PROYECTO DE INNOVACIÓN DOCENTE COMPUTA.CONM: Talleres Computacionales de Álgebra Conmutativa

Memoria Final

Ana Cristina López Martín
Esteban Gómez González
José Ignacio Iglesias Curto
Daniel Hernández Serrano
Darío Sánchez Gómez

24 de junio de 2011

Índice general

El proyecto COMPUTA.CONM: *Talleres Computacionales de Álgebra Conmutativa* se ha desarrollado con normalidad en el ámbito de actuación de las asignaturas “Álgebra Conmutativa y Computacional” y “Ampliación de Álgebra Conmutativa”del tercer curso del Grado en Matemáticas. Ya que este curso académico ha sido el primero en el cual se han impartido tales asignaturas, dentro del actual plan de estudios de Grado, la experiencia recogida durante la ejecución de este proyecto debe ayudar al equipo docente implicado en su ejecución a mejorar, tanto el desarrollo de las mismas como a proponer propuestas de cambio en su programación de manera que los contenidos, competencias y habilidades sean más realistas y se garantice su consecución.

El desarrollo y ejecución del proyecto se ha articulado sobre tres ejes de actuación que enunciamos ahora y analizaremos a continuación:

- Diseño y organización de actividades prácticas para las asignaturas “Álgebra Conmutativa y Computacional” y “Ámpliación de Álgebra Conmutativa”del tercer curso del Grado en Matemáticas, utilizando paquetes de cálculo específicos con el software de álgebra computacional MATHEMATICA.

- Desarrollo de talleres prácticos para ambas asignaturas donde los estudiantes han realizado prácticas diseñadas bajo la supervisión de un tutor.

- Desarrollo de sistemas de auto-evaluación on-line a través de la plataforma STUDIUM que han servido para verificar la adquisición de algunas de las competencias.

Capítulo 1

Diseño y organización de actividades prácticas

El primer elemento en el que se ha articulado este proyecto de innovación docente ha sido el diseño de material y la organización necesaria para realizar actividades formativas de carácter práctico que contribuyan a la adquisición de las competencias propias de las asignaturas incluidas en el ámbito de actuación del mismo. Los aspectos computacionales de las materias han requerido la utilización de paquetes de cálculo específicos con software de álgebra computacional.

Concretamente la actuación por parte de los docentes del equipo ha consistido en la recopilación del material disponible así como el diseño del nuevo material necesario para la realización de prácticas de ordenador con el programa de álgebra computacional MATHEMATICA, con el fin de que contribuyeran a la adquisición de las siguientes competencias asociadas al módulo de Ampliación de Álgebra del actual plan de estudio de Grado, dentro del cual se encuentran las dos asignaturas de actuación de este proyecto:

1. Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en Matemáticas y resolver problemas (Competencia CE-2 según la memoria de enseñanzas de Grado en Matemáticas de la USAL).

2. Desarrollar programas que resuelvan problemas metemáticos utilizando en cada caso un entorno computacional adecuado (Competencia CE-

3 según la memoria de enseñanzas de Grado en Matemáticas de la USAL).

Inicialmente se consideró la posibilidad de diseñar estas prácticas usando diferentes software. Tras la reunión inicial mantenida por los miembros del equipo docente se acordó usar el programa MATHEMATICA ya que la mayor parte de los estudiantes están familiarizados con él.

Además de la elaboración de tales prácticas se ha confeccionado una serie de tests con el propósito de que sirvieran, tanto a los estudiantes para el autocontrol de su proceso de aprendizaje como a los docentes a modo de prototipo de evaluación.

Para poner a disposición de los estudiantes los tests de autocontrol, así como las prácticas desarrolladas se utilizó la plataforma STUDIUM.

1.1. Puntos fuertes

- Los programas informáticos de álgebra computacional permiten elaborar una gran variedad de material docente.
- Uso de la plataforma STUDIUM como canal óptimo de comunicación con los estudiantes, tanto para facilitarles material docente como para resolución de dudas y consultas.

1.2. Puntos débiles

- Necesidad de valorar la utilización de otros programas existentes.
- Pocas referencias bibliográficas a disposición del profesorado.
- Poca disponibilidad de horas para desarrollar las clases prácticas.

1.3. Material didáctico

Se adjuntan los siguientes documentos:

1. Material docente elaborado por los miembros del equipo con los contenidos tericos necesarios para el seguimiento de los talleres prácticos.
2. Modelo de práctica diseada para el programa MATHEMATICA.

Capítulo 2

Desarrollo de talleres prácticos

El segundo eje de actuación ha sido el desarrollo de las actividades mencionadas en el capítulo anterior.

Dicha actividad se ha llevado a cabo a través de la puesta en marcha de talleres prácticos tutelados en el aula de informática del Departamento de Matemáticas. En estos talleres los estudiantes se dedicaron a la realización de las prácticas diseñadas, una vez que los correspondientes contenidos teóricos eran conocidos, bajo la supervisión de uno de los docentes del equipo.

Teniendo en cuenta los horarios aprobados por la Comisión de Docencia de la Facultad de Ciencias para el curso 2010-2011, y después de acordarlo con los estudiantes, estas actividades se realizaron en sesiones semanales de dos horas durante el mes de Diciembre (en el caso de Álgebra Conmutativa y Computacional) y Abril (en el caso de Ampliación de Álgebra Conmutativa).

2.1. Puntos fuertes

- Los estudiantes mostraron un alto índice de participación en el desarrollo de las prácticas.
- Se complementan los ejercicios desarrollados en clase con los realizados en estas sesiones.
- La flexibilidad y rápidez de cálculo que supone el uso de programas informáticos permite a los estudiantes disponer de un mayor número

de ejercicios resueltos.

- El uso de software permite visualizar ciertos conceptos geométricos de una forma limpia, cómoda e interactiva.
- Las actividades realizadas en estas sesiones se complementan también con los tests realizados a través de la plataforma STUDIUM.

2.2. Puntos débiles

- Reacciones adversas por parte de algunos estudiantes al hecho de que la asistencia a las prácticas les supone una carga extra lectiva.
- Dificultad a la hora de desarrollar las sesiones de manera dinámica e interactiva debido a las carencias de algunos estudiantes en el manejo del programa informático.
- Reacciones adversas al hecho de tener que saber manejar un determinado programa de álgebra computacional.
- Poca bibliografía disponible para los estudiantes.

2.3. Material didáctico

Se adjuntan los siguientes documentos:

1. Modelo ejercicio realizado por los estudiantes en los talleres prácticos desarrollados.

Capítulo 3

Desarrollo de sistemas de auto-evaluación

Por último se han revisado los sistemas de auto-evaluación y diseñado sistemas de calificación de las actividades formativas de carácter práctico anteriormente referidas.

Para la ejecución de este objetivo se ha utilizado en algunos casos los test de autocontrol que estaban a disposición de los estudiantes vía on-line a través de la plataforma STUDIUM. No obstante, la falta de tiempo del profesorado participante en este proyecto ha impedido el trasaldo de todo el material diseado a la plataforma STUDIUM, por ello algunos de los test planteados a los estudiantes ha modo de autocontrol ha tenido que ser realizados bajo el sistema tradicional, que aunque sea muy válido, deja fuera posibilidades de las nuevas tecnologías.

3.1. Puntos fuertes

- La realización de los tests de autocontrol ayuda al estudiante a tener un ritmo de trabajo más constante.
- La realización de los tests de manera autónoma e independiente muestra al estudiante un dato real de su comprensión de la asignatura.
- La corrección instantánea de los tests permite al estudiante conocer en

el acto su nivel de conocimiento de la asignatura.

- El diseño de los sistemas de evaluación de tipo test supone un beneficio también para el docente al servirle como protocolo de evaluación.

3.2. Puntos débiles

- La falta de recursos humanos ha imposibilitado el que todos los test se puedan realizar a traves de la plataforma STUDIUM.
- El carácter no presencial dificulta conocer hasta qué punto el estudiante ha adquirido las competencias.
- La baja repercusión de estas actividades en la evaluación final hace que algunos estudiantes pierdan el interés.

3.3. Material didáctico

Se adjuntan los siguientes documentos:

1. Modelo de test de autocontrol realizado via STUDIUM.
2. Modelo de test realizado por los alumnos bajo del sistema tradicional en la asignatura de Álgebra conmutativa y computacional.
3. Modelo de test realizado por los alumnos bajo del sistema tradicional en la asignatura de Ampliación de Álgebra conmutativa.

Capítulo 4

Anexos

Material docente para talleres prácticos.

Modelo de práctica.

Modelo ejercicio.

Modelos de test.

1. BASES DE GROEBNER: MOTIVACIÓN Y PRIMERAS APLICACIONES

Estas notas se corresponden aproximadamente con los contenidos del capítulo 1 de [CLO2].

1.1. Operaciones con los ideales de un anillo de polinomios y su significado geométrico

Vamos a trabajar en el anillo de polinomios $A = \mathbf{k}[X_1, \ldots, X_n]$ con coeficientes en un cuerpo $\mathbf{k}$, que podemos identificar (con propiedad, cuando $\mathbf{k}$ sea infinito) con la funciones polinómicas en $\mathbf{A}^n_k$. Los polinomios de A definen *variedades algebraicas* en $\mathbf{A}^n_k$. Una variedad algebraica X es el lugar de ceros común de un conjunto G de polinomios; al lugar de ceros de G lo denotamos $V(G)$. La variedad X es también el lugar de ceros $V(I)$ de los polinomios del ideal I que genera G. Como A es *noetheriano* (por el teorema de la base de Hilbert; véanse [CLO1, Teoremas 2.4.5 y 2.5.4] o [R, Teorema 3.6]), sus ideales y en particular I están generados por un conjunto finito de elementos, por tanto toda variedad algebraica está definida por un número finito de ecuaciones polinómicas. Por tanto interesa estudiar los ideales de A porque sus lugares de ceros son las variedades algebraicas. Por otra parte, si X es una variedad algebraica (o, en general, un subconjunto) de $\mathbf{A}^n_k$, los polinomios que se anulan en todos los puntos de X forman un ideal, $I(X)$, al que llameremos el *ideal de la variedad* X.

Introduciremos las bases de Groebner en primer lugar como un método para realizar operaciones "sencillas" con ideales de $A = \mathbf{k}[X_1, \ldots, X_n]$. Estas operaciones tienen una traducción o una interpretación geométrica. Como ya hemos comentado los ideales de a están finitamente generados y por lo tanto un ideal lo exhibimos dando un conjunto finito de generadores. Ésta es una lista de cuestiones y operaciones que queremos ser capaces de resolver:

(1) Decidir si un polinomio pertenece a un ideal I (*ideal membership*).
(2) Decidir cuándo dos ideales son iguales.
(3) Calcular sumas de ideales (trivial).
(4) Calcular productos de ideales (trivial).
(5) Calcular intersecciones de ideales.
(6) Calcular cocientes de ideales, i.e., dados ideales I y J, calcular $I : J$.
(7) Eliminar variables.

