ESTRUCTURAS ALGEBRAICAS
Curso 2003–2004

Tema 1 Anillos e ideales. Operaciones. Divisibilidad y factorización.

Tema 2 Conjuntos algebraicos afines y sistemas de ecuaciones polinómicas. Anillos noetherianos. Cálculos en los anillos de polinomios: bases de Gröbner.

Tema 3 Teorema de los ceros de Hilbert.

Tema 4 Módulos sobre un anillo. Operaciones. Hom(M,N).

Tema 5 Aplicaciones multilineales. Producto tensorial de módulos. Álgebras.

Tema 6 Teorema de estructura de los módulos finitamente generados sobre un D.I.P.. Aplicaciones: ecuaciones lineales con coeficientes enteros, formas canónicas de Jordan.

Bibliografía

1. Atiyah, M.F., Macdonald, I.G., "Introducción al Álgebra conmutativa". Ed. Reverté, Barcelona, 1989.

2. Cox, D., Little, J., O'Shea, D., " Ideals, varieties, and algorithms (An introduction to computational algebraic geometry and commutative algebra)". Second edition. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997. (ISBN: 0-387-94680-2)

3. Fulton, W., "Curvas algebraicas : introducción a la geometría algebraica". Ed. Reverté, Barcelona, 1971.

4. Jacobson, N., "Basic Algebra I". Second edition. W. H. Freeman and Company, New York, 1985. (ISBN: 0-7167-1480-9)

5. Kunz, E., " Introduction to commutative algebra and algebraic geometry". Birkhäuser Boston, Inc., Boston, MA, 1985. (ISBN: 3-7643-3065-1)

6. Lang, S., "Álgebra". Ed. Aguilar, Madrid, 1971.

7. Serre, J.P., "Representaciones lineales de los grupos finitos". Omega, Barcelona, 1970.

1 Anillos e ideales. Operaciones. Divisibilidad y factorización.

1.1 Anillos e ideales. Operaciones.

Esta parte se corresponde con el capítulo 1 del libro

Atiyah, M.F., Macdonald, I.G., "Introducción al Álgebra conmutativa". Ed. Reverté, Barcelona, 1989.

1.2 Divisibilidad

Definición 1.1 *Sea A un dominio de integridad.*

1. *Sean $a, b \in A$, con $a \neq 0$. Se dirá que a divide a b, o que a es un* divisor *de b si existe $c \in A$ tal que $b = ac$. Este elemento c es único por ser A un dominio de integridad, y se le designará por b/a. También se dirá, en este caso, que b* es divisible por *a. Se escribirá $a|b$ para designar esta relación. Es evidente que una unidad divide a cualquier otro elemento de A.*

2. *Se dirá que a y b, con $a, b \neq 0$, son* asociados *si y sólo si $a|b$ y $b|a$. En este caso se puede escribir $b = ac$ y $a = bc'$, luego $a = acc'$, de donde $a(1 - cc') = 0$, y así $cc' = 1$. De aquí se ve ya fácilmente que a, b son asociados si y sólo si uno de ellos es igual al otro multiplicado por una unidad.*

3. *Sean $a, b \in A$ distintos de cero. Un* máximo común divisor *de a y b es un elemento $d \in A$ que verifica:*

   (a) $d|a$ y $d|b$.

   (b) Si $d' \in A$ es tal que $d'|a$ y $d'|b$, entonces $d'|d$.

   De lo anterior se deduce que, si d, d' son dos máximos comunes divisores de a, b, entonces $d|d'$ y $d'|d$, luego son asociados. Así pues, el máximo común divisor de a, b está unívocamente determinado, salvo producto por unidades, y se escribe $\mathrm{m.\,c.\,d.}(a, b)$.

4. *Sean $a, b \in A$, distintos de cero. Un mínimo común múltiplo de a y b es un elemento $m \in A$ que verifica:*

   (a) $a|m$ y $b|m$.

   (b) Si $m' \in A$ es tal que $a|m'$ y $b|m'$, entonces $m|m'$.

   De lo anterior se deduce que, si m, m' son dos mínimos comunes múltiplos de a, b, entonces $m|m'$ y $m'|m$, luego son asociados. Así pues, el mínimo común múltiplo de a, b está unívocamente determinado, salvo producto por unidades, y se escribe $\mathrm{m.c.m.}(a, b)$.

5. *Un elemento $p \in A$ se llama* irreducible *si sólo es una no unidad distinta de cero, divisible únicamente por sus asociados y por las unidades.*

6. *Un elemento $p \in A$ se llama* primo *si $p|(ab) \Rightarrow p|a$ ó $p|b$.*

Proposición 1.2 *Todo elemento primo de un dominio de integridad es irreducible.*

Ejemplo 1.3 *El recíproco de la proposición anterior no es cierto. Si consideramos el domino de integridad*

$$A = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

se tiene la igualdad $2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ y $2 \in A$ es irreducible pero no divide a $1 + \sqrt{-3}$ (los detalles se verán más adelante).

Nota 1.4 1. *Sea $d = \mathrm{m.\,c.\,d.}(a, b)$ y escribamos $a' = a/d$, $b' = b/d$; entonces*

$$\mathrm{m.\,c.\,d.}(a', b') = 1.$$

En efecto, supongamos que existiese una no unidad $e \in A$, distinta de cero, tal que $e|a'$ y $e|b'$. Entonces $(ed)|a$ y $(ed)|b$, luego $(ed)|d$, lo que implicaría que ed, d son asociados. Esto no es posible, pues e no es una unidad.

2. *Nótese que, hasta ahora, no hemos afirmado nada sobre la existencia del máximo común divisor de dos elementos. Nos hemos limitado a dar propiedades de él, caso de que exista.*

Ejemplo 1.5 *En $\mathbb{Z}$ sabemos que existe el máximo común divisor y el mínimo común múltiplo de cualquier par de enteros no nulos.*

Definición 1.6 *Un* dominio de factorización única *(DFU) es un dominio de integridad A que verifica las siguientes condiciones:*

(DFU1) *Toda no unidad distinta de cero es producto finito de factores irreducibles.*

(DFU2) *La descomposición anterior es única salvo orden y producto por unidades. Se llama la* descomposición factorial *del elemento en cuestión.*

Ejemplo 1.7 *$\mathbb{Z}$ es un dominio de factorización única.*

Proposición 1.8 *Sea A un dominio de integridad que satisface la condición* (DFU1)*. Entonces A satisface* (DFU2) *si y sólo si satisface la siguiente:*

(DFU3) *Todo elemento irreducible de A es primo (esta propiedad se la conoce con el nombre de* teorema de Euclides*, por analogía con el caso de los números enteros).*

Demostración: Supongamos que A satisface (DFU2), y sean p, a, b como en el enunciado. Supongamos que p no divide a a, y sea $ab = pq$. Sean

$$a = p_1 \cdots p_s \ , \ b = q_1 \cdots q_t \ , \ q = r_1 \cdots r_u$$

las descomposiciones factoriales de a, b, q. Como

$$(p_1 \cdots p_s)(q_1 \cdots q_t) = pr_1 \cdots r_u,$$

la unicidad indica que p (o un asociado) tiene que figurar entre los elementos irreducibles del miembro de la izquierda de la anterior igualdad. Como no puede figurar entre los p_i, porque no divide a a, debe figurar entre los q_j. Así $p|b$, lo que prueba (DFU3).

Recíprocamente, supongamos que A verifica (DFU3), y sean

$$a = p_1 \cdots p_s = q_1 \cdots q_t$$

dos descomposiciones de a en producto de irreducibles. Por (DFU3), p_1 (o un asociado suyo) debe coincidir con un q_i, digamos q_1. Cancelando ambos en la igualdad anterior, se tiene la igualdad

$$p_2 \cdots p_s = q_2 \cdots q_t,$$

con la que se procede como antes, y así sucesivamente. Esto prueba (DFU2). ■

Corolario 1.9 *Sea A un dominio de factorización única; cualquier par de elementos $a, b \in A$ distintos de cero tienen un máximo común divisor $d \in A$.*

Demostración: Considerando las descomposiciones factoriales de a, b basta tomar como d el producto de todos los factores irreducibles comunes a las dos. En efecto, sean

$$a = (p_1 \cdots p_r)(p'_1 \cdots p'_s) \ , \ b = (p_1 \cdots p_r)(q'_1 \cdots q'_t)$$

las descomposiciones factoriales, donde

$$\{p'_1, \ldots, p'_s\} \cap \{q'_1, \ldots, q'_t\} = \emptyset,$$

y sea $d = p_1 \cdots p_r$. Claramente $d|a$ y $d|b$. Sea $d' \in A$ tal que $d'|a$ y $d'|b$. Si p es un elemento irreducible que divide a d', entonces p (o un asociado) debe coincidir con un p_i, digamos p_1. De aquí se deduce que $(d'/p_1)|(a/p_1)$ y $(d'/p_1)|(b/p_1)$. Repitiendo el razonamiento cuantas veces sea necesario se deduce que $d'|d$. Esto prueba el corolario. ■

Definición 1.10 *Sean $a, b \in A$; entonces* $\mathrm{m.c.d.}(a, b) = 1$ *si y sólo si ningún elemento irreducible divide a ambos. En este caso se dice que a, b* son primos entre sí.

Corolario 1.11 *Sean $a, b, c \in A$ tales que $c|(ab)$ y a, c son primos entre sí. Entonces c divide a b.*

La demostración se hace al estilo de la del corolario 1.9, considerando sucesivamente divisores irreducibles de c y viendo que dividen a b.

Corolario 1.12 *Sea A un dominio de factorización única, $a, b \in A$ distintos de cero, $d = \mathrm{m.\,c.\,d.}(a, b)$. Entonces a, b tienen un mínimo común múltiplo, que es $m = ab/d$.*

1.3 Dominios euclídeos.

En este punto ya hemos utilizado propiedades elementales de la división euclídea en $\mathbb{Z}$:"Dados $D, d \in \mathbb{Z}$, $d \neq 0$, existen unos únicos $c, r \in \mathbb{Z}$ (cociente y resto) tales que: $D = dc + r$ y $0 \leq r < |d|$".

De una manera análoga en $k[X]$, anillo de polinomios en la variable X sobre un cuerpo k, hay una división euclídea de polinomios: "Dados $D(X), d(X) \in k[X]$, $d \neq 0$, existen unos únicos $c(X), r(X) \in k[X]$ (cociente y resto) tales que: $D(X) = d(X)c(X) + r(X)$ y $r = 0$ ó bien $\mathrm{gr}(r) < \mathrm{gr}(d)$". La demostración informal de lo anterior se conoce desde la secundaria. Una demostración formal se puede hacer por inducción en $n = \mathrm{gr}(D) - \mathrm{gr}(d)$.

Vamos a definir los dominios euclídeos como los anillos en donde se da una propiedad análoga a las anteriores.

Definición 1.13 *Sea A un dominio de integridad. Diremos que A es un* dominio euclídeo *si existe una aplicación $\delta : A \setminus \{0\} \to \mathbb{N}$ tal que:*

1. *Si $a, b \in A \setminus \{0\}$ y $a|b$, entonces $\delta(a) \leq \delta(b)$.*
2. *(*División entera con resto respecto de δ*) Dados $D, d \in A$, $d \neq 0$, existen $c, r \in A$ tales que: $D = dc + r$ y $\delta(r) < \delta(d)$ si $r \neq 0$.*

Por el comentario anterior es obvio que $\mathbb{Z}$ y $k[X]$ son dominios euclídeos, para $\delta(a) = |a|$ en el primer caso, y $\delta(f) = \mathrm{gr}(f)$ en el segundo.

En la segunda propiedad de la definición no se exige que el "cociente" c y el "resto" r sean únicos. De hecho después veremos ejemplos en los que no se da esta unicidad.

Proposición 1.14 *Sea (A, δ) un dominio euclídeo.*

1. *Si u es una unidad de A, $\delta(u)$ es el valor mínimo de δ.*
2. *Si $a, b \in A \setminus \{0\}$ son asociados, entonces $\delta(a) = \delta(b)$.*
3. *Si $a, b \in A \setminus \{0\}$, $a|b$ y $\delta(a) = \delta(b)$, entonces a y b son asociados.*
4. *Un elemento $a \in A \setminus \{0\}$ es una unidad, si y sólo si $\delta(a) = \delta(1)$.*

Demostración: La primera afirmación es consecuencia inmediata de que una unidad divide a todo elemento, y de la primera condición de dominio euclídeo. La segunda afirmación es trivial. Para la tercera afirmación, dividimos a por b: $a = cb + r$. Si $r \neq 0$, entonces $\delta(r) < \delta(b)$. Como $a|b$, existe $a' \in A$ tal que $b = a'a$. Por tanto $r = a - cb = (1 - ca')a$, por lo que $\delta(a) \leq \delta(r)$, que contradice la hipótesis. Por ello $r = 0$, y $b|a$ como queríamos. La última afirmación es consecuencia fácil de las anteriores. ■

Un ejemplo de dominios es $A = \mathbb{Z}[\sqrt{m}] \subset \mathbb{C}$, con m entero libre de cuadrados. En ellos podemos definir una aplicación "norma", que verifica siempre la primera condición de dominio euclídeo, y en algunos casos también la segunda:

$$N : A \to \mathbb{N}, \quad \text{con} \quad N(a + b\sqrt{m}) = |(a + b\sqrt{m})(a - b\sqrt{m})| = |a^2 - mb^2|.$$

Proposición 1.15 *N verifica las siguientes propiedades:*

1. *$N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{m}]$.*
2. *Si $u \in \mathbb{Z}[\sqrt{m}]$, $N(u) = 1$ si y sólo si u es una unidad.*
3. *Si $x, y \in \mathbb{Z}[\sqrt{m}]$, $x|y$ y $N(x) = N(y)$, si y sólo si x e y son asociados.*
4. *Si $x \in \mathbb{Z}[\sqrt{m}]$ y $N(x)$ es un número primo, entonces x es irreducible.*

La demostración es un fácil ejercicio.

