INTRODUCCIÓN A LA TEORÍA DE ELIMINACIÓN

NICOLÁS BOTBOL

Resumen. El objeto de estudio de estas notas es la teoría de eliminación, y en particular, nos concentraremos en estudiar resultantes. Cuando hablamos de resultantes, precisamente nos referimos a resultantes homogéneas en el espacio proyectivo, que llamaremos, resultante de Macaulay. Esta resultante surge como una generalización de la resultante de Sylvester para dos polinomios univariados.

Dado un conjunto de n polinomios homogéneos $f_1, \dots, f_n$ en n variables con coeficientes en un anillo A, introduciremos la noción de ideal eliminante, $\mathfrak{A}$ de A, que resultará bajo ciertas condiciones un ideal principal, y cuyo generador llamaremos Resultante homogénea de $f_1, \dots, f_n$. Veremos que el conjunto de ceros de $\mathfrak{A}$ en $\mathrm{Spec}(A)$ parametriza los coeficientes para los cuales los polinomios $f_1, \dots, f_n$ tienen un cero común.

Veremos además que esta resultante puede ser calculada como el determinate de un complejo de A-módulos y que además coincide con la parte en codimensión 1 de un ideal de menores maximales de una cierta matriz M, que se lo conoce como ideal inicial de Fitting de M.

Índice

Date: 1 de julio de 2012.

1991 *Mathematics Subject Classification.* 13P15, 13P20, 13D02, 13D45, 14Q10.

Partially supported by UBACYT 20020100100242, CONICET PIP 112-200801-00483, and ANPCyT PICT 2008-0902.

Introducción

El objeto de estudio de estas notas es la teoría de eliminación, y en particular, nos concentraremos en estudiar resultantes. Cuando hablamos de resultantes, precisamente nos referimos a resultantes homogéneas en el espacio proyectivo, que llamaremos, resultante de Macaulay. Esta resultante surge como una generalización de la resultante de Sylvester para dos polinomios univariados, que repasaremos en la Sección 1.

El contexto será el siguiente: A un anillo conmutativo con unidad que se supondrá casi siempre íntegro y noetheriano, $R = A[X_1, \dots, X_n]$ el anillo de polinomios con coeficientes en A con la graduación habitual, donde $\deg(X_i) = 1$ y $\deg(a) = 0$ para todo $a \in A$ y R_+ su ideal irrelevante de elementos de grado positivo. Sea $f_1, \dots, f_n$ una sucesión regular de n polinomios homogéneos, con $\deg(f_i) = d_i > 0$, e $I = (f_1, \dots, f_n)$.

El anillo cociente $B = R/I$ es un anillo graduado, con la graduación heredada de R. El ideal homogéneo 0 de B, tiene una descomposición $0 = \mathfrak{p} \cap \mathfrak{q}$, donde $\mathfrak{q}$ es la componente R_+-primaria o componente irrelevante y $\mathfrak{p} = H^0_{R_+}(B)$ es un ideal homogéneo que se define pasando al cociente por I al ideal $\mathrm{TF}_{R_+}(I)$ de *formas de inercia* de I en R.

Escribamos $\overline{B} := B/H^0_{R_+}(B)$. Naturalmente, los subesquemas cerrados de $\mathrm{Proj}(R)$ definidos por $\mathrm{Proj}(B)$ y $\mathrm{Proj}(\overline{B})$ coinciden. Además, llamando B_ν y $\overline{B}_\nu$ a las partes homogéneas de grado ν, se tiene que $B_\nu = \overline{B}_\nu$ si ν es suficientemente grande. Precisamente, para que B_ν y $\overline{B}_\nu$ coincidan, basta encontrar un valor ν_0 tal que $H^0_{R_+}(B)_\nu = 0$ si $\nu \geq \nu_0 := \sum_i (d_i - 1) + 1$, que llamaremos índice de saturación de I (el estudio del valor ν_0 está contenido en la última parte del Apéndice B, dedicado a la regularidad de Castelnuovo-Mumford).

Como R es un anillo graduado sobre A, $\mathrm{Proj}(R)$ es un esquema proyectivo sobre $\mathrm{Spec}(A)$, y también lo es $\mathrm{Proj}(B) = \mathrm{Proj}(\overline{B})$. Llamando π a la proyección $\pi : \mathrm{Proj}(R) \to \mathrm{Spec}(A)$, así como a la proyección inducida $\pi : \mathrm{Proj}(B) \to \mathrm{Spec}(A)$, obtenemos que la imagen de $\mathrm{Proj}(B)$ por π está dada por el *ideal eliminante* $H^0_{R_+}(B) \cap A = H^0_{R_+}(B)_0$, que denotaremos por $\mathfrak{A}$. Esto será estudiado en detalle en la Sección 2, donde además probaremos el Teorema Principal de Eliminación, Teorema 2.7, que establece la relación entre el ideal de coeficientes $\mathfrak{A}$ y la existencia de ceros comunes de I para esos coeficientes.

Mejor que el ideal de eliminación $\mathfrak{A}$, es el ideal de Fitting $\mathfrak{F} := \mathrm{Fitt}_0(B_\nu)$ con $\nu \geq \nu_0$ (típicamente $\nu = \nu_0$), ya que no sólo es principal en codimensión 1, con el mismo

conjunto de ceros que $\mathfrak{A}$, sino que además verifica propiedades funtoriales muy convenientes, como ser estable por cambios de base. Además, su parte de codimensión 1 puede ser calculado mediante un producto alternado de determinantes.

Como lo señaló Jouanolou, Hurwitz demostró en 1913 (ver [Hur13]) que, en el caso de polinomios homogéneos genéricos $f_1, \ldots, f_r$ -y este será nuestro contexto- el complejo Koszul es acíclico en grados positivos si el número de polinomios r es menor o igual al número de variables n, ya que forman una sucesión regular. Desde alrededor de 1930 se sabe que las resultantes homogéneas se pueden calcular como el invariante de McRae de este complejo, y a esto es a lo que nos referíamos al decir que la parte de codimensión 1 de $\mathfrak{F} := \mathrm{Fitt}_0(B_\nu)$ con $\nu \geq \nu_0$ puede ser calculado mediante un producto alternado de determinantes, que vienen de los diferenciales de este complejo de Koszul graduado, en grado ν con $\nu \geq \nu_0$.

En la Sección 3 recordaremos la definición de este complejo, y desarrollaremos las herramientas necesarias para nuestras aplicaciones. En la Sección 4 veremos, en el Teorema 4.1 que el ideal $\mathfrak{A}$ es primo y principal y que por lo tanto define una subvariedad de $\mathrm{Spec}(A)$ de codimensión 1. Luego, probaremos que $\mathfrak{A} = \mathrm{ann}_A(B_\nu)$ si $\nu \geq \nu_0$, es decir, que es un A-módulo de torsión. Al final de esa sección, mostraremos que (con hipótesis) todo A-módulo M de torsión define un divisor $\mathrm{div}(M)$, y que dada una resolución libre de M, este divisor puede ser calculado mediante un producto alternado de determinantes. Como mencionamos, esta resolución será el complejo de Koszul de $f_1, \ldots, f_r$ en grado $\nu \geq \nu_0$. En la Sección 5 definiremos y estudiaremos los ideales de Fitting mencionados, así como el invariante de MacRae, lo que completará el estudio de la resultante de Macaulay.

Es importante entender la diferencia que estamos marcando entre los ideales $\mathfrak{A}$ y $\mathfrak{F}$: Mientras que el primero es principal e irreducible y describe la *imagen cerrada de* $\pi : \mathrm{Proj}(B) \to \mathrm{Spec}(A)$, el segundo no lo será y describe la *imagen de Fitting de* π, pero el divisor asociado a $\mathfrak{F}$ coincide con $\mathfrak{A}$ lo cual dice que la parte en codimensión 1 de $V(\mathfrak{F})$ coincide con $V(\mathfrak{A})$, y en particular como conjuntos también coinciden.

Como ya se dijo, a lo largo de estas notas, estudiaremos la relación y propidades de estos dos ideales, ya que, como mencionamos, el primero es más intuitivo geométricamente, pero el segundo presenta mejores propiedades algebraicas. Un estudio más detallado sobre imágenes cerradas e imágenes de Fitting se puede encontrar en [EH00, Cap. V].

Notación. En estas notas, los anillos serán todos conmutativos y con unidad, éstas son hipótesis habituales en el área, aunque parte de la teoría pueda desarrollarse sin ellas.

Cuando llamemos A a un anillo, en general estaremos pensando en que A es el anillo de coeficientes universales $\mathbb{Z}[\{U_{i,\alpha}\}]$ o un anillo de coeficientes arbitrario, pero esto es simplemente una intuición que debería ayudar al lector a entender la geometría de fondo. En general A no será provisto de una graduación, y por lo tanto el esquema que le asociaremos será $\mathrm{Spec}(A)$. Cuando querramos indicar que A es un cuerpo, comúnmente escribiremos k en lugar de A.

El anillo R, por lo general será un anillo de polinomios en n variables X_i, con coeficientes en A o en k. Nos interesará dotar a R de la graduación habitual, donde $\deg(X_i) = 1$ y $\deg(a) = 0$ para todo $a \in A$. Esta graduación nos permitirá definir en R el ideal maximar irrelevante de elementos de grado positivos $R_+ := (X_1, \ldots, X_n)$ y

geométricamnte le asociamos a R el esquema proyectivo $\mathrm{Proj}(R)$ que se escribe $\mathbb{P}^{n-1}_A$ o $\mathbb{P}^{n-1}_k$ según corresponda.

Notaremos con $f_1, \dots, f_r$ al conjunto de R polinomios homogéneos, en n variables X_i, con coeficientes en A, es decir, elementos homogéneos de R. Típicamente f_i tendrá grado d_i, es decir, $f_i \in R_{d_i}$. Estudiaremos principalmente el caso en que $r = n$, y que forman una sucesión regular en R. Esto dice que el cociente $B := R/I$ es una intersección completa.

Frecuentemente escribiremos,

$$f_i = \sum_{|\alpha|=d_i} u_{\alpha,i} X^\alpha$$

con $u_{\alpha,i} \in A$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $|\alpha| = \alpha_1 + \cdots + \alpha_n$, $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ y $f_{\alpha,i} \in A$ para todo α y todo i. También nos permitiremos reemplzar las $u_{\alpha,i}$ por $U_{\alpha,i}$, cuando querramos indicar que son variables. Es decir, la diferencia radica en que en el primer caso tenderíamos a creer que están especializadas y que A es un anillo de coeficientes cualquiera, mientras que en el segundo no lo están y $A = \mathbb{Z}[\{U_{i,\alpha}\}]$ es el anillo de coeficintes universales.

En cualquier caso, escribamos $I := (f_1, \dots, f_r) \subset R_+$, ideal homogéneo de R, y $B := R/I$. Como I es homogéneo, B es un R-módulo graduado, con la graduación heredada de R. Escribiremos $\mathrm{Proj}(B)$ para denotar el subesquema de $\mathrm{Proj}(R)$ definido por I, que comúnmente se escribe $V(I)$.

Más en general, dado un ideal J de un anillo S, escribiremos $V(J)$ par denotar $\mathrm{Spec}(S/J)$. También, si S fuera un anillo graduado estándar y J homogéneo, $V(J)$ podrá denotar $\mathrm{Proj}(S/J)$. Esta notación es habitual y hace referencia a la intuición de pensar $V(J)$ como una subvariedad del espacio afín o proyectivo asociado al anillo de polinomios S definida por "los ceros" de f, donde f recorre todos los elementos de J.

1. Resultante univariada

En esta primera parte, estudiaremos la resultante de dos polinomios univariados y de dos polinomios homogéneos en dos variables. Esta teoría clásica que data del siglo XIX nos permitirá comprender con facilidad el contexto geométrico y algebraico de la teoría de eliminación general, así como de remarcar el caracter universal de la resultante.

1.1. Definición. Sea A un anillo conmutativo con unidad. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Escribamos

$$f_1(X) = \sum_{i=0}^{d_1} a_i X^i, \text{ y } f_2(X) = \sum_{i=0}^{d_2} b_i X^i. \tag{1.1}$$

A estos dos polinomios les asociamos la matriz Sylvester definida como sigue.

Definición 1.1. Sean A un anillo conmutativo con unidad, $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$, como en (1.1). La matriz

$$\mathrm{Syl}(f_1, f_2) = \begin{pmatrix} a_{d_1} & 0 & \cdots & 0 & b_{d_2} & 0 & \cdots & 0 \\ a_{d_1-1} & a_{d_1} & & \vdots & \vdots & b_{d_2} & & \vdots \\ \vdots & a_{d_1-1} & \ddots & 0 & b_0 & \vdots & \ddots & \\ a_0 & \vdots & & a_{d_1} & 0 & b_0 & & 0 \\ 0 & a_0 & & a_{d_1-1} & \vdots & 0 & \ddots & b_{d_2} \\ \vdots & & \ddots & \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

de $(d_1 + d_2) \times (d_1 + d_2)$ con coeficientes en A, se llama *matriz de Sylvester* de f_1, f_2.

Definición 1.2. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Definimos la *Resultante de Sylvester* de f_1, f_2, como

$$\mathrm{Res}_X(f_1, f_2) = \det(\mathrm{Syl}(f_1, f_2))$$

1.2. Propiedades elementales. Los polinomios f_1, f_2 definen un morfismo de A-módulos

$$\begin{array}{ccc} A[X]_{<d_2} \oplus A[X]_{<d_1} & \xrightarrow{\partial} & A[X]_{<d_1+d_2} \\ (h_1, h_2) & \mapsto & h_1 f_1 + h_2 f_2 \end{array} \tag{1.2}$$

En estos términos, la Proposición 1.3 dice que $\mathrm{Res}_X(f_1, f_2) \in \mathrm{im}(\partial)$. Además, es fácil ver que la matriz de ∂ en bases canónicas coincide con la matriz $\mathrm{Syl}(f_1, f_2)$ (ver ejercicio 2).

Proposición 1.3. *Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Entonces, existen dos polinomios h_1, h_2 tales que $\deg(h_i) < d_i$, $i = 1, 2$ y $\mathrm{Res}_X(f_1, f_2) = f_1 h_1 + f_2 h_2 \in A[X]$.*

Demostración. Es inmediato verificar que se tiene la siguiente igualdad de vectores

$$(X^{d_1+d_2-1}, X^{d_1+d_2-1}, \ldots, X, 1)\,\mathrm{Syl}(f_1, f_2) = (X^{d_2} f_1, \ldots, X f_1, f_1, X^{d_1} f_2, \ldots, X f_2, f_2)$$

Desarrollando la regla de Cramer se tiene que

$$\mathrm{Res}_X(f_1, f_2) \cdot 1 = \det M,$$

donde M es la matriz que se obtiene a partir de $\mathrm{Syl}(f_1, f_2)$ reemplazando la última fila por el vector $(X^{d_2} f_1, \ldots, X f_1, f_1, X^{d_1} f_2, \ldots, X f_2, f_2)$.

Calculando $\det(M)$ por la última fila, se tiene lo buscado. □

Para polinomios sobre un anillo íntegro, se tiene el sigueinte resultado, que es una de las motivaciones principales para el estudio de las resultantes.

Proposición 1.4. *Sea A un anillo íntegro con cuerpo de fracciones K. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$ y sea ∂ un morfismo de A-módulos como en (1.2). Entonces son equivalentes*

1. *∂ es inyectivo,*
2. *$\mathrm{Res}_X(f_1, f_2) \neq 0$,*
3. *f_1 y f_2 son coprimos en $K[X]$.*

Demostración. La equivalencia entre los puntos 1. y 2. se desprende del Ejercicio 3. Para ver que 1. y 3. son equivalentes, supongamos primero que f_1 y f_2 son coprimos en $K[X]$, y que existen polinomios h_1 y h_2 tales que $\deg(h_i) < d_i$, $i = 1, 2$, y $\partial(h_1, h_2) = 0$. Esto último dice que $h_1 f_1 = -h_2 f_2$, y entonces, $f_1 | h_2$ y $f_2 | h_1$, de lo cual se deduce, observando los grados, que $h_1 = h_2 = 0$. Si f_1 y f_2 no son coprimos en $K[X]$, entonces existe un polinomio h de grado positivo tal que $f_i = hg_i$, con $\deg(g_i) < \deg(f_i) = d_i$, $i = 1, 2$. Sea $d \in A$ el producto de los denominadores de g_1 y g_2. La no-inyectividad de ∂ se defuce del hecho que $0 = d(f_2 f_1 - f_1 f_2) = h(g_2 f_1 - g_1 f_2)$, es decir de que $0 \neq (g_2, -g_1) \in \ker(\partial)$. □

Como consecuencia de esto se tiene que $\mathrm{Res}_X(f_1, f_2) \neq 0$ si y solo si f_1 y f_2 tienen una raíz común en una extensión algebraica de K (ver Ejercicios 4 y 5).