De los conceptos anteriores todos son conocidos para quien posea unas nociones básicas sobre anillos excepto quizá el concepto de cociente de dos ideales y el de eliminación:

Definición 1.1. *Sean I y J ideales de A. Entonces $I : J = \{f \in A : fg \in I$ para todo $g \in J\}$.*

Ejercicio 1.2. *Demuestra que si I y J son ideales de A, $I : J$ es ideal de A.*

Definición 1.3. *Sea I un ideal de $A = \mathbf{k}[X_1, \dots, X_n]$. El ideal de eliminación l–ésimo de I es $I_l = I \cap \mathbf{k}[X_{l+1}, \dots, X_n]$.*

Ejercicio 1.4. *Demuestra que si I es un ideal de A, entonces $I \cap \mathbf{k}[X_{l+1}, \dots, X_n]$ es un ideal de $\mathbf{k}[X_{l+1}, \dots, X_n]$ (es decir, ideal de eliminación l–ésimo de I es en efecto un ideal).*

Daremos una interpretación geométrica de lo que quieren decir todas estas operaciones:

(1) Pertenencia de un polinomio a un ideal: Si I es el ideal de una variedad algebraica X, decidir si $f \in I$ es decidir si f se anula en todos los puntos de X. Por ejemplo, si tenemos una curva C en $\mathbf{A}^3_{\mathbf{C}}$ dada como el lugar de ceros $V(f_1, \dots, f_n)$, $f_1, \dots, f_n \in \mathbf{C}[X, Y, Z]$ y queremos saber si la superficie $S = V(f)$ de $\mathbf{A}^3_{\mathbf{C}}$ contiene a C, según el teorema 1.9 bastaría con comprobar que para algún $n \in \mathbf{N}$, $f^n \in (f_1, \dots, f_n)$ (el ideal generado por $\{f_1, \dots, f_n\}$). O también, si calculamos el *radical* (véase la definición 1.7) $\sqrt{(f_1, \dots, f_n)}$ de $(f_1, \dots, f_n)$, bastaría, de nuevo por el teorema 1.9, con comprobar que $f \in \sqrt{(f_1, \dots, f_n)}$.

(3) Suma de ideales: Si I y J son los ideales de sendas variedades X e Y, o, más en general, si I y J cumplen $X = V(I)$ e $Y = V(J)$, tenemos que $V(I + J) = V(I \cup J) = X \cap Y$. Lo que quiere decir $I + J$ es más complejo. En general, $I + J$ no es el ideal de $X \cap Y$ (incluso si $I = I(X)$ y $J = I(Y)$), pero estudiándo la suma entendemos las multiplicidades de la intersección de X e Y. En realidad, si $I = I(X)$ y $J = I(Y)$, $I + J$ es el ideal de la *intersección esquemática* de X e Y, que de hecho se define a partir del ideal suma. Se tiene también que $I(X \cap Y)$ es el *radical* (véase 1.7) de $I + J$ si $\mathbf{k} = \overline{\mathbf{k}}$.

(4,5) Intersección y producto de ideales: Si I y J son los ideales de sendas variedades X e Y , el ideal $I \cap J$ es el ideal de $X \cup Y$. Además, si $X = V(I')$ e $Y = V(J')$, $X \cup Y = V(I'J') = V(I' \cap J')$.

(6) Cociente de ideales: la interpretación geométrica de este concepto está relacionada con la *clausura de Zariski* de las variedades quasi–proyectivas, así que primero recordamos la definición de clausura de Zariski $\overline{S}$ de un subconjunto S del espacio afín. También necesítamos la definición de radical de un ideal y de ideal radical, y el enunciado del teorema de los ceros de Hilbert:

Definición 1.5. *Sea $S \subset \mathbf{A}^n_k$. La clausura de Zariski $\overline{S}$ de S es la variedad algebraica más pequeña que contiene a S, es decir, $S \subset \overline{S}$ y si es Z es una variedad algebraica tal que $S \subset Z$, entonces $\overline{S} \subset Z$.*

Ejercicio 1.6. *Demuestra que $\overline{S} = V(I(S))$ y que $I(\overline{S}) = I(S)$.*

Definición 1.7. *Sea I un ideal de A.*
(1) *El radical de I es $\sqrt{I} = \{f \in A | f^n \in I, \quad$ para algún $n \in \mathbf{N}\}$.*
(2) *El ideal I es un ideal radical si $I = \sqrt{I}$.*

Ejercicio 1.8. a) *Demuestra que si I es un ideal de A, $\sqrt{I}$ también lo es.*
b) *Demuestra que $I(X)$ es radical (incluso si $\mathbf{k} \neq \overline{\mathbf{k}}$).*

Teorema 1.9. *(de los ceros de Hilbert o Nullstellensatz) Sea $\mathbf{k}$ un cuerpo algebraicamente cerrado (por ejemplo, $\mathbf{k} = \mathbf{C}$) y sea I un ideal de $\mathbf{k}[X_1, \ldots, X_n]$. Entonces $I(V(I)) = \sqrt{I}$.*

Demostración. Puedes encontrar una demostración en [CLO1, Teorema 4.1.2] o en [R, Teorema 5.6]). □

Con estas herramientas damos la interpretación geométrica del cociente de ideales:

Proposición 1.10. *Sean I y J ideales de A y sea $Y = V(J)$. Supongamos que*
(1) *I es el ideal de una variedad X; o*
(2) *$\mathbf{k}$ es algebraicamente cerrado, I es un ideal radical y $X = V(I)$.*
Entonces $V(I : J) = \overline{X \smallsetminus Y}$ e $I : J$ es el ideal de $\overline{X \smallsetminus Y}$.

Proposición 1.11. *Sean I y J ideales de A y sea $Y = V(J)$. Si I es el ideal de una variedad X (por ejemplo, si $\mathbf{k}$ es algebraicamente cerrado, I es un ideal radical y $X = V(I)$), entonces $V(I : J) = \overline{X \smallsetminus Y}$ e $I : J$ es el ideal de $\overline{X \smallsetminus Y}$.*

Demostración. Queremos ver que $V(I : J) = \overline{X \smallsetminus Y}$. Vemos primero que $X \smallsetminus Y \subset V(I : J)$. Sea $x \in X \smallsetminus Y$ y sea $f \in I : J$; queremos ver que $f(x) = 0$. Como $x \notin Y$, existe $g \in J$ tal que $g(x) \neq 0$. Como $f \in I : J$, $fg \in I$, por lo que $f(x)g(x) = 0$ y $f(x) = 0$. Vemos ahora que si $Z = V(I')$ es tal que $X \smallsetminus Y \subset Z$, entonces $V(I : J) \subset Z$. Para esto bastaría ver que $I' \subset I : J$. Sea $h \in I'$; queremos ver que para todo $g \in J$, $hg \in I$, es decir, $h(x)g(x) = 0$ para todo $x \in X$. Si $x \in X \cap Y$, $g(x) = 0$ por lo que $h(x)g(x) = 0$. Si $x \in X \smallsetminus Y$, entonces $x \in Z$, por lo que $h(x) = 0$ y $h(x)g(x) = 0$. Para ver que $I : J = I(\overline{X \smallsetminus Y})$, razonamos así: como $V(I : J) = \overline{X \smallsetminus Y}$, se tiene que $I : J \subset I(\overline{X \smallsetminus Y})$. Para el otro contenido, llamemos I' a $I(\overline{X \smallsetminus Y})$. Como $X \smallsetminus Y \subset \overline{X \smallsetminus Y} = V(I')$, tenemos por el argumento anterior que $I' \subset I : J$. Comentamos finalmente la afirmación hecha entre paréntesis: si $\mathbf{k}$ es algebraicamente cerrado e I es un ideal radical, el teorema 1.9 implica que $I(X) = \sqrt{I} = I$. Puedes encontrar más detalles sobre este resultado en [CLO2, Ex. 1.4.11] y [CLO1, Theorem 4.4.7]. □

Continuamos con la interpretación geométrica de las operaciones con ideales de nuestra lista. Sólo quedaba:

(7) Eliminar variables: geométricamente, cuando eliminamos variables lo que estamos haciendo es proyectar desde $\mathbf{A}^n_{\mathbf{k}}$ a un espacio afín de menor dimensión (que identificamos con un subespacio lineal de $\mathbf{A}^n_{\mathbf{k}}$). De hecho, la *extensión (finitamente generada) de álgebras* $\mathbf{k}[X_{l+1}, \ldots, X_n] \subset \mathbf{k}[X_1, \ldots, X_n]$ corresponde al *morfismo* (aplicación cuyas coordenadas viene dadas por expresiones polinómicas)
$$F : \mathbf{A}^n_{\mathbf{k}} \longrightarrow \mathbf{A}^{n-l}_{\mathbf{k}}$$
que consiste en proyectar sobre las últimas $n-l$ coordenadas ("olvidándonos" por tanto de las l primeras). Para variedades algebraicas de $\mathbf{A}^n_{\mathbf{k}}$ ésta es la relación entre el morfismo F y los ideales de eliminación:

Proposición 1.12. *Con la notación anterior, sea $X = V(I') \subset \mathbf{A}^n_{\mathbf{k}}$ una variedad algebraica.*

(1) *Si I es el ideal de X (i.e, $I = I(X)$), entonces I_l es el ideal de la clausura de Zariski de $F(X)$.*
(2) *Si $\mathbf{k}$ es algebraicamente cerrado, entonces $V(I'_l) = \overline{F(X)}$.*

Ejercicio 1.13. *Demuestra la proposición 1.12.*

Observación 1.14. *Si $\mathbf{k}$ es infinito pero no necesariamente algebraicamente cerrado (por ejemplo, si $\mathbf{k} = \mathbf{R}$), la tesis del apartado (2) de la proposición 1.12 sigue siendo cierta (véase la demostración de* [CLO1, Theorem 3.3.1]*).*

Después de haber visto el significado geométrico de la lista de operaciones sencillas con los ideales de $\mathbf{k}[X_1, \ldots, X_n]$ nos planteamos ahora cómo ser capaces de realizar estas operaciones en casos concretos y de manera sistemática. Para eso usaremos las bases de Groebner, que introducimos en la siguiente sección. Estas bases aparecen ya al intentar resolver el primero de los problemas que queremos resolver: decidir cuándo un polinomio está en un ideal determinado. Una forma de abordar esto es *dividiendo* en $\mathbf{k}[X_1, \ldots, X_n]$, cosa que en principio no sabemos hacer, por lo que nos dotaremos en primer lugar de un algoritmo de división. Luego, para ver si $f \in \mathbf{k}[X_1, \ldots, X_n]$ está en un ideal I, *dividiremos* f por un sistema de generadores de I. Si el resto que obtenemos es 0, podremos asegurar que $f \in I$. Sin embargo resulta que si elegimos un sistema de generadores de I cualquiera para hacer la división, este método no nos da una caracterización que nos asegure que f esté en I (es decir, podría ocurrir que el resto de la división no fuera 0 y aun así f estuviera en I). Los sistemas de generadores “buenos”, que sí nos dan una caracterización al dividir por ellos de si f está en I, son justamente las bases de Groebner. Lo vemos con detalle en la siguiente sección.