Nota 1.16

1. *Con las propiedades anteriores, es un ejercicio elemental probar que $\mathbb{Z}[\sqrt{-3}]$ no es DFU, puesto que 2 es un elemento irreducible, pero no primo, ya que divide a $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, pero no divide a ningún factor.*

2. *El caso $m = -1$ es el del anillo de los enteros de Gauss, $\mathbb{Z}[i]$, que es dominio euclídeo, cuando definimos una división entera en él.*

   Sean $x, y \in \mathbb{Z}[i]$, $b \neq 0$. Entonces el cociente complejo de x y y es $u + vi \in \mathbb{C}$, con $u, v \in \mathbb{Q}$. Sean $m, n \in \mathbb{Z}$ unas aproximaciones enteras que redondean u, v, es decir tales que

   $$|m - u| \leq \frac{1}{2} \qquad \text{y} \qquad |n - v| \leq \frac{1}{2}.$$

   Entonces $r = x - (m + ni)y \in \mathbb{Z}[i]$. Por la elección anterior, se tiene que $r = y[(u - m) + i(v - n)]$, por lo que $N(r) \leq \frac{1}{2}N(y) < N(y)$. Se tiene así que

   $$x = (m + ni)y + r, \quad \text{con} \quad N(r) < N(y),$$

   por lo que $\mathbb{Z}[i]$ queda dotado de estructura de dominio euclídeo, con la norma N como aplicación δ.

3. *De un modo análogo se podría dotar a $\mathbb{Z}[\sqrt{2}]$ de una estructura de dominio euclídeo.*

Definición 1.17 *Un dominio A se dice de* ideales principales*, (DIP), cuando todos sus ideales lo son.*

El resultado siguiente nos da una gran cantidad de ejemplos.

Proposición 1.18 *Todo dominio euclídeo es un dominio de ideales principales.*

Demostración: Sea (A, δ) un dominio euclídeo, e I un ideal no nulo de A. Sea $a \in I \setminus \{0\}$ un elemento con $\delta(a)$ mínimo. Vamos a probar que $I = (a)$. Una inclusión es clara. Recíprocamente, sea $b \in I$, que dividimos por a, obteniendo $b = ca+r$. Si r no es cero, como está en I y $\delta(r) < \delta(a)$, llegamos a contradicción con la elección de a. Por tanto $r = 0$, y se tiene lo deseado. ■

No es cierto el recíproco. Hay dominios de ideales principales que no son euclídeos, como $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, pero esta comprobación es bastante difícil.

$\mathbb{Z}[X]$, con X una variable, es un ejemplo de un dominio que no es DIP. Para ello verifíquese que $(2, X)$ no es un ideal principal en $\mathbb{Z}[X]$.

1.4 Factorización.

El resultado fundamental de esta sección es el siguiente:

Teorema 1.19 *Todo DIP es un DFU.*

Definición 1.20 *Se dice que un anillo A verifica la* condición de cadena ascendente para ideales *(o, brevemente, la CCA) si toda cadena estrictamente creciente de ideales de A*

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

es finita. Equivalentemente, toda cadena ascendente infinita de ideales

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

es estacionaria, es decir, existe un entero $n > 0$ tal que $I_j = I_n$, para todo $j \geq n$.

Proposición 1.21 *Sea A un DIP; entonces verifica la CCA.*

Demostración: Sea

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

una cadena ascendente de ideales, y sea

$$I = \bigcup_{j \geq 1} I_j$$

la unión de todos ellos; entonces I es un ideal. En efecto, sean $a, b \in I$, digamos $a \in I_j$ y $b \in I_k$. Si, por ejemplo, $k \geq j$, entonces $a, b \in I_k$, luego $a - b \in I_k \subseteq I$. Si $a \in I$, digamos $a \in I_j$, y $x \in A$, entonces $ax \in I_j \subseteq I$. Ahora bien, el ideal I es principal; escribamos $I = Ad$. Entonces $d \in I_n$ para un cierto n, luego $I_n = I$. Así, para todo $j \geq n$ es $I_j = I = I_n$. Esto prueba la proposición. ■

Proposición 1.22 *Sea A un DIP; entonces A verifica la condición* (DFU1).

Demostración: Sea a una no unidad distinta de cero. Tenemos que probar que a se descompone en producto finito de elementos irreducibles. Si a es irreducible, no hay nada que probar. Si a no es irreducible, se puede escribir $a = bc$ donde b y c no son asociados de a, ni unidades. Así $Aa \subset Ab$ y $Aa \subset Ac$. Repitiendo el razonamiento con b, por ejemplo, y así sucesivamente, la CCA implica que este proceso es finito, lo que nos lleva a que a debe tener un divisor irreducible p_1. Entonces

$$Aa \subset A\frac{a}{p_1}.$$

Si $a_1 = a/p_1$ es irreducible, entonces $a = a_1 p_1$ es una descomposición factorial de a, y nuestra demostración habrá concluido. Supongamos que a_1 no es irreducible. Aplicando a $a_1 = a/p_1$ el mismo razonamiento, llegamos a la existencia de un divisor irreducible p_2 de a_1, y a una terna

$$Aa \subset Aa_1 \subset Aa_2,$$

con $a_1 = p_2 a_2$. Por CCA, este proceso debe tener un fin, es decir, debe existir un entero positivo n tal que $a/(p_1 \cdots p_{n-1}) = p_n$ sea irreducible. Así $a = p_1 \cdots p_{n-1} p_n$, lo que prueba la proposición. ■

Proposición 1.23 *(*Identidad de Bezout*) Sea A un DIP, y sean $a, b \in A$ dos elementos no nulos. Entonces existe un elemento $d = \alpha a + \beta b$ con $\alpha, \beta \in A$, tal que $d = \mathrm{mcd}(a, b)$.*

Demostración: Sea (a, b) el ideal engendrado por a, b; entonces existe $d \in A$ tal que $(a, b) = Ad$. Como $Aa \subseteq Ad$ y $Ab \subseteq Ad$, es $d|a$ y $d|b$. El hecho de que $d = \mathrm{mcd}(a, b)$ viene, ahora, de que d es de la forma $d = \alpha a + \beta b$. ■

La demostración del teorema 1.19 termina con la siguiente

Proposición 1.24 *Sea A un DIP; entonces A verifica* (DFU3).

Demostración: Sea $p \in A$, irreducible, con $p|ab$, y supongamos que p no divide a a. Entonces $1 = \mathrm{mcd}(a, p)$ y, por la proposición anterior, $1 = \alpha a + \beta p$. Así, $b = \alpha ab + \beta bp$, de donde se deduce que $p|b$. Esto prueba la proposición. ■

Nota 1.25 *En el caso de un dominio euclídeo A, se puede generalizar el algoritmo de Euclides para $\mathbb{Z}$, de cálculo del máximo común divisor de dos elementos $a, b \in A \setminus \{0\}$:*

Se construye la sucesión $r_0, r_1, r_2, \ldots, r_n$, poniendo $r_0 = a$, $r_1 = b$, y para cada $j \geq 2$, r_j es el resto de dividir r_{j-2} por r_{j-1}. El proceso acaba alcanzando el cero en cierto r_n. Entonces $r_{n-1} = \mathrm{mcd}(a, b)$. La validez del algoritmo se basa en dos cuestiones. Por una parte $\mathrm{mcd}(r_i, r_{i+1}) = \mathrm{mcd}(r_{i+1}, r_{i+2})$, para cada $i = 0, \ldots, n-3$, y por otra que el algoritmo debe acabar puesto que δ va decreciendo en la sucesión creada.

Hay un procedimiento simple de construir un DFU: si A es un DFU, también lo es $A[X]$. Se basa en el lema de Gauss que los alumnos conocen sólo en el caso de polinomios con coeficientes enteros. Generalizamos los resultados necesarios para demostrar el teorema.

Se considera A un dominio de factorización única.

Definición 1.26 *Si $f(X) \in A[X]$ es un polinomio no nulo, llamamos* **contenido** *de $f(X)$ a un máximo común divisor de los coeficientes de $f(X)$, y lo notaremos por $c(f(X))$.*

Decimos que el polinomio es **primitivo** *si $c(f) = 1$.*

Lema 1.27 *(*Lema de Gauss*) Sea A un dominio de factorización única y $f(X)$, $g(X)$ polinomios no nulos de $A[X]$. Entonces,*

$$c(f(X)g(X)) = c(f(X))c(g(X)).$$

En particular, si $f(X)$ y $g(X)$ son primitivos entonces el producto $f(X)g(X)$ es primitivo.

Demostración: Análoga al caso $A = \mathbb{Z}$. ■

Lema 1.28 *Se considera A un dominio de factorización única con cuerpo de fracciones K. Si $f(X) \in K[X]$ es un polinomio no nulo, entonces $f(X) = \alpha f_1(X)$ con $\alpha \in K$ y $f_1(X)$ un elemento primitivo de $A[X]$. Esta factorización es única salvo producto por una unidad de A.*

Demostración: Análoga al caso $A = \mathbb{Z}$. ■

Lema 1.29 *Sea A un dominio de factorización única con cuerpo de cocientes K y $f(X) \in A[X]$. Son equivalentes:*

1. *$f(X)$ tiene grado positivo y es irreducible en $A[X]$.*
2. *$c(f(X)) = 1$ y $f(X)$ es irreducible en $K[X]$.*

Demostración: Análoga al caso $A = \mathbb{Z}$. ■

Teorema 1.30 *Si A es un dominio de factorización única, entonces $A[X]$ es un dominio de factorización única.*

Demostración: Sea K el cuerpo de cocientes de A y tomemos $f(X) \in A[X]$ no nulo. Si tiene grado cero, es un elemento de A, y su factorización es única. Podemos suponer que $f(X)$ es de grado positivo.

Como $K[X]$ es un dominio euclídeo, es un dominio de factorización única, por lo que existen $p_1(X), \ldots, p_r(X)$ polinomios irreducibles en $K[X]$ tales que

$$f(X) = p_1(X) \ldots p_r(X).$$

Existen entonces $\alpha_i \in K$ tales que $p_i(X) = \alpha_i q_i(X)$, $q_i(X) \in A[X]$ polinomio primitivo para cada $i = 1, \ldots, r$.

Sea $\alpha = \alpha_1 \ldots \alpha_r = \frac{a}{b}$, $a, b \in A$.

Se tiene entonces, $bf(X) = aq_1(X) \ldots q_r(X)$. Por el lema de Gauss,

$$c(bf(X)) = b(c(f(X))) = a.$$

Así b divide a A y $c(f(X)) = \alpha \in A$.

Por ser A dominio de factorización única, $\alpha = d_1 \ldots d_s$ con $d_i \in A$ elementos irreducibles en A, y por tanto en $A[X]$. Obtenemos

$$f(x) = d_1 \cdots d_s q_1(X) \cdots q_r(X),$$

una factorización en irreducibles en $A[X]$ porque $q_i(X)$ es irreducible en $A[X]$ por ser primitivo e irreducible en $K[X]$ (lema previo).

Veamos la unicidad de la descomposición.

Supongamos que tenemos otra factorización

$$f(x) = b_1 \cdots b_t q_1'(X) \cdots q_k'(X),$$

donde $q_i'(X) \in A[X]$ es de grado positivo e irreducible, y b_i irreducible en A. Por el lema previo, se tiene que $q_i'(X)$ es primitivo e irreducible en $K[X]$.

Esto proporciona una factorización en irreducibles en $K[X]$, de donde $r = k$ y los $q_i(X)$ y $q_i'(X)$ son asociados en $A[X]$ (por primitivos).

Se tiene entonces

$$d_1 \ldots d_s = ub_1 \ldots b_t$$

con $u \in A$ unidad en A. Por el lema de Gauss, éstas son dos descomposiciones factoriales del contenido de f, y por tanto $s = t$ y los d_i y b_i asociados en A.

■

2 Conjuntos algebraicos afines y sistemas de ecuaciones polinómicas. Anillos noetherianos. Cálculos en los anillos de polinomios: bases de Gröbner

2.1 Conjuntos algebraicos afines y sistemas de ecuaciones polinómicas. Anillos noetherianos.

Esta parte se corresponde con el capítulo 1, secciones 2,3,4 y 5 del libro Fulton, W., "Curvas algebraicas : introducción a la geometría algebraica". Ed. Reverté, Barcelona, 1971.

2.2 Cálculos en los anillos de polinomios: bases de Gröbner

[1]

Definición 2.1 *Diremos que una relación de orden $\leq$ en $\mathbb{N}^n$ es un orden monomial si verifica:*

(1) Es un orden total.

(2) Para todo $\alpha, \beta \in \mathbb{N}^n$ tales que $\alpha < \beta$, y para todo $\gamma \in \mathbb{N}^n$, $\alpha + \gamma < \beta + \gamma$. A esta propiedad la llamaremos ser estable para la suma.

(3) Es un buen orden, es decir, todo subconjunto no vacío tiene un primer elemento.

Nota 2.2 *Para cualquier orden monomial, $0 = (0, \ldots, 0)$ es el primer elemento de $\mathbb{N}^n$. En efecto, si el primer elemento fuera $\alpha \neq 0$, se tendría $0 > \alpha$, y el ser estable para la suma aseguraría que*

$$\alpha > 2\alpha > 3\alpha > \ldots$$

sería una cadena infinita, en contra de ser un buen orden.

Ejemplo 2.3 *(1) En $\mathbb{N}$, el orden usual $\leq$ es monomial. Si $n \geq 2$, en $\mathbb{N}^n$ se considera el orden natural $\leq$: $\alpha = (\alpha_1, \ldots, \alpha_n) \leq \beta = (\beta_1, \ldots, \beta_n)$ si $\alpha_i \leq \beta_i$, para todo $i = 1, \ldots, n$. Este orden no es total, y por tanto, no es monomial. Para referirnos a él, lo llamaremos orden parcial natural en $\mathbb{N}^n$.*

(2) (Orden lexicográfico).