Si introducimos una nueva variable Y para homogeneizar a los polinomios f_1, f_2, podemos definir la resultante homogénea de dos polinomios homogéneos bivaluados de la siguiente forma:

Definición 1.5. Sean $f_1, f_2 \in A[X, Y]$ dos polinomios homogeéneos de grado $d_1, d_2 > 0$. Definimos

$$\mathrm{Res}_{X,Y}(f_1(X, Y), f_2(X, Y)) := \mathrm{Res}_X(f_1(X, 1), f_2(X, 1)).$$

1.3. La universalidad de la resultante. Una de las propiedades más importantes de la resultante, es su carácter universal. Para ello, escribamos

$$f_1(X) = \sum_{i=0}^{d_1} a_i X^i, \text{ y } f_2(X) = \sum_{i=0}^{d_2} b_i X^i, \tag{1.3}$$

y sea $A = \mathbb{Z}[a_0, \ldots, a_{d_1}, b_0, \ldots, b_{d_2}]$ el anillo de polinomios en $d_1 + d_2 + 2$ variables, llamado *anillo de coeficientes universales* de f_1, f_2. Sea k un anillo conmutativo con unidad, y $\epsilon : A \to k$ un morfismo de anillos que se extiende a $\epsilon : A[X] \to k[X]$ poniendo $\epsilon(X) = X$.

Considere el siguiente diagrama:

$$\begin{array}{ccc} A[X] \times A[X] & \xrightarrow{\mathrm{Res}_X} & A \\ \downarrow{\scriptstyle \epsilon \times \epsilon} & & \downarrow{\scriptstyle \epsilon} \\ k[X] \times k[X] & \xrightarrow{\mathrm{Res}_X} & k \end{array} \tag{1.4}$$

La universalidad de la resultante se traduce a decir que el diagrama (1.4) conmuta, es decir que, dados dos polinomios $f_1, f_2 \in A[X]$ como en (1.3)

$$\mathrm{Res}_X(\epsilon(f_1), \epsilon(f_2)) = \epsilon \, \mathrm{Res}_X(f_1, f_2) \in k.$$

Esta propiedad de la resultante es una de las propiedades principales que desearemos conservar al extender la teoría al contexto multivaluado.

La intuición detrás de esta propiedad esencial es que una especialización de coeficientes corresponde a un morfismo de evaluación $\epsilon : A \to k$. Por ejemplo, si $\mathfrak{p}$ es un primo de A, podemos considerar el morfismo $\epsilon_\mathfrak{p}$ que resulta de la composición $A \to A_\mathfrak{p} \to \kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, donde el primero es el morfismo inyectivo de localización en $\mathfrak{p}$ y el segundo es pasar al cociente por el único ideal maximal de $A_\mathfrak{p}$. El morfismo $\epsilon_\mathfrak{p}$ corresponde a "una evalución". Esto es claro si $\mathfrak{p} = \mathfrak{m}$ es maximal, ya que en ese caso $\kappa(\mathfrak{m}) := A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} = A/\mathfrak{m}$. Interpretamos geométricamente al morfismo $\epsilon_\mathfrak{p}$ como la inclusión del punto $\mathrm{Spec}(\kappa(\mathfrak{p}))$ en $\mathrm{Spec}(A)$.

Gracias a esta universalidad, podremos concentrarnos en estudiar las propiedades de la resultante sobre el anillo de coeficientes universales $\mathbb{Z}[\{U_{i,\alpha}\}]$, y luego deducir propiedades en otros contextos mediante un cambio de base (o aplicando un morfismo de evaluación ϵ).

Ejercicios.

1. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Entonces $\operatorname{Res}_X(f_1, f_2) = (-1)^{d_1 d_2} \operatorname{Res}_X(f_2, f_1)$.
2. Probar que la matriz de ∂ definida en (1.2) en bases canónicas coincide con la matriz $\operatorname{Syl}(f_1, f_2)$ y deducir que $\operatorname{Res}_X(f_1, f_2) \in \operatorname{im}(\partial)$. Comparar con la Proposición 1.3.
3. Sea $\partial : A^n \to A^n$ un morfismo de A-módulos. Sea M la matriz de ∂ en dos bases cualesquiera de A^n. Entonces ∂ es inyectivo sii $\det(M) \neq 0$.
4. Sea A un anillo íntegro con cuerpo de fracciones K y sean $f_1, f_2 \in A[X]$. Entonces $\operatorname{Res}_X(f_1, f_2) \neq 0$ si y solo si f_1 y f_2 tienen una raíz común en una extensión algebraica de k.
5. Sea k un cuerpo y $f_1, f_2 \in k[X]$. Entonces, $\dim_k \ker \operatorname{Syl}(f_1, f_2) = \deg(\gcd(f_1, f_2))$

2. Teoría de Eliminación

En esta sección demostraremos el Teorema Principal de la Teoría de eliminación. Éste puede formularse en un lenguaje geométrico, como haremos en la primera parte, y en uno más algebraico como haremos más adelante. En la Sección 4 relacionaremos estos resultados con lo que llamaremos la resultante homogénea o resultante de Macaulay.

Sea A un anillo (conmutativo con unidad). Consideremos el anillo de polinomios $R := A[X_1, \ldots, X_n]$, con la $\mathbb{Z}$-graduación dada por $\deg(X_i) = 1$ para todo i y $\deg(a) = 0$ para todo $a \in A$, y escribamos $R_+ := (X_1, \ldots, X_n)$ el ideal irrelevante de R.

Sean $f_1, \ldots, f_r$ elementos homogéneos de R, con $\deg(f_i) = d_i$ para todo i. Concretamente, cada f_i se escribe de la forma

$$f_i = \sum_{|\alpha|=d_i} u_{\alpha,i} X^\alpha$$

con $u_{\alpha,i} \in A$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $|\alpha| = \alpha_1 + \cdots + \alpha_n$, $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ y $f_{\alpha,i} \in A$ para todo α y todo i.

Escribamos $I := (f_1, \ldots, f_r) \subset R_+$, ideal de R, y $B := R/I$. Como I es homogéneo, B es un R-módulo graduado, con la graduación heredada de R.

Antes de continuar, permitámosnos observar algunas propiedades del anillo cociente B que serán de utilidad.

Observación 2.1. Sea $B := R/I$ el anillo graduado, con $B_d = R_d/(I \cap R_d)$. Se tiene que

1. Como $I \cap A = 0$, entonces $B_0 = A$.
2. B está generado como anillo por A y B_1.
3. Para todo entero no-negativo d, B_d es un A-módulo finitamente generado.

Trabajaremos, frecuentemente en el contexto universal, es decir, supondremos que los coeficientes $u_{\alpha,i}$ son variables, que notaremos $U_{\alpha,i}$, y el anillo A será el anillo, $A := \mathbb{Z}[U_{\alpha,i} : i = 1, \ldots, r, |\alpha| = d_i]$, de *coeficientes universales* de los polinomios f_i.

2.1. El Teorema Principal de Eliminación geométricamente. Obsérvese que los elementos f_i son polinomios en las variables X_j, con coeficientes en A, con los cual A puede ser pensado como el anillo de coeficientes que parametriza al sistema $\{f_1 = \cdots = f_n = 0\}$, del cual queremos eliminar las variables X_j's.

Desde un punto de vista geométrico, siendo B un anillo graduado con coeficientes en A, se tiene que:

$$\mathrm{Proj}(B) \hookrightarrow \mathrm{Proj}(R) := \mathbb{P}^{n-1}_A = \mathbb{P}^{n-1}_{\mathbb{Z}} \times \mathrm{Spec}(A).$$

Esta inclusión de esquemas está inducida por el morfismo suryectivo de anillos $R \to B$ que consiste en pasar al cociente por I.

Asociado al espacio $\mathbb{P}^{n-1}_A$ hay una proyección natural $\pi : \mathbb{P}^{n-1}_A \to \mathrm{Spec}(A)$. La restricción de π a $\mathrm{Proj}(B)$, $\pi : \mathrm{Proj}(B) \to \mathrm{Spec}(A)$ define un subesquema (cerrado) de $\mathrm{Spec}(A)$, $Z := \pi(\mathrm{Proj}(B))$. El ideal de definición de Z en $\mathrm{Spec}(A)$, que notaremos $\mathfrak{A}$, está dado por el núcleo del morfismo natural de anillos asociado a la proyección π, es decir:

$$\mathfrak{A} := \ker(A \to \Gamma(\mathrm{Proj}(B), \mathcal{O}_{\mathrm{Proj}(B)})) = \ker(A \to \prod_i B_{(X_i)}) = (I :_R (R_+)^\infty) \cap A = H^0_{R_+}(B)_0.$$

La primera igualdad se deduce de que cada sección $s \in \Gamma(\mathrm{Proj}(B), \mathcal{O}_{\mathrm{Proj}(B)})$ está unívocamente determinada por sus restricciones a cada abierto afin $D^+(X_i) = \mathrm{Spec}(B_{(X_i)})$. La segunda y tercera igualdad es simplemente observar que

$$H^0_{R_+}(B) := \bigcup_{\ell \geq 1} (0 :_B (R_+)^\ell) = \ker(B \to \prod_i B_{(X_i)})$$

y que A se incluye en B en grado cero, es decir, que

$$\ker(A \to \prod_i B_{(X_i)}) = \ker(B \to \prod_i B_{(X_i)}) \cap A = H^0_{R_+}(B)_0.$$

A partir del razonamiento anterior concluimos que el proceso de eliminación consiste en calcular $H^0_{R_+}(B)_0$. Es interesante notar que $H^0_{R_+}(B) = (I :_R (R_+)^\ell)/I = I^{\mathrm{sat}}/I$, donde I^{sat} es la saturación de I respecto del ideal irrelevante R_+. El lector más familiarizado con la teoría de esquemas, podrá observar que los anillos B y $B/H^0_{R_+}(B)$ definen el mismo subesquema proyectivo de $\mathbb{P}^{n-1}_A$.

Definición 2.2. Definimos el *ideal eliminante de* I como

$$\mathfrak{A} := H^0_{R_+}(B)_0 = (I :_A (R_+)^\infty).$$

Si A es el anillo de polinomios $k[U_1, \ldots, U_m]$, $\mathrm{Spec}(A) = \mathbb{A}^m_k$ el espacio afín de dimesnión m sobre k. Sea $\mathbb{P}^{n-1}_k$ el espacio proyectivo de dimensión n sobre k. El espacio producto $\mathbb{P}^{n-1}_k \times \mathbb{A}^m_k$, viene provisto de sus dos proyecciones naturales, y nos centraremos en estudiar la proyección respecto de la segunda coordenada, que llamaremos π, definida como $\pi(x, y) = y \in \mathbb{A}^m_k$. Sea

$$W := \{(x, y) \in \mathbb{P}^{n-1}_k \times \mathbb{A}^m_k : f_i(x, y) = 0,\ \forall i\}$$

un subconjunto de $\mathbb{P}^{n-1}_k \times \mathbb{A}^m_k$.

Lo anteriormente dicho demuestra el siguiente resultado:

Corolario 2.3. *Con la notación precedente, se tiene que*

$$\pi(W) = V(\mathfrak{A}).$$

En la subsección siguiente daremos una herramienta necesaria para calcular un (el) generador del ideal eliminante $\mathfrak{A}$.

2.2. Sobre la R_+-torsión de B. Pasaremos ahora a dar una interpretación del ideal $\mathfrak{A}$ en término de anuladores.

Lema 2.4. *Se tiene la siguiente igualdad de ideales de A*

$$\mathfrak{A} := H^0_{R_+}(B)_0 = \bigcup_{\ell\geq 1} \operatorname{ann}_A(B_\ell).$$

Demostración. Para cada par $(\nu,\ell) \in \mathbb{Z}^2_{\geq 0}$, definimos el morfismo A-lineal

$$\Theta_{\nu,\ell} : B_\nu \to \operatorname{Hom}_A(B_\ell, B_{\nu+\ell})$$

definido por $\Theta_{\nu,\ell}(b) = (c \mapsto c\cdot b)$, con $b \in B_\nu$, $c \in B_\ell$ y $c\cdot b \in B_{\nu+\ell}$.

Como $H^0_{R_+}(B) := \bigcup_{\ell\geq 1}(0 :_B (R_+)^\ell)$, se tiene que para cada $\nu \geq 1$,

$$H^0_{R_+}(B)_\nu = \bigcup_{\ell\geq 1} \ker(\Theta_{\nu,\ell}). \tag{2.1}$$

Como $I \subset R_+$, entonces $A \cap I = 0$ y por lo tanto $B_0 = A$, con lo cual

$$\operatorname{ann}_A(B_\ell) = \ker(\Theta_{0,\ell}) \text{ para todo } \ell \geq 0. \tag{2.2}$$

A partir de (2.1) y (2.2) se tiene que $H^0_{R_+}(B)_0 = \bigcup_{\ell\geq 1} \operatorname{ann}_A(B_\ell)$. □

Obsérvese que como B está generado en grado 1 como se mencionó en la Observación 2.1, el morfismo de multiplicación $B_1 \otimes B_\ell \to B_{\ell+1} : c_1 \otimes c_\ell \mapsto c_1 c_\ell$ es suryectivo, y todo elemento $c \in B_{\ell+1}$ puede ser descompuesto como $c = \sum_i c_1^i \otimes c_\ell^i$. Con la notación del Lema 2.4 , dado $b \in \ker(\Theta_{\nu,\ell})$ se tiene que $bc = b(\sum_i c_1^i \otimes c_\ell^i) = \sum_i c_1^i \otimes bc_\ell^i = 0$ en $B_{\nu+\ell+1}$ y por lo tanto, se tiene para cada $(\nu,\ell) \in \mathbb{Z}^2_{\geq 0}$ la inclusión

$$\ker(\Theta_{\nu,\ell}) \subset \ker(\Theta_{\nu,\ell+1}).$$

Esto dice que $\operatorname{ann}_A(B_\ell) \subset \operatorname{ann}_A(B_{\ell+1})$ para todo $\ell \geq 0$, y por lo tanto $H^0_{R_+}(B)_0$ puede ser calculado mediante el colímite filtrante $\varinjlim_\ell \operatorname{ann}_A(B_\ell)$.

Una pregunta que surge en este punto es ¿Existe un valor de ℓ a partir del cual esta cadena ascendiente de anuladores se estaciona? ¿Cuál?

El siguiente resultado responde la primera pregunta, el Lema B.4 responde a la segunda cuando I está generado por una sucesión regular.

Lema 2.5. *Sea $\nu_0 \geq 0$ un entero tal que $H^0_{R_+}(B)_{\nu_0} = 0$. Entonces, para todo entero $\ell \geq 0$ se tiene que*

$$\operatorname{ann}_A(B_{\nu_0}) = \operatorname{ann}_A(B_{\nu_0+\ell}).$$

Demostración. A partir de (2.1), con la notación del Lema 2.4 y la hipótesis sobre ν_0, se tiene que

$$0 = H^0_{R_+}(B)_{\nu_0} = \bigcup_{\ell\geq 1} \ker(\Theta_{\nu_0,\ell}),$$

de lo se obtiene que $\ker(\Theta_{\nu_0,\ell}) = 0$ para todo $\ell \geq 1$. Repitiendo los argumentos anteriores, se tiene que si $a \in \operatorname{ann}_A(B_{\nu_0+\ell})$ entonces $aB_{\nu_0} \subset \ker(\Theta_{\nu_0,\ell}) = 0$ para todo $\ell \geq 0$. Luego $aB_{\nu_0} = 0$ y se concluye que $a \in \operatorname{ann}_A(B_{\nu_0})$. □

Obsérvese que un tal entero $\nu_0 \geq 0$ tal que $H^0_{R_+}(B)$ siempre existe ya que $H^0_{R_+}(B)$ es un R-módulo de torsión (ver Ejercicio 2) y será estudiado en el Lema B.4 cuando I está generado por una sucesión regular.

El lema anterior prueba que una vez alcanzado un entero ν_0 para el cual $H^0_{R_+}(B)_{\nu_0} = 0$, entonces el ideal eliminante $\mathfrak{A}$ puede ser calculado como $\mathrm{ann}_A(B_{\nu_0})$, y lo resumimos en el siguiente corolario. Un tal entero ν_0 se llama *índice de saturación de* I, ya que $I^{\mathrm{sat}}_{\nu_0} = I_{\nu_0}$.

Corolario 2.6. *Sea $\nu_0 \geq 0$ un entero tal que $I^{\mathrm{sat}}_{\nu_0} = I_{\nu_0}$. Entonces,*

$$\mathfrak{A} = \mathrm{ann}_A(B_{\nu_0}).$$

2.3. El Teorema Principal de eliminación. Recordemos que el Lema 2.4 nos permitía escribir al ideal eliminante $\mathfrak{A}$ en término de anuladores, de la siguiente forma

$$\mathfrak{A} := H^0_{R_+}(B)_0 = \bigcup_{\ell \geq 1} \mathrm{ann}_A(B_\ell).$$

Es fácil ver que el ideal $\mathfrak{A}$ también puede ser escrito como sigue

$$\mathfrak{A} = \{f \in A : fX_i^\ell \in I, \text{ para todo } i \text{ y algún } \ell \geq 1\}. \tag{2.3}$$

El siguiente resultado es conocido como Teorema Principal de Eliminación y constituye el resultado principal de esta sección.