1.2. Órdenes monomiales, algoritmo de división y bases de Groebner

Abordemos este problema: decidir cuándo un polinomio está en un ideal determinado. En una variable el problema es fácil. En ese caso tenemos el algoritmo de división tradicional por lo que $\mathbf{k}[X]$ es un *dominio euclídeo.* Como consecuencia del mismo se demuestra que todos los ideales de $\mathbf{k}[X]$ son principales. Además, si $I = (g)$, es fácil ver (como consecuencia de la unicidad del resto) que $f \in I$ si y sólo si el resto de dividir f entre g es 0. Se trata entonces de desarrollar un algoritmo de división que funcione de igual manera para solventar la cuestión de pertenencia a un ideal en el caso de varias variables. Si observamos el algoritmo de división en $\mathbf{k}[X]$ vemos que implícitamente estamos ordenando los términos del dividendo y del divisor por grados y usamos el término de mayor grado del divisor para ir cancelando los términos de de mayor grado de los dividendos intermedios. Así usamos que los monomios de $\mathbf{k}[X]$ están ordenados de forma obvia. Así pues, en $A = \mathbf{k}[X_1, \ldots, X_n]$ lo primero que haremos será *ordenar* los monomios.

Definición 2.1. *Un orden monomial es una relación de orden en el conjunto de los monomios que cumple lo siguiente:*

(1) *Es total.*
(2) *Es compatible con el producto ($x^\alpha > x^\beta$ implica $x^{\alpha+\gamma} > x^{\beta+\gamma}$).*

(3) *Es un buen orden (toda colección de monomios tiene un elemento mínimo)*

En la definición anterior (1) significa que cualesquiera dos monomios son comparables (si son distintos, uno es mayor que el otro o al revés) y usaremos (3) para asegurarnos de que los algoritmos terminan (típicamente intentaremos usar algoritmos que en cada paso produzcan un monomio más pequeño según el orden monomial elegido).

Ejemplo 2.2. *Es fácil ver que en* $\mathbf{k}[X]$ *existe un único orden monomial. En efecto, tenemos que o bien* $1 > X$ *o bien* $X > 1$*, por (1) de la definición 2.1, pero ha de ser lo segundo, pues si fuera* $1 > X$*, aplicando reiteradamente (2) (multipicando por* X*) obtendríamos una sucesión* $1 > X > X^2 > X^3 > \cdots$*, sin mínimo. Por tanto es* $X > 1$ *y usando (2) y la propiedad transitiva ordenamos todos los monomios.*

En cambio para varias variables, incluso habiendo fijado cómo ordenamos las mismas (usualmente $X_1 > X_2 > \cdots > X_n$) existen muchos ordenes monomiales. Vemos un par de ejemplos muy importantes:

Definición 2.3. *Órden lexicográfico. Véase* [CLO2, pág. 8].

Definición 2.4. *Órden lexicográfico inverso graduado (*grevlex*) Véase* [CLO2, pág. 8]*.*

Es fácil ver que son órdenes monomiales.

Ejercicio 2.5. *Comprueba que el órden lexicográfico y el órden lexicográfico inverso graduado son distintos comparándolos para varios monomios. Comprueba que son distintos incluso para los monomios de un mismo grado total (aunque coinciden para los monomios de un mismo grado cuando* $n = 2$*) (véase* [CLO2, pág. 8]*).*

El interés de poder trabajar con distintos órdenes monomiales es que unos u otros serán más o menos útiles dependiendo del problema que abordemos.

Siguiendo con la cuestión de determinar cuándo un polinomio pertenece a un ideal, la idea es imitar el argumento para polinomios en una variable en el que se usaba el algoritmo de división. Pero ahora los ideales de $A = \mathbf{k}[X_1, \dots, X_n]$ no son necesariamente principales, aunque por el teorema de la base de Hilbert sabemos que están finitamente generados (A es *noetheriano*).

Entonces, por lo dicho anteriormente, conviene dividir por un conjunto de varios polinomios. Imitando el algoritmo en una variable no es difícil concluir que existe el siguiente teorema de división:

Teorema 2.6. *Fijamos un orden monomial* $\geq$ *en* A*. Sean* $f_1, \dots, f_s \in A$ *y sea* $f \in A$*. Existen* $a_1, \dots, a_s \in A$ *y* $r \in A$ *tales que* $f = a_1 f_1 + \cdots + a_s f_s + r$ *y ningún término de* r *es divisible por ningún término inicial (respecto de* $\geq$*; definición obvia) de* $f_1, \dots, f_s$*.*

Demostración. (Más detalles en [CLO1, Theorem 2.3.3]). Idea: ordenamos los $f_1, \dots, f_s$, vamos mirando, ordenados por $\geq$, los términos de f; si un término de f (o más bien del dividendo parcial) es divisible por alguno de los términos iniciales de $f_1, \dots, f_s$, lo cancelamos, obteniendo un dividendo parcial (que seguimos dividiendo) y un término que pasa a ser parte del cociente a_i correspondiente. Si un término del dividendo parcial no es divisible por ninguno de los términos iniciales de $f_1, \dots, f_s$, se lo restamos y lo pasamos al resto. El algoritmo termina cuando el dividendo parcial es 0 y esto siempre ocurre porque en cada paso el término inicial del dividendo parcial es estrictamente menor (según $\geq$) que el del anterior y $\geq$ es un buen orden. (Supongo que el proceso nunca termina y considero el conjunto formado por los términos iniciales de los dividendos; este conjunto no tiene mínimo; si lo tuviera, sería el término inicial del dividendo de cierto paso n pero el término inicial del dividendo del paso $n+1$ sería menor que él por lo que no sería el mínimo). $\square$

El algoritmo de división nos da el siguiente criterio: si $I = (f_1, \dots, f_s)$ (o más en general, si $f_1, \dots, f_s \in I$) y el resto de dividir f por $f_1, \dots, f_s$ es 0, entonces $f \in I$. Sin embargo, aunque $f_1, \dots, f_s$ generen I, puede haber elementos de I que no den resto 0. Simplemente, puede existir un elemento de I con algún término que no es divisible por ninguno de los términos iniciales de $f_1, \dots, f_s$.

Ejemplo 2.7. *Para ilustrar lo anterior véase* [CLO2, Exercise 1.3.1] *o* [CLO1, Example 2.3.5].

Otra observación es que el resto de la división no es único (al contrario de en una variable) sino que depende no sólo del orden monomial elegido sino también del orden en que listamos los $f_1, \dots, f_s$ (en el algoritmo, comprobamos por orden si algún término inicial de los $f_1, \dots, f_s$ divide al término inicial del dividendo parcial, y usamos el primer f_i que lo hace).

El primer problema (que dar resto 0 no caracteriza a los elementos de I) motiva que busquemos sistemas de generadores de I que sí nos den la caracterización. Es decir, fijado $>$, necesitamos un sistema de generadores $f_1, \dots, f_s$ tal que sus términos iniciales $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s)$ dividan al término inicial de cualquier $f \in I$ (es necesario, porque si hay un $f \in I$ cuyo término inicial no es divisible, entonces el resto de dividir f no será 0; es suficiente, porque si $f \in I$, cualquier dividendo parcial está también en I). Por tanto definimos:

Definición 2.8. *Fijamos $>$. Sea I ideal, sea $LT(I) = \{LTf, f \in I\}$ y sea $(LT(I))$ el ideal inicial de I. Decimos que $f_1, \dots, f_s \in I$ son una base de Groebner de I si para todo $f \in I$, algún f_i cumple que LTf_i divide a LTf.*

Observación 2.9. *$(LT(I))$ es, por construcción, un ideal monomial (es decir, un ideal generado por monomios; un polinomio está un ideal monomial si y sólo si todo término suyo está en el ideal).*

Observación 2.10. *Es fácil ver que $f_1, \dots, f_s \in I$ es una base de Groebner si y sólo si $LTf_1, \dots, LTf_s$ generan el ideal inicial de I.*

Nótese que en la definición de base de Groebner no hemos pedido que $f_1, \dots, f_s$ generen I, pero esto va a ser así a posteriori.

Teorema 2.11. *El resto (que satisface las propiedades del teorema 2.6) al dividir por una base de Groebner es único.*

Demostración. Sea $G = \{g_1, \dots, g_s\}$ una base de Groebner de I y sea $f = a_1g_1 + \dots + a_sg_s + r = b_1g_1 + \dots + b_sg_s + r'$. Ningún término de r ni de r' es divisible por los $\mathrm{LT}(g_i)$, así que lo mismo pasa con los términos de $r - r'$. Consideramos $h = b_1g_1 + \dots + b_sg_s - (a_1g_1 + \dots + a_sg_s) = r - r'$. Como $h \in I$ y G es una base de Groebner, si $h \neq 0$, el término inicial de h es divisible por algún $\mathrm{LT}(g_i)$, pero eso contradice que ninguno de los términos de $r - r'$ es divisible por ningún $\mathrm{LT}(g_i)$. Por tanto $h = 0$, y $r = r'$. □

Teorema 2.12. *Sea I ideal, fijamos $>$. Si $F = \{f_1, \dots, f_s\}$ es una base de Groebner de I, entonces $f \in I$ si y sólo si el resto de dividir f por F es $\overline{f}^F = 0$.*

Demostración. Si el resto de $f \in I$ no fuera 0, éste sería un polinomio de I con todos sus términos, y en particular el inicial, no divisibles por los iniciales de $f_1, \dots, f_s$. □

De hecho veremos más adelante que $F \subset I$ es una base de Groebner si y sólo si $\overline{f}^F = 0$ para todo $f \in I$.