[1] Estas notas han sido elaboradas con la colaboración de Sara Arias de Reyna, Alumna Interna del Departamento de Álgebra (curso 2002-03).

Sea $n \geq 1$, y sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$. Entonces se define el orden lexicográfico del siguiente modo: $\alpha >_{lex} \beta$ si y sólo si la primera componente por la izquierda no nula de $\alpha - \beta$ es positiva.

(3) (Orden graduado lexicográfico).
Sea $n \geq 1$, y sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$. Se define la norma o longitud de α como $|\alpha| = \sum_{i=1}^{n} \alpha_i$.
Entonces el orden lexicográfico graduado se define del siguiente modo:

$$\alpha >_{grlex} \beta \leftrightarrow \begin{cases} |\alpha| > |\beta| \\ \acute{o} \\ |\alpha| = |\beta| \quad y \quad \alpha >_{lex} \beta \end{cases}$$

(4) (Otros órdenes monomiales).
Sea $n \geq 1$, y sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$. Sean $w_1, \ldots, w_n \in \mathbb{R}^+$, y definamos $\mathrm{L}(\alpha) = \sum_{i=1}^{n} w_i \alpha_i$.
Entonces el podemos definir un orden monomial $\prec$ del siguiente modo:

$$\alpha \succ \beta \leftrightarrow \begin{cases} \mathrm{L}(\alpha) > \mathrm{L}(\beta) \\ \acute{o} \\ \mathrm{L}(\alpha) = \mathrm{L}(\beta) \ y \ \alpha >_{lex} \beta \end{cases}$$

Nota 2.4 *Cualquier orden monomial refina el orden parcial natural. En efecto, sean $\alpha, \beta \in \mathbb{N}^n$ donde $\beta = \alpha + \gamma$ con $\gamma \in \mathbb{N}^n - \{0\}$. Si respecto a un orden monomial $\alpha > \beta$, por ser estable para la suma, $\beta = \alpha + \gamma > \beta + \gamma$, en contra de*

$$0 < \gamma \Longrightarrow \beta < \gamma + \beta.$$

Por tanto, $\alpha < \beta$.

Definición 2.5 *Sea $f \in k[\mathbf{X}] = k[X_1, \ldots, X_n]$. El monomio $X_1^{\alpha_1} \cdots X_1^{\alpha_n}$ se representará como X^α, donde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Se tendrá, $f = \sum_{\alpha \in J} a_\alpha X^\alpha$, donde $a_\alpha \in k$, $J \subset \mathbb{N}^n$ es un subconjunto finito. El soporte de f es el conjunto*

$$\mathrm{sop}(f) = \{\alpha \in \mathbb{N}^n \quad | \quad a_\alpha \neq 0\}.$$

Definición 2.6 *Sea $\prec$ un orden monomial, y sea $f = \sum_{\alpha \in \mathrm{sop}(f)} a_\alpha X^\alpha \in k[\mathbf{X}]$ no nulo, donde $a_\alpha \in k$.*

(1) Se define el exponente o multigrado de f para $\prec$, y se denota $\exp_\prec(f)$, como

$$exp_\prec(f) := \max \mathrm{sop}(f),$$

donde se toma máximo respecto de $\prec$.

(2) Se define el coeficiente líder de f con respecto a $\prec$ como

$$\mathrm{CL}_\prec(f) := a_{\exp_\prec(f)}.$$

Proposición 2.7 *(1) Sean $f, g \neq 0$. Entonces,*

$$\exp_{\prec}(f \cdot g) = \exp_{\prec}(f) + \exp_{\prec}(g).$$

(2) Sean $f, g \neq 0$ tales que $f + g \neq 0$. Entonces,

$$\exp_{\prec}(f + g) \leq \max(\exp_{\prec}(f), \exp_{\prec}(g)).$$

Si además $\exp\prec(f) \neq \exp_{\prec}(g)$*, entonces se tiene la igualdad.*

Demostración: Denotemos $\alpha_0 = \exp_{\prec}(f)$ y $\beta_0 = \exp_{\prec}(g)$.
(1) Veamos que

$$\alpha_0 + \beta_0 > \alpha + \beta$$

para cualesquiera $\alpha \in \text{sop}(f)$, $\beta \in \text{sop}(g)$ con $\alpha \neq \alpha_0$ ó $\beta \neq \beta_0$.
Si $\alpha \in \text{sop}(f)$ y $\alpha \neq \alpha_0$, tenemos que $\alpha < \alpha_0$. Por ser $\prec$ estable para la suma, $\alpha + \beta < \alpha_0 + \beta$ para todo $\beta \in \mathbb{N}^n$. Por tanto,

$$\alpha + \beta < \alpha_0 + \beta \leq \alpha_0 + \beta_0,$$

para cualesquiera $\beta \in sop(g)$. Análogamente se tiene el resultado en el otro caso.
De esta forma tenemos garantizado que en $f \cdot g$ aparece el monomio $X^{\alpha_0+\beta_0}$ ya que no puede cancelarse con ningún otro, y que es el mayor de todos los que aparecen. Por tanto, $\exp_{\prec}(f \cdot g) = \alpha_0 + \beta_0$.
(2) Podemos suponer que $\alpha_0 = \max(\alpha_0, \beta_0)$. Sólo en el caso, $\alpha_0 = \beta_0$ y $\text{CL}_{\prec}(f) + \text{CL}_{\prec}(g) = 0$ se tendrá $\exp_{\prec}(f + g) < \alpha_0$. En los demás casos se da la igualdad.

■

Teorema 2.8 *(*Teorema de división de Hironaka*) Consideremos un orden monomial $\prec$. Sean $f_1, \ldots, f_r \in k[X_1, \ldots, X_n] = k[\mathbf{X}]$ polinomios no nulos. Entonces, para cada $f \in k[\mathbf{X}]$ existen $q_1, \ldots, q_r, h \in k[\mathbf{X}]$ tales que*

$$f = q_1 f_1 + \cdots + q_r f_r + h,$$

y de modo que se verifica

$$\text{sop}(h) \subset \mathbb{N}^n \setminus \bigcup_{i=1}^{r} (\exp_{\prec}(f_i) + \mathbb{N}^n).$$

Es decir, o bien $h = 0$ o, en caso contrario, ningún monomio puede dividirse por ninguno de los $X^{\exp_{\prec}(f_i)}$, $i = 1, \ldots, r$.
Además, si $f \neq 0$ y $q_i f_i \neq 0$, entonces $\exp_{\prec}(f) \geq \exp_{\prec}(q_i f_i)$.

Demostración:
Si $f = 0$ basta tomar todos nulos. Si $f \neq 0$ sean $\exp_{\prec}(f) = \alpha$ y $\text{CL}_{\prec}(f) = a$. Denotemos también, $\exp_{\prec}(f_i) = \alpha_i$ y $\text{CL}_{\prec}(f_i) = a_i$.

Pueden darse dos casos:
Caso A: Si X^α no es divisible por ningún X^{α_i}, consideramos $g = f - aX^\alpha$.
Caso B: Si existe i, $1 \leq i \leq r$ tal que $X^{\alpha_i} | X^\alpha$, **fijamos un** i y consideramos $g = f - \frac{a}{a_i} X^{\alpha-\alpha_i} f_i$.
Si $g = 0$:
En el caso A, basta tomar $q_j = 0$ para cada j, y $h = aX^\alpha$.
En el caso B, basta tomar $q_j = 0$ para cada $j \neq i$, $q_i = \frac{a}{a_i} X^{\alpha-\alpha_i}$ y $h = 0$. Notar (2.7) que $\exp_\prec(f) = \exp_\prec(q_i f_i)$.
Si $g \neq 0$, tendremos que $\exp_\prec(g) < \exp_\prec(f)$. Por ser $\prec$ buen orden, podemos probar el resultado por inducción.
Si $\alpha = 0$ (primer elemento para el orden monomial) el resultado se tiene pues, en este caso, f sería una constante y $g = 0$.
Supongamos entonces el resultado cierto para todo $g' \in k[\mathbf{X}]$ con $\exp_\prec(g') < \exp_\prec(f)$. Se tendrá entonces que si $g \neq 0$, existen $q'_i \in k[\mathbf{X}]$ y $h' \in k[\mathbf{X}]$ tales que $g = q'_1 f_1 + \cdots + q'_r f_r + h'$ donde si $h' \neq 0$ sus monomios no son divisibles por ningún X^{α_j} y si $q'_j f_j \neq 0$ entonces $\exp_\prec(g) \geq \exp_\prec(q'_j f_j)$. Por tanto:
En el caso A: $f = g + aX^\alpha$, bastará tomar $q_j = q'_j$ para todo j, y $h = h' + aX^\alpha$.
En el caso B: $f = g + \frac{a}{a_i} X^{\alpha-\alpha_i} f_i$, bastará tomar $q_j = q'_j$ para todo $j \neq i$, $q_i = q'_i + \frac{a}{a_i} X^{\alpha-\alpha_i}$ y $h = h'$.

■

Definición 2.9 *Si la expresión*

$$f = q_1 f_1 + \cdots + q_r f_r + h,$$

verifica las condiciones del Teorema de división (2.8), diremos que es una división de f por $f_1, \ldots, f_r$. Además diremos que los polinomios q_i son cocientes y que h es resto de división de f por $f_1, \ldots, f_r$.

Nota 2.10 *La demostración del teorema es constructiva. Bastará calcular g a partir de f y razonar con g como con f en sucesivos pasos. Se construye en cada paso un polinomio g_i a partir de g_{i-1}, $g = g_1$, con $\exp_\prec(g_i) < \exp_\prec(g_{i-1})$. El número de pasos es finito porque el exponente decrece y el orden monomial es un buen orden.*
Si se determina de forma única cómo elegir el índice i en la demostración (ver Caso B), obtenemos un algoritmo de división *que, dado un polinomio f, devuelve unos polinomios q_i y un resto h determinados.*

Ejemplo 2.11 *Ni los cocientes ni el resto de división son únicos. Tomar por ejemplo, en $k[x, y]$ respecto del orden lexicográfico los polinomios $f_1 = x^3$, $f_2 = x^2 y - y^3$ y $f = x^3 y$. Se tiene que $f = y f_1 + 0 f_2 + 0$ y $f = 0 f_1 + x f_2 + x y^3$ verifican el Teorema de división.*

Nota 2.12 *Dada una división de f por $f_1, \ldots, f_r$,*

$$f = q_1 f_1 + \cdots + q_r f_r + h,$$

entonces existe un algoritmo de división concreto que nos da h como resto de división de f por $f_1, \ldots, f_r$.
En efecto, si $f = 0$ está claro que $h = 0$ y hemos acabado. Si $f \neq 0$, sean $\exp_\prec(f) = \alpha$ y $\mathrm{CL}_\prec(f) = a$. Denotemos también, $\exp_\prec(f_i) = \alpha_i$ y $\mathrm{CL}_\prec(f_i) = a_i$.
Si X^α no es divisible por ningún X^{α_i}, $\alpha \in \mathrm{sop}(h)$ y consideramos el polinomio $f' = f - aX^\alpha$. En otro caso, fijamos i, tal que $\alpha = \exp_\prec(q_i f_i)$ y consideramos el polinomio $f' = f - \frac{a}{a_i} X^{\alpha - \alpha_i}$. En ambos casos, f' se obtiene de f mediante un paso de la demostración para el i concreto elegido. Si $f' = 0$ hemos terminado. Si $f' \neq 0$, como $\exp_\prec(f') < \exp_\prec(f)$, sigue por inducción. En efecto, para $\alpha = 0$, $f \in k$. Si $f_i \notin k$ para todo i, serían $q_i = 0$ para cada i y $f = h$ se obtendría como resto de cualquier algoritmo de división. Si existe $f_i \in k$, sería $h = 0$ que se obtendría como resto de cualquier algoritmo de división. Supuesto cierto para polinomios de exponente menores que $\exp_\prec(f)$, para $f' \neq 0$ consideramos la expresión

$$f' = q'_1 f_1 + \cdots + q'_r f_r + h',$$

donde, en el primer caso, $h' = h - aX^\alpha$ y $q'_i = q_i$, para cada i; y en el segundo, para el i elegido, $q'_i = q_i - \frac{a}{a_i} X^{\alpha - \alpha_i}$, $q'j = q_j$ para todo $j \neq i$, y $h' = h$.
Por hipótesis de inducción, h' se obtiene como resto de un algoritmo de división de f' por $f_1, \ldots, f_r$. Basta ahora añadir el paso concreto de f a f', para obtener el algoritmo de división que buscamos.

En lo sucesivo, consideraremos **fijado un algoritmo de división**, de forma que cuando hagamos referencia al resto h, nos estaremos refiriendo a un resto concreto bien determinado. Usaremos la notación $h = fRf_1, \ldots f_r$, o también, $h = fRF$, donde $F = \{f_1, \ldots, f_r\}$. La nota anterior asegura que estaremos trabajando con cualquier resto.

Definición 2.13 *Sea $A \subset \mathbb{N}^n$, sea $\leq$ el orden parcial natural. Denotaremos*

$$\mathrm{Mnl}(A) := \{\alpha \in A \ \mid \ \alpha \text{ es minimal para } \leq \text{ en } A\ \}.$$

Si $1 \leq i \leq n$ y $t \in \mathbb{N}$, denotaremos $A(i,t) := \{\alpha \in A \ \mid \ \alpha_i = t\}$.