Teorema 2.7 (de Eliminación)**.** *Sea A un anillo conmutativo, $R := A[X_1, \ldots, X_n]$, $I \subset R_+$ un ideal homogéneo de R, $\mathfrak{A}$ su ideal eliminante, k un cuerpo y $\rho : A \to k$ un morfismo de anillos. Entonces $\rho(\mathfrak{A}) = 0$ sii existe un cero no-trivial de I en $\overline{k}$.*

Para demostrar el teorema anterior, haremos uso del siguiente lema:

Lema 2.8. *Sea A un anillo conmutativo, M un A-módulo de tipo finito, k un cuerpo y $\rho : A \to k$ un morfismo de anillos. Entonces, $M \otimes_A k \neq 0$ sii $\rho(\mathrm{ann}_A(M)) = 0$.*

Demostración. Si existe un elemento $a \in \mathrm{ann}_A(M)$ tal que $\rho(a) \in \rho(\mathrm{ann}_A(M))$ es no nulo en k, entonces $\rho(a)$ anula $M \otimes_A k$ ya que a anula a M. Como $M \otimes_A k$ es un k-espacio vectorial, entonces no tiene torsión, entonces debería ser $M \otimes_A k = 0$.

Veamos que si $M \otimes_A k \neq 0$ entonces $\rho(\mathrm{ann}_A(M)) = 0$. Para ello, supongamos que $M \otimes_A k \neq 0$. Como M es de tipo finito, existe una sucesión exacta de la forma

$$0 \longrightarrow K \xrightarrow{\iota} A^p \xrightarrow{\pi} M \longrightarrow 0.$$

Tensorizando por k se obtiene la sucesión exacta

$$K \otimes_A k \xrightarrow{\iota \otimes id_k} k^p \longrightarrow M \otimes_A k \longrightarrow 0.$$

El hecho de que $M \otimes_A k \neq 0$ dice que $\iota \otimes id_k : K \otimes_A k \to k^p$ es suryectiva. Luego, existen elementos $a_1, \ldots, a_p \in K$ tales que la familia $\{\iota(a_1) \otimes_a k, \ldots, \iota(a_p) \otimes_a k\}$ es una base de k^p. Sea $[a] = [a_1|\cdots|a_p] \in \mathrm{Mat}_{p,p}(A)$ la matriz de multiplicación por $a_1, \ldots, a_p$ en base canónica. La observación anterior nos dice que $\rho([a])$ es una matriz inversible, y que por lo tanto $\det(\rho([a])) \neq 0$, y como ρ es morfismo, $\det([a]) \neq 0$. El Ejercicio 3 dice que $\det([a])A^p \subset K$ y por lo tanto, $0 \neq \det([a]) \in \mathrm{ann}_A(M)$, lo cual prueba que $\mathrm{ann}_A(M) \neq 0$. □

Estamos ahora en condiciones de demostrar el Teorema 2.7.

Demostración del Teorema 2.7. Supongamos que existe $0 \neq \zeta \in \overline{k}^n$, que es un cero común de I, es decir, $\rho(f)(\zeta) = 0$ en $k \subset \overline{k}$ para todo $f \in I$. Sea $f \in \mathfrak{A}$, como vimos en (2.3) se tiene que $fX_i^\ell \in I$, para todo i y algún $\ell \geq 1$. En particular, se tiene que

$$\rho(fX_i^\ell)(\zeta) = (\rho(f)X_i^\ell)(\zeta) = \rho(f)\zeta_i^\ell = 0.$$

Como $\zeta \neq 0$, existe un i tal que $\zeta_i \neq 0$, de lo cual se deduce que $\rho(f) = 0$. Esto prueba que $\rho(\mathfrak{A}) = 0$.

Supongamos ahora que $\rho(\mathfrak{A}) = 0$, y consideremos $B = R/I$. Recordemos que (por la Observación 2.1) B es graduado con B_d finitamente generado como A-módulo para cada d y B como anillo está generado por A y B_1, es decir que la multiplicación

$$B_1 \otimes_A B_d \to B_{d+1} : b \otimes b' \mapsto bb'$$

es suryectiva. El Lema 2.4 dice que $\mathfrak{A} = \bigcup_{\ell \geq 1} \operatorname{ann}_A(B_\ell)$, y entonces para $d \geq 1$, $\operatorname{ann}_A(B_d) \subset \mathfrak{A}$, y por lo tanto $\rho(\operatorname{ann}_A(B_d)) = 0$. Aplicando el Lema 2.8 con $M = B_d$ se tiene que $B_d \otimes_A k \neq 0$.

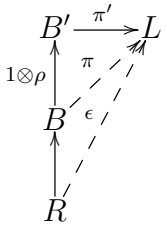
Tensorizando B con k sobre A se tiene $B' := B \otimes_A k$, que es graduado y que verifica que $B'_0 = k$ y que B'_d es un k espacio vectorial no nulo de dimensión finita. Además B'_1 está generado por $\{x_1, \ldots, x_n\}$, siendo x_i la clase de X_i en B', y el morfismo de multiplicación $B'_1 \otimes_A B'_d \to B'_{d+1} : b \otimes b' \mapsto bb'$ es suryectivo. De esta forma, si existiera un entero ℓ tal que $x_i^\ell = 0$ en B' para todo i, se tendría que $B'_d = 0$ para todo $d \geq n(\ell - 1) + 1$, lo que contradiría la no nulidad de B'_d.

Esto dice que existe un elemento $\zeta \in B'_1$ tal que $0 \neq \zeta^d \in B'_d$ para todo $d \geq 1$.

Supongamos que $1 - \zeta \in B'$ fuera inversible, es decir, que existe $\sigma \in B'$ tal que $(1 - \zeta)\sigma = 1$ y $\sigma = \sum_{i=0}^m \sigma_i$, con $\sigma_i \in B'_i$. Desarrollando se tiene que $\sigma_0 + \sum_{i=1}^m (\sigma_i - \zeta\sigma_{i-1}) - \zeta\sigma_m = 1$, lo cual prueba que $\sigma_0 = 1$, $\sigma_i = \zeta\sigma_{i-1}$ es decir que $\sigma_i = \zeta^i$ para $i = 1, \ldots m - 1$, y que $\zeta^{m+1} = 0$, lo cual es absurdo. Esto prueba que $1 - \zeta \in B'$ no es inversible en B'.

Como $1 - \zeta \in B'$ no es inversible en B', existe un ideal maximal $\mathfrak{m}$ que lo contiene. Sea $L = B'/\mathfrak{m}$ el cuerpo cociente y $\pi' : B' \to L$ la proyección natural. Claramente $(\zeta) = 1$, y la restricción de π' a $B'_0 = k$ da un morfismo natural $\iota : k \hookrightarrow L \subset \overline{k}$.

El diagrama conmutativo



muestra que el morfismo π' se levanta a un mofismo π, que a su vez se levanta a un morfismo ϵ. El morfismo $\epsilon : R \to L \subset \overline{k}$ satisface que $\epsilon(X_i) = \pi'(x_i)$. Definiendo $\zeta_i := \epsilon(X_i) \in L$, se tiene que $(\zeta_1, \ldots, \zeta_n) \in \overline{k}^n$, y que $f(\zeta_1, \ldots, \zeta_n) = 0$ para todo $f \in I$. □

Ejercicios.

1. Sea R un anillo conmutativo, sea I un ideal de R y M un R-módulo. Entonces $(0 :_M I^\ell) = \operatorname{Hom}_R(R/I^\ell, M)$.
2. Sea R un anillo graduado y M un R-módulo de R_+-torsión. Entonces, existe un entero ν_0 tal que $H^0_{R_+}(M)_\nu = 0$ para todo $\nu \geq \nu_0$.
3. En el contexto de la demostración del Lema 2.8, pruebe que $\det([a])A^p \subset K$.

3. El complejo de Koszul

El complejo de Koszul fue primeramente introducido por Jean-Louis Koszul para definir una teoría de cohomología para álgebras de Lie, y resultó ser una construcción homológica muy valiosa para el álgebra conmutativa.

En esta sección, supondremos que R es un anillo conmutativo, con unidad (y no necesariamente noetheriano ni local por ahora). Sea M un R-módulo.

Si y es un elemento de R, entonces el endomorfismo de R-módulos, multiplicar por y (que se denotará con y), nos da un complejo: $\mathbf{K}_\bullet(y) : 0 \to R \xrightarrow{y} R \to 0$, que resulta ser el complejo de Koszul asociado a y.

Este caso simple ilustra dos propiedades importantes del complejo de Koszul. Si se indexa con la posición cero a la copia de R que está a la derecha y con uno a la que está a la izquierda, se puede observar que la homología en lugar cero es la imagen homomórfica de R módulo los múltiplos de y. Mientras que la homología en primer lugar representa el anulador del elemento y. Es decir: $H_1(\mathbf{K}_\bullet(y)) = \operatorname{ann}(\{y\})$ y $H_0(\mathbf{K}_\bullet(y)) = R/R(y)$.

Supóngase ahora que se tienen dos elementos x, y en R, considérese la sucesión (ordenada) x, y, que se puede pensar como un vector en R^2. Se construye el complejo de Koszul, $\mathbf{K}_\bullet(x, y)$, asociado a la sucesión x, y, de la siguiente forma:

$$\mathbf{K}_\bullet(x, y) : \quad 0 \to R \xrightarrow{\partial_1} R^2 \xrightarrow{\partial_0} R \to 0.$$

Donde los morfismos ∂_0 y ∂_1 son tales que ∂_0 es la matriz vertical $(x, y)^t$ y ∂_1 es la matriz horizontal $(-y, x)$. La condición $(x, y)^t \cdot (-y, x) = 0$ dice que $\mathbf{K}_\bullet(x, y)$ resulta ser un complejo.

Más generalmente, dados elementos $x_1, \ldots, x_n$ del anillo R, se construye el complejo de Koszul asociado a la sucesión (importa el orden) $x_1, \ldots, x_n$, denotado por $\mathbf{K}_\bullet(x_1, \ldots, x_n)$, como el producto tensorial en la categoría de R-complejos de los complejos $\mathbf{K}_\bullet(x_i)$, para cada i. Asumiremos ahora que los productos tensoriales, y las construcciones de álgebras simétricas y exteriores son como R-módulos.

Recordemos que el producto tensorial de complejos se define de la siguiente forma: Dados $\mathbf{F}_\bullet$ y $\mathbf{G}_\bullet$ dos complejos de cadenas de R-módulos, acotados inferiormente.

$$\mathbf{F}_\bullet : \quad \cdots \to F_i \xrightarrow{\varphi_i} F_{i-1} \xrightarrow{\varphi_{i-1}} \cdots, \text{ y } \mathbf{G}_\bullet : \quad \cdots \to G_i \xrightarrow{\psi_i} G_{i-1} \xrightarrow{\psi_{i-1}} \cdots.$$

Se tiene el siguiente diagrama asociado al producto tensorial:

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \uparrow{\scriptstyle 1\otimes\psi_{j-1}} & & \uparrow{\scriptstyle 1\otimes\psi_{j-1}} & & \uparrow{\scriptstyle 1\otimes\psi_{j-1}} & \\
\cdots & \to F_{i+1}\otimes G_{j-1} & \xrightarrow{\varphi_{i+1}\otimes 1} & F_i\otimes G_{j-1} & \xrightarrow{\varphi_i\otimes 1} & F_{i-1}\otimes G_{j-1} & \xrightarrow{\varphi_{i-1}\otimes 1} \cdots \\
 & \uparrow{\scriptstyle 1\otimes\psi_{j}} & & \uparrow{\scriptstyle 1\otimes\psi_{j}} & & \uparrow{\scriptstyle 1\otimes\psi_{j}} & \\
\cdots & \to F_{i+1}\otimes G_{j} & \xrightarrow{\varphi_{i+1}\otimes 1} & F_i\otimes G_{j} & \xrightarrow{\varphi_i\otimes 1} & F_{i-1}\otimes G_{j} & \xrightarrow{\varphi_{i-1}\otimes 1} \cdots \\
 & \uparrow{\scriptstyle 1\otimes\psi_{j+1}} & & \uparrow{\scriptstyle 1\otimes\psi_{j+1}} & & \uparrow{\scriptstyle 1\otimes\psi_{j+1}} & \\
\cdots & \to F_{i+1}\otimes G_{j+1} & \xrightarrow{\varphi_{i+1}\otimes 1} & F_i\otimes G_{j+1} & \xrightarrow{\varphi_i\otimes 1} & F_{i-1}\otimes G_{j+1} & \xrightarrow{\varphi_{i-1}\otimes 1} \cdots \\
 & \uparrow{\scriptstyle 1\otimes\psi_{j+2}} & & \uparrow{\scriptstyle \psi_{j+2}} & & \uparrow{\scriptstyle 1\otimes\psi_{j+2}} & \\
 & \vdots & & \vdots & & \vdots &
\end{array}$$

El complejo total asociado a este complejo doble se lo llama complejo producto tensorial de $\mathbf{F}_\bullet$ y $\mathbf{G}_\bullet$ y se lo escribe $\mathbf{F}_\bullet \otimes_R \mathbf{G}_\bullet : \quad \cdots \xrightarrow{\phi_{k+2}} D_{k+1} \xrightarrow{\phi_{k+1}} D_k \xrightarrow{\phi_k} D_{k-1} \xrightarrow{\phi_{k-1}} \cdots$, donde $D_k = \bigoplus_{i+j=k} F_i \otimes G_j$, y los morfismos ϕ_k están definidos de la siguiente forma:

$\phi_k|_{F_i\otimes G_j} : F_i \otimes G_j \to F_r \otimes G_s$

$\phi_k|_{F_i\otimes G_j} = \varphi_{i-1} \otimes 1$, si $r = i - 1$

$\phi_k|_{F_i\otimes G_j} = (-1)^i 1 \otimes \psi_{j-1}$, si $s = j - 1$

$\phi_k|_{F_i\otimes G_j} = 0$, en caso contrario.

Se verifica fácilmente que con estos morfismos $\mathbf{F}_\bullet \otimes_R \mathbf{G}_\bullet$ es un complejo de cadenas, que es el producto tensorial de $\mathbf{F}_\bullet$ con $\mathbf{G}_\bullet$ en la categoría de complejos.

Como se comentó antes se puede obtener el complejo de Koszul asociado a una sucesión arbitraria (finita), $x_1, \ldots, x_n$, de elementos del anillo R, $\mathbf{K}_\bullet(x_1, \ldots, x_n)$, mediante la tensorización de los complejos $\mathbf{K}_\bullet(x_i)$, es decir

$$\mathbf{K}_\bullet(x_1, \ldots, x_n) = \bigotimes_{1 \leq i \leq n} \mathbf{K}_\bullet(x_i).$$

De esto se deduce que como el producto tensorial de complejos es conmutativo (salvo isomorfismos), entonces el complejo de Koszul asociado a una sucesión, resulta invariante (salvo isomorfismos) por reordenamientos en la sucesión. Es decir, dado σ un elemento del grupo de automorfismos G_n, se tiene que

$$\mathbf{K}_\bullet(x_1, \ldots, x_n) = \bigotimes_{1 \leq i \leq n} \mathbf{K}_\bullet(x_i) \simeq \bigotimes_{1 \leq i \leq n} \mathbf{K}_\bullet(x_{\sigma(i)}) = \mathbf{K}_\bullet(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Esta construcción puede automatizarse usando el álgebra exterior (cf. [Eis95]).

Recordemos (sin demostración), algunos de los resultados más importantes para nuestras aplicaciones que involucran al complejo de Koszul. Las demostraciones de estos resultados se pueden consultar en [Eis95].

Primero veamos que si bien el complejo no determina si una dada sucesión es regular o no, determina algo aun más importante: dada una sucesión $x_1, \ldots, x_n$, éste permite determinar la longitud de una sucesión regular maximal en el ideal $I = (x_1, \ldots, x_n)$.

Teorema 3.1. *Sea N un módulo finitamente generado sobre un anillo R. Supóngase que $H_j(\mathbf{K}_\bullet(x_1, \ldots, x_n) \otimes N) = 0$ para $j > n - r$, y que $H_{n-r}(\mathbf{K}_\bullet(x_1, \ldots, x_n) \otimes N) \neq 0$, entonces toda N-sucesión maximal en $I = (x_1, \ldots, x_n) \subseteq R$ tiene longitud r.*

Se notará también por $\mathbf{K}_\bullet(x_1, \ldots, x_n; N)$ al complejo $\mathbf{K}_\bullet(x_1, \ldots, x_n) \otimes N$. (Se suele notar $\mathbf{K}^R_\bullet(x_1, \ldots, x_n; N)$, cuando no se sobrentiende que el anillo de base es R).