Corolario 2.13. *Una base de Groebner G de I genera I.*

Demostración. Por definición, $G \subset I$, luego $(G) \subset I$. Sea $f \in I$. Entonces $\overline{f}^G = 0$, luego f es combinación de los elementos de G. □

Proposición 2.14. *Todo ideal I no nulo tiene bases de Groebner.*

Demostración. El ideal inicial de I está generado por un número finito de polinomios (ya que A es noetheriano) y como es un ideal monomial (por lo que un polinomio está en el ideal si y sólo si todos sus términos lo están), está generado por un número finito de monomios $\{X^\alpha\}$. Esto también se sigue directamente del lema de Dickson (véase [CLO1, Theorem 2.4.5]). Por otra parte, cada uno de esos monomios X^α es $X^\beta \cdot \mathrm{LT} f_\alpha$ para algún $f_\alpha \in I$ porque los $\mathrm{LT} f$, $f \in I$ generan el ideal inicial. Por tanto, $(LT(I)) = (\{X^\alpha\}) \subset (\{LT f_\alpha\}) \subset (LT(I))$. Entonces $\{f_\alpha\}$ es una base de Groebner de I. □

Esta demostración tiene la pega de no ser constructiva. Veremos ahora un criterio para ver cuándo un conjunto finito G de generadores G de I es una base de Groebner. Ese criterio da lugar a un algoritmo para, a partir de un conjunto de generadores finito de I (la forma en que usualmente se da I como *input*), obtener una base de Groebner de I. (El algoritmo da otra demostración, esta vez constructiva, de la existencia de bases de Groebner). Para más detalles sobre esto véase [CLO1, 2.6, 2.7]. Antes definimos

Definición 2.15. *Sean $f, g \in \mathbf{k}[X_1, \dots, X_n]$. Sea X^α el mínimo común múltiplo de los términos iniciales de f y g. Entonces $S(f,g) := \frac{x^\alpha}{LTf} \cdot f - \frac{x^\alpha}{LTg} \cdot g$.*

Teorema 2.16. *(Criterio de Buchberger (véase* [CLO1, Theorem 2.6.6]*)). Sea G un sistema de generadores de I. Entonces G es una base de Groebner de I si y sólo si para todo $f, g \in G$, $\overline{S(f,g)}^G = 0$*

Demostración. Para que G sea una base de Groebner hace falta que los términos iniciales de los polinomios de G dividan al término inicial de cualquier polinomio f de I. Si $G \subset I$, una combinación f de los elementos de G es también un elemento de I. El problema (para que G no sea base de Groebner) puede ser que al hacer una combinación de los elementos de G eliminemos los términos iniciales de los elementos de G y aparezca un polinomio con un término inicial que no es divisible por los de G, o con uno de los términos no divisible, puesto que al dividir por G el resto seguirá estando en I, y dicho resto contendrá a ese término. Una forma en la que pueden surgir esos polinomios "malos" es haciendo el S–polinomio de dos de G (estamos usando una relación que satisfacen los términos iniciales de f y g para cancelarlos, obteniendo así un polinomio cuyo término inicial será un múltiplo de un término no inicial de f ó g). Por tanto una condición necesaria para que G sea base de Groebner es que los restos al dividir los S–polinomios por G sean 0. (Recuérdese (teorema 2.12) que si G es base de Groebner y $f \in I$, entonces $\overline{f}^G = 0$.

Falta ver que es una condición suficiente. Si G no fuera base de Groebner es porque existe un $f \in I$ tal que LTf no es divisible por ninguno de los términos iniciales de los polinomios de G. Por otro lado, como G genera I, $f = \sum f_i g_i$, así que lo anterior implica que el término inicial de f no es el término inicial de ninguno de los $f_i g_i$. Eso ocurre porque el máximo entre los términos iniciales de los $f_i g_i$ se alcanza para varios $f_k g_k$ y se cancelan entre ellos. Así, si δ es el multigrado máximo de los $f_i g_i$, el multigrado de f, mg$f < \delta$. Por tanto la suma $\sum f_i g_i$ se escribe:

$$f = \sum f_i g_i = \sum_{\mathrm{mg}(f_i g_i)=\delta} \mathrm{LT}(f_i) g_i + \sum_{\mathrm{mg}(f_i g_i)=\delta} (f_i - \mathrm{LT}(f_i)) \cdot g_i + \sum_{\mathrm{mg}(f_i g_i)<\delta} f_i g_i.$$

De los tres grupos de sumandos, sólo los sumandos del primero tienen multigrado δ; los demás tienen multigrado menor. Como f tiene multigrado menor que δ, el multigrado del primer bloque de sumandos es también menor que δ, así que los términos iniciales de los sumandos de ese primer bloque se cancelan. Por ello (véase el enunciado y la demostración del [CLO1, Lema 2.6.5]) el primer bloque de sumandos es una combinación, con coeficientes monomiales, de los $S(g_j, g_k)$. Restando de f esa combinación de $S(g_j, g_k)$s obtenemos o bien 0 o bien un $f^1 \in I$ que tiene una expresión $f_1 = \sum f_{1,i} g_i$ en función de los g_i cuyos sumandos $f_{1,i} g_i$ tienen multigrado menor que δ. Por otra parte, como el resto de los S–polinomios al dividir por G es 0 tenemos que el término inicial f ha de ser el término inicial de f^1, por lo que este último no es el término inicial de ninguno de los $f_{1,i} g_i$. Así puedo realizar a f^1 el mismo razonamiento que a f y producir una sucesión $f, f^1, f^2, \ldots$ en la cual el multigrado de los sumandos en la expresión de cada f^l en función de los g_i es menor en cada paso. Como los multigrados están bien ordenados, el proceso tiene que parar, lo cual ocurre cuando algún f^l lo pueda escribir como combinación de S–polinomios. Pero eso implicaría que el término inicial de f^l y por tanto, el de f, es divisible por algún LT(g_i), $g_i \in G$, llevandonos a contradicción. La contradicción viene de suponer que G no es base de Groebner. $\square$

El criterio de Buchberger permite el siguiente algoritmo para obtener una base de Groebner a partir de un sistema de generadores del ideal.

Teorema 2.17. *(Algoritmo de Buchberger) Sea I un ideal de $\mathbf{k}[X_1, \ldots, X_n]$ y sea F un sistema de generadores de I. Entonces podemos construir una base de Groebner de I a partir de F en un número finito de pasos, con el siguiente algoritmo. Sea G' un conjunto obtenido de forma inductiva a partir de F*

(1) *Para cada par $g_i, g_j \in G'$, define $S_{ij} = \overline{S(g_i, g_j)}^{G'}$*
(2) *Se define un nuevo G' como el antiguo G' unión $\{S_{ij} | S_{ij} \neq 0\}$.*

(3) (a) *3.1) Si en 2) el G' antiguo y el nuevo coinciden, se acaba el algoritmo y $G := G'$ es una base de Groebner de I*
(b) *3.2) Si en 2) el G' nuevo es estrictamente mayor que el antiguo, se comienza otra vez el bucle para el nuevo G'.*

Demostración. Primero vemos que $G' \subset I$ en todos los pasos (y en particular $G \subset I$): $F \subset I$ y en cada paso $G' \subset I$ (por inducción $g_i, g_j \in I$ luego $S_{i,j} \in I$). Además por construcción $F \subset G'$, luego G genera I. (observación no necesaria).

Vemos que cuando el algoritmo termina G es en efecto una base de Groebner: Si el algoritmo termina es porque a G' no el añadimos nada en la última vuelta del bucle. Eso quiere decir que para todo $g_i, g_j \in G'$, $\overline{S(g_i, g_j)}^{G'} = 0$. Como G' es un sistema de generadores de I, por 2.16, G' es una base de Groebner.

Finalmente vemos que el algoritmo termina en un número finito de pasos. En un mismo paso seguimos llamando G' al G' antiguo y llamamos G^* al G' nuevo. Observamos que si $G' \subsetneq G^*$ entonces $(\mathrm{LT}G') \subsetneq (\mathrm{LT}G^*)$ (claramente $(\mathrm{LT}G') \subset (\mathrm{LT}G^*)$). En efecto, si $G' \neq G^*$ es porque algún $\overline{S(g_i, g_j)}^{G'} \neq 0$. En ese caso, $\overline{S(g_i, g_j)}^{G'} \in G^*$ pero su término inicial h no es divisible por los términos iniciales de G'. Por otra parte sabemos que $\mathbf{k}[X_1, \ldots, X_n]$ es noetheriano por lo que toda cadena asecendente de ideales estaciona. □

Observación 2.18. El algortimo de Buchberger tal como lo hemos enunciado en 2.17 puede producir bases de Groebner muy grandes (siempre vamos añadiendo elementos a G') en el sentido de que algunos elementos sean irredundantes. Por eso conviene transformar la base obtenida en una base minimal y en un base reducida, como se indica más abajo. Por otra parte el algoritmo se puede refinar. Una mejora sencilla es que las parejas g_i, g_j para las que S_{ij} sea 0 en un paso determinado del algoritmo van a seguir teniendo esa propiedad en los pasos siguientes (los elementos del G' dado cuyos términos iniciales nos sirven para que el resto dé 0 siguen estando en los siguientes G'), por lo que no hace falta calcular S_{ij} a partir del momento en que este da 0. Otras mejoras más profundas del algoritmo se pueden encontrar en [CLO1, Sección 2.9]

Definición 2.19. *Una base de Groebner reducida es una base de Groebner tal que para cualesquiera $g_i, g_j \in G$, ningún término de g_i es múltiplo de $LT(g_j)$ (y viceversa). Una base de Groebner es mónica si es reducida y el coeficiente inicial cada elemento de G es* 1.

Proposición 2.20. *Todo ideal tiene una base de Groebner reducida y una base de Groebner mónica; esta última es única.*

Demostración. Existencia: Tomamos una base de Groebner de I y a partir de ella producimos una base *minimal* de I (una base tal que para todo $g_i \in G$, $\mathrm{LT}(g_i)$ no es divisible por ningún $\mathrm{LT}(g_j)$, $g_j \in G$, $g_j \neq g_i$). Esto se puede hacer gracias a la siguiente

Observación 2.21. *Sea G una base de Groebner. Si $LT(g_i)$ fuera divisible por algún $LT(g_j)$, entonces $G - \{g_i\}$ también es una base de Groebner*

La demostración de la observación 2.21 es obvia. Entonces quitando uno a uno los miembros prescindibles, como G es finita, acabamos con teniendo una base de Groebner minimal.

Así pues, sea $G = \{g_1, g_2, \ldots, g_s\}$ una base de Groebner minimal. Decimos que $g_i \in G$ es reducido respecto a G si ningún término de g_i es divisible por los iniciales de $G - \{g_i\}$. Entonces empezamos con g_1 y producimos g_1' como el resto de dividir g_1 por $G - \{g_1\}$. Sea $G_1 = \{g_1', g_2, \ldots, g_s\}$. Claramente $g_1' \in I$. Como G era minimal, $\mathrm{LT}(g_1)$ pasa al resto al dividir por $G - \{g_1\}$, por lo que $\mathrm{LT}(g_1) = \mathrm{LT}(g_1')$. Entonces los términos iniciales de los elementos de G_1 son los mismos que los términos iniciales de los de G, por lo que G_1 sigue siendo una base de Groebner y sigue siendo minimal. Por otra parte g_1' es reducido con respecto a G_1 y lo seguirá siendo para cualquier base de Groebner cuyos elementos tengan los mismos términos iniciales que los elementos de G. Así vamos construyendo $g_1', g_2', \ldots$ (podemos aplicar el mismo argumento a $g_2 \in G_1$ ya que G_1 es minimal como lo era G) y $G_1, G_2, \ldots$. Finalmente G_s será una base reducida. A partir de ella se obtiene de forma obvia una base mónica.