Lema 2.14 *Si $A \subset \mathbb{N}^n$, y $\alpha \in A$, entonces existe $\beta \in \mathrm{Mnl}(A)$ tal que $\beta \leq \alpha$.*

Demostración: Basta observar que el conjunto de elementos menores que α es finito. Concretamente,

$$\{\beta \in \mathbb{N}^n \ \mid \ \beta \leq \alpha\} = \{\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n \ \mid \ 0 \leq \beta_i \leq \alpha_i, \ \ 1 \leq i \leq n\}.$$

■

Proposición 2.15 *Si $\gamma \in A \subset \mathbb{N}^n$, entonces, $\mathrm{Mnl}(A) = \mathrm{Mnl}(F)$ con*

$$F = \{\gamma\} \cup \bigcup_{i=1}^{n} \bigcup_{t=0}^{\gamma_{i-1}} \mathrm{Mnl}(A(i,t)).$$

Demostración: Puesto que $F \subset A$ bastará probar que para cualquier elemento $\alpha \in A$, existe $\beta \in F$ tal que $\beta \leq \alpha$. Si $\alpha \geq \gamma$ se toma $\beta = \gamma$. Si $\alpha \not\geq \gamma$, existe i, $1 \leq i \leq n$, tal que $\alpha_i < \gamma_i$. Tenemos que $\alpha \in A(i, \alpha_i)$, $0 \leq \alpha_i \leq \gamma_i - 1$. Por el lema 2.14, existe $\beta \in \mathrm{Mnl}(A(i, \alpha_i))$, con $\beta \leq \alpha$. ■

Corolario 2.16 *(Lema de Dickson)* $\mathrm{Mnl}(A)$ *es finito para cualquiera* $A \subset \mathbb{N}^n$.

Demostración: Por inducción en n. Si $n = 1$, por el principio de buena ordenación de $\mathbb{N}$ tenemos que $\mathrm{Mnl}(A)$ es unitario si $A \neq \emptyset$. Supuesto cierto para $n-1$ lo probaremos para n. Bastará probar que en la proposición anterior F es finito. Podemos considerar $A(i,t)$ como un subconjunto de $\mathbb{N}^{n-1}$, y entonces, $\mathrm{Mnl}(A(i,t))$ es finito por la hipótesis de inducción. Por tanto, F es finito ya que se obtiene como un número finito de uniones de conjuntos finitos. ■

Nota 2.17 *El lema de Dickson puede considerarse como una generalización del principio de buena ordenación de* $\mathbb{N}$.

Definición 2.18 *Diremos que* $E \subseteq \mathbb{N}^n$ *es un ideal de* $\mathbb{N}^n$*, o escalera de* $\mathbb{N}^n$*, si se verifica que* $E + \mathbb{N}^n \subseteq E$.

Nota 2.19 *Sea* $E \subset \mathbb{N}^n$. *E es una escalera si y sólo si*

$$E = \bigcup_{\alpha \in \mathrm{Mnl}(E)} (\alpha + \mathbb{N}^n).$$

Definición 2.20 *Consideremos un orden monomial* $\prec$*, y sea un ideal no nulo* $I \subset k[X_1, \ldots, X_n]$. *La escalera de I respecto de* $\prec$*, es el subconjunto de* $\mathbb{N}^n$ *definido como:*

$$E_\prec(I) = \{\exp_\prec(f) | f \in I, f \neq 0\}$$

Nota 2.21 $E_\prec(I)$ *es una escalera de* $\mathbb{N}^n$. *Si no hay posibilidad de confusión la denotaremos* $E(I)$.

Definición 2.22 *Sea* $I \subset k[X_1, \ldots, X_n]$ *un ideal no nulo, y consideremos un orden monomial* $\prec$. *Una base de Gröbner de I respecto de* $\prec$*, es un conjunto de polinomios* $f_1, \ldots, f_r$ *tales que*

$$E(I) = \bigcup_{i=1}^{r} (\exp_\prec(f_i) + \mathbb{N}^n).$$

Equivalentemente, si

$$\mathrm{Mnl}(E(I)) \subset \{\exp_\prec(f_1), \ldots, \exp_\prec(f_r)\}.$$

Ejemplo 2.23 *(1) Sea $f \in k[X_1, \ldots, X_n]$ un polinomio no nulo. Entonces f es una base de Gröbner de $I = (f)$.*

(2) Sea $I \subset \mathbb{R}[X_1, X_2, X_3]$ el ideal generado por $f = X_1 + X_2 + X_1^2 X_2^3$ y $g = X_1 - X_2 + X_1^3 X_2^2$. Consideramos el orden monomial $<_{lex}$. Sea $h = X_1 f - X_2 g \in I$. Entonces $\exp_{<_{lex}}(h) \notin (\exp_{<_{lex}}(f) + \mathbb{N}^n) \cup (\exp_{<_{lex}}(g) + \mathbb{N}^n)$.
Por tanto f, g no es una base de Gröbner de I.

Proposición 2.24 *Sean $I \subset k[X_1, \ldots, X_n]$ un ideal no nulo, y $\prec$ un orden monomial. Sea $f_1, \ldots, f_r$ una base de Gröbner de I.*
Entonces, para todo $f \in k[X_1, \ldots, X_n]$, existe un único $h \in k[X_1, \ldots, X_n]$ tal que:
(1) $f = g + h$, con $g \in I$.
(2) $\mathrm{sop}(h) \subset \mathbb{N}^n \setminus E(I)$.
En particular, existe un único resto de la división de f por $f_1, \ldots, f_r$.

Demostración: Bastará tomar h resto de una división de f por $f_1, \ldots, f_r$, $f = q_1 f_1 + \cdots + q_r f_r + h$. Se tiene que $g = q_1 f_1 + \cdots + q_r f_r \in I$.
Para probar la unicidad, supongamos que $f = g' + h'$ verifican el resultado. Se tendrá $h - h' \in I$. Si $h \neq h'$, $\exp(h - h') \in E(I)$ en contra de (2). ■

Teorema 2.25 *Sean $I \subset k[X_1, \ldots, X_n]$ un ideal no nulo, y $\prec$ un orden monomial. Sea $G = \{f_1, \ldots, f_r\} \subset I$. Las siguientes condiciones son equivalentes:*
(1) G es base de Gröbner de I.
(2) Si $f \in k[\mathbf{X}]$, entonces $f \in I$ si y sólo si $0 = fRf_1, \ldots, f_r$.

Demostración: Supongamos que G es base de Gröbner. Si $f \in I$ y suponemos que $h = fRf_1, \ldots, f_r$, se tiene $h \in I$. Por tanto, $h = 0$ ya que $E(I) = \bigcup_{i=1}^r (\exp_\prec(f_i) + \mathbb{N}^n)$.
Por otro lado, supongamos que se verifica (2). Si G no fuera base de Gröbner, existiría $f \in I$ con $\exp_\prec(f) \notin \bigcup_{i=1}^r (\exp_\prec(f_i) + \mathbb{N}^n)$. Entonces, $h = fRG \neq 0$ en contra de (2). ■

Como consecuencia inmediata obtenemos el siguiente corolario.

Corolario 2.26 *Toda base de Gröbner de I es un sistema de generadores de I.*

Nota 2.27 *El teorema anterior proporciona un criterio para decidir si un polinomio f pertenece a un ideal I. De hecho, conocida una base de Gröbner del ideal, tenemos un criterio algorítmico para decidir si un polinomio pertenece o no al ideal. Por tanto, el problema de pertenencia a un ideal se reduce entonces al de cálculo de una base de Gröbner.*

Definición 2.28 *Sean $f, g \in k[X_1, \ldots, X_n]$ polinomios no nulos, y sea $\prec$ un orden monomial. Sean $\alpha = \exp_\prec(f) \in \mathbb{N}^n$, $\beta = \exp_\prec(g) \in \mathbb{N}^n$. Designemos por*

α_i a las coordenadas de α en $\mathbb{N}^n$, y por β_i a las coordenadas de β en $\mathbb{N}^n$. Sea $\gamma \in \mathbb{N}^n$ definido por $\gamma_i = \max\{\alpha_i, \beta_i\}$, es decir, $X^\gamma = m.c.m.(X^\alpha, X^\beta)$.
Entonces el S-polinomio de f y g se define como

$$S(f,g) = \frac{1}{\mathrm{CL}_\prec(f)}\mathbf{X}^{\gamma-\alpha}f - \frac{1}{\mathrm{CL}_\prec(g)}\mathbf{X}^{\gamma-\beta}g.$$

Teorema 2.29 *(Criterio de Buchberger) Sean $I = (f_1, \ldots, f_r) \subset k[X_1, \ldots, X_n]$ un ideal no nulo, y $\prec$ un orden monomial. Son equivalentes:*
(1) $f_1, \ldots, f_r$ es base de Gröbner de I.
(2) $S(f_i, f_j)Rf_1, \ldots, f_r = 0$, para todo i, j, con $1 \leq i < j \leq r$.

Demostración: Por ser $S(f_i, f_j) \in I$, (1) implica (2) por el teorema anterior (2.25). Recíprocamente, supongamos (2). Por el mismo teorema, bastará probar que si $f \in I$ entonces $0 = fRf_1, \ldots, f_r$.
Para ello vamos a definir la altura de una expresión $g_1f_1 + \cdots + g_rf_r$ como

$$alt(\sum_{i=1}^{r} g_if_i) = \max\{\exp_\prec(g_if_i) \ \mid \ g_if_i \neq 0\}.$$

Notar (2.7) que la altura de una suma es menor o igual que la suma de las alturas.
Sea $f \in I$ y sea $h = fRf_1, \ldots, f_r$. Se tiene $h \in I$. Si $h \neq 0$, tomamos $h = g_1f_1 + \cdots + g_rf_r$ con altura mínima posible β. Podemos suponer sin pérdida de generalidad $\beta = \exp_\prec(g_if_i)$ para todo $i = 1, \ldots, s$ y $\beta > \exp_\prec(g_if_i)$ si $i > s$ y $g_if_i \neq 0$.
Denotemos $\exp_\prec(f_i) = \alpha_i$, $\exp_\prec(g_i) = \beta_i$, $\mathrm{CL}_\prec(f_i) = a_i$ y $\mathrm{CL}_\prec(g_i) = b_i$, $1 \leq i \leq s$.
Por ser h resto de división, se tendrá:

$$(*) \ \ a_1b_1 + \cdots + a_sb_s = 0,$$

y en particular $s \geq 2$.
Escribimos $g_i = b_iX^{\beta_i} + g_i'$, para cada $i = 1, \ldots, s$.
Se tendrá

$$h = \sum_{i=1}^{s} b_iX^{\beta_i}f_i + \sum_{i=1}^{s} g_i'f_i + \sum_{i=s+1}^{r} g_if_i.$$

Está claro que $\sum_{i=1}^{s} g_i'f_i + \sum_{i=s+1}^{r} g_if_i$ tiene altura menor que β. Llegaremos a contradicción viendo que $(1) = \sum_{i=1}^{s} b_iX^{\beta_i}f_i$ puede escribirse como una expresión de altura menor que β.
Podemos escribir

$$(1) = a_1b_1(\frac{1}{a_1}\mathbf{X}^{\beta_1}f_1 - \frac{1}{a_2}\mathbf{X}^{\beta_2}f_2) + (a_1b_1 + a_2b_2)(\frac{1}{a_2}\mathbf{X}^{\beta_2}f_2 - \frac{1}{a_3}\mathbf{X}^{\beta_3}f_3) + \cdots +$$

$$(a_1b_1 + \cdots + a_{s-1}b_{s-1})(\frac{1}{a_{s-1}}\mathbf{X}^{\beta_{s-1}}f_{s-1} - \frac{1}{a_s}\mathbf{X}^{\beta_s}f_s) + (a_1b_1 + \cdots + a_sb_s)\frac{1}{a_s}\mathbf{X}^{\beta_s}f_s.$$

Observar que usando $(*)$ y la definición de los S-polinomios se tiene

$$(1) = \sum_{j=2}^{s} u_j S(f_{j-1}, f_j),$$

siendo $u_j = (a_1 b_1 + \cdots + a_{j-1} b_{j-1}) X^{\beta - \gamma_j}$, donde $X^{\gamma_j} = m.c.m.(X^{\alpha_{j-1}}, X^{\alpha_j})$.
Además, $(**) : \exp_\prec(u_j S(f_{j-1}, f_j)) < \beta$.
Por otra parte, al ser $S(f_{j-1}, f_j) R f_1, \ldots, f_r = 0$, tenemos que existen $q_{ji} \in k[\mathbf{X}]$ tales que $S(f_{j-1}, f_j) = \sum_{i=1}^{r} q_{ji} f_i$, y si $q_{ji} f_i \neq 0$,

$$(***) : \exp_\prec(q_{ji} f_i) \leq \exp_\prec(S(f_{j-1}, f_j)).$$

Por tanto,

$$(1) = \sum_{j=2}^{s} u_j (\sum_{i=1}^{r} q_{ji} f_i) = \sum_{i=1}^{r} (\sum_{j=2}^{s} u_j q_{ji}) f_i.$$

La última expresión tiene altura menor que β porque para cada i, $1 \leq i \leq r$, usando $(**)$ y $(***)$ se tiene que para cada j, $2 \leq j \leq s$,

$$\exp_\prec[(\sum_{j=2}^{s} u_j q_{ji}) f_i] \leq \exp_\prec(u_j q_{ji} f_i) \leq \exp_\prec(u_j S(f_{j-1}, f_j)) < \beta.$$

De esta forma hemos llegado a contradicción y el resultado está probado. ■

Nota 2.30 *Este criterio nos proporciona un algoritmo para la construcción de una base de Gröbner de un ideal a partir de un sistema de generadores del mismo. Concretamente, si suponemos que partimos de un sistema de generadores de I, $\{f_1, \ldots, f_r\}$, si se verifica la segunda condición del teorema tenemos que es base de Gröbner. Si no, elegimos i, j, $1 \leq i < j \leq r$ con $S(f_i, f_j) R f_1, \ldots, f_r = h \neq 0$. Llamamos $f_{r+1} = h$ y consideramos $\{f_1, \ldots, f_{r+1}\}$ como nuevo sistema generador de I. Si para él se verificase la segunda condición del teorema, habríamos acabado. En otro caso, construiríamos un nuevo polinomio f_{r+2} resto no nulo de un S-polinomio. Este proceso recurrente debe de acabar. En efecto, en otro caso, se tendría una sucesión infinita $\{f_i\}_{i \in \mathbb{N}}$ y consideraríamos el conjunto $A = \{\exp_\prec(f_i)\}_{i \in \mathbb{N}}$. Por el lema de Dickson (2.16),* $\mathrm{Mnl}(A)$ *es finito. Existiría entonces $s \in \mathbb{N}$ tal que*

$$\mathrm{Mnl}(A) \subset \{\exp_\prec(f_1), \ldots, \exp_\prec(f_s)\}.$$

Ahora bien esto contradice que,

$$\exp_\prec(f_{s+1}) \notin \bigcup_{i=1}^{s} (\exp_\prec(f_i) + \mathbb{N}^n),$$

pues $f_{s+1} = S(f_i, f_j) R f_1, \ldots, f_s$ para algún (i, j) con $1 \leq i < j \leq s$.

