $c_0 : A \times A \to A$ denota el morfismo constante igual a 0.

(IV) la suma es conmutativa, lo que se exprtese e ne lsiguietne diagrama conmutativo



donde $\sigma : A \times A \to A \times A$ es la trasposición $\sigma(a, b) = (b, a)$.

(2) el producto m es asociativo: si notamos el producto como como $\cdot$, tenemos que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in A$, lo que puede resumirse en el siguiente diagrama conmutativo:



(3) se cumple la *prodiedad distributiva de la suma respecto al producto*: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ para todo $a, b, c \in A$, lo que también puede expresarse en un diagrama conmutativo, que dejamos a cargo del lector.

Notación 1.2. A partir de ahora asumiremos las notaciones usuales de los cursos de álgebra: elinamos (algunos) paréntesis con la convención que el producto tiene precedencia ante la suma (a no ser que haya paréntesis), no escribiremos el $\cdot$ para el producto cuando no de lugar a confusión, etc. Por supuesto, abusaremos la notación y diremos que A es un anillo, sin hablar de su sume, producto , opuesto y 0.

Definición 1.3. Un *anillo con unidad* es un séxtuple $(A, s, m, \mathrm{op}, 0, 1)$, donde A es un conjunto, $s, m : A \times A \to A$, $\mathrm{op} : A \to A$ tres funciones y $0, 1 \in A$ dos elementos distintos, tales que

(I) $(A, s, m, \mathrm{op}, 0)$ es un *anillo*;

(II) 1 es un neutro para el producto (dejamos a cargo del lector el correspondiente diagrama conmutativo)

(1) Un anillo se dice *conmutativo* si el producto es conmutativo (dejamos al lector la terea de completar qué quiere decir esto, y escribir el correspondiente diagrama conmutativo).

Recordemos ahora varias definiciones:

Definición 1.4. (1) Un elemento de un anillo con unidad es *invertible* (se dice también que es *una unidad*) su tiene inverso (a ambos lados) para el producto. Notaremos al *grupo de las unidades* como $A^* = \{a \in A : \text{ existe } a^{-1}\}$ — notar que $1 \in A^*$ y que A^* es un grupo, ya que el producto de invertibles es invertible.

(2) Un *cuerpo* es un anillo conmutativo con unidad tal que todo elemento no nulo es invertible.

(3) Un *divisor de cero* en un anillo (conmutativo, con unidad) es un elemento $a \in A$ tal que existe $b \in A \setminus \{0\}$ con $ab = 0$.

(4) Un *dominio* es un anillo conmutativo con unidad sin divisores de cero (no triviales).

(5) Un elemento $a \in A$ *divide* a $b \in A$ si existe $c \in A$ tal que $ac = b$. Notaremos $a \big| b$.

(6) Un elemento $a \in A$ de un dominio A es *irreducible* si toda vez que $a = bc$, entonces o b o c es una unidad.

(7) Un *dominio de factorización unica* es un dominio en donde todo elemento se escribe de modo único como producto de irreducibles.[2]

Observación 1.5. Recordar que si eliminamos la restricción $0 \neq 1$, entonces $\big(\{0\}, c_0, c_0, \mathrm{id}, 0, 0\big)$ es el único anillo con $0 = 1$.

Notación 1.6. A partir de ahora los anillos que consideramos son conmutativos, con unidad.

Definición 1.7. Un *morfismo de anillos* (no necesariamente con unidad) $f : A \to B$ es una función entre los anillos A, B, tal que $f(a+b) = f(a)+f(b)$ y $f(ab) = f(A)f(c)$ para todo $a, b \in A$. Si los anillos tiene unidad, se agrega la condición $f(1_A) = 1_B$.

Ejemplo 1.8. La identidad es un morfismo de anillos. La composición de morfismos de anillos es un morfismo de anillos.

Ejemplo 1.9. Consideremos la función $\Bbbk \to \mathrm{M}_{n\times n}(\Bbbk)$ dada por

$$f(a) = \left(\begin{smallmatrix} 1 & 0_{1\times n-1} \\ 0_{n-1\times 1} & 0_{n-1\times n-1} \end{smallmatrix}\right)$$

Esta función respeta la suma y el producto, pero $f(1) \neq \mathrm{id}_{n\times n}$.

[2]Por supuesto, a menos de elemetnos invertibles: si $a = p_1 \dots p_n = q_1 \dots q_m$, con p_i, q_J irreducibles, entonces $m = n$ y a menos de reordenamiento tenemos que $p_i = u_i q_i$, donde $u_i \in A^*$.

Recordemos ahora la definición de ideal, e ideal generado.

Definición 1.10. Dado un anillo A, un *ideal de* A es un subconjunto $I \subset A$ tal que

(1) I es un subgrupo para la suma (en particular $0 \in I$).

(2) I es estable por la multiplicación por elementos de A: $ax \in I$ para todo $a \in A$, $x \in I$ — como estamos asumiendo que A es conmutativo, tenemos también que $xa \in I$.

Definición 1.11. Sea A un anillo. Un ideal $I \subset A$ es

(1) *propio* si $I \neq A$.

(2) *primo* si es propio y toda vez que $ab \in I$, se tiene que o $a \in I$ o $b \in I$;

(3) *maximal* si es maximal en la familia de los ideales propios, para el orden de la inclusión: I es propio, y si si $J \supsetneq I$ es un ideal, entonces $J = A$.

(4) *radical* si es propio y toda vez que $a^n \in I$ para $n \geq 0$, entonces $a \in I$.

(5) *primario* si es propio y toda vez que $ab \in I$, se tiene que o $a \in I$ o $b^n \in I$ para algún $n > 0$.

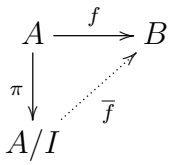
Ejercicio 1.1. Si $f : A \to B$ es un morfismo de anillos, entonces el *núcloe* de f, $\ker(f) = \big\{a \in A : f(a) = 0\big\}$ es un ideal.