Unicidad: Observamos primero que una base reducida es minimal. Entonces si G y $\tilde{G}$ son dos bases mónicas (basta con que sean minimales y con términos iniciales 1 para todos sus elementos) tienen los mismos términos iniciales como demuestra este

Lema 2.22. *Sean G y $\tilde{G}$ dos bases de Groebner minimales y con términos iniciales 1 para todos sus elementos. Entonces los términos iniciales de los elementos de G son los mismos que los términos iniciales de los elementos de $\tilde{G}$.*

Demostración. Sea $g_i \in G$; como $\tilde{G}$ es base de Groebner y $g_i \in I$, existe $\tilde{g}_j \in \tilde{G}$ tal que $\mathrm{LT}(\tilde{g}_j)$ divide a $\mathrm{LT}(g_i)$. De igual forma existe $g_k \in G$ tal que $\mathrm{LT}(g_k)$ divide a $\mathrm{LT}(\tilde{g}_j)$, con lo que $\mathrm{LT}(g_k)$ divide a $\mathrm{LT}(g_i)$. Como G es minimal $g_i = g_k$ y $\mathrm{LT}(g_i)$ y $\mathrm{LT}(\tilde{g}_j)$ son iguales salvo producto por una constante. Como ambos son mónicos, son iguales. Esto demuestra que los $\mathrm{LT}g_i$ están entre los $\mathrm{LT}\tilde{g}_j$. El razonamiento recíproco da el otro contenido y la igualdad. □

Seguimos con la demostración de la unicidad. Sea $g \in G$ y $\tilde{g} \in \tilde{G}$ tales que $\mathrm{LT}g = \mathrm{LT}\tilde{g}$. Consideramos $g - \tilde{g} \in I$. Como sus términos iniciales son iguales, en $g - \tilde{g}$ se cancelan y los otros términos de $g - \tilde{g}$, lo son o bien de g o bien de $\tilde{g}$ (pero no sus términos iniciales). Si se trata de un término de g, no es divisible por los términos iniciales de $G - \{g\}$, porque G es reducida y tampoco por $\mathrm{LT}g$, porque no era el término inicial de g sino uno menor. Si es un término de $\tilde{g}$, tenemos el mismo argumento para $\tilde{G}$, y como $\mathrm{LT}G = \mathrm{LT}\tilde{G}$, concluimos que tampoco es divisible por ningún término inicial de G. Por tanto $\overline{g - \tilde{g}}^{G} = g - \tilde{g}$, pero $g - \tilde{g} \in I$, luego el resto es 0, y $g - \tilde{g} = 0$. □

1.3. Primeras aplicaciones de las bases de Groebner

Con la definición, la existencia y el algoritmo de Buchberger (u otro más eficiente) para calcular bases de Groebner, obtenemos ya varias aplicaciones:

Ejercicio 3.1. *Esboza un algoritmo para decidir la pertenencia de un polinomio f a un ideal I.*

Ejercicio 3.2. *Da un método para decidir si dos ideales son iguales*

Para seguir comentando aplicaciones necesitamos hablar de cómo calcular los ideales de eliminación (véase 1.3) de un ideal I dado. Fijando un orden monomial adecuado, las bases de Groebner dan una respuesta satisfactoria al problema:

Teorema 3.3. *Sea I un ideal de $\mathbf{k}[X_1,\dots,X_n]$. Fijamos en $\mathbf{k}[X_1,\dots,X_n]$ el orden lexicográfico $<$ con $X_1 > X_2 > \cdots > X_n$. Si G es una base de Groebner de I con respecto de $<$, entonces $G_l := G \cap \mathbf{k}[X_{l+1},\dots,X_n]$ es una base de Grobner del ideal de eliminación l–ésimo $I_l = I \cap \mathbf{k}[X_{l+1},\dots,X_n]$ de I.*

Demostración. Obviamente $G_l \subset I_l$, pues $G = \{g_1,\dots,g_s\} \subset I$. Vemos que G_l genera I_l (en $\mathbf{k}[X_{l+1},\dots,X_n]$). Ordenamos los elementos de G de forma que G_l consiste en los r primeros $g_1,\dots,g_r$. Basta ver que todo elemento $f \in I_l$ es una combinación de los de G_l. Para eso dividimos f (con el algoritmo de división descrito en la demostración del teorema 2.6 por G. Como G es una base de Groebner de I, $\overline{f}^G = 0$ por el teorema 2.12. Por otra parte, como $g_{r+1},\dots,g_s \in I$ pero no están en I_l, $g_{r+1},\dots,g_s$ poseen términos no nulos que involucran alguna variable $X_1,\dots,X_l$. Por el orden elegido, los términos iniciales de $g_{r+1},\dots,g_s$ han de involucrar alguna variable $X_1,\dots,X_l$. Como los términos de f no involucran a ninguna variable $X_1,\dots,X_l$, en el algoritmo de división no uso los $g_{r+1},\dots,g_s$, por lo que éstos no aparecen en el cociente, por lo que (siendo como hemos dicho 0 el resto de dividir f por G) se tiene que f es combinación de $g_1,\dots,g_r$ y además con coeficientes en $\mathbf{k}[X_{l+1},\dots,X_n]$.

Vemos finalmente que G_l no es sólo un sistema de generadores para I_l sino también una base de Groebner. Por el criterio de Buchberger (véase teorema 2.16) basta ver que para cualesquiera $g_i, g_j \in G_l$, $\overline{S(g_i,g_j)}^{G_l} = 0$ (dentro de $\mathbf{k}[X_{l+1},\dots,X_n]$). Por otra parte $S(g_i,g_j) \in I_l$ ($g_i, g_j \in I$ luego $S(g_i,g_j) \in I$; como $g_i, g_j \in \mathbf{k}[X_{l+1},\dots,X_n]$, por contrucción $S(g_i,g_j) \in \mathbf{k}[X_{l+1},\dots,X_n]$). Entonces por las observaciones del apartado anterior el resto de dividir $S(g_i,g_j)$ por G es 0 y coincide con el resto de dividir $S(g_i,g_j)$ por G_l dentro de $\mathbf{k}[X_{l+1},\dots,X_n]$. □

Cálculo de la intersección de dos ideales. Usamos el teorema 3.3 para dar un método para calcular la intersección de dos ideales: Sean I y J dos ideales de $\mathbf{k}[X_1,\dots,X_n]$. Consideramos el ideal $TI + (1-T)J$ de $\mathbf{k}[X_1,\dots,X_n,T]$ (si $a \in A$ y I es un ideal de A, definimos aI como el ideal generado por todos los elementos de la forma $a \cdot i$, con $i \in I$; es decir, aI es el ideal producto $(a)I$). Demostramos que $(TI + (1-T)J) \cap \mathbf{k}[X_1,\dots,X_n] = I \cap J$ (Fácil: el contenido hacia la izquierda, trivial; para el contenido hacia la derecha, sean $h_i \in \mathbf{k}[X_1,\dots,X_n,T], f_i \in I, g_i \in J$ y sean $\sigma \sum h_i(tf_i + (1-t)g_i) \in \mathbf{k}[X_1,\dots,X_n]$. Entonces $\sigma = \sigma(X_1,\dots,X_n,0) \in J$ y $\sigma = \sigma(X_1,\dots,X_n,1) \in I$). Entonces, partiendo de sendos sistemas de generadores de I y de J, obtenemos uno de $TI + (1-T)J$, y a partir de él obtenemos una base de Groebner G respecto de un orden lexicográfico en el que $T > X_i$ para todo i y usamos el teorema 3.3.

Cálculo del ideal cociente $I : (h)$. Dado un ideal I calculamos $I \cap (h)$ (por ejemplo, por el método anterior) y obtenemos que $I \cap (h) = (g_1,\dots,g_s)$. Entonces $I : (h) = (g_1/h,\dots,g_s/h)$ (esto es válido no sólo para $A = \mathbf{k}[X_1,\dots,X_n]$ sino para A dominio de integridad. En efecto, $g_i/h \in I : (h)$, puesto que, para todo $b \in A$, $bh \cdot g_i/h = bg_i \in I$. Por otro lado, si $a \in I : (h)$, entonces $h \cdot a \in I$, es decir,

$h \cdot a = a_1 g_1 + \cdots + a_s g_s$. Como los g_i son múltiplos de h y A es un dominio de integridad, podemos dividir la igualdad por h y queda $a = a_1 g_1/h + \cdots + a_s g_s/h$.

Terminamos este capítulo con otra aplicación de la eliminación: la **implicitación**. El problema que abordamos es el siguiente. En $\mathbf{A}^n_{\mathbf{k}}$ consideramos un subconjunto X dado por unas ecuaciones paramétricas polinómicas (sean $h_1, \ldots, h_n \in \mathbf{k}[T_1, \ldots, T_m]$; $X = \{\underline{x} = (x_1, \ldots, x_n) \in \mathbf{A}^n_{\mathbf{k}} |$ existe $\underline{t} = (t_1, \ldots, t_m) \in \mathbf{A}^m_{\mathbf{k}}$ tal que $\underline{x} = (h_1(\underline{t}), \ldots, h_n(\underline{t})\})$ o racionales (igual que antes pero ahora $h_1 = f_1/g_1, \ldots, h_n = f_n/g_n \in \mathbf{k}(T_1, \ldots, T_m)$). Se trata entonces de encontrar las ecuaciones (implıćitas) de X en $\mathbf{A}^n_{\mathbf{k}}$ (en realidad X es una variedad algebraica si la parametrización es polinómica y $\mathbf{k}$ es algebraicamente cerrado, pero no lo es en general en caso contrario; lo que obtendremos en cualquier caso serán las ecuaciones de la clausura de Zariski $\overline{X}$ de X). Para resolver este problema tenemos el siguiente resultado:

Teorema 3.4. *Sea* $\mathbf{k}$ *un cuerpo algebraicamente cerrado (también vale si* $\mathbf{k}$ *es infinito; véase la observación 1.14). Sean* $B = \mathbf{k}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ *y* $\hat{B} = \mathbf{k}[Y, T_1, \ldots, T_m, X_1, \ldots, X_n]$. *Con la notación del párrafo anterior, sea* $I = (X_1 - h_1, \ldots, X_n - h_n) \subset B$ *si* X *está dada por una parametrización polinómica y sea* $J = (g_1 X_1 - f_1, \ldots, g_n X_n - f_n, g_1 \cdots g_n Y - 1) \subset B$ *si* X *está dada por una parametrización racional. Sea* $I_m = I \cap \mathbf{k}[X_1, \ldots, X_n]$ *y sea* $J_{m+1} = J \cap \mathbf{k}[X_1, \ldots, X_n]$. *Si* X *está dada por una parametrización polinómica, entonces* $\overline{X} = V(I_m)$ *y si* X *está dada por una parametrización racional, entonces* $\overline{X} = V(J_{m+1})$.