Ejemplo 2.31 *Una base de Gröbner de* $I = (X^3, X^2Y - Y^3) \in k[X, Y]$ *respecto del orden lexicográfico es* $\{f_1, f_2, f_3, f_4\}$*, donde* $f_1 = X^3$*,* $f_2 = X^2Y - Y^3$*,* $f_3 = XY^3$ *y* $f_4 = Y^5$*.*
También lo sería $\{f_1 + af_3, f_2, f_3, f_4\}$*, para cualquier* $a \in k$*.*

Definición 2.32 *Sean* $I \subset k[X_1, \ldots, X_n]$ *un ideal no nulo, y* $\prec$ *un orden monomial. Sea* $f_1, \ldots, f_r$ *una base de Gröbner de* I*. Diremos que es una base de Gröbner minimal si*

$$\mathrm{Mnl}(E(I)) = \{\exp_\prec(f_1), \ldots, \exp_\prec(f_r)\}.$$

Definición 2.33 *Sean* $I \subset k[X_1, \ldots, X_n]$ *un ideal no nulo, y* $\prec$ *un orden monomial.*
Diremos que $f_1, \ldots, f_r$ *es una base de Gröbner reducida de* I *respecto de* $\prec$ *si:*
(1) Es una base de Gröbner minimal de I*.*
(2) Los polinomios f_i *son mónicos.*
(3)

$$\mathrm{sop}(f_i) \subset \mathbb{N}^n \setminus \bigcup_{\substack{j=1,\ldots,r \\ j \neq i}} (\exp_\prec(f_j) + \mathbb{N}^n).$$

Nota 2.34 *La condición (3) implica la (1), e incluso que* $\sharp\mathrm{Mnl}(E(I)) = r$*.*

Proposición 2.35 *Sean* $I \subset k[X_1, \ldots, X_n]$ *un ideal no nulo, y* $\prec$ *un orden monomial.*
La base de Gröbner reducida de I *respecto de* $\prec$ *existe y es única.*

Demostración: Sea $\{f_1, \ldots, f_r\}$ una base de Gröbner de un ideal I respecto de un orden monomial fijado. Podemos suponer sin pérdida de generalidad que es minimal y que $\sharp\mathrm{Mnl}(E(I)) = r$. En otro caso, bastaría tomar por cada elemento minimal un elemento de la base que lo tenga por exponente y obtendríamos una nueva base de Gröbner de I.
Sea $f_1' = f_1 R f_2, \ldots, f_r$. Se tiene que $f_1' \in I$, $\exp_\prec(f_1) = \exp_\prec(f_1')$ y

$$\mathrm{sop}(f_1') \subset \mathbb{N}^n \setminus \bigcup_{j=2,\ldots,r} (\exp_\prec(f_j) + \mathbb{N}^n).$$

El conjunto $\{f_1', f_2, \ldots, f_r\}$ es una nueva base de Gröbner minimal de I.
Para $i \geq 2$, supuesto construidos $f_1', \ldots, f_{i-1}'$, bastará tomar

$$f_i' = f_i R f_1', \ldots, f_{i-1}', f_{i+1}, \ldots, f_r.$$

Se tendrá que $\{f_1', \ldots, f_r'\}$ es una base de Gröbner reducida de I sin más que hacerlos mónicos dividiendo por los coeficientes líderes.
Para ver la unicidad, supongamos que $\{f_1, \ldots, f_r\}$ y $\{f_1', \ldots, f_r'\}$ sean dos bases de Gröbner reducidas de I respecto del orden. Podemos suponer sin pérdida de generalidad que $\exp_\prec(f_i) = \exp_\prec(f_i')$ para todo i, pues bastaría reordenar en caso necesario.

Veamos que $f_1 = f_1'$. Análogamente se tendría para otro i. Si suponemos que $f_1 \neq f_1'$, $\alpha = \exp_\prec(f_1 - f_1') \in E(I)$. Además $\alpha < \exp_\prec(f_1)$ porque f_1 y f_1' son mónicos. El orden monomial refina al orden parcial natural (2.4), luego $\alpha \notin \exp_\prec(f_1) + \mathbb{N}^n$. Por la condición (3) de ser reducida, tenemos que $\alpha \notin \bigcup_{j=2,\ldots,r}(\exp_\prec(f_j) + \mathbb{N}^n)$. Luego llegamos a contradicción con que $E(I) = \bigcup_{j=1,\ldots,r}(\exp_\prec(f_j) + \mathbb{N}^n)$. ■

Nota 2.36 *La demostración anterior es constructiva. Por tanto, usando 2.30 existen algoritmos de cálculo de la base de Gröbner reducida a partir de un sistema de generadores.*

Ejemplo 2.37 *Sean $f_1 = X + Y + Z$, $f_2 = X - 3Y$, $I = (f_1, f_2) \subset k[X, Y, Z]$. Respecto del orden lexicográfico, 2.30 nos asegura que $\{f_1, f_2, f_3\}$ es una base de Gröbner de I, siendo $f_3 = 4Y + Z = S(f_1, f_2)Rf_1, f_2$. Una base minimal es $\{f_1, f_3\}$. La reducimos sustituyendo f_1 por $f_1' = X + \frac{3}{4}Z = f_1 R f_3$. Haciendo mónicos los polinomios, obtenemos la base de Gröbner reducida de I*

$$\{X + \frac{3}{4}Z, Y + \frac{1}{4}Z\}.$$

Nota 2.38 *La base de Gröbner reducida depende del orden monomial fijado.*

Ejemplo 2.39 *Sea $I = (X^3 - 2XY, X^2Y - 2Y^2 + X) \subset k[X, Y]$. La base de Gröbner reducida de I respecto de grlex es*

$$\{X^2, XY, Y^2 - \frac{1}{2}X\}.$$

Respecto de lex, la base de Gröbner reducida de I es

$$\{X - 2Y^2, Y^3\}.$$

Los diferentes sistemas de cálculo formal, fijado un orden monomial, calculan la base reducida a partir de un sistema generador.

Corolario 2.40 *Dados dos ideales no nulos de $k[X_1, \ldots, X_n]$, $I = (f_1, \ldots, f_r)$, $J = (g_1, \ldots, g_s)$, y fijado un orden monomial, $I = J$ si y sólo si las bases de Gröbner reducidas de I y de J coinciden.*

Demostración: Se deduce de la unicidad de la base de Gröbner reducida (2.35). ■

3 Teorema de los ceros de Hilbert

[2]

Sean k un cuerpo, y $k[\mathbf{X}] = k[X_1, \ldots, X_n]$ el anillo de polinomios en n indeterminadas con coeficientes en k. $\mathbb{A}^n(k) = \mathbb{A}^n$ representa k^n con la estructura de espacio afín.

3.1 Teorema de los ceros (Nullstellensatz) de Hilbert

En esta sección demostraremos el teorema de los ceros de Hilbert en sus distintas versiones (teorema débil y teorema fuerte) y veremos sus consecuencias. Usaremos el siguiente resultado algebraico de Zariski que demostraremos en la sección siguiente.

Lema 3.1 *(*Lema de Zariski*) Sea k algebraicamente cerrado subcuerpo de un cuerpo $L = k[\alpha_1, \ldots, \alpha_r]$. Entonces, $k = L$.*

Nota 3.2 *Sea A un anillo. Si $\alpha_1, \ldots, \alpha_r \notin A$, $A[\alpha_1, \ldots, \alpha_r]$ es el menor anillo que contiene a A y a los α_i. A este tipo de anillos los llamaremos A-álgebras finitamente generadas.*

Teorema 3.3 *(*Teorema débil*) Sea k algebraicamente cerrado. Si I es un ideal de $k[\mathbf{X}]$, $I \neq (1)$, entonces $\mathcal{V}(I) \neq \emptyset$.*

Demostración: Podemos suponer que I es maximal, pues si no lo fuera, existiría J maximal con $I \subset J$, y por tanto, $\mathcal{V}(J) \subset \mathcal{V}(I)$.
Sea $L = k[\mathbf{X}]/I$. Por I maximal, L es un cuerpo. Además, $L = k[\alpha_1, \ldots, \alpha_n]$ siendo $\alpha_i = X_i + I$, para todo $i = 1, \ldots, n$. Por el lema de Zariski, $k = L$. Por tanto, para cada i, existe $a_i \in k$ tal que $a_i + I = X_i + I$. Es decir, $X_i - a_i \in I$. Así el ideal $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ está contenido en I. Por ser tanto $\mathfrak{m}$ como I ideales maximales se tiene $\mathfrak{m} = I$. De aquí, $\mathcal{V}(I) = \{P\}$, donde $P = (a_1, \ldots, a_n)$. ■

Corolario 3.4 *Sea k algebraicamente cerrado y sea I un ideal de $k[\mathbf{X}]$. Fijado un orden monomial, las siguientes condiciones son equivalentes:*

1. *$\mathcal{V}(I) = \emptyset$.*
2. *$I = (1)$.*
3. *La base de Gröbner reducida de I es $\{1\}$.*

[2] Estas notas han sido elaboradas con la colaboración de Belén Medrano y Beatriz Rodríguez, alumnas internas del Departamento de Álgebra (curso 2002-03).

Demostración: $1 \iff 2$ es consecuencia inmediata del Teorema débil (3.3). $2 \iff 3$ por la unicidad de la base de Gröbner reducida (2.35). ■

Teorema 3.5 *(*Teorema fuerte*) Sea k algebraicamente cerrado y sea I un ideal de $k[\mathbf{X}]$. Se verifica que*

$$\mathcal{IV}(I) = \sqrt{I}.$$

Demostración:
Sabemos que $\mathcal{I}(\mathcal{V}(I))$ es siempre un ideal radical y que se verifica $I \subset \mathcal{I}(\mathcal{V}(I))$, entonces

$$\sqrt{I} \subset \sqrt{\mathcal{I}(\mathcal{V}(I))} = \mathcal{I}(\mathcal{V}(I)).$$

Veamos la contención contraria. (La prueba que damos se conoce con el nombre de truco de Ravinobitsch.)

Sea $g \in \mathcal{I}(\mathcal{V}(I))$. Consideramos X_{n+1} una nueva variable y el siguiente ideal de $k[X_1, \ldots, X_n, X_{n+1}]$

$$J = I^e + (1 - gX_{n+1}).$$

Es decir, si suponemos $I = (f_1, \ldots, f_r)$, se tendrá que

$$J = (f_1, \ldots, f_r, 1 - gX_{n+1}).$$

Veamos que $\mathcal{V}(J) = \emptyset$.
Si $P = (a_1, \ldots, a_{n+1}) \in \mathcal{V}(J)$, $f_i(a_1, \ldots, a_n) = 0$ para cada $i = 1, \ldots, n$, y $1 = g(a_1, \ldots, a_n)a_{n+1}$. Por tanto, $(a_1, \ldots, a_n) \in \mathcal{V}(I)$, luego $g(a_1, \ldots, a_n) = 0$ lo que es una contradicción porque entonces $1 = 0$.
Por el Teorema débil tendremos que $J = (1)$. Entonces, se puede escribir:

$$1 = \sum_{i=1}^{n} h_i(X_1, \ldots, X_n, X_{n+1}) f_i + h_{n+1}(X_1, \cdots, X_n, X_{n+1})(1 - gX_{n+1}),$$

con $h_i \in k[X_1, \ldots, X_n, X_{n+1}]$, para todo $i = 1, \ldots, n+1$. Haciendo $X_{n+1} = 1/Y$ en la relación anterior y quitando denominadores, obtenemos $s \in \mathbb{N}$ tal que

$$Y^s = \sum_{i=1}^{n} h_i'(X_1, \ldots, X_n, Y) f_i + h_{n+1}'(X_1, \cdots, X_n, Y)(Y - g).$$

Haciendo $Y = g$,

$$g^s = \sum_{i=1}^{n} h_i''(X_1, \ldots, X_n) f_i$$

lo que prueba que $g \in \sqrt{I}$.