Teorema 1.12. *Sea A un anillo e $I \subsetneq A$ un ideal propio. Entonces:*

(1) el cociente por la relación de equivalencia $a \sim b$ si $b - a \in I$ admite una estructura de anillo, tal que la proyección canónica $\pi A \to A/I$ es un morfismo de anillos, con núcleo $\ker(\pi) = I$*;*

(2) la proyección canónica establece una biyección entre los ideals de l cociente y los ideales de A que contienen a I,

(3) se cumple además la propiedad universal del cociente*: si $f : A|toB$ es un morfismo de anillos tal que $I \subset \mathrm{Ker}(f)$, entonces existe un único morfismo de anillos $\overline{f} : A/I \to B$ tal que $\overline{f} \circ \pi = f$, es decir el diagrama siguiente es conmutativo*



En particular, $\ker\big(\overline{f}\big) = \pi\big(\mathrm{Ker}(f)\big)$.

Prueba: ¡Ejercicio! □

Proposición 1.13. *Sea A un anillo e $I \subsetneq A$ un ideal. Entonces*

(1) I es primo si y sólo si A/I es un dominio.

(2) I es maximal si y sólo si A/I es un cuerpo.

(3) I es radical si y sólo si A/I es no tiene nilpotentes

PRUEBA: ¡Ejercicio! □

Definición 1.14. Sea $X \subset A$ un subconjunto del anillo A. El *ideal generado por X* es el menor ideal que contiene a X (ver Observación 1.15); lo notaremos por $\langle X \rangle$.

Observación 1.15. Si $X \subset A$, entonces

$$\langle X \rangle = \bigcap_{J \subset X} J = \Big\{ \sum_{i=1}^{n} a_i x_i : n \in \mathbb{N}\,,\ a_i \in A\,,\ x_i \in X \Big\}$$

donde la intersecicón se toma entre los ideales que contienen a X, y si $X = \emptyset$, entonces se entiende que las sumatorias en el lado derecho producen el 0 (es decir $\langle \emptyset \rangle = \{0\}$).

Definición 1.16. Un anillo es un *dominio de ideales principales* si todo ideal es principal, es decir generado por un elemento.

Un anillo es *nœtheriano* si todo ideal es finitamente generado, es decir está genderdo pro una cantidad ifnita de elementos.[3]

Definición 1.17. Si A es un anillo con unidad, entonces la *característica* de A se define así: se considera el morfismo de anillos $f : \mathbb{Z} \to A$, $f(n) = 1 + \cdots + 1$ (n veces). Entonces $\text{char}(A) = n$ tal que $\ker(f) = \langle n \rangle$, con $n \geq 0$.

Notación 1.18. Cuando trabajemos en un anillo A notaremos $n = f(n) = 1 + \cdots + 1$ (n veces). Así, en $\mathbb{Z}_2$ tenemos que $4 = 0$.

Ejercicio 1.2. Hacer los ejercicios para Sage 1.15 — 1.16.

2. Polinomios en una variable

Definición 1.19. Si A es un anillo, en *anillo de polinomios con coeficientes en A*, que notaremos por $A[x]$, se define así:

(1) Se considera el conjunto de las expresiones $\sum_{n=0}^{\infty} a_n x^n$, donde $a_n \in A$, nulo salvo para una cantidad finita de subíndices.

(2) Se define la suma de dos polinomios $p = \sum_{n=0}^{\infty} a_n x^n$ y $q = \sum_{n=0}^{\infty} b_n x^n$ como

$$p + q = \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$

[3]Esta no es la "definición usual", que es que toda cadena ascendente de ideales estabilice. Esta definición es equivalente a la que dimos, y es equivalente también a que si M es un A–módulo finitamente generado, entonces todo sub-módulo es finitamente generado.

(3) Se define el producto de dos polinomios $p = \sum_{n=0}^{\infty} a_n x^n$ y $q = \sum_{n=0}^{\infty} b_n x^n$ como

$$pq = p \cdot q = \sum_{n=0}^{\infty} \Big(\sum_{t+s=n} a_t + b_s \Big) x^n.$$

Observar que el polinomio $0 = \sum_{n=0}^{\infty} 0x^n$ es el neutro de la suma, y el polinomio $1 = 1 + \sum_{n=1}^{\infty} 0x^n$ es el neutro del producto.

Observación 1.20. Si A es un anillo, entonces $A[x]$ es una A-álgebra; ya que inc : $A \to A[x]$, $\mathrm{inc}(a) = a + \sum_{n=1}^{\infty} 0x^n$, es un morfismo de anillos inyectivo.

Notación 1.21. Si $p = \sum_{i=0}^{\infty} a_i x^i \in A[x]$ es tal que $a_i = 0$ para todo $i > n$ lo notaremos como $= p \sum_{i=0}^{n} a_i x^i$. Si podemos asumirlo, asumiremos que $a_n \neq 0$.

Definición 1.22. Consideremos un polinomio $p = \sum_{i=0}^{\infty} a_i x^i \in A[x]$ tal que $a_i = 0$ para todo $i > n$, con $a_n \neq 0$.

(1) Si $p \neq 0$, diremos que p tiene *grado* n y notaremos $\mathrm{gr}(p) = n$. El polinomio 0 tiene, por definición, grado $-\infty$.[4]

(2) Diremos que $a_i x^i$ es el *término de grado* i – en general supondremos que $i \leq n$, pero esto no es necesario para la definición. La expresión x^i es el *monomio de grado* i; a_i es el *coeficiente de* p en el grado i.

(3) Si $\mathrm{gr}(p) = nm \geq 0$, diremos que $a_n x^n$ es el *término líder*, a_n es el *coeficiente líder*, y x^n el *monomio líder* — ¡notemos que 0 no tiene término lider!. Notaremos $a_n x^n = \mathrm{LT}(p)$, $a_n = \mathrm{LC}(p)$ y $x^n = \mathrm{LM}(p)$.; así $\mathrm{LT}(p) = \mathrm{LC}(p)\,\mathrm{LM}(p)$.

Notación 1.23. Notaremos $A_n[x] = \big\{ p \in A[x] : \mathrm{gr}(p) \leq n \big\}$ — observar que $A_n[x]$ es un A-submódulo de $A[x]$.