Demostración. El conjunto X es la imagen del morfismo $F : \mathbf{A}^m_{\mathbf{k}} \longrightarrow \mathbf{A}^n_{\mathbf{k}}$ (resp. aplicación racional) definido como $F(\underline{t}) = (h_1(\underline{t}), \ldots, h_n(\underline{t}))$. En ese caso $V(I) \subset \mathbf{A}^{m+n}_{\mathbf{k}}$ es claramente el grafo Γ de F (y los puntos $(\underline{t}, \underline{x}) \in \mathbf{A}^{m+n}_{\mathbf{k}}$ que para los que existe un $y \in \mathbf{k}$ tal que $(y, \underline{t}, \underline{x}) \in V(J) \subset \mathbf{A}^{m+n+1}_{\mathbf{k}}$ son el grafo de F en el caso en que F es una aplicación racional (El introducir la variable Y es por lo siguiente: un punto $(\underline{t}, \underline{x})$ podriá ser un cero común de $g_1 X_1 - f_1, \ldots, g_n X_n - f_n$ siendo $\underline{t}$ un cero de alguno de los g_i, pero justamente para tal $\underline{t}$, F no está definida, por lo que $(\underline{t}, \underline{x})$ no estaría en el grafo de F; sin embargo como $(\underline{t}, \underline{x})$ ha de cumplir que exista y tal que $(y, \underline{t}, \underline{x})$ sea también un cero de $g_1 \cdots g_n Y - 1$), eliminamos esos $\underline{t}$ "malos")). Entonces loss puntos de X son justamente los que aparecen al proyectar en las segundas variables (en $\mathbf{A}^n_{\mathbf{k}}$) los puntos de Γ (en el caso en que F es racional, los puntos de Γ son los proyectados a $\mathbf{A}^{m+n}_{\mathbf{k}}$ de los puntos de $V(J)$, por los que los puntos de X son la proyección a $\mathbf{A}^n_{\mathbf{k}}$ desde $\mathbf{A}^{m+n+1}_{\mathbf{k}}$ de los puntos de $V(J)$). Por otra parte vimos en la proposición 1.12 y en la observación 1.14 que el lugar de ceros del ideal de eliminación I_m es la clausura de Zariski de la proyección de Γ (y si F es racional, el lugar de ceros del ideal de eliminación J_{m+1} es la clausura de Zariski de la proyección de $V(J)$), con lo que queda demostrado el teorema. □

Ejercicio 3.5. *Esboza un algoritmo que calcule las ecuaciones implícitas de la clausura de Zariski de* X, *cuando* X *viene dada por unas ecuaciones paramétricas* $h_1, \ldots, h_m$.

Referencias

[CLO1] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2007.

[CLO2] D. Cox, J. Little, D. O'Shea, *Using algebraic geometry*, Second edition. Graduate Texts in Mathematics **185**. Springer, New York, 2005.

[R] M. Reid, *Undergraduate commutative algebra.*, London Mathematical Society Student Texts, **29**. Cambridge University Press, Cambridge, 1995.

Práctica 4 : Algebra computacional :

Dada una curva proyectiva plana, calcular sus puntos singulares.

```
Sing[p_,{x0_,x1_,x2_}]:=
 Module[{i},
  If[
   TrueQ[(Gr[p,{x0,x1,x2},{a1,a2,a3}])!=1],
             (Message[msg::nhom];Break),
             {x0,x1,x2}/. Complement[Union[Solve[{p==0,
                                                  D[p,x0]==0,
                                                  D[p,x1]==0,
                                                  D[p,x2]==0},
                                                  {x0,x1,x2}] ],
                                      {{x0->0,x1->0,x2->0}}]
          ]
           ]
```

```
Sing[x1^3-x2^2 x0,{x0,x1,x2}]
```

Solve::svars : Equations may not give solutions for all "solve" variables. ≫

```
{{x0, 0, 0}}
```

```
Sing[Expand[x1^4+x1^2 x0^2+x2^2 x0^2+x2 x0^3], {x0,x1,x2}]
```

Solve::svars : Equations may not give solutions for all "solve" variables. ≫

```
{{0, 0, x2}}
```

```
AEMTOTAL[Expand[x1^4+x1^2 x0^2+x2^2 x0^2+x2 x0^3],
 {x0,x1,x2},{0,0,1}]
```

```
{2}
{2}
{{1, 1}}
```

```
x1^3 x0-x2 (x2-x0) (x2-2x0) (x2+3x0)/.{x0->1,x1->1,x2->1}
```

```
1
```

```
Needs["Explosiones`"]
```

```
Sing[Expand[x2^7- x1^4 (x1+x0) (x1-x0)^2] ,{x0,x1,x2}]
```

Solve::svars : Equations may not give solutions for all "solve" variables.

```
{{x1, x1, 0}, {x0, 0, 0}}
```

```
AEMTOTAL[Expand[x2^7- x1^4 (x1+x0) (x1-x0)^2 ],
{x0,x1,x2},{1,1,0}]
```

```
{2}

{2}

{{2}}

{{{1}}}
```

```
ExplosionTotal[Expand[x2^7 - x1^4 (x1 + x0) (x1 - x0)^2], {x0, x1, x2}, {1, 1, 0}]
```

$\{-2\,x0^{10}\,x1^{2}-9\,x0^{8}\,x1^{3}\,x2-16\,x0^{6}\,x1^{4}\,x2^{2}-14\,x0^{4}\,x1^{5}\,x2^{3}-6\,x0^{2}\,x1^{6}\,x2^{4}+x0^{7}\,x2^{5}-x1^{7}\,x2^{5},$
$\{x0, x1, x2\}, \{\{1, 0, 0\}\}\}$

$\{\{-2\,x0^{15}\,x1^{2}-9\,x0^{12}\,x1^{3}\,x2^{2}+x0^{14}\,x2^{3}-16\,x0^{9}\,x1^{4}\,x2^{4}-14\,x0^{6}\,x1^{5}\,x2^{6}-6\,x0^{3}\,x1^{6}\,x2^{8}-x1^{7}\,x2^{10},$
$\{x0, x1, x2\}, \{\{1, 0, 0\}\}\}\}$

$\{\{\{-2\,x0^{20}\,x1^{2}+x0^{21}\,x2-9\,x0^{16}\,x1^{3}\,x2^{3}-16\,x0^{12}\,x1^{4}\,x2^{6}-14\,x0^{8}\,x1^{5}\,x2^{9}-6\,x0^{4}\,x1^{6}\,x2^{12}-x1^{7}\,x2^{15},$
$\{x0, x1, x2\}, \{\{1, 0, 0\}\}\}\}\}$

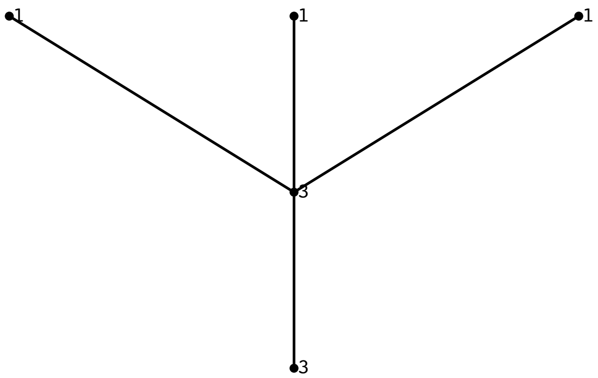
```
AEMTOTAL[Expand[x2^7- x1^3 (x1+x2) (x1-x0)^2 x0 ],
{x0,x1,x2},{1,0,0}]
```

```
{4}
{1, 3}
{{}, {1, 1, 1}}
```

```
AEMTOTAL[Expand[x2^6 x0 - x1^3 (x1 -x0)^4],
{x0,x1,x2},{0,1,0}]
```

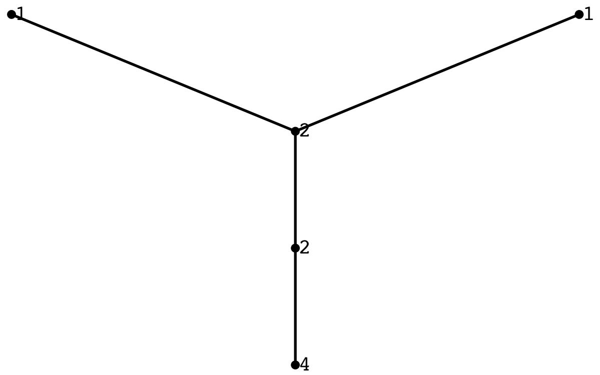
```
{0}
                    8        6              4    2    2        2    3    3
{Multiplicidad[-x0   + 4 x0   x1 x2 - 6 x0   x1   x2   + 4 x0   x1   x2   -

     4    4        7
   x1   x2   + x1 x2 , {x0, x1, x2}, 1],

                    8        6              4    2    2        2    3    3
  Multiplicidad[-x0   + 4 x0   x1 x2 - 6 x0   x1   x2   + 4 x0   x1   x2   -

     4    4        7
   x1   x2   + x1 x2 , {x0, x1, x2}, Explosiones`Private`z0$2411],

                    8        6              4    2    2        2    3    3
  Multiplicidad[-x0   + 4 x0   x1 x2 - 6 x0   x1   x2   + 4 x0   x1   x2   -

     4    4        7
   x1   x2   + x1 x2 , {x0, x1, x2}, Explosiones`Private`z1$2411]}
```

```
ArbolExplosion[Expand[x1^3 (x1-x0)^4 - x2^6 x0 ],
{x0,x1,x2},{1,0,0}]
```



- Graphics -

```
ArbolExplosion[Expand[x1^3 (x1-x0)^4 - x2^6 x0 ],
{x0,x1,x2},{1,1,0}]
```

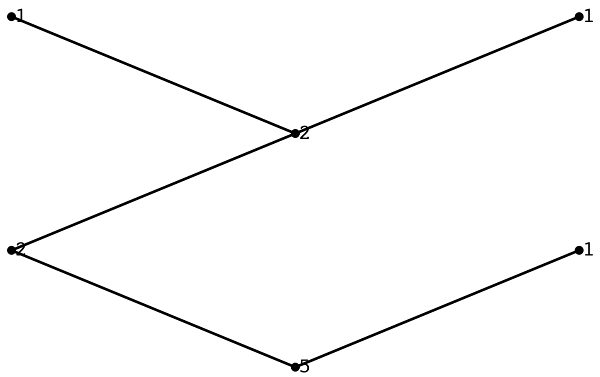


-Graphics-

```
AEMTOTAL[-x1^5*x0^2+x1^4*x2*x0^2+x2^7,
{x0,x1,x2},{1,0,0}]
```

```
{5}
{2, 1}
{{2}, {}}
{{{1, 1}}, {}}
```

```
ArbolExplosion[-x1^5*x0^2+x1^4*x2*x0^2+x2^7,
{x0,x1,x2},{1,0,0}]
```