■

Corolario 3.6 *Sea k algebraicamente cerrado y sea I un ideal radical de $k[\mathbf{X}]$. Se verifica que $\mathcal{IV}(I) = I$. En particular, las correspondencias $\mathcal{V}$ y $\mathcal{I}$ entre los ideales radicales de $k[\mathbf{X}]$ y los conjuntos algebraicos de $\mathbb{A}^n(k)$ son una la inversa de la otra.*

Demostración: Siempre se tiene que $\mathcal{VI} = \mathrm{id}$. Basta probar que $\mathcal{IV} = \mathrm{id}$. Ahora bien, por ser k algebraicamente cerrado, $\mathcal{IV}(I) = \sqrt{I} = I$ por ser I radical. ■

Corolario 3.7 *Sea k algebraicamente cerrado. Existe una correspondencia uno a uno entre los ideales primos de $k[\mathbf{X}]$ y los conjuntos algebraicos irreducibles no vacíos. A los ideales maximales les corresponden los puntos. En particular,*

$$Spec_m(k[\mathbf{X}]) = \{(X_1 - a_1, \ldots, X_n - a_n) \mid a_i \in k, \quad 1 \leq i \leq n\}.$$

Demostración: Sabemos que en cualquier cuerpo se tiene que un conjunto algebraico no vacío V es irreducible si y sólo si $\mathcal{I}(V)$ es un ideal primo.
Veamos el recíproco. Sea $\mathfrak{p}$ un ideal primo de $k[\mathbf{X}]$, por tanto radical. Por ser k algebraicamente cerrado, se tiene por 3.3 que $\mathcal{V}(\mathfrak{p}) \neq \emptyset$ pues $\mathfrak{p} \neq (1)$, y por 3.5 que

$$\mathcal{IV}(\mathfrak{p}) = \sqrt{\mathfrak{p}} = \mathfrak{p}.$$

Luego, $\mathcal{V}(\mathfrak{p})$ es irreducible.
Para un punto $P = (a_1, \ldots, a_n)$ siempre se verifica

$$\mathcal{I}(P) = (X_1 - a_1, \ldots, X_n - a_n),$$

que es un ideal maximal. Por ser k algebraicamente cerrado, en la demostración del Teorema débil (3.3) vimos que los ideales maximales son todos de este tipo, luego se tiene que la correspondencia es uno a uno. ■

Nota 3.8 *Sea $f \in k[\mathbf{X}]$ no nulo y no unidad, es decir, f no constante. Sea $f = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ la descomposición factorial de f. El polinomio reducido de f es $f_{red} = f_1 \cdots f_r$.*

Corolario 3.9 *Sean k algebraicamente cerrado, $f \in k[\mathbf{X}]$ no constante, $f = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ la descomposición factorial de f. Entonces,*

$$\mathcal{V}(f) = \mathcal{V}(f_1) \cup \cdots \cup \mathcal{V}(f_r)$$

es la descomposición en componentes irreducibles de $\mathcal{V}(f)$ y $\mathcal{IV}(f) = (f_{red})$. Además, existe una correspondencia uno a uno entre las hipersuperficies irreducibles y los polinomios irreducibles.

Demostración: Se verifica siempre que

$$\mathcal{V}(f) = \mathcal{V}(f_1^{\alpha_1}) \cup \cdots \cup \mathcal{V}(f_r^{\alpha_r}).$$

Basta ahora sustituir $\mathcal{V}(f_i^{\alpha_i}) = \mathcal{V}(f_i)$ para cada i. Además, (f_i) es un ideal primo, ya que f_i es irreducible y $k[\mathbf{X}]$ DFU.
Por ser k algebraicamente cerrado, se tiene que $\mathcal{V}(f_i)$ es irreducible. Además, si $i \neq j$, $(f_i) \neq (f_j)$, se tiene $\mathcal{V}(f_i) \neq \mathcal{V}(f_j)$ y no existe relación de inclusión entre ellos. Por tanto, son las componentes irreducibles.
Por otra parte, se tiene que $\sqrt{(f)} = (f_{red})$. Luego, en el caso k algebraicamente cerrado, $\mathcal{IV}(f) = (f_{red})$.
Ahora la correspondencia uno a uno es evidente, ya que una hipersuperficie es $\mathcal{V}(f)$ con f no constante. ■

Corolario 3.10 *Sea k algebraicamente cerrado y sea I un ideal de $k[\mathbf{X}]$. Entonces, $\mathcal{V}(I)$ es finito si y sólo si la dimensión como k espacio vectorial de $k[\mathbf{X}]/I$ es finita. Además,*

$$\sharp\mathcal{V}(I) \leq dim_k(k[\mathbf{X}]/I).$$

Demostración: Supongamos que $\dim_k(k[\mathbf{X}]/I)$ sea finita. Sean $P_1, \ldots, P_r \in \mathcal{V}(I)$ puntos distintos.
Veamos que para cada $i = 1, \ldots, r$, existen polinomios $f_i \in k[\mathbf{X}]$ tales que $f_i(P_i) = 1$ y $f_i(P_j) = 0$ si $i \neq j$. Construimos explícitamente f_1 y análogamente se tendrá para los demás.
Por ser $P_1 = (a_{11}, \ldots, a_{1n})$ y $P_2 = (a_{21}, \ldots, a_{2n})$ distintos, existe i, $1 \leq i \leq n$ tal que $a_{1i} \neq a_{2i}$. Sea $g_2 = \frac{X_i - a_{2i}}{a_{1i} - a_{2i}}$. Se verifica que $g_2(P_1) = 1$ y $g_2(P_2) = 0$. Análogamente, para cada $j = 3, \ldots, r$ se construye un polinomio g_j tal que $g_j(P_1) = 1$ y $g_j(P_j) = 0$. Basta ahora tomar, $f_1 = g_2 g_3 \ldots g_r$.
Entonces, se tiene que $f_i + I = \overline{f}_i$ son polinomios linealmente independientes sobre k, $i = 1, \ldots, r$. En efecto, si $\sum_{i=1}^r \lambda_i \overline{f}_i$, con $\lambda_i \in k$, el polinomio $\sum_{i=1}^r \lambda_i f_i \in I$, luego $(\sum_{i=1}^r \lambda_i f_i)(P_j) = \lambda_j$, para todo $j = 1, \ldots, r$. Por tanto se tiene que $\sharp\mathcal{V}(I) \leq \dim_k(k[\mathbf{X}]/I)$.
Recíprocamente, supongamos $\mathcal{V}(I)$ finito. Observar que en general, $k[\mathbf{X}]/I$ está generado por los monomios $X_1^{\alpha_1} \cdots X_n^{\alpha_n} + I$, con $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Probaremos que basta con un número finito de éstos.
Si $\mathcal{V}(I) = \emptyset$, como k es algebraicamente cerrado (3.3), $I = (1)$ y $k[\mathbf{X}]/I = 0$. Luego se tendría el resultado trivialmente.
Si $\mathcal{V}(I) = \{P_1, \ldots, P_r\}$, supongamos $P_i = (a_{i1}, \ldots, a_{in})$, $i = 1, \ldots, r$. Consideramos el polinomio $f_j = \Pi_{i=1}^r (X_j - a_{ij}) \in k[X_j]$ de grado r y mónico, para cada $j = 1, \ldots, n$. Por ser k algebraicamente cerrado y $f_j(P_i) = 0$ para cada $i = 1, \ldots, r$, se tiene que $f_j \in \mathcal{IV}(I) = \sqrt{I}$. Luego existen, $s_j \in \mathbb{N}$, tal que $f_j^{s_j} \in I$, para cada $j = 1, \ldots, n$. Tomando s el máximo de los s_j, $f_j^s \in I$ para cada j. Por tanto, si $\overline{X}_j = X_j + I$, se tiene que $\overline{X}_j^{rs}$ es combinación lineal en k de $1, \overline{X}_j, \ldots, \overline{X}_j^{rs-1}$, para cada $j = 1, \ldots, n$. Luego el conjunto

$$\{\overline{X}_1^{\alpha_1} \cdots \overline{X}_n^{\alpha_n} \mid 0 \leq \alpha_i \leq rs - 1\},$$

genera $k[\mathbf{X}]/I$ como k-espacio vectorial.

■

Proposición 3.11 *Fijamos un orden monomial en $k[\mathbf{X}]$ y sea I un ideal de $k[\mathbf{X}]$. Entonces, $\{\mathbf{X}^\alpha + I \mid \alpha \notin E(I)\}$ es un base de $k[\mathbf{X}]/I$ como k-espacio vectorial.*

Demostración: Supongamos $f_1, \ldots, f_r$ una base de Gröbner de I. Dado $f \in k[\mathbf{X}]$, lo dividimos por la base anterior y obtenemos

$$f = q_1 f_1 + \cdots + q_r f_r + h,$$

con $h = \sum_{\alpha \notin E(I)} a_\alpha \mathbf{X}^\alpha$. Como $f + I = h + I$, tenemos probado que el conjunto genera.
Para ver la independencia lineal, supongamos $\{\alpha_1, \ldots, \alpha_s\} \subset \mathbb{N}^n - E(I)$ y

$$\sum_{i=1}^{s} a_i \mathbf{X}^{\alpha_i} \in I, \quad a_i \in k, \quad i = 1, \ldots, s.$$

Al tomar resto de la división por la base de Gröbner obtenemos

$$(\sum_{i=1}^{s} a_i \mathbf{X}^{\alpha_i}) R f_1, \ldots, f_r = \sum_{i=1}^{s} a_i \mathbf{X}^{\alpha_i},$$

que debe ser 0 por estar el elemento en I. Como el resto es único para una base de Gröbner (2.24), $a_i = 0$ para cada $i = 1, \ldots, s$.

■

Como corolario inmediato se tiene el siguiente criterio de finitud de un conjunto algebraico.

Corolario 3.12 *Sea k algebraicamente cerrado y sea I un ideal de $k[\mathbf{X}]$. Fijado un orden monomial en $k[\mathbf{X}]$, $\mathcal{V}(I)$ es finito si y sólo si $\mathbb{N}^n - E(I)$ es finito. Equivalentemente, si G es una base de Gröbner de I, entonces, para cada i, $1 \leq i \leq n$, existe $m_i \geq 0$ tal que $X_i^{m_i}$ es el exponente de algún $g \in G$.*

3.2 Resultado de Zariski

Para la demostración del resultado de Zariski 3.1 necesitamos los siguientes lemas.

Lema 3.13 *Si k es un cuerpo y X una indeterminada, en $k[X]$ existen infinitos polinomios irreducible no asociados*

Demostración: Supongamos que sólo existieran un número finito de tales polinomios, $h_1, \ldots, h_s$. Entonces, el polinomio $h_{s+1} = h_1 \ldots h_s + 1$ no sería divisible por ningún irreducible, lo que contradice que $k[X]$ es DFU. ■

Definición 3.14 *Sea A subanillo de un anillo B. Se dice que $b \in B$ es entero sobre A si existen $a_i \in A$, $1 \leq i \leq m$ tales que*

$$(*) \quad b^m + a_1 b^{m-1} + \cdots + a_m = 0.$$

Es decir, b verifica un polinomio mónico con coeficientes en A.

Nota 3.15 *A $(*)$ la llamaremos una ecuación de dependencia entera de b sobre A.*

Lema 3.16 *Sea A subanillo de un anillo B, entonces*

$$C = \{\alpha \in B \ \mid \ \alpha \text{ es entero sobre } A\}$$

es un anillo. Además, $A \subset C \subset B$.

Demostración: Que $A \subset C \subset B$, se tiene pues cualquier elemento $a \in A$ verifica el polinomio $X - a$.
Sean $\alpha, \beta \in C$. Para probar que C es anillo, bastará ver que $\alpha - \beta \in C$ y que $\alpha\beta \in C$. Consideramos la A-álgebra finitamente generada $R = A[\alpha, \beta]$. Supongamos que

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, \quad a_i \in A, \quad 1 \leq i \leq m,$$

$$\beta^l + b_1\beta^{l-1} + \cdots + b_l = 0, \quad b_i \in A, \quad 1 \leq i \leq l,$$

son ecuaciones de dependencia entera. Estas ecuaciones aseguran que los elementos de R son combinación lineal en A de los elementos $\alpha^i\beta^j$, $0 \leq i \leq m-1$, $0 \leq j \leq l-1$. Denotamos $e_i \in R$ a éstos elementos, es decir

$$\{e_i \ \mid \ 1 \leq i \leq r\} = \{\alpha^i\beta^j \ \mid \ 0 \leq i \leq m-1, \quad 0 \leq j \leq l-1\}.$$

Definimos el endomorfismo de grupos $\varphi : R \longrightarrow R$, $\varphi(\gamma) = (\alpha - \beta)\gamma$. Se tendrá que $\varphi(e_i) = \sum_{j=1}^{r} a_{ij}e_j$, donde $a_{ij} \in A$, $1 \leq i, j \leq r$.
Expresando matricialmente las relaciones anteriores obtenemos lo siguiente:

$$[(\alpha - \beta)I - (a_{ij})] \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Llamamos M a la matriz $[(\alpha - \beta)I - (a_{ij})]$ y mutiplicamos ambos miembros de la igualdad anterior por la matriz adjunta de M traspuesta. Como se verifica que $adj(M)^t M = \det(M)I$, tenemos:

$$\det(M)I \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

De esto se deduce que $\det(M)e_i = 0$, para todo i. Entonces $\det(M)c = 0$ para todo $c \in R$. En particular $1 \in R$, con lo cual $\det(M) = 0$. Pero $\det(M)$ nos proporciona un polinomio mónico con coeficientes en A que es verificado por $\alpha - \beta$. Por tanto $\alpha - \beta$ es entero sobre A.
Para probar $\alpha\beta \in C$, se razona análogamente con el endomorfismo de R consistente en multiplicar por $\alpha\beta$.

■

Lema 3.17 *Sea A un DFU y sea K su cuerpo de fracciones. Si $\alpha \in K$ es entero sobre A, entonces $\alpha \in A$.*

Demostración: Sea $a/b \in K$ con m.c.d.$(a,b) = 1$ un elemento entero sobre A. Entonces, a/b verifica una ecuación de dependencia entera de la forma:

$$0 = \left(\frac{a}{b}\right)^m + a_1\left(\frac{a}{b}\right)^{m-1} + \ldots + a_{m-1}\left(\frac{a}{b}\right) + a_m, \quad a_i \in A,\, i = 1, \ldots, m.$$

Multiplicando la ecuación anterior por b^m, obtenemos lo siguiente:

$$0 = a^m + a_1 b a^{m-1} + \ldots + a_{m-1} b^{m-1} a + a_m b^m.$$

Luego: $-a^m = b(a_1 a^{m-1} + \ldots + a_{m-1} b^{m-2} a + a_m b^{n-1})$.
Podemos considerar esta igualdad en A, con lo que $b \mid a^m$. Por tanto, todos los factores irreducibles de b lo son de a. Como m.c.d.$(a,b) = 1$, se verifica que b debe ser unidad, lo cual prueba que $a/b \in A$. ■

Definición 3.18 *Sea A un dominio de integridad, y sea $K = Q(A)$ su cuerpo de fracciones. Se dice que A es* íntegramente cerrado *si $\alpha \in K$ entero sobre A, implica que $\alpha \in A$.*

Nota 3.19 *Sea $k \subset K$ una extensión de cuerpos y sea $\alpha \in K$:*

1. *Si α es algebraico sobre k, entonces $k[\alpha] = k(\alpha)$.*
2. *Si α no es algebraico, o sea, es trascendente sobre k, entonces $k[\alpha] \simeq k[X]$.*

En efecto, el homomorfismo de anillos sobreyectivo $\varphi : k[X] \longrightarrow k[\alpha]$ tal que $\varphi(X) = \alpha$, nos da el isomorfismo

$$k[X]/ker(\varphi) \simeq k[\alpha].$$

Si α es algebraico, $ker(\varphi) = (f)$ donde f es el polinomio mínimo de α que es irreducible. Por tanto, el ideal (f) es maximal y $k[\alpha]$ es un cuerpo.
Si α es trascendente, $ker(\varphi) = (0)$ y $k[X] \simeq k[\alpha]$.