En particular se tiene el siguiente resultado:

Corolario 3.2. *: Si $x_1, \ldots, x_n$ es una N-sucesión en I, que genera I. Entonces el complejo de Koszul $\mathbf{K}_\bullet(x_1, \ldots, x_n; N)$ resulta acíclico, es decir, es una resolución libre del módulo $R/I \otimes N$.*

Como es sabido, todo módulo libre es proyectivo, entonces el complejo $\mathbf{K}_\bullet(\mathbf{X}; N)$ resulta una resolución proyectiva del módulo $R/I \otimes_R N$. De esto último, tomando homología, se obtienen los funtores derivados del funtor $\_ \otimes_R N$, con lo cual, resulta que $H_i(\mathbf{K}_\bullet(\mathbf{X}; N)) = \mathrm{Tor}^R_i(R/I, N)$.

Además, resulta que esta es la resolución más corta posible del módulo. Como la longitud del complejo es finita, entonces también se tiene que sólo finitas homologías pueden ser no nulas, esto nos permite asociarle al módulo $R/I \otimes_R N$ un valor entero no negativo que se denomina *profundidad* del módulo.

3.1. El complejo de Koszul graduado. Lamentablemente la recíproca del corolario anterior es falsa en el caso general, aunque resulta cierta si el anillo de base es local o graduado. Éste último es el contexto general de estas notas, ya que en nuestras aplicaciones R es un anillo de polinomios sobre un anillo conmutativo A.

Teorema 3.3. *Sea N un módulo finitamente generado sobre un anillo local (o graduado) R con ideal maximal (o maximal homogéneo) $\mathfrak{m}$. Sea $x_1, \ldots, x_n$ una sucesión en*

$\mathfrak{m}$. *Supóngase que para algún* i *se tiene que* $H_i(N \otimes \mathbf{K}_\bullet(x_1, \dots, x_n)) = 0$, *entonces se tiene que* $H_j(N \otimes \mathbf{K}_\bullet(x_1, \dots, x_n)) = 0$ *para todo* $j \geq i$.

En particular si $H_1(N \otimes \mathbf{K}_\bullet(x_1, \dots, x_n)) = 0$, *entonces* $x_1, \dots, x_n$ *forma una sucesión* N*-regular en* $\mathfrak{m}$.

Esto permite dar para el caso local una versión más fuerte del corolario anterior

Corolario 3.4. *Dado un anillo local (o graduado)* R *con ideal maximal (o maximal homogéneo)* $\mathfrak{m}$, *y* N *un* R*-módulo finitamente generado . Sea* $I = (x_1, \dots, x_n)$ *un ideal propio de* R, *que contiene una sucesión* N*-regular de longitud* n. *Entonces* $x_1, \dots, x_n$ *es una sucesión* N*-regular.*

De aquí se deduce un resultado de importante valor geométrico, ya que éste expresa la naturaleza geométrica del concepto de profundidad anteriormente mencionado.

Corolario 3.5. *Dado un anillo* R *y* N *un* R*-módulo finitamente generado, se tiene que si* $x_1, \dots, x_r$ *es una sucesión* N*-regular, entonces* $x_1^m, \dots, x_r^m$ *también lo es, para todo natural* m.

Nos concentraremos ahora en estudiar al complejo de Koszul en el contexto específico de nuestras aplicaciones. Para ello, sea R un anillo graduado, $R = \oplus_{i \geq 0} R_i$, M un R-módulo graduado, e $I = (x_1, \dots, x_n)$ un ideal homogéneo de R, donde $\deg(x_i) = d_i$ para todo i. Entonces el complejos de Koszul $\mathbf{K}_\bullet(x_1, \dots, x_n; M)$ hereda la graduación de R y se escribe

$$\mathbf{K}_\bullet(x_1, \dots, x_n; M): \quad \cdots \to \bigoplus_{1 \leq i < j \leq r} M(-d_i - d_j) \to \bigoplus_{1 \leq i \leq r} M(-d_i) \to M \to M/I \to 0,$$

donde $M(-d)_e = M_{e-d}$, y las flechas son morfismos de módulos graduados, de grado cero.

Sea r, n y $d_1, \dots, d_r$ enteros positivos, y sean $f_1, \dots, f_r$ polinomios homegéneous de grado $d_1, \dots, d_r$ en las variables $\mathbf{X} := X_1, \dots, X_n$ definidos como

$$f_i(\mathbf{X}) = \sum_{|\alpha| = d_i} U_{i,\alpha} \mathbf{X}^\alpha,$$

para todo $i = 1, \dots, r$, donde $\alpha \in \mathbb{N}^n$.

Sea $A := \mathbb{Z}[U_{i,\alpha} : |\alpha| = d_i,\ i = 1, \dots, r]$ y escribamos $R = A[\mathbf{X}]$.

Lema 3.6. *Si* $r \leq n$ *entonces* $f_1, \dots, f_r$ *es una sucesión regular en* R.

Demostración. Para cada $i = 1, \dots, r$ sea $\epsilon_i := U_{i,(0,\dots,0,d_i,0,\dots,0)}$ el coeficiente correspondiente a $X_i^{d_i}$ del polinomio f_i.

Obsérvese que todos los coeficientes $U_{i,\alpha}$ restantes forman una sucesión regular en R. Además, el cociente de R por estos $U_{i,\alpha}$ es isomorfo a $\mathbb{Z}[\epsilon_1, \dots, \epsilon_r][\mathbf{X}]$ y $f_i = \epsilon_i X_i^{d_i}$ en el cociente.

Es fácil ver que en $\mathbb{Z}[\epsilon_1, \dots, \epsilon_r][\mathbf{X}]$ los polinomios $X_1 - \epsilon_1, \dots, X_r - \epsilon_r$ también forman una sucesión regular, que el anillo cociente queda isomorfo a $\mathbb{Z}[\mathbf{X}]$, y que $f_i = X_i^{d_i+1}$ en el cociente.

Finalmente, sabemos que $X_1^{d_1+1}, \dots, X_r^{d_r+1}$ es una sucesión regular en $\mathbb{Z}[\mathbf{X}]$ independientemente del orden. □

Se tiene entonces como corolario el siguiente resultado

Corolario 3.7. *Sea $I = (f_1, \dots, f_n)$, entonces el complejo de Koszul*

$$\mathbf{K}_\bullet(f_1, \dots, f_n; R): \quad \cdots \to \bigoplus_{1 \le i < j \le r} R(-d_i - d_j) \to \bigoplus_{1 \le i \le r} R(-d_i) \to R \to 0,$$

es una resolución libre graduada y finita de R/I.

Ejercicios.

1. Sea (R, R_+) un anillo local (o graduado) $x_1, \dots, x_n \in R_+$. Entonces $x_1, \dots, x_n$ es una sucesión regular en R sii para todo $i = 0, \dots, n-1$, x_{i+1} no está en ningún primo asociado de $(x_1, \dots, x_{i-1})$.
2. Si los elementos $x_1, \dots, x_n \in R$ forman una sucesión regular en R, entonces $x_1^{\ell_1}, \dots, x_n^{\ell_n}$ también.
3. Si un ideal I de un anillo conmutativo Noetheriano puede ser generado por una sucesión regular, entonces puede ser generado por un conjunto de elementos que son una sucesión regular en cualquier orden.
4. Sea $\phi : R \to S$ un morfismo de anillos, sean $r_1, \dots, r_n \in S$ y $s_i := \phi(r_i) \in R$. Si $r_1, \dots, r_n$ forman una sucesión regular en R, entonces para todo R-módulo M, $H_i(\mathbf{K}_\bullet(r_1, \dots, r_n) \otimes_R M) = \operatorname{Tor}_i^S(S/(s_1, \dots, s_n), M)$.
5. Sea $\mathbf{K}_\bullet(\mathbf{X})$ el complejo de Koszul asociado a la sucesión $\mathbf{X}$, y supongamos que x_j es una unidad de A. Entonces el complejo $\mathbf{K}_\bullet(\mathbf{X})$ resulta acíclico.

4. Resultante

En esta sección definiremos y estudiaremos el objeto principal de estas notas, que es la resultante homogénea, o resultante de Macaulay.

4.1. Resultante de Macaulay. Sea r, n y $d_1, \dots, d_r$ enteros positivos, y sean $f_1, \dots, f_r$ polinomios homegéneous de grado $d_1, \dots, d_r$ en las variables $\mathbf{X} := X_1, \dots, X_n$ definidos como

$$f_i(\mathbf{X}) = \sum_{|\alpha| = d_i} U_{i,\alpha} \mathbf{X}^\alpha,$$

para todo $i = 1, \dots, r$, donde $\alpha \in \mathbb{N}^n$.

Sea $A := \mathbb{Z}[U_{i,\alpha} : |\alpha| = d_i,\ i = 1, \dots, r]$ y escribamos $R = A[\mathbf{X}]$.

Teorema 4.1. *Si $r = n$ entonces el ideal $\mathfrak{A}$ es un ideal primo y principal de A, generado por un elemento que llamaremos Resultante de $f_1, \dots, f_n$, que denotaremos* $\operatorname{Res}(f_1, \dots, f_n)$*, y que verifica que* $\operatorname{Res}(X_1^{d_1}, \dots, X_n^{d_n}) = 1$.

Para demostrar este teorema, vamos a seguir la demostración dada por Jean-Pierre Jouanolou en [Jou91]. Cabe mencionar que el anillo $\mathbb{Z}$ puede ser reemplazado por un anillo conmutativo reducido, con el solo fin de que la resultante no quede definida a menos de constantes.

Para demostrar el Teorema 4.1 anterior, nos apoyaremos en tres lemas. Antes de eso, introducimos la siguiente notación.

Definición 4.2. Dado I un ideal de un anillo graduado R, con ideal irrelevante R_+, se definen las *formas de inercia* de I como

$$\operatorname{TF}_{R_+}(I) := \bigcup_{\ell \ge 0} (I :_R (R_+)^\ell).$$

Esta notación proviene de su nombre *Trägheitsformen*, en alemán, introducidas por Hurwitz en el contexto de la teoría de eliminación.

Lema 4.3. *Para todo entero $j = 1, \dots, n$ se tiene*

$$\mathrm{TF}_{R_+}(I) = \bigcup_{\ell \geq 0} (I :_R X_j^\ell) = \ker(R \to B_{X_j}).$$

Además, $\mathrm{TF}_{R_+}(I)$ *es un ideal primo de* R.

De la segunda parte, intersecando con A, se tiene que $\mathfrak{A}$ es un ideal primo de A.

Demostración. Sea $1 \leq j \leq n$ un entero, y para cada $i = 1, \dots, r$, escribimos U_i para denotar al coeficiente correspondiente al monomio $X_j^{d_i}$ del polinomio f_i. Es decir, si $\beta = d_i \mathbf{e}_j$, siendo $\mathbf{e}_j$ el j-ésimo vector canónico, $U_i = U_{i,\beta}$.

En el anillo $R' := R[X_j^{-1}]$, el polinomio f_i se escribe de la siguiente forma:

$$f_i(\mathbf{X}) = X_j^{d_i}(U_i + \sum_{\alpha \neq \beta} U_{i,\alpha} \mathbf{X}^\alpha X_j^{-d_i}).$$

Sea $A' := \mathbb{Z}[U_{i,\alpha} : i = 1, \dots, r, \alpha \neq \beta]$, con lo cual $A = A'[U_1, \dots, U_r]$, y escribamos $g_{i,\beta} := \sum_{\alpha \neq \beta} U_{i,\alpha} \mathbf{X}^\alpha X_j^{-d_i}$.

Se obtiene así un isomorfismo de anillos

$$B_{X_j} \xrightarrow{\sim} A'[\mathbf{X}][X_j^{-1}] : U_i \mapsto U_i - f_i / X_j^{d_i} = -g_{i,\beta}.$$

Esto prueba que cualesquiera sean i, j, X_i no es un divisor de cero en B_{X_j}. Entonces la primera parte se desprende de que

$$\ker(R \to B_{X_i}) = \ker(R \to B_{X_i X_j}) = \ker(R \to B_{X_j X_i}) = \ker(R \to B_{X_j})$$

Además, como $\mathbb{Z}$ es íntegro, B_{X_j} también lo es, y por lo tanto, $\mathrm{TF}_{R_+}(I)$ es un ideal primo de R. □

Lema 4.4. *Si $r < n$ entonces* $\mathrm{TF}_{R_+}(I) = I$.

Demostración. De la definición de $\mathrm{TF}_{R_+}(I)$ se desprende que $\mathrm{TF}_{R_+}(I) \supset I$. Demostraremos entonces que $\mathrm{TF}_{R_+}(I) \subset I$. Por el Lema 4.3, basta mostrar que si existe un entero ℓ para el cual $X_n^\ell f \in I$ entonces $f \in I$. Si esto valiera para $\ell = 1$, entonces siendo verdadero para $\ell - 1$ también se tendría para ℓ ya que $X_n^\ell f = X_n(X_n^{\ell-1} f)$. Veamos que vale si $\ell = 1$.

Sea $f \in R$ y escribamos

$$X_n f = \sum_{i=1}^r h_i f_i \in I. \tag{4.1}$$

Se tiene que $\sum_{i=1}^r \overline{h_i f_i} = 0$ en $\overline{R} := R/(X_n)$ y los polinomios f_i son genéricos en las variables $X_1, \dots, X_{n-1}$. Sabemos (por el Lema 3.6) que, como $r \leq n-1$, los polinomios $\overline{f_1}, \dots, \overline{f_r}$ forman una sucesión regular en $\overline{R}$ y entonces el complejo de Koszul $\mathbf{K}_\bullet(\overline{f_1}, \dots, \overline{f_r}; \overline{R})$ es acíclico (ver el Corolario 3.2). Además, la exactitud en la posición 1

$$\cdots \to \bigoplus_{1 \leq i < j \leq r} \overline{R}(-d_i - d_j) \xrightarrow{\partial_2} \bigoplus_{1 \leq i \leq r} \overline{R}(-d_i) \xrightarrow{\partial_1} \overline{R} \to \overline{R}/(\overline{f_1}, \dots, \overline{f_r}) \to 0.$$

del complejo $\mathbf{K}_\bullet(\overline{f_1}, \dots, \overline{f_r}; \overline{R})$ dice que $(\overline{h_1}, \dots, \overline{h_r}) \in \ker(\partial_1)$ si y solo si $(\overline{h_1}, \dots, \overline{h_r}) \in \mathrm{im}(\partial_2)$, es decir, si existe $h' := (\dots, h'_{i,j}, \dots) \in \oplus_{1 \leq i < j \leq n-1} \overline{R}(d_i - d_j)$ tal que $\partial_2(h') =$

$(\overline{h_1}, \ldots, \overline{h_r})$. Esta última condición es equivalente (Ejercicio 1) a que exista una matriz antisimétrica $H \in \mathrm{Mat}_{r,r}(\overline{R})$ tal que

$$H \cdot (\overline{f_1}, \ldots, \overline{f_r})^t = (\overline{h_1}, \ldots, \overline{h_r}).$$

Interpretando $\overline{R}$ como $R' := A[X_1, \ldots, X_{n-1}]$, y $H \in \mathrm{Mat}_{r,r}(R')$ definimos $g_i \in R$ de forma tal que

$$H \cdot (f_1, \ldots, f_r)^t = (g_1, \ldots, g_r),$$

donde $\overline{g_i} = \overline{h_i}$ para todo i, es decir que que existe para cada i, existe un polinomio p_i tal que $h_i - g_i = X_n p_i$. Además, como H es antisimétrica, se tiene que $\sum f_i g_i = 0$. Retomando la ecuación (4.1), se tiene

$$X_n f = \sum_{i=1}^{r} (g_i + X_n p_i) f_i = \sum_{i=1}^{r} g_i f_i + X_n \sum_{i=1}^{r} p_i f_i. \tag{4.2}$$

De (4.2) se deduce que $X_n f = X_n \sum_{i=1}^r p_i f_i$ en R o equivalentemente (ya que X_n no es divisor de ceros en R) $f = \sum_{i=1}^r p_i f_i$, es decir, que $f \in I$. □

Lema 4.5. *Supongamos $r = n$ y sea $f \in \mathrm{TF}_{R_+}(I) \in R$. Entonces $f \in I$ ó f depende de todos los coeficientes $U_{i,\alpha}$ de todos los f_i.*

Demostración. Sea $U = U_{i,\alpha}$ un coeficiente cualquiera, es decir, fijemos algún i y algún α. El coeficiente U corresponde al monomio X^α que aparece en f_i. Supongamos ahora que $f \in \mathrm{TF}_{R_+}(I)$ no depende U, y veamos que $f \in I$.

Escribamos $g_i := f_i - UX^\alpha$ y consideremos el morfismo de álgebras $\phi : R_{X_1 \cdots X_n} \to R_{X_1 \cdots X_n}$ definido como $U \mapsto -g_i/X^\alpha$, $U_{j,\beta} \mapsto U_{j,\beta}$ si $(j,\beta) \neq (i,\alpha)$ y $X_j \mapsto X_j$ para todo j. Obsérvese que $\phi(f_i) = 0$ para todo i, y que como f y f_j no dependen de U si $j \neq i$, entonces $\phi(X_n^\ell f) = X_n^\ell f$ para todo ℓ y $\phi(f_j) = f_j$ para todo $j \neq i$.