Ejercicio 1.3. Sean $p, q \in A[x]$.

(1) Se cumple que $\mathrm{gr}(p+q) \leq \mathrm{máx}\big\{\mathrm{gr}(p), \mathrm{gr}(q)\big\}$ y $\mathrm{gr}(pq) \leq \mathrm{gr}(p) + \mathrm{gr}(q)$.

(2) Si A no tiene divisores de cero, entonces $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$. ¿Puede mejorar este enunciado?

(3) Dar ejemplos para (1) donde las desigualdades son estrictas.

Ejercicio 1.4. El objetivo de este ejercicio es detectar los polinomios *invertibles* y *nilpotentes* (es decir tales que $p^m = 0$ para algún m).

(1) Probar que si A es un anillo y $x \in A$ es nilpotente, entonces $1 + x$ es nilpotente.

(2) Deducir que si $u \in A^*$ es un elemento invertible (una *unidad*, A^* denotará el grupo de las unidades de A) y $x \in A$ es nilpotente, entonces $u + x$ es una unidad.

[4]Otra opción es decir que el polinomio nulo no tiene definido su grado. Para trabajar con operaciones depolinomios es más conveniente decir que $\mathrm{gr}(0) = -\infty$, pero para trabajar con nociones como la de valuacuión, es mejor decir que el grado de 0 no está definido.

(3) Probar que un polinomio $p = a_0 + \cdots + a_n x^n \in A[x]$ es invertible si y sólo si a_0 es invertible y $a_1, \ldots, a_n$ son nilpotentes. SUGERENCIA: si $q = b_0 + \cdots + b_m x$ es la inversa de p, probar por inducción en r que $(a_n 0^{r+1} b_{m-r} = 0$, para así probar que a_n es nilpotente. Entonces aplicando la parte (2) tenemos por inducción lo que queremos.

(4) Probar que un polinomio $p = a_0 + \cdots + a_n x^n \in A[x]$ es nilpotente si y sólo si $a_0, \ldots, a_n$ es nilpotente.

Ejercicio Optativo 1.5. (1) Probar que $p = a_0 + \cdots + a_n x^n \in A[x]$ es un *divisor de cero* (es decir existe $0 \neq q \in A[x]$ con $pq = 0$) si y sólo si existe $0 \neq a \in A$ tal que $ap = 0$ — en otras palabras, podemos tomar $q = a$. SUGERENCIA: tomar q con el menor grado posible. Si $q = b_0 + \ldots b_m x^m$, entonces $a_n b_m = 0$, como $a_n qp = 0$, tenemos que $a_n q = 0$. Por inducción, tenemos que $a_{n-r} q = 0$ para $0 \leq r \leq n$. Para terminar, observar que $a_i b_0 - 0$, de donde tenemos que $pb_0 = 0$.

(2) Deducir que si A es un *dominio* (es decir no tiene divisores de cero), entonces $A[x]$ también es dominio.

Definición 1.24. Dados dos polinomios $q, q \in A[x]$, diremos que p *divide a* q, y notaremos $p \big| q$, si existe $h \in A[x]$ tal que $q = hp$.

Ejercicio 1.6. Sean $p, q \in \Bbbk[x]$ ($\Bbbk$ nota un cuerpo). Probar que $\operatorname{gr}(p) \leq \operatorname{gr}(q)$ si y sólo si $\operatorname{LT}(p) \big| \operatorname{LT}(q)$. Probar que si en vez de un cuerpo $\Bbbk$ consideramos un anillo cualquiera, entonces el resultado no es necesariamente cierto.

Proposición 1.25. *Sea $f : A \to B$ un morfismo de anillos. Si $b \in B$, entonces existe un único morfismo de anillos $f_b : A[x] \to B$ que extiende f y tal que $f_b(x) = b$.*

PRUEBA: Es claro que $f_b\big(\sum a_i x^i\big) = \sum a_i b^i$ es la única extensión posible. □

Definición 1.26. Sea A un anillo y $a \in A$. Definimos la *evaluación en A* como el morfismo de anillos $\operatorname{ev}_a : A[x] \to A$ inducido por $\operatorname{id}_A : A \to A$, tal que $\operatorname{ev}_a(x) = a$. Si $p \in A[x]$, notaremos $p(a) = \operatorname{ev}_A(p)$.

Los *ceros* de un polinomio $p \in A[x]$ son los elementos de A tales que $\operatorname{ev}_a(p) = 0$.

El siguiente teorema será una consecuencia del primer algoritmo que veremos, que será el de división de polinomios con coeficientes en un cuerpo (Algoritmo 1.1).

Teorema 1.27. *Sea A un dominio (es decir, A no tiene divisores de cero), y consideremos dos polinomios $p, q \in A[x]$. Entonces existen $h, r \in A[x]$, $a \in A \setminus \{0\}$, con $\operatorname{gr}(r) < \operatorname{gr}(q)$ tales que*

$$ap = hq + r.$$

Si $b \in A \setminus \{0\}$, $j, s \in A[x]$ con $\operatorname{gr}(s) < \operatorname{gr}(q)$ son tales que $bp = jq + s$, entonces $br = aj$ y $bh = aj$.

PRUEBA: Supongamos probado el teorema cuando A es un cuerpo. Entonces aplicamos el algoritmo 1.1 y tenemos una solución al problema, que todavía no sabemos que sea única. Si A es un dominio cualquiera, entonces tenemos una solución al problema para el cuerpo de fraccciones de A, que notaremos $[A]$. Entonces, tenemos $\overline{h}, \overline{r} \in [A][x]$ tales que $\text{gr}(r) < \text{gr}(q)$ y

$$p = \overline{h}q + \overline{r}. \tag{1}$$

Si $\overline{h} = \sum \frac{c_i}{d_i} x^i$ y $\overline{r} = \sum \frac{e_i}{f_i} x^i$, con $c_i, e_i \in A$ y $d_i, f_i \in A \setminus \{0\}$[5], entonces multiplicando ambos lados de la ecuación (1) por $a = \prod d_i \prod f_i$ tenemos que

$$ap = a\overline{h}q + a\overline{r}$$

donde $a\overline{h}, a\overline{r} \in A[x]$, y $\text{gr}(a\overline{r}) < \text{gr}(q)$.