Proposición 3.20 *Sea k un cuerpo,y $L \supset k$ una k-álgebra finitamente generada por $\alpha_1, \ldots, \alpha_r$ (i.e. $L = k[\alpha_1, \ldots, \alpha_r]$). Si L es un cuerpo, entonces α_i es algebraico sobre k, para todo $i = 1, \ldots, r$.*

Demostración: Bastará probar que la extensión $k \subset L = k[\alpha_1, \ldots, \alpha_r]$ es algebraica. Lo haremos por inducción en r.
El caso r=1 es trivial, ya que si α_1 fuese transcendente sobre k, $k[\alpha_1]$ sería un anillo de polinomios en una variable con lo cual no podría ser un cuerpo.

Supongamos, pues, el resultado cierto para r-1,y veámoslo para el caso r. Como L es cuerpo, debe verificarse $k(\alpha_1) \subset L$, por tanto $L = k(\alpha_1)[\alpha_2, \ldots, \alpha_r]$ es un cuerpo. Por hipótesis de inducción, tenemos que α_i es algebraico sobre $k(\alpha_1)$, para todo $i = 2, \ldots, r$.

Así, la extensión $k(\alpha_1) \subset k(\alpha_1)[\alpha_2, \ldots, \alpha_r]$ es algebraica. Luego basta probar que α_1 es algebraico sobre k por la transitividad de las extensiones algebraicas. Razonando por reducción al absurdo, supongamos que α_1 es trascendente sobre k. Se tendrá por (3.19) que $k[\alpha_1] \simeq k[X]$ que es íntegramente cerrado (lema 3.17).
Por ser $\alpha_2, \ldots, \alpha_r$ algebraicos sobre $k(\alpha_1)$. Se verificará

$$0 = {\alpha_i}^{m_i} + a_{i1}{\alpha_i}^{m_i-1} + \ldots + a_{im_i-1}\alpha_i + a_{im_i},$$

donde $a_{ij} \in k(\alpha_1)$, $1 \leq j \leq m_i$, para cierto $m_i \in \mathbb{N}$, $i = 2, \ldots, r$. Tomamos un denominador común de todos los a_{ij}. Es decir $a \in k[\alpha_1]$, tal que $aa_{ij} \in k[\alpha_1]$ para todo (i, j). Multiplicando la expresión anterior por a^{m_i}, obtenemos:

$$0 = (a\alpha_i)^{m_i} + aa_{i1}(a\alpha_1)^{m_i-1} + \ldots + a^{m_i-1}a_{im_i-1}(a\alpha_i) + a^{m_i}a_{im_i}.$$

Luego, hemos obtenido una ecuación de dependencia entera sobre $k[\alpha_1]$ para $a\alpha_i$, $i = 2, \ldots, r$.
Dado $z \in L = k[\alpha_1, \ldots, \alpha_r]$,

$$z = \sum_{d \in \mathbb{N}^r} b_d \alpha_1^{d_1} \cdots \alpha_r^{d_r},$$

donde $d = (d_1, \ldots, d_r) \in \mathbb{N}^r$, y $b_d \in k$ es nulo salvo para un número finito de elementos d. Tomando $N \in \mathbb{N}$ suficientemente grande obtenemos

$$a^N z = \sum_{d \in \mathbb{N}^r} b_d a^{N(d)} \alpha_1^{d_1} (a\alpha_2)^{d_2} \cdots (a\alpha_r)^{d_r}, \quad \text{con} \quad N(d) \in \mathbb{N}.$$

Por tanto, $a^N z$ será entero sobre $k[\alpha_1]$ por constituir los elementos enteros un anillo (lema 3.16).
Como $k(\alpha_1) \subset L$, la propiedad anterior se verificará en particular para los elementos de $k(\alpha_1)$. Así, si $z \in k(\alpha_1)$ entonces $a^N z \in k(\alpha_1)$ es entero sobre $k[\alpha_1]$ para cierto $N \in \mathbb{N}$. Como $Q(k[\alpha_1]) = k(\alpha_1)$ y $k[\alpha_1]$ es íntegramente cerrado, debe ser $a^N z \in k[\alpha_1]$. Basta tomar $z = \frac{1}{c}$ con c que no divida a a para llegar a contradicción. (Existe c por el lema 3.13.) ■

Como corolario inmediato se tiene el resultado de Zariski 3.1.

4 Módulos sobre un anillo. Operaciones. Hom(M,N).

Este tema se corresponde con las 6 primeras secciones del Capítulo 2 del libro Atiyah, M.F., Macdonald, I.G., "Introducción al Álgebra conmutativa". Ed. Reverté, Barcelona, 1989.

5 Aplicaciones multilineales. Producto tensorial de módulos. Álgebras.

Este tema se corresponde con las 5 últimas secciones del Capítulo 2 del libro Atiyah, M.F., Macdonald, I.G., "Introducción al Álgebra conmutativa". Ed. Reverté, Barcelona, 1989.

6 Teorema de estructura de los módulos finitamente generados sobre un D.I.P.. Aplicaciones: ecuaciones lineales con coeficientes enteros, formas canónicas de Jordan.

6.1 Teorema de estructura de los módulos finitamente generados sobre un D.I.P.

En lo que sigue A denotará un dominio de ideales principales y K su cuerpo de fracciones.

Lema 6.1 *Sean $v_1, \ldots, v_m \in A^n$. Entonces los v_i son A-linealmente independientes (en A^n) si y sólo si son K-linealmente independientes en K^n.*[3]

Definición 6.2 *Dado un subconjunto cualquiera no vacío $S \subset A^n$, definimos el* rango *de S, que notaremos $\mathrm{rg}(S)$, como el número máximo de elementos de S que sean A-linealmente independientes, que por el lema anterior, coincide con el número máximo de elementos de S que sean K-linealmente independientes en K^n, o lo que es lo mismo, con $\dim_K L_K(S)$, donde $L_K(S)$ denota el subespacio vectorial de K^n generado por S.*

Lema 6.3

1. *Si $S \subset A^n$, entonces $\mathrm{rg}(S) \leq n$.*
2. *Si $M \subset A^n$ es un submódulo, entonces los elementos de $L_K(M)$ son de la forma $a^{-1}m$, con $a \in A, a \neq 0$ y $m \in M$.*
3. *Si $S = A^n$, entonces $\mathrm{rg}(A^n) = n$.*
4. *Si $M_1, M_2 \subset A^n$ son dos submódulos tales que $M_1 \cap M_2 = 0$, entonces $\mathrm{rg}(M_1 \oplus M_2) = \mathrm{rg}(M_1) + \mathrm{rg}(M_2)$.*

Nota 6.4 *Un módulo M finitamente generado sobre un anillo A es* libre *si posee una base $\{m_1, \ldots, m_r\}$, es decir, un sistema de generadores que es linealmente independiente. Además, dos bases cualesquiera de M tienen el mismo número de elementos.*

Proposición 6.5 *Sea M un módulo libre de rango $n \geq 1$ y sea $M' \subset M$. Entonces, M' es libre y tiene una base de $q \leq n$ elementos .*

Demostración: Ver
Jacobson, N., "Basic Algebra I". Second edition. W. H. Freeman and Company, New York, 1985. ■

[3] Este resultado es válido siempre que A sea un dominio de integridad.

Ejemplo 6.6 *El teorema anterior no es cierto si A no es un D.I.P.. En tal caso existirá un ideal $I \subset A$ no principal, por lo que I no podrá tener una base con un solo elemento. Tampoco podrá tener una base con dos o más elementos, pues dos elementos no nulos de un anillo siempre son linealmente dependientes.*

Teorema 6.7 *Sea Q una matriz $m \times n$ con coeficientes en A. Entonces existen unas matrices P y R de orden $m \times m$ y $n \times n$ respectivamente, con coeficientes en A e inversibles (i.e.* $\det(P)$ *y* $\det(R)$ *son unidades de A) tales que*

$$PQR = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_q & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

donde $q = \operatorname{rg}(Q)$ y $a_1|a_2|\cdots|a_q, a_i \in A - \{0\}$.
Además, se tiene lo siguiente:
Si denotamos por Δ_i el máximo común divisor de los menores $i \times i$ no nulos de Q, con $i = 1, \ldots, q$, se tiene:

$$a_1 = \Delta_1, \quad a_i = \frac{\Delta_i}{\Delta_{i-1}}, \quad i = 2, \ldots, q.$$

Demostración: Ver
Jacobson, N., "Basic Algebra I". Second edition. W. H. Freeman and Company, New York, 1985. ■

Definición 6.8 *Se llama forma normal canónica de Smith de la matriz Q a la matriz PQR del teorema anterior. (Está definida unívocamente salvo asociados de los a_i)*
A los elementos no nulos de su diagonal se les llama factores invariantes de la matriz Q. (Están definidos unívocamente salvo asociados)

Nota 6.9 *Las matrices P y R (no son únicas en general), pueden obtenerse como producto de ciertas matrices elementales. Concretamente:*
Si A es un dominio euclídeo, basta con los siguientes tipos de matrices:

1. *Si $b \in A$, $T_{ij}(b)$, $i \neq j$, es la matriz cuadrada que tiene en la diagonal todos unos, y en el resto ceros salvo en el lugar (i, j) que aparece b.*

2. *Sea $u \in A$ una unidad, $D_i(u)$ es la matriz diagonal con todos sus elementos no nulos unos, salvo en el lugar (i,i) que aparece u.*

3. *Sea P_{ij}, $i \neq j$, la matriz cuadrada en cuya diagonal aparecen todos unos salvo en los lugares (i, i) y (j, j) que hay ceros, y en el resto ceros salvo en los lugares (i, j) y (j, i) que aparecen unos.*

Si A es un dominio de ideales principales que no sea dominio euclídeo, además de los tipos anteriores, hay que añadir matrices cuadradas de la forma

$$\begin{pmatrix} x & s & 0 & \cdots & 0 \\ y & t & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \text{ donde } \begin{pmatrix} x & s \\ y & t \end{pmatrix} \text{ es una matriz inversible .}$$

Teorema 6.10 *Sea M un módulo libre de rango $n \geq 1$ y sea $M' \subset M$ un submódulo de rango $q \geq 0$. Entonces, existe una base $\{e_1, \ldots, e_n\}$ de M y unos elementos $a_1, \ldots, a_q \in A - \{0\}$ tales que:*

1. *$\{a_1e_1, a_2e_2, \ldots, a_qe_q\}$ es una base de M',*
2. *$a_1|a_2|\cdots|a_q$.*

Demostración: Sea $\{f_1, \ldots, f_q\}$ una base de M' y sea $\{e_1, \ldots, e_n\}$ una base de M. Se tendrá que

$$f_i = \sum_{j=1}^{n} a_{ij}e_j, \text{ con } a_{ij} \in A,$$

para cada $i = 1, \ldots, q$. Sea $Q = (a_{ij})$ matriz $q \times n$. Por el Teorema 6.7, existen P y R inversibles tales que

$$PQR = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_q & 0 & \cdots & 0 \end{pmatrix}$$

Sean $f'_l = \sum_{i=1}^{q} p_{lj}f_j$, para cada $l = 1, \ldots, q$, siendo $P = (p_{lj})$. Se tiene que $f'_1, \ldots, f'_q$ es otra base de M', por ser P inversible.
Si $R^{-1} = (r'_{ij})$, sea $e'_i = \sum_{j=1}^{n} r'_{ij}e_j$, para cada $i = 1, \ldots, n$. El conjunto $\{e'_1, \ldots, e'_n\}$ es otra base de M.
Basta ahora observar que $f'_i = a_ie'_i$, para cada $i = 1, \ldots, q$.

■

Corolario 6.11 *Si E es un A-módulo finitamente generado no nulo, entonces existen unos ideales $\mathfrak{a}_m \subset \mathfrak{a}_{m-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1 \subset A$, con $\mathfrak{a}_1 \neq A$, tales que:*

$$E \simeq (A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_m)\,.$$

Demostración: Como E es un módulo finitamente generado, se puede expresar como cociente de un módulo libre A^n por un cierto submódulo M'. Aplicando el teorema anterior, si ninguno de los a_i es unidad, basta tomar $\mathfrak{a}_i = Aa_i$, $i = 1, \ldots, q$ y $\mathfrak{a}_i = 0$ para $q < i \leq n$. En caso contrario, procederíamos a quedarnos sólo con los $\mathfrak{a}_i = Aa_i$ tales que a_i no sea unidad.