Como $f \in \mathrm{TF}_{R_+}(I)$, se tiene que $X_n^\ell f = \sum_i h_i f_i \in I$ para algún $\ell \in \mathbb{N}$. Aplicando ϕ a la identidad anterior, usando que $\phi(f_i) = 0$, $\phi(f_j) = f_j$ si $j \neq i$, y escribiendo $h_i' := \phi(h_i)$ se tiene que

$$X_n^\ell f = \phi(X_n^\ell f) = \sum_{j \neq i} h_j' f_j \in R_{X_1 \cdots X_n}.$$

Multiplicando por una potencia conveniente X^β de las X_i's se obtiene la siguiente igualdad en R

$$X^\beta \phi(X_n^\ell f) = X^\beta X_n^\ell f = \sum_{j \neq i} h_j'' f_j \in R.$$

Esto último dice que si escribimos $I' := (f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$ el ideal generado por $n-1$ polinomios, entonces $f \in \mathrm{TF}_{R_+}(I')$. El Lema 4.4 aplicado con $r = n-1$ nos dice que $\mathrm{TF}_{R_+}(I') = I' \subset I$. □

Vayamos entonces a la demostración del Teorema de eliminación.

Teorema 4.1. *Si $r = n$, entonces el ideal $\mathfrak{A}$ es un ideal primo y principal de A, generado por un elemento que llamaremos Resultante de $f_1, \ldots, f_n$, que denotaremos $\mathrm{Res}(f_1, \ldots, f_n)$, y que verifica que $\mathrm{Res}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$.*

Demostración. Sea $U = U_{i,\alpha}$ un coeficiente cualquiera, y escribamos $A' := \mathbb{Z}[U_{j,\beta} : (j,\beta) \neq (i,\alpha)]$. Con esta notación, $A = A'[U]$. Como $I \cap A = 0$, el Lema 4.5 dice que todo $0 \neq f \in \mathfrak{A}$ satisface que $\deg_U(f) \geq 1$. Definamos entonces

$$s := \mín\{\deg_U(f) : 0 \neq f \in \mathfrak{A}\}.$$

Sea $f \in \mathfrak{A}$ que satisface $\deg_U(f) = s$. Como A' es factorial, entonces existe una factorización $f = \prod q_i$ en finitos q_i, con q_i primo en $A = A'[U]$.

Como $\mathrm{TF}_{R_+}(I)$ es un ideal primo y $f \in \mathfrak{A}$, por el Lema 4.3, entonces existe un i tal que $q_i \in \mathfrak{A}$. Como $q_i | f$, se tiene que $1 \leq \deg_U(q_i) \leq \deg_U(f) = s$. Como $q_i \in \mathfrak{A}$, por definición de s se tiene que $\deg_U(q_i) = \deg_U(f) = s$. Esto prueba que existe un elemento primo $\mathfrak{r} := q_i \in \mathfrak{A}$.

Veamos ahora que $\mathfrak{A} = \mathfrak{r}A$. En efecto, como A' es íntegro, dado $g \in \mathfrak{A}$, aplicando el algoritmo de de división en $A'[U]$ podemos escribir en A, $tg = u\mathfrak{r} + v$, donde $t \in A'$, $u \in A$ y v verifica que $v = 0$ ó $\deg_U(v) < s$. Como $v = tg - u\mathfrak{r}$, entonces $v \in \mathfrak{A} \subset A$ y $A \cap I = 0$, si $v \neq 0$, entonces por el Lema 4.5 v depende de todos los coeficientes de los f_i, en particular depende de U, pero la elección de s, se tendría que $\deg_U(v) \geq s$, lo cual lleva a una contradicción. Entonces se tiene que $v = 0$ y por lo tanto $tg = u\mathfrak{r}$. Como t no depende de U y $\mathfrak{r}$ tiene grado positivo en U y es primo, entonces $\mathfrak{r} | g$

Como esto vale para U arbitrario, se tiene que $\mathfrak{r}$ es único a menos de un elemento inversible de A', es decir, de $\mathbb{Z}$. Este elemento es 1 por la normalización elegida en el enunciado. □

4.2. Resultante y divisores. Hemos visto en el Lema 3.6 que si $f_1, \ldots, f_r$ son r polinomios genéricos y $r \leq n$, entonces forman una sucesión regular en R. El Corolario 3.7 dice que entonces el complejo de Koszul $\mathbf{K}_\bullet(f_1, \ldots, f_r; R)$ es un complejo acíclico de R-módulos, y en particular, complejo Koszul es acíclico en grados positivos si el número de polinomios r es menor o igual al número de variables n

Veremos ahora cómo $\mathrm{ann}_A(B_\nu)$ puede ser calculado mediante un producto alternado de determinantes, que vienen de los diferenciales de este complejo de Koszul graduado, en grado $\nu \geq \nu_0 := \sum(d_i - 1) + 1$.

En la Sección 4 vimos, en el Teorema 4.1 que el ideal $\mathfrak{A}$ es primo y principal y que por lo tanto define una subvariedad de $\mathrm{Spec}(A)$ de codimensión 1. Luego, probamos entre el Lema 2.4 y el Corolario 2.6 que $\mathfrak{A} = \mathrm{ann}_A(B_\nu)$ si $\nu \geq \nu_0$, es decir, que es un A-módulo de torsión.

Mostraremos ahora que todo A-módulo M de torsión con A un dominio noetheriano y factorial, define un divisor $\mathrm{div}(M)$, y que dada una resolución libre de M, este divisor puede ser calculado mediante un producto alternado de determinantes.

En lo que sigue, sólo nos interesará la estructura de A-módulo de los objetos. Es importante que el lector tenga en cuenta que si bien lo que desarrollaremos en esta parte es general para cualquier A-módulo con A un dominio noetheriano y factorial, nuestro es interés está en el caso en que A es el anillo de coeficientes universales de n polinomios genéricos, $M = B_\nu$ con $\nu \geq \nu_0$ y la resolución libre $\mathbf{F}_\bullet$ de M es $\mathbf{K}_\bullet(f_1, \ldots, f_r; R)_\nu$ con $\nu \geq \nu_0$.

Sea A un dominio noetheriano y factorial con cuerpo de fracciones k.

Definición 4.6. Sea A un anillo noetheriano y factorial y sea M un A-módulo de torsión de tipo finito. Denotemos por $\mathrm{div}(M)$ al divisor asociado a M:

$$\mathrm{div}(M) = \sum_{\mathfrak{p} \in \mathrm{ass}_A(M), \mathrm{ht}(\mathfrak{p}) = 1} \ell(M_\mathfrak{p})\mathfrak{p},$$

donde $\mathrm{ass}_A(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \exists m \in M, \mathrm{ann}_A(m) = \mathfrak{p}\}$ es el conjunto de primos asociados a M, $\mathrm{ht}(\mathfrak{p})$ es la altura de $\mathfrak{p}$ y $\ell(M_\mathfrak{p})$ la longitud de $M_\mathfrak{p}$.

Definición 4.7. Si I es un ideal de A, la parte principal de I, que frecuntemente se denota por $[I]$, consiste en el gcd de los generadores de I.

Obsérvese que acá entran la hipótesis de factorialidad requerida sobre A, así como la finita generación de I, que está garantizada por la noetherianidad de A.

Con esta notación, si el ideal I se descompone en factores irreducibles de forma tal que su parte principal es $[I] = \prod_i \mathfrak{p}_i^{\ell_i}$, entonces $\operatorname{div}(A/I) = \sum_i \ell_i \mathfrak{p}_i$.

Teorema 4.8. *A un dominio noetheriano y factorial y* $\mathbf{F}_\bullet$ *un complejo finito de A-módulos libres finitamente generados. Escribamos*

$$\mathbf{F}_\bullet : 0 \to F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \to 0$$

y supongamos que $F_i = E_{i+1} \oplus E_i$, $E_0 = E_{n+1} = 0$, $\partial_p = \begin{pmatrix} a_p & \phi_p \\ b_p & c_p \end{pmatrix}$, *donde* $\phi_p : E_p \to E_p$ *es un endomorfismo inyectivo. Entonces,* $H_i(\mathbf{F}_\bullet)$ *es un A-módulo de torsión para todo* i, *y*

$$\sum_i (-1)^i \operatorname{div}(H_i(\mathbf{F}_\bullet)) = \sum_i (-1)^i \operatorname{div}(\det \phi_i).$$

En particular, si $\mathbf{F}_\bullet$ *es acíclico, la parte principal de* $H_0(\mathbf{F}_\bullet)$, $[H_0(\mathbf{F}_\bullet)]$, *está dada por el elemento* $\prod_i (\det \phi_i)^{(-1)^{i+1}}$ *de A.*

Demostración. Sea k el cuerpo de fracciones de A. Debemos probar que $H_i(\mathbf{F}_\bullet)$ es un A-módulo de torsión para todo i, para ello, veamos que $H_i(\mathbf{F}_\bullet) \otimes_A k = 0$. Como A es íntegro, k es la localización en el ideal 0, es playo sobre A, entonces $H_i(\mathbf{F}_\bullet) \otimes_A k = H_i(\mathbf{F}_\bullet \otimes_A k)$.

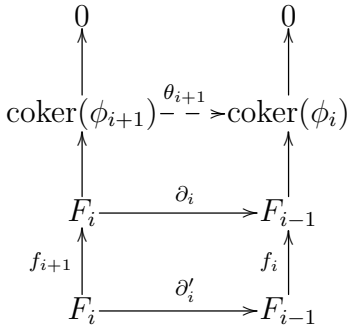
Además, la homología de $\mathbf{F}_\bullet \otimes_A k$ es cero porque $\partial_i \otimes 1$ restringido a $E_i \otimes_A k$ es un automorfismo. Entonces $H_i(\mathbf{F}_\bullet)$ es de torsion para todo i.

Sea $\partial'_i = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}$, entonces el complejo $(\mathbf{F}_\bullet, \partial'_\bullet)$ tiene homología cero. Definimos la aplicación $f_n = id$, $f_i = \begin{pmatrix} \phi_{i+1} & 0 \\ c_{i+1} & I \end{pmatrix} : F_i \to F_i$ para todo $i < n$. Como

$$\partial_i \circ f_i = \begin{pmatrix} a_i & \phi_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} \phi_{i+1} & 0 \\ c_{i+1} & I \end{pmatrix} = \begin{pmatrix} 0 & \phi_i \\ 0 & c_i \end{pmatrix} = \begin{pmatrix} \phi_i & 0 \\ c_i & I \end{pmatrix} \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix} = f_{i-1} \circ \partial'_i,$$

se tiene que los $\{f_i\}$ definen un morfismo $f_\bullet : (\mathbf{F}_\bullet, \partial'_\bullet) \to (\mathbf{F}_\bullet, \partial_\bullet)$.

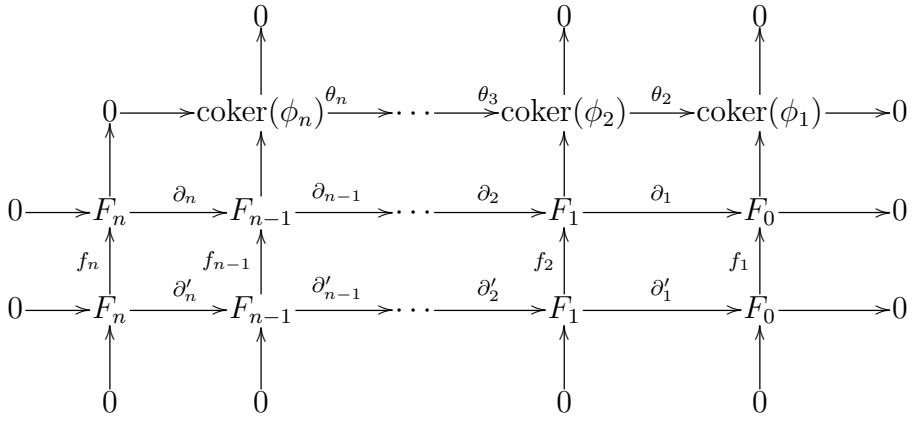
Además, f_i es inyectiva y $\operatorname{coker}(f_i)$ puede ser identificado con $\operatorname{coker}(\phi_{i+1})$. Los morfismos ∂_i y ∂'_i inducen morfismos Θ_{i+1} de acuerdo al siguiente diagrama



Esto dice que se tiene una sucesión exacta corta de complejos

$$0 \to (\mathbf{F}_\bullet, \partial'_\bullet) \xrightarrow{f_\bullet} (\mathbf{F}_\bullet, \partial_\bullet) \to (\operatorname{coker}(\phi_\bullet), \theta_\bullet)[1] \to 0. \tag{4.3}$$

que se escribe en forma de digrama como sigue, donde las columnas son exactas



La sucesión exacta (4.3) da una sucesión exacta larga en homología

$$\cdots \to H_i(\mathbf{F}_\bullet, \partial'_\bullet) \to H_i(\mathbf{F}_\bullet, \partial_\bullet) \to H_{i+1}(\operatorname{coker}(\phi_\bullet), \theta_\bullet) \to H_{i-1}(\mathbf{F}_\bullet, \partial'_\bullet) \to \cdots .$$

Como el complejo $(\mathbf{F}_\bullet, \partial'_\bullet)$ es exacto, se tiene que el complejo $(\operatorname{coker}(\phi_\bullet), \theta_\bullet)[1]$ tiene la misma homología que $(\mathbf{F}_\bullet, \partial_\bullet)$. Esto es, $H_i(\mathbf{F}_\bullet, \partial_\bullet) \cong H_{i+1}(\operatorname{coker}(\phi_\bullet), \theta_\bullet)$, y en particular sus divisores asociados coinciden, de lo cual se deduce que

$$\operatorname{div}(\operatorname{coker}\phi_i) = \operatorname{div}(\operatorname{im}\theta_{i-1}) + \operatorname{div}(\ker\theta_{i-1}) = \operatorname{div}(\operatorname{im}\theta_{i-1}) + \operatorname{div}(\operatorname{im}\theta_i) + \operatorname{div}(H_{i-1}(\mathbf{F}_\bullet)).$$

La conclusión sigue del siguiente resultado clásico de Bourbaki [Bou98, Cap. 7, Sec. 4, n. 6, Corolario de la Prop. 13]:

Sea M un A-módulo finitamente generado y ϕ un endomorfismo inyectivo de M. Entonces $\operatorname{div}(\operatorname{coker}\phi) = \operatorname{div}(\det\phi)$. □

Volvamos a nuestro contexto habitual y sea $A = \mathbb{Z}[U_{i,\alpha}]$ es el anillo de coeficientes universales de n polinomios genéricos $f_1, \dots, f_n$, $M = B_\nu$ con $\nu \geq \nu_0$ y la resolución libre $\mathbf{F}_\bullet$ de M es $\mathbf{K}_\bullet(f_1, \dots, f_n; R)_\nu$ con $\nu \geq \nu_0$. Se tiene el siguiente resultado.

Corolario 4.9. *El complejo $\mathbf{K}_\bullet(f_1, \dots, f_n; R)_\nu$ de A-módulos es una resolución de B_ν con diferenciales ∂_i^ν. Además, la parte principal de B_ν, es decir $\operatorname{ann}_A(B_\nu)$, está dada por $\prod_i (\det \partial_i^\nu)^{(-1)^{i+1}}$.*

Esto permite calcular, teniendo una descomposición como la del Teorema 4.8, un (el) generador de $\operatorname{ann}_A(B_\nu)$ como producto alternado de matrices que vienen de los diferenciales ∂_i^ν de $\mathbf{K}_\bullet(f_1, \dots, f_n; R)_\nu$.

Ejercicios.

1. En el contexto de la demostración del Lema 4.4, $H_1(\mathbf{K}_\bullet(\overline{f_1}, \dots, \overline{f_r}; \overline{R})) = 0$ es equivalente a que exista una matriz antisimétrica $H \in \operatorname{Mat}_{r,r}(\overline{R})$ tal que

$$H \cdot (\overline{f_1}, \dots, \overline{f_r})^t = (\overline{h_1}, \dots, \overline{h_r}).$$

5. Ideales de Fitting

En esta sección desarrollaremos el contenido básico sobre ideales de Fitting, y determinantes de complejos, lo que está estrictamente vinculado con el invariante de McRae, que se define a partir de un A-módulo M, y que bajo buenas condiciones describe la parte de codimensión uno del soporte de M. Quien esté interesado en profundizar las ideas rápidamente expuestas en esta sección, puede consultar el trabajo de McRae [Mac65], que es la fuente original, y el artículo de Northcott [Nor76] en el cuál se trata la existencia y algunas propiedades de este invariante.

Para el cálculo de este invariante, que definiremos a partir de ideales de Fitting, haremos uso de una técnica desarrollada por Cayley conocida como determinante de un complejo. Para esto se puede consultar unas notas de Demazure [Dem84] y un tratamiento más general se puede obtener en el Apéndice del libro [GKZ94].