Supongamos ahora que tenemos otra solución $bp = jq + s$, con $b \in A \setminus \{0\}$, $j, s \in A[x]$, y $\text{gr}(s) < \text{gr}(q)$. Entonces, tenemos que

$$a(jq + s) = b(hq + r),$$

de donde

$$(aj - bh)q = br - as. \tag{2}$$

Como A no tiene divisores de cero, el grado de la ecuación (2) tiene grado mayor o igual a $\text{gr}(q)$, y el grado del lado derecho estrcitamente menor a $\text{gr}(q)$, a no ser que ambos polinomios sean el polinomio 0. Eso sólo puede pasar cuando $as = br$, y $aj = bh$, pues q no es el polinomio nula (estamos aquí aplicando el Ejercicio 1.5 para poder garantizar que en $A[x]$ no hay divisores de cero). □

Corolario 1.28. *Si $\Bbbk$ es un cuerpo, entonces dados $p, q \in \Bbbk[x]$, $q \neq 0$, existen únicos $h, r \in \Bbbk[x]$, con $\text{gr}(r) < \text{gr}(q)$, tales que $p = hq + r$.*

PRUEBA: Ejercicio. □

Veamos entonces el algoritmo de división para polinomios en una variable.

Algoritmo 1.1. INPUT: Dos polinomios $p, q \in \Bbbk[x]$, con $q \neq 0$.
OUTPUT: Dos polinomios $h, r \in \Bbbk[x]$, tales que $\text{gr}(r) < \text{gr}(qw)$ y $p = ghq + r$

CONSTRUCCIÓN DEL PSEUDO-CÓDIGO:
Idea de la construcción: Consideramos como invariante la ecuación $p = hq + r$. La inicializamos en $h = 0$ y $r = p$. Si $\text{gr}(p) < \text{gr}(q)$ el algoritmo termina. Si no, consideramos el monomio bx^s tal que el término líder de $bx^s q$ es el término lider de r. Se lo agregamos a h y se lo sacamos a r (por lo que le baja el grado). Para que la igualdad siga siendo cierta, tenemos que restar a r también el polinomio $bx^s q - \text{LT}(r)$ — como $\text{LT}(bx^s q) = \text{LT}(r)$ tenemos que $\text{gr}\big(r - bx^s q - \text{LT}(r)\big) < gr(r)$. Tenemos entonces que

[5]Estamos asumiendo que si c_i o e_i son nulos, entonces el denominador correspondiente es 1.

$p = hq + r$, donde $h = h + bx^s$ y $r = r - bx^s q$, con el grado del nuevo r estrictamente menor al que teníamos.

Repetimos este proceso hasta que obtenemos que el grado del r sea estrictamente menor de $\mathrm{gr}(q)$, y ahí el algoritmo para, ya que los grados están acotados por 0 — mejor dicho: los grados *polionomios no nulos* están acotados por 0, y el grado del polinomio 0 es estrictamente menor que 0.

Pseudo-código

Input: p, q

Output: h, r

$h := 0$; $r = p$

WHILE $r \neq 0$ and $\mathrm{LT}(q) \big| \mathrm{LT}(r)$ DO
    $h := h + \mathrm{LT}(r)/\mathrm{LT}(q)$
    $r := r - \mathrm{LT}(r)/\mathrm{LT}(q)q$

RETURN h, r

El psuedo-código es válido: [6]

Para ver que el algoritmo produce el resultado deseado, observemos que la igualdad $p = hq + r$ se mantiene a lo largo de todo el algoritmo:

En la primera etapa la ifgualdad se cumple po cosntrucción. Si en la etapa J se cumple, en la etapa $j + 1$ o bien verificamos que $\mathrm{gr}(r) < \mathrm{gr}(q)$ y el algoritmo termina, o bien tenemos nuevos polinomios. Tenemos entonces que ver que $p = \big(h + \mathrm{LT}(r)/\mathrm{LT}(q)\big)q + \big(r - \mathrm{LT}(r)/\mathrm{LT}(q)\big)$, lo que es una cuenta fácil.

Ya vimos que el algoritmotermina: en cada etapa el grado del polinomio r decrece estrictamente, por lo que tendremos que en algún momento será menor que $\mathrm{gr}(q)$. □

Ejercicio 1.7 (Algoritmo de Euclides)**.** (1) Construir el algoritmo de división para los números enteros.

(2) Construir el algotirmo de división para el máximo común divisor de

(i) Dos números enteros.

(ii) Dos polinomios con coeficientes en un cuerpo.

Ejercicio 1.8. Es un buen momento para hacer los ejercicio para sage 1.17 y 1.19

Una consecuencia inmediata del algoritmo de división, es que si $\Bbbk$ es un cuerpo, entonces $\Bbbk[x]$ es un dominio de ideales principales:

[6] Es decir, el algoritmo termina y produce el resultado deseado.

Proposición 1.29. *Sea $\Bbbk$ un cuerpo. Entonces $\Bbbk[x]$ es un dominio de ideales principales. Más aún, si $q \neq 0$, entonces $p \in \langle q \rangle$, si y sólo si el resto de dividir p por q es cero, y $\langle \ell \rangle = \langle p \rangle$ si y sólo si existe $a \in \Bbbk$ tal que $ap = \ell$.*

PRUEBA: Sea I un ideal, y tomemos $q \in I \setminus \{0\}$ del menor grado posible (tal q existe porque el conjunto $\{\mathrm{gr}(\ell) : \ell \in I\} \subset \mathbb{N}$ está acotado inferiormente). Dado $p \in I$, sean h, r como en el algoritmo de división. Entonces $r = p - hq \in I$, con $\mathrm{gr}(r) < \mathrm{gr}(q)$, por lo que $r = 0$. El recíproco es claro.