-Graphics-

```
AEMTOTAL[x1^4+x1^2 x2^2-2x1^2 x2 x0-x1 x2^2 x0+x2^2 x0^2,
{x0,x1,x2},{1,0,0}]
```

```
{2}
{2}
{{1}}
```

```
AEMTOTAL[x1^4+x1^2 x2^2-2x1^2 x2 x0-x1 x2^2 x0+x2^2 x0^2,
{x0,x1,x2},{1,1,1}]
```

```
{1}
{1}
```

```
ArbolExplosion[x1^4+x1^2 x2^2-2x1^2 x2 x0-x1 x2^2 x0+x2^2 x0^2,
{x0,x1,x2},{1,1,1}]
```


```
-Graphics-
```

```
Sing[u^6 - 2*u^3*v^3 + v^6 - 2*u^3*w^3 -

     2*v^3*w^3 + w^6,{u,v,w}]
```

```
Solve::svars: Warning: Equations may not give solutions for all "solve"
     variables.

Solve::svars: Warning: Equations may not give solutions for all "solve"
     variables.

Solve::svars: Warning: Equations may not give solutions for all "solve"
     variables.

General::stop:
   Further output of Solve::svars
     will be suppressed during this calculation.
```

$$\{\{v, v, 0\}, \{-((-1)^{1/3} v), v, 0\}, \{(-1)^{2/3} v, v, 0\}, \{w, 0, w\}, \{-((-1)^{1/3} w), 0, w\}, \{(-1)^{2/3} w, 0, w\}, \{0, w, w\}, \{0, -((-1)^{1/3} w), w\}, \{0, (-1)^{2/3} w, w\}, \{0, 0, 0\}, \{0, 0, 0\}\}$$

```
AEMTOTAL[u^6 - 2*u^3*v^3 + v^6 - 2*u^3*w^3 -

     2*v^3*w^3 + w^6,{u,v,w},{1,1,0}]
```

```
{2}
{1}
```

```
AEMTOTAL[u^6 - 2*u^3*v^3 + v^6 - 2*u^3*w^3 -

     2*v^3*w^3 + w^6,{u,v,w},{1^(1/3),0,1}]
```

```
{2}
{1}
```

```
ArbolExplosion[u^6 - 2*u^3*v^3 + v^6 - 2*u^3*w^3 -

     2*v^3*w^3 + w^6,{u,v,w},{1^(1/3),0,1}]
```


```
-Graphics-
```

```
In[1]:= GroebnerBasis[{x^3 - 2 x y, x^2 y - 2 y^2 + x}, {x, y}, MonomialOrder → DegreeLexicographic]
```

Out[1]= $\{-x + 2 y^2, x y, x^2\}$

```
In[2]:= GroebnerBasis[{2 x + y + z, x + 2 y - z}, {x, y, z}]
```

Out[2]= $\{y - z, x + z\}$

```
(*Por defecto siempre usa el orden lexicográfico,
las otras posibilidades son DegreeLexicographic, o DegreeReverseLexicographic*)
(* Para polinomios en una variable,
calcular una base de Groeber es lo mismo que calcular el MCD
 luego esta función produce el mismo resultato que PlynomialGCD*)
(*Para polinomios lineales en cualquier número de variables,
el cálculo de una base de Groebner reducida es
 el mismo que el del método de eliminación de Gauss*)
(*Esta función siempre da bases de Groebner REDUCIDAS*)

(*El conjunto de polinomios en la base de Grobner tiene
 la misma coleccion de raices de los polinomios originales*)
```

Una base de Gröbner con el orden lexicográfico :

```
In[3]:= polys = {x^2 + y^2 + z^2 - 1, x - z + 2, z^2 - x y};

In[4]:= GroebnerBasis[polys, {x, y, z}]
```

Out[4]= $\{12 - 28 z + 27 z^2 - 12 z^3 + 3 z^4, -6 + 4 y + 11 z - 6 z^2 + 3 z^3, 2 + x - z\}$

Base de Gröbner con el orden lexicográfico inverso:

```
In[5]:= GroebnerBasis[polys, {x, y, z}, MonomialOrder → DegreeReverseLexicographic]
```

Out[5]= $\{2 + x - z, -2 y + y z - z^2, 3 + y^2 - 4 z + 2 z^2, -6 + 4 y + 11 z - 6 z^2 + 3 z^3\}$

Eliminación de una variable:

```
In[6]:= GroebnerBasis[{x^2 + y^2 + z^2 - 1, x y - z + 2, z^2 - 2 x + 3 y}, {x, y}, {z}]
```

Out[6]= $\{28 + 8 y + 41 y^2 - 26 y^3 + 55 y^4 - 8 y^5 + 7 y^6 - 6 y^7 + y^8,$
$16 + 20 x - 10 y + 28 y^2 - 57 y^3 + 4 y^4 - 6 y^5 + 6 y^6 - y^7\}$

```
In[7]:= GroebnerBasis[polys, ParameterVariables → x]
```

$\{2 + 8 x + 113 x^2 + 212 x^3 + 938 x^4 + 364 x^5 + 1980 x^6 - 1000 x^7 + 1625 x^8,$
$-289\,274 - 1\,958\,323 x - 7\,458\,871 x^2 - 14\,140\,053 x^3 - 20\,245\,223 x^4 - 19\,904\,560 x^5 +$
$4\,016\,500 x^6 - 24\,451\,375 x^7 + 202\,126 z, -46\,518 + 1\,236\,672 x + 1\,655\,875 x^2 +$
$15\,987\,939 x^3 + 2\,473\,650 x^4 + 39\,330\,525 x^5 - 23\,125\,875 x^6 + 31\,086\,250 x^7 + 202\,126 y\}$

Out[7]= $\{16 + 32 x + 27 x^2 + 12 x^3 + 3 x^4, -2 - x + z, 16 + 23 x + 12 x^2 + 3 x^3 + 4 y\}$

Out[8]= $\{2 + 8 x + 113 x^2 + 212 x^3 + 938 x^4 + 364 x^5 + 1980 x^6 - 1000 x^7 + 1625 x^8,$
$-289\,274 - 1\,958\,323 x - 7\,458\,871 x^2 - 14\,140\,053 x^3 - 20\,245\,223 x^4 - 19\,904\,560 x^5 +$
$4\,016\,500 x^6 - 24\,451\,375 x^7 + 202\,126 z, -46\,518 + 1\,236\,672 x + 1\,655\,875 x^2 +$
$15\,987\,939 x^3 + 2\,473\,650 x^4 + 39\,330\,525 x^5 - 23\,125\,875 x^6 + 31\,086\,250 x^7 + 202\,126 y\}$

Resolución de ecuaciones polinómicas:

```
In[9]:= polys = {x^2 + y^2 - 1, y^3 - 2*x*y - 3};
```

Una base Gröbner posee las mismas raíces que el conjunto inicial de polinomios

In[14]:=
```
gb = GroebnerBasis[polys, {y, x}]
```

Out[14]= $\{8 + 4 x - x^2 - 8 x^3 + x^4 + 4 x^5 + x^6, -1 + 2 x + 2 x^2 - 2 x^3 - x^4 + 3 y\}$

Resolvemos el primer polinomila de la base en la variable *x*:

In[15]:=
```
solx = Solve[gb[[1]] == 0, x]
```

Out[15]=
```
{{x → Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 1]},
 {x → Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 2]},
 {x → Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 3]},
 {x → Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 4]},
 {x → Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 5]},
 {x → Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 6]}}
```

Y después el segundo polinomio en la variable *y*:

In[16]:=
```
soly = Solve[gb[[2]] == 0, y]
```

Out[16]= $\left\{\left\{y \to \frac{1}{3}\left(1 - 2 x - 2 x^2 + 2 x^3 + x^4\right)\right\}\right\}$

Raíces comunes del conjunto de polinomios *polys*:

In[17]:=
```
RootReduce[(polys /. soly) /. solx]
```

Out[17]= {{{0, 0}}, {{0, 0}}, {{0, 0}}, {{0, 0}}, {{0, 0}}, {{0, 0}}}

`Reduce` y `Solve` usan las basses de Gröbner para resolver los sistemas de ecuciones:

In[18]:=
```
Reduce[Thread[polys == 0], {x, y}]
```

Out[18]=
```
(x == Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 1] ||
   x == Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 2] ||
   x == Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 3] ||
   x == Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 4] ||
   x == Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 5] ||
   x == Root[8 + 4 #1 - #1^2 - 8 #1^3 + #1^4 + 4 #1^5 + #1^6 &, 6]) && y == 1/3 (1 - 2 x - 2 x^2 + 2 x^3 + x^4)
```

Universidad de Salamanca
Departamento de MATEMÁTICAS
Plaza de la Merced 1–4
37008–SALAMANCA

ÁLGEBRA CONMUTATIVA Y COMPUTACIONAL. Diciembre 2010

Contestar razonadamente las cuestiones que no sean de tipo test:

1. Sea M el $\mathbb{Z}$-módulo definido por M=$\mathbb{Z}\oplus\mathbb{Z}/\langle(3,5)\rangle$. Entonces, sólo una de las afirmaciones siguientes es cierta:

(a) M es de torsión.
(b) M tiene rango 1.
(c) La localización de M en el punto genérico es cero.
(d) M no es un módulo plano.

2. Sea A un anillo noetherino y sea $B = A[x]/(x^2-1)$. Entonces,

(a) B es noetheriano como A-módulo y como $A[x]$-módulo.
(b) B es noetheriano como A-módulo, pero no como $A[x]$-módulo.
(c) B es noetheriano como $A[x]$-módulo, pero no como A-módulo.
(d) B no es noetheriano ni A-módulo ni como $A[x]$-módulo.

3. Sea M un A-módulo libre y finito generado y $N \subseteq M$ un submódulo suyo. ¿Cuál de las siguientes afirmaciones es cierta?

(a) N es libre.
(b) N es libre y finito generado.
(c) N es finito generado.
(d) N no tiene porque ser ni libre ni finito generado.

4. Sea M un A-módulo y $N_1, N_2 \subseteq M$ dos submódulos tales que $M = N_1 + N_2$. ¿cúal de los siguientes enunciados es correcto?

(a) M es noetheriano si y sólo si N_1 y N_2 son noetherianos.
(b) Si M es noetheriano, sólo uno de los submódulos es noetheriano.
(c) Si N_1 o N_2 es noetheriano, entonces M es noetheriano.
(d) M puede ser noetheriano y que no lo sean ni N_1 ni N_2.