5.1. Ideales de Fitting. Sea A un anillo conmutativo, F y G dos A-módulos libres, y $\varphi : F \to G$ un morfismo de A-módulos. Consideremos bases para estos módulos, y notemos por $|\varphi|$ a la matriz de φ escrita en estas bases. Definimos $\det_\nu(\varphi)$ como el ideal de A generado por los menores de tamaño $\nu \times \nu$ de $|\varphi|$. Haremos la convención de que la matriz de tamaño nulo tiene determinante 1, con lo cual $\det_\nu(\varphi) = A$ para todo $\nu \leq 0$.

Proposición 5.1. *Sea M un A-módulo finitamente generado, y sean $F \xrightarrow{\varphi} G \to M \to 0$ y $F' \xrightarrow{\varphi'} G' \to M \to 0$ dos presentaciones libres de M. Entonces para todo $\nu \in \mathbb{Z}$ se tiene que*

$$\det{}_{rg(G)-\nu}(\varphi) = \det{}_{rg(G')-\nu}(\varphi').$$

Una demostración de este resultado, como de los siguientes, se puede consultar en [Nor76, Cap. 3.1.]. Podemos ahora dar la definición de los ideales de Fitting:

Definición 5.2. Sea M un A-módulo finitamente generado, y sea $F \xrightarrow{\varphi} G \to M \to 0$ una presentación libre de M, definimos para cada $i \in \mathbb{N}$, el ν-ésimo *invariante de Fitting de M*, como el ideal

$$\mathrm{Fitt}_\nu(M) := \det{}_{rg(G)-\nu}(\varphi).$$

El invariante $\mathrm{Fitt}_0(M)$ suele ser denotado por Fitt y llamado invariante de Fitting inicial de M.

Enunciaremos a continuación algunas propiedades relevantes sobre estos invariantes. Nótese que el item 2, es la mencionada propiedad de cambio de base deseada en nuestra aplicación al cálculo de resultantes.

Proposición 5.3. *Sea M un A-módulo finitamente generado.*

1. *Los invariantes de Fitting de M forman una sucesión creciente:*

$$\mathrm{Fitt}(M) = \mathrm{Fitt}_0(M) \subset \mathrm{Fitt}_1(M) \subset \mathrm{Fitt}_2(M) \subset \cdots .$$

   Más aún, si M puede ser generado por m elementos, entonces $\mathrm{Fitt}_m(M) = A$.
2. *Dado un morfismo $A \to B$ de anillos, se tiene que, para todo $\nu \in \mathbb{N}$*

$$\mathrm{Fitt}_\nu(M \otimes_A B) = \mathrm{Fitt}_\nu(M)B \ .$$

3. *Para todo $\nu \geq 1$ se tiene que* $\mathrm{ann}(M)\,\mathrm{Fitt}_\nu(M) \subset \mathrm{Fitt}_{\nu-1}(M)$. *Más aún, si M puede ser generado por m elementos, entonces*

$$\mathrm{ann}(M)^m \subset \mathrm{Fitt}(M) \subset \mathrm{ann}(M).$$

4. *Si M es un A-módulo que admite una presentación finita (se dice que M es finitamente presentado), entonces cada uno de sus invariantes de Fitting es un ideal finitamente generado de A.*

Enunciaremos a continuación un resultado muy importante conocido como Lema de McCoy, que tampoco demostraremos.

Lema 5.4. *(McCoy) Sea $\varphi : F \to G$ un morfismo entre dos A-módulos libres de rango r_1 y r_2 respectivamente. Entonces φ es inyectiva si y solo si $\operatorname{ann}_A(\det_{r_1}(\varphi)) = 0$. más aún, cuando se está en esta situación se tiene que $r_1 \leq r_2$.*

Utilizaremos este resultado al final de esta sección para obtener una descomposición de un complejo libre, como la deseada en el Teorema 4.8.

5.2. La Característica de Euler. Nuevamente aquí A es un anillo conmutativo, y M es un A-módulo. Antes de poder definir el invariante de McRae de M, que denotaremos por $\mathfrak{S}(M)$, debemos definir algunos conceptos previos que están íntimamente ligados a él.

Definiremos previamente otro invariante, conocido como *Característica de Euler*, que tiene la propiedad de caracterizar a aquellos módulos que tienen anulador trivial.

Lema 5.5. *Sea M un A-módulo, y consideremos dos resoluciones libre finitas $\mathbf{F}_\bullet$ y $\mathbf{F}'_\bullet$ de M, entonces se tiene que $\sum_i (-1)^i r_i = \sum_i (-1)^i r'_i$, donde $r_i = rg(F_i)$ y $r'_i = rg(F'_i)$.*

Ahora podemos definir la Característica de Euler de M como sigue:

Definición 5.6. Sea M un A-módulo que admite una resolución libre finita $\mathbf{F}_\bullet$ por módulos F_i de rango r_i. Definimos la característica de Euler de M como

$$\chi(M) = \sum_{i=0}^{n} (-1)^i r_i.$$

El siguiente teorema, debido a Vasconcelos, caracteriza los módulos cuya característica de Euler es cero, y que serán de interés próximamente.

Lema 5.7. *Sea M un A-módulo que admite una resolución libre finita de longitud finita. Entonces la característica de Eurler de M es un entero no negativo y*

1. *$\chi(M) > 0$ si y solo si $\operatorname{ann}_A(M) = 0$;*
2. *$\chi(M) = 0$ si y solo si $\operatorname{ann}_A(M) \neq 0$, si y solo si $0 :_A \operatorname{ann}_A(M) = 0$.*

Aplicando este resultado en el contexto habitual, donde $M = B_\nu$ para $\nu \geq \nu_0$, deducimos que $\chi(B_\nu) = 0$ ya que $\operatorname{ann}_A(B_\nu) \neq 0$ y está generado por la resultante. La última parte dice que $\operatorname{ann}_A(B_\nu)$ contiene un elemento que no es divisor de cero, que justamente es la resultante mencionada.

5.3. El Invariante de McRae. Estamos ahora en condiciones de definir el invariante de McRae de un A-módulo que admite una resolución libre finita y tal que $\chi(M) = 0$. Nuestra aplicación será como siempre al caso en que A es el anillo de coeficientes universales, y $M = B_\nu$ para $\nu \geq \nu_0$.

De acuerdo con los establecido en el trabajo de Northcott [Nor76], daremos la siguientes definiciones:

Definición 5.8. Si M es un A-módulo que tiene una resolución libre finita de longitud uno de la forma $0 \to F_1 \to F_0 \to M \to 0$ y tal que $\chi(M) = 0$, diremos que M es un *módulo elemental*.

Si M es un A-módulo elemental, entonces el ideal de Fitting inicial $\mathrm{Fitt}(M)$ es principal (además es integro y fraccionario).

Definición 5.9. Notaremos por $\mathfrak{S}(M)$ al ideal de Fitting inicial de estos módulos y lo llamaremos *invariante de McRae* de M. Más en general, si M es un A-módulo. Dada una resolución finita $\mathbf{F}_\bullet$ por módulos elementales F_i, se le asocia un ideal invertible fraccionario

$$\mathfrak{S}(M) = \prod_{i=0}^{n} \mathrm{Fitt}(F_i)^{(-1)^i},$$

que se denomina *invariante de McRae de* M.

Enunciaremos a continuación algunas propiedades importantes del invariante de McRae que están para probar en los ejercicios de esta sección, y cuya demostración se encuentra completa en [Nor76, Cap. 3.6 y 6.2].

Sea M un A-módulo que tiene una resolución finita de módulos elementales. Entonces el ideal $\mathfrak{S}(M)$ de A es un ideal principal generado por un elemento que no es divisor de cero. Además, satisface que $\mathrm{Fitt}(M) \subset \mathfrak{S}(M)$ y es minimal con esta propiedad, es decir, si I es un ideal principal de A que contiene a $\mathrm{Fitt}(M)$, entonces también contiene a $\mathfrak{S}(M)$.

La propiedad anterior implica que si A es un DFU, como lo es el anillo de coeficientes universales, entonces $\mathfrak{S}(M)$ está generado por el gcd de los generadores de $\mathrm{Fitt}(M)$.

Además, hay una serie de equivalencias al hecho de tener una resolución por módulos elementales, que se resumen en el siguiente resultado:

Lema 5.10. *Si M es un A-módulo, entonces las siguientes tres afirmaciones son equivalentes:*

1. *M admite una resolución finita por módulos elementales;*
2. *M admite una resolución libre finita de característica de Euler cero;*
3. *M admite una resolución libre finita y $\mathrm{ann}(M)$ contiene un elemento que no es divisor de cero.*

Esto último nos dice que M admite una resolución libre finita y $\mathrm{ann}(M)$ contiene un elemento que no es divisor de cero, entonces M admite un resolución finita por módulos elementales y por lo tanto podemos definir el invariante de McRae como en la Definición 5.9.

en la próxima parte daremos un método constructivo para calcular el ideal $\mathfrak{S}(M)$.

5.4. Un algoritmo par calcular $\mathfrak{S}(M)$. A partir de ahora supondremos que A es un dominio íntegro, y que M es un A-módulo que admite una resolución finita libre de longitud $n \geq 1$,

$$\mathbf{F}_\bullet: \qquad 0 \to F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} \cdots \to F_1 \xrightarrow{\partial_1} F_0 \to M \to 0,$$

tal que $\chi(M) = \sum_i (-1)^i r_i = 0$, donde r_i es el rango del módulo F_i.

Descompongamos ahora los módulos F_i del complejo $\mathbf{F}_\bullet$, empezando desde la izquierda.

Sea $F_n^{(0)} := 0$ y $F_n^{(1)} := F_n$, escribimos entonces $F = F_n^{(0)} \oplus F_n^{(1)}$. Como ∂_n es inyectivo, entonces por el Lema de McCoy, 5.4, se tiene que:

1. F_{n-1} se escinde en $F_{n-1}^{(0)} \oplus F_{n-1}^{(1)}$, donde estos dos módulos son libres de rango r_n y $r_{n-1} - r_n$ respectivamente. El morfismo $\partial_n : F_n \to F_{n-1}$ se puede escribir

matricialmente como $\partial_n = (\phi_n \ c_n)$, donde $\det(\phi_n) \neq 0$. Se reescribe el comienzo de la resolución anterior de la forma

$$\begin{array}{ccccccc} 0 & \longrightarrow & 0 & \longrightarrow & F_{n-1}^{(0)} & \longrightarrow & \cdots \\ & & \oplus & \overset{\phi_n}{\nearrow} & \oplus & & \\ 0 & \longrightarrow & F_n^{(1)} & \xrightarrow{c_n} & F_{n-1}^{(1)} & \longrightarrow & \cdots \end{array}$$

2. Ahora, como el morfismo ϕ_n es biyectivo sobre el cuerpo de fracciones de A y como $\mathrm{im}(c_n) = \ker(c_{n-1})$, se deduce que F_{n-2} se parte en $F_{n-2}^{(0)} \oplus F_{n-2}^{(1)}$, en dos módulos libres de rango $r_{n-1} - r_n$ y $r_{n-2} - (r_{n-1} - r_n)$ respectivamente. El morfismo $\partial_{n-1} : F_n \to F_{n-1}$ se escribe matricialmente como

$$\partial_{n-1} = \begin{pmatrix} a_{n-1} & \phi_{n-1} \\ b_{n-1} & c_{n-1} \end{pmatrix},$$

donde $\det(\phi_{n-1}) \neq 0$. Se reescribe el comienzo de la resolución $\mathbf{F}_\bullet$ como

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & F_{n-1}^{(0)} & \xrightarrow{a_{n-1}} & F_{n-2}^{(0)} & \longrightarrow & \cdots \\ & & \oplus & \overset{\phi_n}{\nearrow} & \oplus & \overset{\phi_{n-1}\ b_{n-1}}{\searrow\nearrow} & \oplus & & \\ 0 & \longrightarrow & F_n^{(1)} & \xrightarrow{c_n} & F_{n-1}^{(1)} & \xrightarrow{c_{n-1}} & F_{n-2}^{(1)} & \longrightarrow & \cdots \end{array}$$

3. de esta forma se obtiene que para cada $i = 0, \dots, n$ F_i se escinde como $F_i = F_i^{(0)} \oplus F_i^{(1)}$ con ambos módulos libres de rango $\sum_{j=0}^{n-i-1}(-1)^j r_{i+1+j}$ y $\sum_{j=0}^{n-i}(-1)^j r_{i+j}$ repectivamente, y para $i = 1, \dots, n$ el morfismo $\partial_i : F_i^{(0)} \oplus F_i^{(1)} \to F_{i-1}^{(0)} \oplus F_{i-1}^{(1)}$ se escribe matricialmente como

$$\partial_i = \begin{pmatrix} a_i & \phi_i \\ b_i & c_i \end{pmatrix},$$

donde el determinante de ϕ_i es no nulo.
4. Finalmente, dado que $\chi(M) = \sum_{j=0}^{n}(-1)^j r_j = 0$, una descomposición de esta forma termina con un morfismo ∂_1 que se escribe como $(a_1 \ \phi_1)^t$, con $\det(\phi_1) \neq 0$, obteniéndose una resolución libre con morfismos como se ilustra en el diagrama:

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & F_{n-1}^{(0)} & \xrightarrow{a_{n-1}} & F_{n-2}^{(0)} & \longrightarrow \cdots & \cdots & \xrightarrow{a_2} & F_1^{(0)} & \xrightarrow{a_1} & F_0^{(0)} \\ & & \oplus & \overset{\phi_n}{\nearrow} & \oplus & \overset{\phi_{n-1}\ b_{n-1}}{\searrow\nearrow} & \oplus & \overset{\phi_{n-2}}{\nearrow} & & \overset{\phi_2}{\nearrow} & \oplus & \overset{\phi_1\ b_1}{\searrow\nearrow} & \oplus \\ 0 & \longrightarrow & F_n^{(1)} & \xrightarrow{c_n} & F_{n-1}^{(1)} & \xrightarrow{c_{n-1}} & F_{n-2}^{(1)} & \longrightarrow \cdots & \cdots & \xrightarrow{a_2} & F_1^{(1)} & \xrightarrow{c_1} & F_0^{(1)} \end{array}$$

Obsérvese que se obtiene una familia de matrices cuadradas, que están definidas complementando las filas o columnas de la matriz anteriormente definida, y cuyo determinate es no nulo.

Corolario 5.11. *Con la notación anterior, se tiene*

$$\mathfrak{S}(M) = \det(\mathbf{F}_\bullet)A := \prod_{i=1}^{n} \det(\phi_i)^{(-1)^{i-1}} A = \frac{\det(\phi_1)\det(\phi_3)\dots}{\det(\phi_2)\det(\phi_4)\dots} A.$$

Vimos que $\mathfrak{S}(M)$ es el menor ideal principal que contiene a $\mathrm{Fitt}(M)$, esto dice que $\mathfrak{S}(M)$ es la parte de codimensión uno de $\mathrm{Fitt}(M)$. A partir de la Proposición 5.3.3., se tiene que los primos asociados de $\mathrm{Fitt}(M)$ son exactamente los mismos que los primos asociados de $\mathrm{ann}_A(M)$. Más precisamente, si A es un DFU, y $P_1, \dots, P_r$ denotan los factores irreducibles del gcd de un sistema de generadores de $\mathrm{Fitt}(M)$,

entonces $P_1^{\ell_1} \dots P_r^{\ell_r}$ es un generador de $\mathfrak{S}(M)$, donde ℓ_i denota la multiplicidad de $\mathfrak{S}(M)$ en $A/(P_i)$ que también suele escribirse e_i.

Aplicando estos resultados al anillo $A = \mathbb{Z}[U_{i,\alpha}]$ de coeficientes universares, que puede ser reemplazado por otro anillo aplicando la propiedad de cambio de base, tomando $M = B_\nu$ con $\nu \geq \nu_0$, se obtiene que

$$\mathfrak{S}(B_\nu) = \det((\mathbf{K}_\bullet)_\nu)A := \prod_{i=1}^{n} \det(\phi_i^\nu)^{(-1)^{i-1}} A.$$

Además, si $\nu \geq \nu_0$, se tiene que los primos asociados de $\mathrm{Fitt}(B_\nu)$ son exactamente los mismos que los primos asociados de $\mathrm{ann}_A(B_\nu)$, que $\mathrm{ann}_A(B_\nu)$ es principal y primo, y que $\mathfrak{S}(B_\nu)$ es el menor ideal principal que contiene a $\mathrm{Fitt}(B_\nu)$, esto dice que no sólo $\mathfrak{S}(B_\nu)$ es la parte de codimensión uno de $\mathrm{Fitt}(B_\nu)$, sino que $\mathfrak{S}(B_\nu) = \mathrm{ann}_A(B_\nu)$.

Ejercicios.