Sea ahora $\ell, p \in \Bbbk[x]$ tales $\langle \ell \rangle = \langle p \rangle$. Entonces $\ell = hp$, con $h \in \Bbbk[x]$. Luego, $\mathrm{gr}(\ell) = \mathrm{gr}(h) + \mathrm{gr}(p)$. Del mismo modo $p = j\ell$, con $j \in \Bbbk[x]$, por lo que $\mathrm{gr}(p) = \mathrm{gr}(j) + \mathrm{gr}(\ell)$. Deducimos que $\mathrm{gr}\, h = \mathrm{gr}(j) = 0$, y el resultado sigue. □

Observación 1.30. En los cursos de álgebra se ve que tenemos entonces que $\Bbbk[x]$ es un anillo nœtheriano, dominio de factorización única.

Queda entonces la pregunta que pasa cuando consideramos un anillo cualquiera. En ese caso la situaicón es un poco más complicada:

Ejercicio 1.9. Dar un ejemplo de un anillo A y un ideal $I \subset A[x]$ que no sea principal.

Sin embargo, el teorema de la base de Hilbert[7] nos dice que si A es nœtheriano, entonces $A[x]$ también lo es:

Teorema 1.31 (De la base de Hilbert)**.** *Sea A un anillo nœtheriano. Entonces $A[x]$ es un anillo nœtheriano.*

PRUEBA: Veamos ahora una prueba "no algorítmica", luego veremos otra prueba.

Sea $I \subset A[x]$ un ideal. Queremos probar que es finitamente generado. Consideremos

$$J = \{a \in A : a \text{ es coeficiente líder de un polinomio } p \in I\} \subset A$$

Afirmamos que J es un ideal: Si $b \in J$ y $a \in A$, sea $p \in A[x]$ tal que $b = \mathrm{LC}(p)$. Entonces $\mathrm{LC}(ap) = ab$. Si $c \in J$ es otro elemento, sea $q \in A[x]$ tal que $\mathrm{LC}(q) = c$. Entonces $\mathrm{LC}\big(x^{\mathrm{gr}(q)}p + x^{\mathrm{gr}(p)}q\big) = b + c$. Por otra parte $0 = \mathrm{LC}(0)$, por lo que $J \neq \emptyset$.

Como J es unideal de A que es nœtheriano, tenemos que existen $j_1, \ldots, j_t \in J$ tales que $J = \langle j_1, \ldots, j_s \rangle$. Sean $p_1, \ldots, p_s \in I$ tales que $\mathrm{LC}(p_i) = j_i$. Tenemos que $\langle p_1, \ldots, p_s \rangle \subset I$, pero todavía nos falta encontrar algunos generadores más. Primero observemos que podemos tomar cada p_i con grado mínimo entre los polinomios que

[7]La historia de este teorema es muy interesante: Hilbert lo presenta en su trabajo [], para probar un resultado de "generación finita de invariantes". Pero... en la época en que este resultado fue presentado, la comunidad matemática no tenía resuelto aún la discusión sobre la veracidad o no del axioma de elección (que siendo un axioma, se puede incorporar a la teoría o no...), por lo que fuee fuertemente criticado. Entonces ,Hilbert propuso otra prueba para su teorema de generación finita de invariantes en [], usando lo que ahora se conoce como el "truco unitario de Hilbert.

tiene a j_i como coeficiente líder; sea $\ell = min\{gr(p_i)\}$, reordenando, podemos suponer que $\ell = \mathrm{gr}(p_1)$. Sea $M \subset J$ el conjunto de los polinomios con grado menor que r. Es claro M es un A-submódulo de J, por lo que tenemos que es finitamente generado por $q_1, \ldots, q_t$.

Sea ahora p un polinomio cualquiera de I. Entonces existen $a_1, \ldots a_s \in I$ tales que $\mathrm{LC}(p) = \sum a_i j_i$, por lo que $h_1 = p - \sum a_i p_i \in I$¡ con $\mathrm{gr}(h_1) < \mathrm{gr}(p)$. Si $\mathrm{gr}(h_1) < \ell$ entonces $h_1 \in M$, por lo que existen $b_i \in A$ tales que $h_1 = \sum b_i q_i$. Luego $p = h_1 + suma_i p_i + \sum b_i q_i \in \langle p_1, \ldots, p_s, q_1, \ldots, q_t \rangle$. Si no, repetimos el proceso y por inducción llegamos a que existen $c_1, \ldots, c_s, d_1, \ldots, d_t \in A$ tales que $p = \sum c_i p_i + \sum d_i q_i$. □

Ejercicio 1.10 (El algoritmo de Rufini)**.** Observar que el algoritmo de Rufini no es nada más que una implementación astuta del algoritmo de división, en un caso particular.

Veamos ahora cómo utilizar la división de polinomios para describir mejor el comportamiento de un polinomio en relación a sus ceros.

Proposición 1.32. *Sea A un anillo. Entonces $a \in A$ es un cero de $p \in A[x]$ si y sólo si $(x - a)$ divide a A.*

Prueba: Consideremos la división de p por $(x - a)$: existen $b, r \in A$ y $q \in A[x]$ tales que $bp = q(x - a) + r$ — notar que $r \in A$ porque tiene grado ≤ 0. Si $p(a) = 0$, entonces $bp(a) = 0$, por lo que $r = 0$.

Recíprocamente, si $(x-a)\big|p$, tenemos que $p = q((x-a)$, por lo que $p(a) = 0$. □

Corolario 1.33. *Un polinomio no nulo $p \in A[x]$ tiene a lo sumo* $\mathrm{gr}(p)$ *raíces contadas con multiplicidad.*

Proposición 1.34. *Sea A un anillo. Entonces el morfismo de anillos $\varphi_A : A[x] \to A^A$ (las funciones de A en A) dado por $\varphi_A(p)(a) = p(a)$ es inyectivo si y solamente si A es infinito.*

Prueba: Si $A = \{a_0, \ldots, a_n\}$ es finito, entonce $p = \prod(x - a_i)$ es un polinomio *mónico* (es decir su coeficiente líder es 1), por lo que no es el polinomio nulo, pero $\mathrm{ev}_a(p) = 0$ para todo $a \in A$.