■

Definición 6.12 *Dado un A-módulo M, diremos que un elemento $x \in M$ es un* elemento de torsión *si existe un $a \in A, a \neq 0$ tal que $ax = 0$.*
Diremos que M es un módulo de torsión *si todos sus elementos son elementos de torsión.*

Lema 6.13 *Dado un A-módulo M, el conjunto de sus elementos de torsión $\mathrm{Tor}(M)$ es un submódulo de M.*

Corolario 6.14 *Todo A-módulo finitamente generado es suma directa de su módulo de torsión $\mathrm{Tor}(M)$ y de un módulo libre de rango finito, cuyo rango está determinado unívocamente por M. En particular todo A-módulo finitamente generado sin torsión es libre.*

Corolario 6.15 *Dado un A-módulo M finitamente generado existen un entero $d \geq 0$, unos ideales primos $\mathfrak{p}_i \subset A$ no nulos y unos enteros $s_i \geq 1$, $i = 1, \ldots, r$, tales que:*

$$M \simeq (A/\mathfrak{p}_1^{s_1}) \times \cdots \times (A/\mathfrak{p}_r^{s_r}) \times A^d.$$

Además, el isomorfismo anterior establece otro isomorfismo:

$$\mathrm{Tor}(M) \simeq (A/\mathfrak{p}_1^{s_1}) \times \cdots \times (A/\mathfrak{p}_r^{s_r}).$$

Demostración: Basta tener en cuenta que si $\mathfrak{a}$ es un ideal propio de A, de que A sea un DIP deducimos la existencia de unos ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ y unos enteros $e_1, \ldots, e_m \geq 1$ (todos ellos únicos) tales que

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}.$$

■

Definición 6.16 *Sea $p \in A$ un primo y M un A-módulo. Llamaremos p-componente de M a*

$$M_p := \{y \in M \mid p^k y = 0 \text{ para algún } k \in \mathbb{N}\}.$$

Nota 6.17 *$M_p \subset M$ es un submódulo. Además, si $p_1, \ldots, p_r$ son primos distintos, es decir, no asociados,*

$$M_{p_1} \cap (M_{p_2} + \cdots + M_{p_r}) = (0).$$

En efecto, si $y_1 \in M_{p_1} \cap (M_{p_2} + \cdots + M_{p_r})$, $y_1 = y_2 + \cdots + y_r$, con $y_i \in M_{p_i}$. Existen $k_i \in \mathbb{N}$, $1 \leq i \leq r$, tales que $p_i^{k_i} y_i = 0$. Así, $p_1^{k_1}$ y $p_2^{k_2} \cdots p_r^{k_r} \in Ann(y_1)$. Por la identidad de Bezout, $1 = m.c.d.(p_1^{k_1}, p_2^{k_2} \cdots p_r^{k_r}) \in Ann(y_1)$. Luego se tiene que $y_1 = 0$.

Teorema 6.18 *Sea M un A-módulo de torsión finitamente generado. Entonces, la p-componente de M es nula salvo para un número finito de primos p: $p_1, \ldots, p_r$. Además, $M = M_{p_1} \oplus \cdots \oplus M_{p_r}$.*

Demostración: Sean $x_1, \ldots, x_s$, generadores de M. Sean $p_1, \ldots, p_r$ todos los primos que aparecen en la descomposición factorial de los d_i, $\mathrm{Ann}(x_i) = (d_i)$, $1 \leq i \leq s$. Entonces, $Ax_i \subset M_{p_1} + \cdots + M_{p_r}$. En efecto, si $d_i = p_1^{k_1} \cdots p_r^{k_r}$, por ser $1 = \text{m.c.d.}(p_1^{k_1}, p_2^{k_2} \cdots p_r^{k_r})$ la identidad de Bezout asegura que existen α y $\beta \in A$, tales que $1 = \alpha p_1^{k_1} + \beta p_2^{k_2} \cdots p_r^{k_r}$. Entonces, $x_i = x_i \alpha p_1^{k_1} + x_i \beta p_2^{k_2} \cdots p_r^{k_r}$. Al ser $x_i \beta p_2^{k_2} \cdots p_r^{k_r} \in M_{p_1}$, bastará probar que $x_i \alpha p_1^{k_1} \in M_{p_2} + \cdots + M_{p_r}$. Pero esto sigue por inducción, ya que $\mathrm{Ann}(x_i \alpha p_1^{k_1}) = (p_2^{k_2} \cdots p_r^{k_r})$.
Se tiene entonces que $M = M_{p_1} + \cdots + M_{p_r}$. Además, por ser los primos p_i distintos, la suma es directa (Nota 6.17).
Si p es un primo distinto de los p_i, $M_p \subset M_{p_1} + \cdots + M_{p_r}$, luego (Nota 6.17)

$$M_p = M_p \cap (M_{p_1} + \cdots + M_{p_r}) = 0.$$

■

Teorema 6.19 Teorema de estructura de módulos finitamente generados sobre un D.I.P. *Sea M un A-módulo finitamente generado no nulo, A un dominio de ideales principales. Entonces, existen unos ideales únicos $\mathfrak{a}_m \subset \mathfrak{a}_{m-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1 \subset A$, con $\mathfrak{a}_1 \neq A$, tales que*

$$M \simeq A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_m.$$

Demostración: La existencia está probada en Corolario 6.11. Veamos la unicidad. Supongamos

$$M \simeq A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_m \simeq A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_r,$$

con $\mathfrak{a}_m \subset \mathfrak{a}_{m-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1 \subset A$, $\mathfrak{b}_r \subset \mathfrak{b}_{r-1} \subset \cdots \subset \mathfrak{b}_2 \subset \mathfrak{b}_1 \subset A$, $\mathfrak{a}_1 \neq A$ y $\mathfrak{b}_1 \neq A$.
Sean s y t, $1 \leq s \leq m$, $1 \leq t \leq r$, tales que $0 = \mathfrak{a}_m = \mathfrak{a}_{m-1} = \cdots = \mathfrak{a}_{s-1} = \mathfrak{b}_r = \mathfrak{b}_{r-1} = \cdots = \mathfrak{b}_{t-1}$, $\mathfrak{a}_i \neq 0$, para todo $i \leq s$, $\mathfrak{b}_i \neq 0$, para todo $i \leq t$.
Tendremos que

$$M \simeq A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_s \times A^{m-s} \simeq A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_t \times A^{r-t}.$$

Así,

$$\mathrm{Tor}(M) \simeq A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_s \simeq A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_t,$$

y $M/\mathrm{Tor}(M) \simeq A^{m-s} \simeq A^{r-t}$. Por estar el rango de un módulo unívocamente determinado $m - s = r - t$. Luego, $m = r \iff s = t$.
Podemos reducirnos a probar el teorema en el caso en que M sea un módulo de torsión. En este caso, podemos considerar los ideales $\mathfrak{a}_i$ y $\mathfrak{b}_i$ de la forma (p^e), con p primo y $e \in \mathbb{N}$ (Corolario 6.15).
Por tanto, fijando el primo p, la p-componente de M, M_p, se obtendrá tomando la suma directa de todos los sumandos correspondientes a ideales de la forma (p^e). Esta debe coincidir en ambas descomposiciones. Por tanto, podemos reducirnos al caso en que $M = M_p$.

Supongamos entonces

$$M \simeq A/(p^{e_1}) \times \cdots \times A/(p^{e_s}) \simeq A/(p^{f_1}) \times \cdots \times A/(p^{f_t}),$$

con $e_1 \leq \cdots \leq e_s$, y $f_1 \leq \cdots \leq f_t$.
Tenemos que probar que $s = t$ y $e_i = f_i$ para todo $i = 1, \ldots, s$. Sea $k \in \mathbb{N}$. Se tiene que $p^k M = \{p^k x \mid x \in M\}$ es un submódulo. Se verifica:

$$p^k M \subset \cdots \subset p^2 M \subset pM \subset M.$$

Sea $M^{(k)} = p^k M/p^{k+1}M$. $M^{(k)}$ es un A-módulo y un $A/(p)$-módulo porque $\mathrm{Ann}(M^{(k)}) = (p)$. Por ser (p) un ideal maximal de A, $\overline{A} = A/(p)$ es un cuerpo. Así, $M^{(k)}$ es un $\overline{A}$-espacio vectorial.
Si $k \geq e_s$ se tiene que $p^k M = 0$. En otro caso,

$$p^k M = p^k A/(p^{e_{l+1}}) \times \cdots \times p^k A/(p^{e_s}),$$

siendo $e_l \leq k < e_{l+1}$.
El A-módulo $p^k M$ está generado por

$$\begin{aligned} F_1 &= (p^k + (p^{e_{l+1}}), 0, \ldots, 0) \\ &\vdots \\ F_{s-l} &= (0, \ldots, 0, p^k + (p^{e_s})). \end{aligned}$$

Las clases de los F_i generan $M^{(k)}$ como $\overline{A}$-espacio vectorial. Para ver que forman base, bastará ver que son no nulos. Si $F_i \in p^{k+1}M = p(p^k M)$, $F_i = p\sum_{j=1}^{s-l} a_j F_j$, con $a_j \in A$. Por tanto, $p^k + (p^{e_{l+i}}) = a_i p^{k+1} + (p^{e_{l+i}})$. Es decir, $p^k(1 - a_i p) \in (p^{e_{l+i}})$. Como p no divide a $1 - a_i p$, tiene que ser $k \geq e_{l+i}$ lo que es una contradicción.
Es decir, la dimensión como espacio vectorial de $M^{(k)}$ coincide con el número de e_i tales que $k < e_i$. Análogamente, será el número de f_i tales que $k < f_i$.
Tomando $k < \min(e_1, f_1)$, tendremos que $\dim(M^{(k)}) = s = t$.
Si suponemos que $e_1 \neq f_1$, y por ejemplo $e_1 < f_1$, tomando $k = e_1 < f_1$, tendríamos que $\dim(M^{(k)}) = s - 1 = s$, lo cual es imposible. Por tanto, $e_1 = f_1$.
De forma análoga se deduce que $e_i = f_i$ para cada i. ■

Definición 6.20 *Los ideales* $\mathfrak{a}_m \subset \mathfrak{a}_{m-1} \subset \cdots \subset \mathfrak{a}_2 \subset \mathfrak{a}_1$ *se denominan* factores invariantes *del módulo* M.

6.2 Aplicaciones

6.2.1 Formas canónicas de Jordan

En lo que sigue k será un cuerpo y V un k-espacio vectorial de dimensión finita $d \geq 1$. Dado un endomorfismo $f : V \to V$, podemos definir una estructura de $k[X]$-módulo sobre V de la siguiente forma:

$$(\sum_{i=0}^{m} a_i X^i) \cdot v := \sum_{i=0}^{m} a_i f^i(v)$$

para todo polinomio $\sum_{i=0}^{m} a_i X^i \in k[X]$ y todo $v \in V$.

Lema 6.21 *El $k[X]$-módulo V anterior es f.g. y de torsión.*

Demostración: Es claro que todo sistema (finito) de generadores de V como espacio vectorial también es un sistema de generadores de V como $k[X]$-módulo. Para ver que V es un $k[X]$-módulo de torsión, tomemos un $v \in V$ cualquiera y consideremos la familia de elementos de V siguiente:

$$v, f(v), f^2(v), f^3(v), \ldots$$

Como V es de dimensión finita, la familia anterior ha de ser linealmente dependiente, de donde deducimos la existencia de un polinomio no nulo $p(X) \in k[X]$ tal que $p(X) \cdot v = 0$. ■

Consideremos una base $\mathcal{B} = \{u_1, \ldots, u_d\}$ de V (como k-espacio vectorial) y la aplicación $k[X]$-lineal $\pi : k[X]^d \to V$ dada por:

$$\pi(p_1, \ldots, p_d) = \sum_{i=1}^{d} p_i u_i,$$

que es sobreyectiva.

Proposición 6.22 *En la situación anterior, sea $M = (a_{ij})$ la matriz de f respecto de $\mathcal{B}$, i.e. $f(u_i) = \sum_{j=1}^{d} a_{ij} u_j$. Entonces las filas de la matriz*

$$XI - M = \begin{pmatrix} X - a_{11} & -a_{12} & \ldots & -a_{1d} \\ -a_{21} & X - a_{22} & \cdots & -a_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{d1} & -a_{d2} & \ldots & X - a_{dd} \end{pmatrix}$$

forman un sistema de generadores (y de hecho una base) de $\ker \pi$.

Lema 6.23 *Dado $\lambda \in k$, el $k[X]$-módulo $k[X]/((X-\lambda)^n)$ admite una base como k-espacio vectorial $\mathcal{B} = \{e_1, \ldots, e_n\}$ tal que*

$$X \cdot e_1 = \lambda e_1 + e_2, \ldots, X \cdot e_{n-1} = \lambda e_{n-1} + e_n, X \cdot e_n = \lambda e_n,$$

o lo que es lo mismo, la forma matricial de la multiplicación por X respecto de la base $\mathcal{B}$ es

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & \ldots & 0 & 0 \\ 0 & 0 & \lambda & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & \lambda \end{pmatrix}.$$

Nota 6.24 *El teorema de estructura del $k[X]$-módulo V ($k[X]$ es un D.I.P.) (teoremas 6.10, 6.7, corolario 6.15) junto con la proposición 6.22 y el lema 6.23 nos permiten dar una nueva demostración del Teorema de Jordan en el caso de que k sea algebraicamente cerrado, o si se quiere, en el caso en que todos los autovalores de f estén en k. Es más, el teorema 6.7 nos proporciona un método de cálculo de la forma de Jordan.*
En el caso $k = \mathbb{R}$ también podemos obtener una demostración de la existencia de la forma canónica real, así como un método de cálculo.

6.2.2 Ecuaciones lineales con coeficientes enteros

Sea A un dominio de ideales principales. (En particular, para $A = \mathbb{Z}$)

Teorema 6.25 *La condición necesaria y suficiente para que un sistema de ecuaciones lineales con coeficientes en A tenga solución, es que el rango de la matriz ampliada coincida con el rango de la matriz de los coeficientes, y el máximo común divisor de los menores no nulos de orden igual al rango coincida en ambas.*

Nota 6.26 *El cálculo de matrices P y R asociadas a la matriz Q del sistema (Nota 6.9) nos proporciona un método para resolver el sistema.*