1. Sea A un anillo conmutativo, y sea M un A-módulo presentado por
$$A^n \xrightarrow{\phi} A^n \to M \to 0,$$
donde $\det(\phi)$ no es divisor de cero en A. Entonces
$$\mathrm{ann}_A(M) = \mathrm{Fitt}_0(M) :_A \mathrm{Fitt}_1(M).$$
2. En el contexto del ejercicio anterior, si M es un A-módulo presentado por
$$A^n \xrightarrow{\phi} A^m \to M \to 0,$$
donde $\det(\phi)$ no es divisor de cero en A, $m > n$, y $\operatorname{depth} \mathrm{ann}_A M = m - n + 1$. Entonces $\mathrm{ann}_A(M) = \mathrm{Fitt}_0(M)$.
3. Sea M un A-módulo que tiene una resolución finita de módulos elementales. Entonces las siguientes afirmaciones son verdaderas:
   a) Supongamos que se tiene dos resoluciones por módulos elementales
   $$0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$
   y
   $$0 \to F'_{n'} \to F'_{n'-1} \to \cdots \to F'_1 \to F'_0 \to M \to 0$$
   del A-módulo M, entonces
   $$\prod_{i=0}^{n} \mathrm{Fitt}(F_i)^{(-1)^i} = \prod_{i=0}^{n'} \mathrm{Fitt}(F'_i)^{(-1)^i}.$$
   b) Si se tiene una sucesión exacta de la forma $0 \to M' \to M \to M'' \to 0$ de A-módulos, donde M' y M'' admiten ambos una resolución finita de módulos elementales, entonces $\mathfrak{S}(M) = \mathfrak{S}(M')\mathfrak{S}(M'')$.
   c) Sea S un conjunto multiplicativamente cerrado de A. Entonces el A_S-módulo M_S tiene una resolución finita de módulos elementales, y se tiene que $\mathfrak{S}(M)A_S = \mathfrak{S}(M_S)$.
   d) El ideal fraccionario $\mathfrak{S}(M)$ de A, resulta un ideal íntegro de A. Más aún es un ideal principal generado por un elemento que no es divisor de cero, tal que $\mathrm{Fitt}(M) \subset \mathfrak{S}(M)$ y es minimal con esta propiedad, es decir, si I es un ideal principal de A que contiene a $\mathrm{Fitt}(M)$, entonces también contiene a $\mathfrak{S}(M)$.

e) La propiedad (d) implica que cualquier generador de $\mathfrak{S}(M)$ sirve como gcd (máximo común divisor) de cualquier conjunto de generadores de $\mathrm{Fitt}(M)$. En particular, si A es un DFU, $\mathfrak{S}(M)$ está generado por el gcd de los generadores de $\mathrm{Fitt}(M)$.

6. Ejemplos

En esta sección desarrollaremos dos ejemplos de resultantes multihomogéneas, que serán acompañados con el correspondiente códico en Macaulay2 [GS], usando el paquete `EliminationMatrices` desarrollado junto con Laurent Busé y Manuel Dubinsky [BBD12].

Ejemplo 6.1. En este ejemplo veremos un caso muy simple, de dos polinomios homogéneos en dos variables, uno cuadrático y uno lineal. Una aplicación típica de este ejemplo es el caso del cálculo del descriminante de un polinomio f_1.

Sea $A = \mathbb{Q}[a, b, c, d, e]$ y $R = A[x, y]$, $f_1 = ax^2 + bxy + cy^2$ y $f_2 = dx + ey$.

```
i1 : load "EliminationMatrices.m2"

i2 : R=QQ[a,b,c,d,e,x,y];

i3 : f1=a*x^2+b*x*y+c*y^2;

i4 : f2=d*x+e*y;

i5 : vari = {x,y};

i6 : m =matrix {{f1,f2}};

              1       2
o6 : Matrix R  <--- R

i7 : eliminationMatrix(vari,m, Strategy=> Macaulay)

o7 = {2} | a d 0 |
     {2} | b e d |
     {2} | c 0 e |

              3       3
o7 : Matrix R  <--- R

i8 : det(oo)

        2              2
o8 = c*d  - b*d*e + a*e

o8 : R
```

Un ejemplo clásico es calcular la resultante de $f_1 = ax^2 + bxy + cy^2$ y $f_2 = 2ax + by$, que se obtiene substituyendo d por $2a$ y e por b.

```
i9 : substitute(oo,{d=>2*a, e=>b})

          2     2
o9 = - a*b  + 4a c

o9 : R

i10 : factor oo

             2
o10 = (a)(- b  + 4a*c)

o10 : Expression of class Product
```

El hecho de poder evaluar directamente d en $2a$ y e en b es justamente la propiedad de universalidad que tanto hemos remarcado. Eso dice que calcular la resultante conmuta con el morfismo de especialización.

Otra forma de calcular la matriz resultante de Macaulay `Mnu` es como el morfismo

$$M_{\nu_0} := (R(-2) \oplus R(-1) \to R)_{\nu_0}\,.$$

para $\nu_0 = (2-1)+(1-1)+1 = 2$.

```
i11 : K = koszul m

       1      2      1
o11 = R  <-- R  <-- R
      0      1      2

o11 : ChainComplex

i12 : nu = (2-1)+(1-1)+1;

i13 : Mnu = mapsComplex (nu, vari, K)

o13 = {{2} | a d 0 |, 0}
       {2} | b e d |
       {2} | c 0 e |

o13 : List

i14 : de = detComplex (nu, vari, K)

         2              2
o14 = c*d  - b*d*e + a*e

o14 : frac(R)
```

Observar que en el caso en que ν_0 es el índice de saturación, la matriz M_{ν_0} de dos polinomios homogéneos en dos variables, siempre resultará cuadrada. No es así si $\nu > \nu_0$, ni para más polinomios y más variables para ninguún ν. Podemos verificar

este hecho en este ejemplo, así como que el determinante del complejo $\mathbf{K}_\bullet(f_1, f_2; R)_\nu$ no depende de $\nu \geq \nu_0$, y coincide con $cd^2 - bde + ae^2$.

```
i15 : Mnu = mapsComplex (nu+1, vari, K)

o15 = {{3} | a 0 d 0 0 |, {1} | -d |}
       {3} | b a e d 0 |  {1} | -e |
       {3} | c b 0 e d |  {2} | a  |
       {3} | 0 c 0 0 e |  {2} | b  |
                          {2} | c  |

o15 : List
```

Esto dice que el complejo $\mathbf{K}_\bullet(f_1, f_2; R)$ en grado $\nu = 3$ se escribe

$$0 \to R(-3)_\nu \xrightarrow{(-f_2, f_1)} R(-2)_\nu \oplus R(-1)_\nu \xrightarrow{\binom{f_1}{f_2}} R_\nu \to 0,$$

el cual puede escribirse, identificando $R(-3)_\nu$ con A, $R(-2)_\nu \oplus R(-1)_\nu$ con $A^2 \oplus A^3$ y R_ν con A^4

$$0 \to A \xrightarrow{\begin{pmatrix} -d \\ -e \\ a \\ b \\ c \end{pmatrix}} A^2 \oplus A^3 \xrightarrow{\begin{pmatrix} a & 0 & d & 0 & 0 \\ b & a & e & d & 0 \\ c & b & 0 & e & d \\ 0 & c & 0 & 0 & e \end{pmatrix}} A^4 \to 0.$$

```
i16 : de = detComplex (nu+1, vari, K)

         2              2
o16 = c*d  - b*d*e + a*e

o16 : frac(R)
```

Además, el divisor asociado al 0-ésimo ideal de Fitting de M_ν, $\mathrm{Fitt}_0(M_\nu)$, para todo $\nu \geq \nu_0$, no depende de ν. Estudiando la descomposición primaria de $\mathrm{Fitt}_0(M_\nu)$, vemos que la parte principal de $\mathrm{Fitt}_0(M_\nu)$ está dada por el primo $\mathfrak{A} = (cd^2 - bde + ae^2)$.

En este ejemplo, el ideal $\mathrm{Fitt}_0(M_\nu)$ se calcula como el ideal de menores de 4 por 4 (maximales) de la matriz anterior.

```
i17 : minors(4,o15_0)

              2 2                    2         2    2           2       2
o17 = ideal (c d  - b*c*d*e + a*c*e , - b*c*d  + b d*e - a*b*e , a*c*d
      ------------------------------------------------------------------
                  2 2     2         2      3       3      2        2
      - a*b*d*e + a e , c*d e - b*d*e  + a*e , - c*d  + b*d e -a*d*e )

o17 : Ideal of R
```

Su descomposicón primaria se caalcula como sigue

```
i18 : primaryDecomposition oo
```

```
                2              2                  2   2   2
o18 = {ideal(c*d  - b*d*e + a*e ), ideal (c, a, e , d , b )}

o18 : List
```

De acá leemos que

$$\mathrm{Fitt}_0(M_\nu) = \mathfrak{p} \cap \mathfrak{q},$$

donde $\mathfrak{A} = (cd^2 - bde + ae^2)$ es la parte principal de $\mathrm{Fitt}_0(M_\nu)$, y $\mathfrak{q} = (c, a, e^2, d^2, b^2)$ es la componente soportada sobre el ideal (a, b, c, d, e), es decir, $V(\mathfrak{q})$ es un punto múltiple sobre el origen.

Ejemplo 6.2. En este ejemplo veremos un caso apenas más complicados, de tres polinomios homogéneos en tres variables, uno cuadrático y dos lineal. La elección de los grados está limimitada por el comando `primaryDecomposition`.

Sea $A = \mathbb{Q}[a, b, c, d, e, f, g, h, x, y, z]$ y $R = A[x, y, z]$, $f_1 = ax^2 + bxy + cy^2$ y $f_2 = dx + ey$.

```
i1 : load "eliminationMatrices.m2"

i2 : R=QQ[a,b,c,d,e,f,g,h,x,y,z];

i3 : f1=a*x^2+b*x*y+c*y^2+d*z^2;

i4 : f2=e*x+a*y+f*z;

i5 : f3=g*x+h*y+e*z;

i6 : vari = {x,y,z};

i7 : m =matrix {{f1,f2,f3}};

             1       3
o7 : Matrix R  <--- R
```

Calculamos la matriz resultante de Macaulay `Mnu` como el morfismo

$$M_{\nu_0} := (R(-2) \oplus R(-1) \oplus R(-1) \to R)_{\nu_0}.$$

para $\nu_0 = 2$.

```
i8 : K = koszul m

      1      3      3      1
o8 = R  <-- R  <-- R  <-- R
     0      1      2      3

o8 : ChainComplex

i9 : nu = (2-1)+(1-1)+(1-1)+1

o9 = 2
```

Además, podemos verificar que el determinante del complejo $\mathbf{K}_\bullet(f_1, f_2f_3; R)_\nu$ no depende de $\nu \geq \nu_0$. Además agregamos el comando `time` para mostrar el poco tiempo de cómputo que estos cálculos insumen, y verificamos que la matriz `Mnu_0` tiene rango máximo.

```
i10 : Mnu = mapsComplex (nu, vari, K)

o10 = {{2} | a e 0 0 g 0 0 |, {1} | -g |, 0}
       {2} | b a e 0 h g 0 |  {1} | -h |
       {2} | 0 f 0 e e 0 g |  {1} | -e |
       {2} | c 0 a 0 0 h 0 |  {1} | e  |
       {2} | 0 0 f a 0 e h |  {1} | a  |
       {2} | d 0 0 f 0 0 e |  {1} | f  |

o10 : List

i11 : rank Mnu_0 == rank target Mnu_0

o11 = true
```

Esto dice que el complejo $\mathbf{K}_\bullet(f_1, f_2; R)$ en grado $\nu = 2$ se escribe

$$0 \to R(-4)_\nu \xrightarrow{\delta_2^\nu} (R(-3) \oplus R(-3) \oplus R(-2))_\nu \xrightarrow{\delta_1^\nu} (R(-2) \oplus R(-1) \oplus R(-1))_\nu \xrightarrow{\delta_0^\nu} R_\nu \to 0,$$

el se escribe, siendo $\nu = 2$, identificando $R(-4)_\nu = R(-3)_\nu = 0$, $R(-2)_\nu \cong A$, $R(-1)_\nu = A^3$ y $R_\nu \cong A^6$, con

$$0 \to 0 \to 0 \oplus 0 \oplus A \xrightarrow{\begin{pmatrix} -g \\ -h \\ -e \\ e \\ a \\ f \end{pmatrix}} A \oplus A^3 \oplus A^3 \xrightarrow{\begin{pmatrix} a & e & 0 & 0 & g & 0 & 0 \\ b & a & e & 0 & h & g & 0 \\ 0 & f & 0 & e & e & 0 & g \\ c & 0 & a & 0 & 0 & h & 0 \\ 0 & 0 & f & a & 0 & e & h \\ d & 0 & 0 & f & 0 & 0 & e \end{pmatrix}} A^6 \to 0.$$

Obsérvese ahora que el cálculo del ideal de Fitting $\mathrm{Fitt}_0(\texttt{Mnu\_0})$ es casi instantáneo:

```
i12 : fitt= time(minors (rank Mnu_0, Mnu_0))
     -- used 0.003 seconds

                3 2         3       4           2        2 2
o12 = ideal (- a e f + a*b*e f - c*e f - a*b*e*f g + 2c*e f g -
      ------------------------------------------------------------
       2     2      3 2     2   2       2 2                      3
      a d*f*g  - c*f g  + 2a e*f h - b*e f h + 2a*d*e*f*g*h + b*f g*h
      ------------------------------------------------------------
           2   2      3 2   4 2    2   3        4    2
      - d*e f*h  - a*f h , a e  - a b*e  + a*c*e  + a b*e*f*g -
      ------------------------------------------------------------
            2       3   2        2 2     3            2
      2a*c*e f*g + a d*g  + a*c*f g  - 2a e*f*h + a*b*e f*h -
      ------------------------------------------------------------
        2               2           2 2    2 2 2     3 3        4
      2a d*e*g*h - a*b*f g*h + a*d*e h  + a f h , - a e  + a*b*e  -
```

```
      ------------------------------------------------------------------
         5        2          3       2     2        2 2     2 2
      c*e  - a*b*e f*g + 2c*e f*g - a d*e*g  - c*e*f g  + 2a e f*h -
      ------------------------------------------------------------------
         3           2          2         3 2        2 2     3 3
      b*e f*h + 2a*d*e g*h + b*e*f g*h - d*e h  - a*e*f h , - a e  +
      ------------------------------------------------------------------
          4      5        2          3       2     2        2 2
      a*b*e  - c*e  - a*b*e f*g + 2c*e f*g - a d*e*g  - c*e*f g  +
      ------------------------------------------------------------------
        2 2         3           2          2         3 2
      2a e f*h - b*e f*h + 2a*d*e g*h + b*e*f g*h - d*e h  -
      ------------------------------------------------------------------
          2 2   3 2         3       4                      2
      a*e*f h , a e h - a*b*e h + c*e h + a*b*e*f*g*h - 2c*e f*g*h +
      ------------------------------------------------------------------
       2   2       2 2      2     2      2   2             2
      a d*g h + c*f g h - 2a e*f*h  + b*e f*h  - 2a*d*e*g*h  -
      ------------------------------------------------------------------
         2   2      2 3      2 3     3 2         3       4
      b*f g*h  + d*e h  + a*f h , - a e g + a*b*e g - c*e g -
      ------------------------------------------------------------------
              2       2   2    2   3      2 3     2
      a*b*e*f*g  + 2c*e f*g  - a d*g  - c*f g  + 2a e*f*g*h -
      ------------------------------------------------------------------
         2                2       2 2       2   2      2   2
      b*e f*g*h + 2a*d*e*g h + b*f g h - d*e g*h  - a*f g*h )

o12 : Ideal of R
```

Su descomposición primaria se calcula así

```
i13 : primaryDecomposition fitt

               3 2        3      4                    2       2   2
o13 = {ideal(a e  - a*b*e  + c*e  + a*b*e*f*g - 2c*e f*g + a d*g  +
      ------------------------------------------------------------------
         2 2     2          2                       2         2 2
      c*f g  - 2a e*f*h + b*e f*h - 2a*d*e*g*h - b*f g*h + d*e h  +
      ------------------------------------------------------------------
         2 2                    3   4 2   6   4       2 2 2    3   2
      a*f h ), ideal(h, g, f, e , a e , a -2a b*e + a b e + 2a c*e )}
```

y se observa que

$$\mathrm{Fitt}_0(M_\nu) = \mathfrak{A} \cap \mathfrak{q},$$

donde $\mathfrak{A} = (a^3e^2 - abe^3 + ce^4 + abefg - 2ce^2fg + a^2dg^2 + cf^2g^2 - 2a^2efh + be^2fh - 2adegh - bf^2gh + de^2h^2 + af^2h^2)$ es la parte principal de $\mathrm{Fitt}_0(M_\nu)$, y $\mathfrak{q} = (h, g, f, e^3, a^4e^2, a^6 - 2a^4be + a^2b^2e^2 + 2a^3ce^2)$ es la componente soportada sobre el ideal (h, g, f, e, a), es decir, $V(\mathfrak{q})$ es un plano múltiple de codimensión 5.

Obsérvese que, como antes, $\mathfrak{A}$ puede calcularse mediante el determinante del complejo $\mathbf{K}_\bullet(f_1, f_2; R)$ en grado $\nu = 2$, uasando el comando `detComplex (nu, vari, K)`.

Apéndice

El ojectivo de esta sección es complementar el contenido de las notas con dos temas fuertemente vinculados con la teoría de eliminación, y cuyo interés trasciende la aplicación que le daremos.