5. Sea $A = k[x, y, z]/(xy - z^2)$ y sea $\alpha = (x, z)^2$. Sólo una de las siguientes afirmaciones es cierta:

(a) α es un ideal primo de A.
(b) α no es un ideal primo de A, pero es primario.
(c) α no es un ideal primo de A

6. Si A es un anillo, entonces,

(a) $l_A(A) = 1$ siempre.
(b) $l_A(A) = 1$ si y sólo si A es un cuerpo.
(c) $l_A(A) = 1$ si y sólo si A es un dominio de ideales principales.

7. ¿Cuál de las siguientes afirmaciones es falsa?

(a) El espectro de un anillo es irreducible si y sólo si tiene un punto denso.
(b) Si el espectro de un anillo no es conexo, entonces el anillo es producto directo de otro dos.
(c) El espectro de un anillo es irreducible si y sólo si el radical del anillo es un ideal maximal.

(d) Un anillo es íntegro si y sólo si es reducido y su espectro es irreducible.

8. Sea $I = (f_1, f_2) = (y - x^2, z - x^3) \subset k[x, y, z]$. Si se considera en $k[x, y, z]$ el orden lexicográfico, demostrar que f_1, f_2 no es una base de Gröebner de I.

9. Calcular el espectro $Spec\mathbb{Z}[i] = \mathbb{Z}[x]/x^2 + 1$ de los enteros de Gauss.

10. Sea A un anilllo tal que el ideal (0) es producto $\mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_r$ de ideales maximales. Demostrar que A es noetheriano si y sólo si es aritiniano.

Universidad de Salamanca

Departamento de MATEMÁTICAS
Plaza de la Merced 1–4
37008–SALAMANCA

AMPLIACIÓN ÁLGEBRA CONMUTATIVA. 3^0 GRADO MATEMÁTICAS.

30/03/2011

1. Sea X una variedad algebraica afín de dimensión 3 y $S(n) = 5/12n^3 - 2/3n^2 - 3n + 1/5$ un polinomio. ¿Puede ocurrir que $S(n)$ sea el polinomio de Samuel del anillo local de algún punto cerrado de X?
a) Depende de que el punto sea no singular.
b) Sí, si el punto es singular de multiplicidad 5.
c) Sí, porque el grado del polinomio coincide con la dimensión.
d) No.

2. Sean A, B anillos noetherianos y $f\colon A \to B$ morfismo de anillos tal que $f^{-1}(\mathfrak{p}) = \mathfrak{p}'$. Sean $G(f)$ y $\hat{f}$ los morfismos inducidos entre los correspondientes graduados y completados, respectivamente. Sólo una de las siguientes afirmaciones es cierta:
a) Si $G(f)$ es isomorfismo, entonces f es isomorfismo.
b) Si $\hat{f}$ es isomorfismo, entonces f es isomorfismo.
c) Si $G(f)$ es isomorfismo, entonces $\hat{f}$ es isomorfismo.
d) Si $\hat{f}$ es isomorfismo, entonces el morfismo inducido $f\colon A_{\mathfrak{p}'} \to B_{\mathfrak{p}}$ es isomorfismo.

3. Sea A una k-álgebra finito generada y $\mathfrak{m} \subset A$ un ideal maximal tal que el polinomio de Samuel en dicho punto es $S_{\mathfrak{m}}A_{\mathfrak{m}}(n) = \frac{1}{3}n^3 + n^2$. Sólo una de las siguientes afirmaciones es falsa:
a) $m(A_{\mathfrak{m}}) = 1$.
b) $m(A_{\mathfrak{m}}) = 2$.
c) $\dim A_{\mathfrak{m}} = 3$.
d) $\dim A = 3$.

4. Sea X una curva algebraica plana y $x \in X$ un punto tal que su maximal tiene un sistema mínimo de generadores formado por 2 elementos.
a) El punto x es no singular.
b) La multiplicidad del punto x tiene que ser 1.
c) La multiplicidad del punto x tiene que ser mayor que 1.
d) El polinomio de Samuel del anillo local del punto x tiene grado 2.

5. Sea $\mathcal{O}$ un anillo local noetheriano tal que su maximal $\mathfrak{m}$ tiene un sistema mínimo con 3 generadores. Entonces siempre se verifica que:
a) Si $\dim \mathcal{O} = 3$, entonces $G_{\mathfrak{m}}\mathcal{O} \simeq \mathcal{O}/\mathfrak{m}[x_1, x_2, x_3]$.
b) $\dim \mathcal{O} = 3$.
c) $S_{\mathfrak{m}}\mathcal{O}(n) = \frac{1}{3}n^3 + ...$
d) $\dim \hat{\mathcal{O}} = 3$.

6. Sea A un anillo noetheriano y $\mathfrak{m}$ un ideal maximal. ¿Es cierto que el completado $\mathfrak{m}$-ádico de A es un anillo local? Razónese la respuesta.

7. Sea $\mathcal{O}$ un anillo local noetheriano de dimensión 2 y $\mathfrak{m}$ su maximal. Sea $S_{\mathfrak{m}}\mathcal{O}(n) = 3n + 1$ el polinomio de Samuel de $\mathcal{O}$ respecto $\mathfrak{m}$. ¿Si α es un ideal $\mathfrak{m}$-primario, necesariamente su polinomio de Samuel es $S_\alpha\mathcal{O}(n) = 3n + a$ con $a \in \mathbb{Q}$? Razónese la respuesta. ¿Qué sucede si $\alpha = \mathfrak{m}^2$?

8. Sea $A = k[x, y, z]/(P(x, y, z), Q(x, y, z))$. ¿Necesariamente la dimensión de A es 1? Razónese la respuesta y en caso negativo, poner un contraejemplo.

9. ¿Es cierto que si A es una k-álgebra finito generada, entonces para todo ideal primo $\mathfrak{p}$ se verifica que $dimA = h(\mathfrak{p}) + dimA/\mathfrak{p}$? Razónese la respuesta.

10. Sea A una k-álgebra y $\mathfrak{m}$ un ideal maximal de A. Si $k(\mathfrak{m})$ es su cuerpo residual, ¿es cierta la siguiente sucesión exacta?

$$\mathfrak{m}/\mathfrak{m}^2 \longrightarrow \Omega_{A/k} \otimes_A k(\mathfrak{m}) \longrightarrow \Omega_{k(\mathfrak{m})/k} \longrightarrow 0$$

¿Qué sucede si $\mathfrak{m}$ es un punto racional? Razónese la respuesta.

Universidad de Salamanca

Departamento de MATEMÁTICAS
Plaza de la Merced 1–4
37008–SALAMANCA

AMPLIACIÓN ÁLGEBRA CONMUTATIVA. 3^0 MATEMÁTICAS. 27/05/2011

1. Sea A, B son anillos noetherianos, $i\colon A \hookrightarrow B$ un morfismo finito y $f\colon SpecB \to SpecA$ el morfismo inducido entre espectros.
a) La imagen por f de un punto es un punto cerrado.
b) Todas las fibras de f tienen un número finito de puntos.
c) Las fibras de f no tienen porqué ser finitas.
d) i induce un isomorfismo entre los cuerpos de fracciones de A y B.

2. Sea A una k-álgebra finito generada de dimensión 2. Sólo una de las siguientes afirmaciones es falsa:
a) A puede tener un ideal primo principal.
b) Existe un morfismo finito $SpecA \to \mathbb{A}^3$.
c) Existe un morfismo finito $SpecA \to \mathbb{A}^2$.
d) Existe un morfismo $SpecA \to \mathbb{A}^1$.

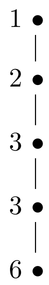
3. Sea $i\colon A \hookrightarrow B$ un morfismo entre anillos. Sólo una de las siguientes afirmaciones es falsa:
a) Si i es finito, entonces $\dim A = \dim B$.
b) Si i es entero, entonces $\dim A = \dim B$.
c) Si i es finito, entonces es entero.
d) Si i es entero, entonces es finito.

4. Sea $\mathcal{O}$ un anillo local noetheriano íntegro tal que para todo morfismo dominante $\mathcal{O} \hookrightarrow \mathcal{O}'$ es isomorfismo. Sólo una de las siguientes afirmaciones es falsa:
a) $\mathcal{O}$ es un anillo de valoración.
b) $\mathcal{O}$ es íntegramente cerrado.
c) $\mathcal{O}$ es regular.
d) Si $\mathcal{O}$ es de dimensión 1, entonces es un anillo principal.

5. Sea $i\colon A \hookrightarrow B$ un morfismo finito tal que $A_{(0)} \simeq B_{(0)}$. Sea $\bar{A}$ el cierre entero de A.
a) $B \subseteq \bar{A}$.
b) $\bar{A} \subseteq B$.
c) A es íntegramente cerrado.
d) Si i es isomorfismo, A es íntegramente cerrado.

6. Sea A una k-álgebra finito generada íntegra de dimensión 1 de cuerpo de fracciones Σ. Sea $\bar{A}$ su cierre entero. Sólo una de las siguientes afirmaciones es falsa:
a) Si A es regular, entonces $\bar{A} = \cap_{x \in \operatorname{Spec} A} A_x$.
b) Todo anillo de valoración sobre Σ que contiene a A centre en un único punto de A.
c) Todos los anillos locales de A son anillos de valoración.
d) $\bar{A} = \cap_{A \subset \mathcal{O}} \mathcal{O}$, con $\mathcal{O}$ anillos de valoración sobre Σ

7. Sea X una curva plana íntegra con árbol de explosión en un punto x:



Entonces:

a) El contacto maximal del punto x es 12.

b) El contacto maximal del punto x es 14.

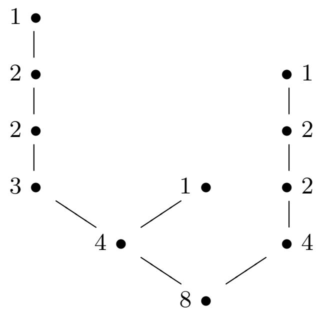
c) El número de direcciones tangentes en x es 1.

d) Existe una curva C no singular en x con $(X \cap C)_x = 15$.

8. Definición de anillo de valoración y de valoración sobre un cuerpo. ¿Existe una correspondencia biyectiva entre ellos?

9. Sea A una k-álgebra finito generada íntegra y $\bar{A}$ su cierre entero. ¿Es cierto que para cada $b \in \bar{A}$, todo anillo de valoración sobre el cuerpo de fracciones de A contiene a b?

10. Contestar razonadamente si puede existir una curva con árbol de explosión en un punto el siguiente árbol:



AMPLIACION ALGEBRA CONMUTATIVA (SOLUCIONES test 05/11)

1. b) ; **2. b)** ; **3. d)** ; **4. c)** ; **5. a)** ; **6. c)** ; **7. c)** ;
8. Sí, módulo las valoraciones equivalentes) ;
9. No, porque el cierre entero es la intersección de todos los anillos de valoración que contiene a A ;
10. No, porque $3 \leq 2 + 2$.