Recíprocamente, si A es infinito, entonces $\varphi_A(p) = 0$ si y sólo si $p(a) = 0$ para todo A, por lo que p es el polinomio nulo, por el Corolario 1.33. □

Terminemos esta sección viendo un resultado muy útil a la hora de trabajar con ideales en anillos de polinomios con coeficientes en un cuerpo

Ejercicio 1.11. Sean $I = \langle p \rangle, J = \langle q \rangle \subset \Bbbk[x]$ dos ideales en un anillo de polinomios con coeficientes en un cuerpo. Entonces

(1) $I \cap J = \big\langle \mathrm{mcm}(p, q) \big\rangle$.

(2) $IJ = \langle pq \rangle$ (recordar que $IJ = \langle fg : f \in I g \in J)$. En particular, $I^n = \langle p^n \rangle$.

(3) $I + J = \big\langle \mathrm{mcd}(p, q) \big\rangle$.

Terminemos esta sección recordando la definición de cuierpo algebraicamente cerrado.

Definición 1.35. Sea $\Bbbk \subset K$ una *extensión* de cuerpos (es decir, $\Bbbk$ y K son cuerpos). Un elemento $a \in K$ es *algebraico sobre* $\Bbbk$ si existe un polinomio $p \in \Bbbk[x]$ tal que a es un cero de p cuando p se considera como elemento de $K[x]$. Si todo elemento de K es algebraico sobre $\Bbbk$, diremos que K es una extensión algebraica de $\Bbbk$.

La *clausura algebraica de* $\Bbbk$ *en* K es el conjunto (¡es más que un conjunto!) de los elementos de K que son algebraicos sobre $\Bbbk$. Si la clausura algebraica de $\Bbbk$ en K coincide con $\Bbbk$, diremos que $\Bbbk$ es algebraicamente cerrado en K.

La noción de clasurua algebraica tiene una versión absoluta:

Definición 1.36. Un cuerpo $\Bbbk$ es *algebraicamente cerrado* si todo polinomio en $\Bbbk[x]$ tiene al menos una raíz.

Observación 1.37. Aplicando la Proposición 1.32 tenemos que un cuerpo $\Bbbk$ es algebraicamente cerrado si todo polinomio no nulo en $\Bbbk[x]$ tiene tantas raíces contadas con multiplicidad como su grado.

Tenemos entonces el siguiente lema

Lema 1.38. *Si un cuerpo* $\Bbbk$ *es algebraicamente cerrado, entonces es algebraicamente cerrado en toda extensión* $\Bbbk \subset K$.

Prueba: Un polinomio $p \in \Bbbk[x]$ ya tiene todas sus posibles raíces en $\Bbbk$. □

Definición 1.39. La *clausura algebraica de* $\Bbbk$, que notaremos $\overline{\Bbbk}$, se define como la mayor extensión algebraica de $\Bbbk$ (hay que probar que existe). Se puede probar que es $\overline{\Bbbk}$ es algebraicamente cerrado.

Ejemplo 1.40. Los complejos $\mathbb{C}$ son la clausura algebraica de $\mathbb{R}$ y $\mathbb{Q}$.

3. El álgebra de polinomios en varias variables

Definición 1.41. Sea A un anillo. Definimos el *Anillo de polinomios en n variblaes con coeficietnes en* A, que notamos $A[x_1, \ldots, x_n]$, se define así:

(1) Se considera el conjunto de las expresiones $\sum_{i_1,\ldots,i_n=0}^{\infty} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$, donde $a_{i_1,\ldots,i_n} \in A$, nulo salvo para una cantidad finita de subíndices.

(2) Se define la suma de dos polinomios

$$p \sum_{i_1,\dots,i_n=0}^{\infty} a_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n} \text{ y } q = \sum_{i_1,\dots,i_n=0}^{\infty} b_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}$$

como

$$p + q = \sum_{i_1,\dots,i_n=0}^{\infty} (a_{i_1,\dots,i_n} + b_{i_1,\dots,b_n}) x_1^{i_1} \dots x_n^{i_n}.$$

(3) Se define el producto de dos polinomios

$$p \sum_{i_1,\dots,i_n=0}^{\infty} a_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n} \text{ y } q = \sum_{i_1,\dots,i_n=0}^{\infty} b_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}$$

como

$$pq = \sum_{t_1,\dots,t_n=0}^{\infty} \Big(\sum_{a_i+b_i=t_i} a_{i_1,\dots,i_n} b_{i_1,\dots,b_n} \Big) x_1^{t_1} \dots x_n^{t_n}.$$

Observar que el polinomio $0 = \sum_{i_1,\dots,i_n=0}^{\infty} 0 x_1^{i_1} \dots x_n^{i_n}$ es el neutro de la suma, y el polinomio $1 = 1 + sum_{i_1,\dots,i_n=0}^{\infty} 0 x_1^{i_1} \dots x_n^{i_n}$ es el neutro del producto.

Observación 1.42. Nuevamente, es claro que la inclusión $A \subset A[x_1, \dots, x_n]$ dada por $a \mapsto a + sum_{i_1,\dots,i_n=0}^{\infty} 0 x_1^{i_1} \dots x_n^{i_n}$ es un morfismo de anillos: $A[x_1, \dots, x_n]$ es una A–álgebra.

Podemos generalizar la propiedad universal de la Proposición 1.25 como sigue.

Proposición 1.43. *Sea $f : A \to B$ un morfismo de anillos. Si $b_1, \dots, b_n \in B$, entonces existe un único morfismo de anillos $f_{b_1,\dots,b_n} : A[x_1, \dots, x_n] \to B$ que extiende f y tal que $f_b(x) = b$.*

Prueba: Es claro que $f_{b_1,\dots b_n}\big(\sum_{i_1,\dots,i_n=0}^{\infty} a_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}\big) = \sum_{i_1,\dots,i_n=0}^{\infty} a_{i_1,\dots,i_n} b_1^{i_1} \dots b_n^{i_n}$ es la única extensión posible. □

Un anillo de polinomios en n variables puede verse (por recurrencia) como un anillo de polinomios en j–varaibles, con $j \leq n$ (pero con coeficientes en otro anillo)

Proposición 1.44. *Sea A un anillo. Entonces $A[x_1, \dots, x_n] \cong \big(A[x_1, \dots, x_{n-1}]\big)[x_n]$.*

Más en general, si $[n] = \{i_1, \dots, i_t\} \cup \{j_1, \dots, j_{n-t}\}$ es una partición del conjunto $[n] = \{1, \dots, n\}$, entonces

$$A[x_1, \dots, x_n] \cong \big(A[x_{i_1}, \dots, x_{i_t}]\big)[x_{j_1}, \dots, x_{j_{n-t}}]$$

Prueba (a completar): Si probamos el primer isomorfismo, el resto del enunciado se deduce por inducción en s, t.

Para probar el primer isomorfismo, usar las propiedades universales (proposiciones 1.25 y 1.43). Observar que nuevamente se peude hacer una inducción para facilitar las cuentas. □

Notación 1.45. Observar que $x_1, \ldots, x_n$ son "variables", por lo que podemos cambiar su notación por otros nombres. Así, la proposición 1.44 se puede enunciar así:

$$A[x_1, \ldots, x_n, y_1, \ldots, y_m] \cong A[x_1, \ldots, x_n][y_1, \ldots, y_m].$$

Notar que eliminamos también un par de paréntesis curvos.

Dejamos como ejercicio opcional un resultado un poco más avanzado (pues se necesita saber la construcción del producto tensorial de módulos)

Ejercicio Optativo 1.12. Sea A un anillo. Entonces $A[x_1, \ldots, x_n, y_1, \ldots, y_n] \cong A[x_1, \ldots, x_n] \otimes_A A[y_1, \ldots, y_m]$ (isomorfismo de álgebras).

La Proposición 1.44 nos da una herramienta para trabajar con polinomios en varias variables de la cual haremos uso y abuso, por lo que vale la pena hacer al menos un ejercicio al respecto:

Ejercicio 1.13. Consideremos $p = x^4y^3z^2 + 2x^2y^2z - 3x^3y^3z^3 + y^3z^2 - 2x + z + 3 \in \mathbb{k}[x, y, z]$. Escribir p como polinomio en $\mathbb{k}[x, y][z]$, $\mathbb{k}[x, z][y]$ y $\mathbb{k}[y, z][x]$.

Si A es nœtheriano, aplicando el Teorema de la bvase de Hilbert (Teorema 1.31) de modo recursivo, tenemos esta generalización:

Teorema 1.46 (De la base de Hilbert)**.** *Sea A un anillo nœtheriano. Entonces $A[x_1, \ldots, x_n]$ es nœtheriano.*

PRUEBA (A COMPLETAR): Aplicar inducción completa en el número de variables. □

Imitando la Definición 1.26, podemos definir "ceros de un polinomio" — esta definición será crucial para poder definir conjuntos algebraicos).

Definición 1.47. Sea A un anillo, $p = \sum_{i_1,\ldots,i_n=0}^{\infty} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \in A[x_1, \ldots, x_n]$ y $a = (a_1, \ldots, a_n) \in A^n$. La *evaluación de p en a*, que notaremos $\mathrm{ev}_a(p) = \mathrm{ev}_{(a_1,\ldots,a_n)}(p) = p(a) = p(a_1, \ldots, a_n)$, se define como $\sum_{i_1,\ldots,i_n=0}^{\infty} a_{i_1,\ldots,i_n} a_1^{i_1} \ldots a_n^{i_n} \in A$.

Diremos que $a = (a_1, \ldots, a_n)$ es un *cero* de p o que anula a P, si $\mathrm{ev}_a(p) = 0$.

Generalicemos ahora la Proposición 1.34

Proposición 1.48. *Sea A un anillo. Entonces el morfismo de A-álgebras $\varphi_{A,n} : A[x_1, \ldots, xc_n] \to A^{A^n}$, dado por $\varphi_{A,n}(p)(a_1, \ldots, a_n) = \mathrm{ev}_{(a_1,\ldots,a_n)}(p)$ es inyectivo si y sólo si A es infinito.*

PRUEBA: Si A es finito, como $A[x_1] \subset A[x_1, \ldots, x_n]$ tenemos que φ no es inyectivo.

Supongamos ahora A infinito, probaremos por inducción que $\varphi_{B,n}$ es inyectivo para cualquier anillo B infinito. Si $n = 1$ es el contenido de la Proposición 1.34. Supongamos el resultado probado para n, lo probaremos para $n + 1$.

Sea $p \in \ker(\varphi_{A,n+1}) \subset A[x_1, \ldots, x_n, y]$ Entonces la función $\varphi_{A,n+1}(p) : A^n \to A$ es constante igual a cero. Como $A[x_1, \ldots, x_n, y] \cong A[x_1, \ldots, x_n][y]$, el morfismo $\mathrm{ev}_{(a_1,\ldots,a_n)} : A[x_1, \ldots, x_n] \to A$ se extiende a un morfimo de álgebras $\psi_{(a_1,\ldots,a_n)} : A[x_1, \ldots, x_n, y] \to A[y]$, que envía y a y (también podríamos directamente considerar el morfismo que extiende $x_i \mapsto a_i$, $y \mapsto y$, pero nos interesa ver a $A[x_1, \ldots, x_n, y]$ como un anillo de polinomios en y).

Ahora bien, $\mathrm{ev}_{(a_1,\ldots,a_n)} = \mathrm{ev}_{a_{n+1}} \circ \psi_{(a_1,\ldots,a_n)} : A[x_1, \ldots, x_n, y] \to A$, por lo que $p \in \ker(\varphi_{A,n+1})$ si y solamente si $\psi_{(a_1,\ldots,a_n)}(p) \in \ker(\varphi_{A,1})$ para todo $a_1, \ldots, a_n \in A$. Por la hipótesis de inducción, tenemos que $\psi_{(a_1,\ldots,a_n)}(p) = 0$ para todo $a_1, \ldots, a_n \in A$.

Escribamos explícitamente lo que acabamos de probar: como polinomio en y, P puede escribirse como:

$$p = \sum_i q_i y^i$$

donde $q_i \in A[x_1, \ldots, x_n]$. Entonces

$$0 = \psi_{(a_1,\ldots,a_n)}(p) = \sum_i \big(\mathrm{ev}_{(a_1,\ldots,a_n)}(q_i)\big) y^i$$

Tenemos entonces que $\mathrm{ev}_{(a_1,\ldots,a_n)}(q_i) = 0$ para todo i, para todo $a_1, \ldots, a_n \in A$, es decir $q_i \in \ker(\varphi_{A,n})$. Aplicando la hipótesis de inducción ahora al anillo $A[x_1, \ldots, x_n]$, deducimos que $q_i = 0$ para todo i, es decir $p = 0$. □

Ejercicio 1.14. Es el momento de hacer el tutorial de Sage para polinomios en varias variables (ejercicio para Sage 1.20

4. Ejercicios para Sage

Ejercicio en Sagemath 1.15. Hacer el tutorial de Sage correspondiente a las secciones

(a) *Assignment, Equality, and Arithmetic*
https://doc.sagemath.org/html/en/tutorial/tour_assignment.html

(b) *Getting Help* y *Functions, Indentation, and Counting*
https://doc.sagemath.org/html/en/tutorial/tour_help.html

(c) *Basic Algebra and Calculus: Solving Equations*
https://doc.sagemath.org/html/en/tutorial/tour_algebra.html#solving-equations

Ejercicio en Sagemath 1.16. Hacer el tutorial de Sage para anillos
https://doc.sagemath.org/html/en/tutorial/tour_rings.html

Ejercicio en Sagemath 1.17. Realizar un hoja de trabajo en sage que implemente la divisisión entera.

Ejercicio en Sagemath 1.18. hacel el tutorial de Sage para polinomios en una variable
https://doc.sagemath.org/html/en/tutorial/tour_polynomial.html#univariate-polynomials

Ejercicio en Sagemath 1.19. (1) Implementar el algoritmo de división de polinomios para algún cuerpo.

(2) Implementar el algoritmo para encontrar el máximo común divisor de dos polinomios, para algún cuerpo.

Ejercicio en Sagemath 1.20. Completar el tutorial de Sage para anillos de polinomios
https://doc.sagemath.org/html/en/tutorial/tour_polynomial.html

Capítulo 2

Conjuntos algebraicos

Más adelante supondremos que $\Bbbk$ es un cuerpo algebraicamente cerrado, pero en este capítulo trabajaremos sobre un cuerpo $\Bbbk$ cualquiera.

1. La topología Zariski de $\Bbbk^n$

Definición 2.1. Dado un conjunto de polimonios $S \subset \Bbbk[x_1, \ldots, x_n]$, definimos el *conjunto de los ceros comunes de* S como el conjunto

$$\mathcal{V}(X) = \big\{a = (a_1, \ldots, a_n) : \mathrm{ev}_a(p) = 0 \ \forall p \in S\big\}$$

Diremos que un subconjunto $X \subset \Bbbk^n$ es *algebraico* si $X = \mathcal{V}(S)$ para algún consjunto S de polinomios.

Ejemplo 2.2. (1) $\mathcal{V}(0) = \Bbbk^n$

(2) $\mathcal{V}(1) = \emptyset$

(3) Si $p \in \Bbbk[x_1, \ldots, x_n]$, entonces el gráfico de p es un conjunto algebraico de $\Bbbk^{n+1}$:

$$\mathrm{Graf}(p) = \mathcal{V}\big(\{p \in \Bbbk[x_1, \ldots, x_n, y], py - 1\}\big)$$

Observemos que estamos usando que p puede verse como un polinomio en $\Bbbk[x_1, \ldots, x_n, y]$.

(4) Si $S \subset D$, entonces $\mathcal{V}(S) \supset \mathcal{V}(D)$.

(5) Los conjuntos algebraicos de $\Bbbk$ son $\emptyset, \Bbbk$ y los conjuntos finitos.

Probaremos en **??** que los conjuntos algebraicos conforman los cerrados de una topología. Antes de ello, veamos algunas propiedades básicas.

Lema 2.3. *Sea $X \subset \Bbbk[x_1, \ldots, x_n]$. Entonces $\mathcal{V}(X) = \mathcal{V}\big(\langle X\rangle\big)$.*

Prueba: Un elemento de $\langle X\rangle$ es de la forma $p = \sum_{i=1}^n q_i p_i$, con $p_i \in X$, $q_i \in \Bbbk[x_1, \ldots, x_n]$. Deducimos que $\mathrm{ev}_a(p) = \sum_{i=1}^n \mathrm{ev}_a(q_i)\,\mathrm{ev}_a(p_i)$. El resultado ahora es fácil. □

Lema 2.4. *Sean $X = \mathcal{V}(I)$ e $Y = \mathcal{V}(J)$. Dos conjuttnos algebraicos. Entonces:*

(1) $X \cap Y = \mathcal{V}\big(I \cup J\big)$.

(2) $X \cup Y = \mathcal{V}\big(\langle I\rangle \cap \langle J\rangle\big) = \mathcal{V}\big(IJ\big)$, *en donde* $IJ = \{pq : p \in I, q \in J\}$.

Prueba:

Bibliografía

[1] Cox, Little y O'Shea *Ideals, Varieties and Algoritms.* (13Pxx COXi) Es la base del curso se tratarán los capítulos 4, 1 y 2 más o menos en ese orden. Usaremos la última edición, accesible a través del portal Timbó.

[2] Cox, Little y O'Shea *Using Algebraic Geometry.* (14-01 COXu) Sólo lo puse como referencia, es en algún sentido la continuación del libro anterior.

[3] Einsenbud, D *Commutative algebra with a view toward algebraic geometry.* Contiene casi todos los temas del curso, pero asume conocimientos de álgebra conmutativa, y no hace énfasis en los aspectos algorítmicos.

[4] Sagemath.org Tutulrial: `https://doc.sagemath.org/html/en/tutorial/tour.html`