Estos dos temas con, primero el estudio de los módulos de cohomología local, y luego uno de los invariantes más importantes de un módulo graduado, la regularidad de Castelnuovo-Mumford.

El primero, cohomología local, aparece en nuestras aplicaciones al definir el ideal eliminante, ya que escribimos $\mathfrak{A} = H^0_{R_+}(B)_0$, es decir, como el 0-ésimo módulo de cohomología local de B en grado 0.

El segundo, el estudio de la regularidad de Castelnuovo-Mumford, aparece al querer conocer a partir de qué grado el módulo $H^0_{R_+}(B)_\nu$ se anula. El Lema B.4 da una respuesta a este problema en el caso en que I esté dado por una sucesión regular.

A.1. Cohomología local. La cohomología local fue desarrollada por Alexander Grothendieck en la década de 1960, en parte, para responder a una conjetura de Pierre Samuel acerca de cuándo ciertos tipos de anillos conmutativos son de dominios de factorización única.

La cohomología local se ha convertido en una herramienta indispensable y es objeto de mucha investigación. Mostraremos acá algunas propiedades y aplicaciones de la cohomología local, principalmente orientadas a la teoría de regularidad.

Entre muchos otros atributos, cohomología local permite responder a muchas preguntas aparentemente difícil. Un buen ejemplo de este problema, donde cohomología local ofrece una respuesta parcial, es cuántos generadores tiene un ideal a menos de radical.

A.1.1. Como funtor derivado de $\Gamma_I(-)$. Sea R un anillo noetheriano, $I \subset R$ un ideal y M un R-módulo. Se define

$$\Gamma_I(M) := \{m \in M : \text{ existe } n \in \mathbb{N} \text{ tal que } I^n m = 0\}$$

Observación A.1. Obsérvese que $\mathrm{Hom}_R(R/I, M) = \{m \in M : Im = 0\}$ para todo ideal I de R, se obtiene el isomorfismo natural

$$\Gamma_I(M) \cong \varinjlim \mathrm{Hom}_R(R/I^n, M).$$

Luego, $M \mapsto \Gamma_I(M)$ define un funtor covariante $\Gamma_I(-)$.

Lema A.2. $\Gamma_I(-)$ *es un funtor aditivo exacto a izquierda.*

Demostración. cf. [Hun07, Sec. 2] o [BH93, Prop. 3.5.1] en el caso $I = \mathfrak{m}$. □

Definición A.3. Los funtores de cohomología local $H^i_I(-)$ son los funtores derivados a derecha de $\Gamma_I(-)$. Es decir, si $\mathcal{I}^\bullet$ es una resolución injectiva del R-módulo M, entonces $H^i_I(M) \cong H^i(\Gamma_I(\mathcal{I}^\bullet))$ para todo $i \geq 0$.

Observación A.4. Sea R un anillo noetheriano.

1. Sea M un R-módulo, entonces $H^0_I(M) \cong \Gamma_I(M)$ y $H^i_I(M) = 0$ para todo $i < 0$;
2. si J es un R-módulo injectivo, entonces $H^i_I(J) = 0$ para todo $i > 0$;

3. para todo R-módulo M y todo $i \geq 0$ se tiene
$$H^i_I(M) \cong \lim_{\to} \operatorname{Ext}^i_R(R/I^n, M);$$

Hay una inyección natural
$$\varphi : \operatorname{Ext}^0_R(R/I^n, M) = \hom(R/I^n, M) \to M$$
dada por $\varphi(f) = f(1)$, tal que $\operatorname{im}(\varphi) = \{m \in M : I^n m = 0\} = 0 :_M I^n$.

Aplicando el funtor límte directo $\lim_{\to} \operatorname{Ext}^0_R(R/I^n, M) = \lim_{\to} \hom(R/I^n, M)$ que coincide con la unión $\cup_n m \in M : I^n m = 0$ que a su vez coincide con $\Gamma_I(M)$ por definición.

El funtor $\operatorname{Ext}^i_R(R/I^{\cdot}, -)$ es el i-ésimo derivado del funtor $\hom_R(R/I^n, -)$. Tomando colímites filtrantes, que conmutan con tomar funtores derivados por ser el colímite filtrante un funtor exacto (cf. [Eis95, Prop. A6.4]) se obtiene la equivalencia deseada.

Observación A.5. Sea R un anillo noetheriano.

1. como $H^\bullet_I(-)$ es un δ-funtor, dada una sucesión exacta corta de R-módulos $0 \to M' \to M \to M'' \to 0$, da una sucesión exacta larga de cohomología
$$0 \to \Gamma_I(M') \to \Gamma_I(M) \to \Gamma_I(M'') \to H^1_I(M') \to \cdots$$
2. además, si I y J son ideales de A, como $\{I^n + J^n\}$ es cofinal con $\{(I+J)^n\}$ y $\{I^n \cap J^n\}$ es cofinal con $\{(I \cap J)^n\}$, y $\Gamma_I(\Gamma_J(M)) = \Gamma_J(\Gamma_I(M)) = \Gamma_{I+J}(M)$, de la sucesión exacta corta
$$0 \to R/(I^n \cap J^n) \to R/I^n \oplus R/J^n \to R/(I^n + J^n) \to 0,$$
aplicando $\operatorname{Hom}_R(-, M)$, se tiene la sucesión exacta larga de Mayer-Vietoris
$$0 \to \Gamma_{I+J}(M) \to \Gamma_I(M) \oplus \Gamma_J(M) \to \Gamma_{I\cap J}(M) \to H^1_{I+J}(M) \to \cdots .$$

A.1.2. Como la homología del complejo de Čech. Sea S un anillo noetheriano, $R = S[x_1, \ldots, x_n]$, $\mathfrak{m} := (x_1, \ldots, x_n)$ el único ideal maximal graduado y M un R-módulo. El morfismo de localización en x_i define un complejo
$$\mathcal{C}^\bullet_{\mathfrak{m}}(M) : 0 \to M \to \oplus_i M_{x_i} \to \oplus_{i,j} M_{x_i x_j} \to \cdots$$
Observe que $\ker(M \to \oplus_i M_{x_i}) = \Gamma_{\mathfrak{m}}(M)$. Por lo tanto, $H^0_{\mathfrak{m}}(M) = H^0(\mathcal{C}^\bullet_{\mathfrak{m}})$

Proposición A.6. *Para todo R-módulo M y para todo $i \geq 0$,*
$$H^i_{\mathfrak{m}}(M) = H^i(\mathcal{C}^\bullet_{\mathfrak{m}}).$$

Si R no es noetheriano, el complejo de Čech recién definido no siempre calcula los funtores derivados de $\Gamma_I(-)$ en la categoría de R-módulos. Ni siquiera si I es finitamente generado. Por esta y otras razones, la definición general de cohomología local probablemente debe hacerse en una categoría más amplia (haces sobre $\operatorname{Spec}(R)$, cf. [Har67]).

Ejemplo A.7. Sea p un número primo. Calculamos $H_{\mathfrak{p}}(\mathbb{Z})$, donde $\mathfrak{p}$ es el ideal generado por p. Dado que $\mathbb{Z}$ es un dominio de ideales principales, todos los módulos divisibles son inyectivos, y entonces una resolución inyectiva de $\mathbb{Z}$ está dada por $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

El funtor $\Gamma_{\mathfrak{p}}(-)$ calcula la p^n-torsión para todo n. Aplicando este funtor a la resolución inyectiva, se obtiene que hay un único término que no se anula, que vivie en lugar cohomológico 1, a saber $\Gamma_{\mathfrak{p}}(\mathbb{Q}/\mathbb{Z})$. Por lo tanto todas las cohomologías locales se

anulan, excepto por $H^1_{\mathfrak{p}}(\mathbb{Z})$, que es isomorfa a la p-torsión en $\mathbb{Q}/\mathbb{Z}$. Por la propiedad de factorización única, este módulo puede ser identificado con $\mathbb{Z}[p^{-1}]/\mathbb{Z}$, donde $\mathbb{Z}[p^{-1}]$ es el anillo de los números racionales cuyos denominadores son una potencia de p.

Ejemplo A.8. Un ejemplo muy similar que sea más en la dirección de estas notas es el cálculo de los $H^i_{R_+}(M)$, donde $R = k[X]$, k es un cuerpo, $R_+ = (X)$, y M es un R-módulo finitamente generado.

Por el teorema de estructura para dominio de ideales principales, M es suma directa de módulos cíclicos. Como los funtores de cohomología local conmutan con sumas directas, que basta con calcular la cohomología local de $R/(g)$ para algún $g \in R$.

En primer lugar, calcular la cohomología local de R sobre sí mismo, es decir, cuando $g = 0$. Como en el ejempoplo anterior, como R es un dominio de ideales principales, todo módulos divisible es inyectivo.

La cápsula inyectiva de R es su cuerpo de fracciones $K = k(X)$, y como K/R es divisible, resulta inyectivo.

Así una resolución inyectiva está dada por

$$0 \to R \to K \to K/R \to 0.$$

Ahora aplicamos $\Gamma_{R_+}(-)$ y calculamos la cohomología local como la cohomología del complejo

$$0 \to \Gamma_{R_+}(K) \to \Gamma_{R_+}(K/R) \to 0.$$

Se desprende que $H^j_{R_+}(R) = 0$ para todo $j \neq 1$ y se puede identificar $\Gamma_{R_+}(K/R) \cong H^1_{R_+}(R)$.

Como antes, la propiedad de factorización única muestra que $H_{R_+}(R) \cong R[X^{-1}]/R = k[X, X^{-1}]/k[X]$.

Este módulo tiene una k-base formada por elementos de la forma $\frac{1}{X^n}$, con $n \geq 1$. La multiplicación por X en actúa de forma usual, $X \cdot \frac{1}{X^n} = \frac{1}{X^{n-1}}$ si $n > 1$, y al final, cuando $n = 1$, $X \cdot \frac{1}{X} = 0$.

Para calcular $H^i_{R_+}(R/(g))$ cuando $g \neq 0$, se utiliza la secuencia exacta corta,

$$0 \to R \xrightarrow{\times g} R \to R/(g) \to 0.$$

Esta sucesión exacta corta induce una larga sucesión exacta en cohomología, con las flechas de $H^i_{R_+}(R)$ a $H^i_{R_+}(R)$ dadas por la multiplicación por g. Dado que sólo hay un sólo módulo de cohomología local no nulo de R, se obtiene una sucesión exacta de cuatro términos:

$$0 \to H^0_{R_+}(R/(g)) \to H^1_{R_+}(R) \xrightarrow{\times g} H^1_{R_+}(R) \to H^1_{R_+}(R/(g)) \to 0.$$

Como cada elemento de $H^1_{R_+}(R)$ es anulado por una potencia de R_+, si h es un elemento coprimo con X, entonces h debe actuar como una unidad en $H^1_{R_+}(R)$. Esto último se debe a que existen $a, b \in R$ tales que $ah = 1 - bX$, y $1 - bX$ actúa como una unidad en este módulo. Escribiendo $g = X^n h$ donde $\gcd(h, X) = 1$, se deduce que $H^0_{R_+}(R/(g))$ es el núcleo de la multiplicación por X^n en $H^1_{R_+}(R)$ y $H^1_{R_+}(R/(g))$ es el conúcleo de la multiplicación por X^n. El conjunto de elementos en $H^1_{R_+}(R)$ anulados por X^n es generado por $\frac{1}{X^n}$ y por lo tanto es isomorfo a $R/(X^n)$. Como $H^1_{R_+}(R) = R[X^{-1}]/R$, este módulo es divisible por R, y por lo tanto el conúcleo es 0.

Resumimos los resultados: si $g = 0$, entonces $H^i_{R_+}(R) = 0$ para todo $i \neq 1$, y $H^1_{R_+}(R) \cong R[X^{-1}]/R = \frac{1}{X}k[X^{-1}]$. Si $g \neq 0$, escribimos $g = X^n h$, donde X no divide h, se tiene que $H^i_{R_+}(R/(g)) = 0$ para todo $i \neq 0$ y $H^0_{R_+}(R/(g)) \cong R/(X^n)$.

Como corolario de este ejemplo se desprenden (por inducción) dos resultados: el primero correspondiente al caso $g = 0$

Corolario A.9. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), y sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R. Entonces*

$$H^i_{R_+}(R) = 0 \text{ para todo } i \neq n, \text{ y } H^n_{R_+}(R) \cong \tfrac{1}{X_1 \cdots X_n} A[X_1^{-1}, \ldots, X_n^{-1}].$$

El segundo corolario corresponde al caso $g \neq 0$.

Corolario A.10. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R y $f_1, \ldots, f_n$ n polinomios homogéneos de R, con $\deg(f_i) = d_i$, que forman una sucesión regular en R. Escribamos $B := R/(f_1, \ldots, f_n)$. Entonces*

$$H^i_{R_+}(B) = 0 \text{ para todo } i \neq 0, \text{ y } H^0_{R_+}(B) \cong R/(X_1^{d_1}, \ldots, X_n^{d_n}).$$

A continuación enunciamos una propiedad fundamental de la cohomología local que nos permite cambiar de bases.

Proposición A.11. *Sea R un anillo noetheriano, I un ideal y M un R-módulo. Sea $\phi : R \to R'$ un morfismo de anillos y M' un R'-módulo. Sea I' el ideal $I \cdot R'$ en R'.*

1. *Si ϕ es playa entonces $H^j_I(M) \otimes_R R' \cong H^j_{I'}(M \otimes_R R')$. En particular, la cohomología local conmuta con localización y completación.*
2. *$H^j_I(N) \cong H^j_{I'}(N)$, donde la primera cohomología local es calculada sobre R y la segunda sobre R'.*

Demostración. Elija generadores $x_1, \ldots, x_n$ de I. El primer punto se sigue del hecho que $\mathcal{C}_\bullet(\mathbf{X}; M) \otimes_R R' \cong \mathcal{C}_\bullet(\mathbf{X}; M \otimes_R R')$, y como R' es playo sobre R la cohomología conmuta con $\otimes$.

El segundo punto es consecuencia de los isomorfismos $\mathcal{C}_\bullet(\mathbf{X}; N) \cong \mathcal{C}_\bullet(\mathbf{X}; R) \otimes_R N \cong \mathcal{C}_\bullet(\mathbf{X}; R) \otimes_R R' \otimes_{R'} N \cong \mathcal{C}_\bullet(\phi(\mathbf{X}); R') \otimes_R N \cong \mathcal{C}_\bullet(\phi(\mathbf{X}); N)$. □

Ésto dice que calcular la cohomología local sobre el anillo de base coincide con hacerlo sobre la localización.

B.2. Regularidad de Castelnuovo-Mumford. La regularidad de Castelnuovo-Mumford es un invariante fundamental en álgebra conmutativa y en geometría algebraica. Es una especie de cota universal para invariantes importantes de álgebras graduadas como por ejemplo para el máximo grado de las syzygies de un ideal y para el máximo grado de no-nulidad de los módulos de cohomología local.

Intuitivamente, mide la complejidad de un módulo o de un haz: la regularidad de un módulo aproxima el mayor grado de un generador minimal y la regularidad de un haz estima el menor twist para el cual el haz está generado por sus secciones globales. Este invariante fue usado para medir la complejidad de problemas computacionales en geometría algebraica y en álgebra conmutativa (ver por ejemplo [EG84] o [BM93]).

Se ha intentado encontrar cotas superiores para la regularidad de Castelnuovo-Mumford en termino de invariantes más simples como por ejemplo lo son la dimensión y la multiplicity. De todas formas, la regularidad de Castelnuovo-Mumford no puede ser acotada en término de ninguno de éstos dos, lo cual hace su cálculo aun más interesante y no trivial en muchos casos.

A pesar de que la definición original, dada por Mumford en 1966 en [Mum66] fue enunciada en término de anulación de la cohomología de haces, daremos una definición

puramente algebraica de esta regularidad, en términos de módulos cohomología local, dada originalmente por Ooishi en 1982 [Ooi82]. Cabe mencionar que las dos definiciones puramente algebraicas más populares de regularidad de Castelnuovo-Mumford son, una en término de números de Betti introducida por Eisenbud y Goto en 1984 en [EG84] y la otra usando cohomología local (ver def. en A.3), que es la que adoptaremos.

Hay dos resultados esenciales que motivan definir la regularidad de Castelnuovo-Mumford en términos de cohomología local: el teorema de Grothendieck que establece que $H^i_{\mathfrak{m}}(M) = 0$ para $i > \dim(M)$ y $i < \operatorname{depth}(M)$, así como la no nulidad de estos módulos para $i = \dim(M)$ y $i = \operatorname{depth}(M)$; y el teorema de anulación de Serre que determina la anulación de las piezas graduadas $H^i_{\mathfrak{m}}(M)_\mu$ para todo i, y todo $\mu \gg 0$. La regularidad de Castelnuovo-Mumford es una cota inferior para este grado de anulación.

Si $H^i_{\mathfrak{m}}(M) \neq 0$, se define

$$a_i(M) := \sup\{\mu \mid H^i_{\mathfrak{m}}(M)_\mu \neq 0\}, \tag{B.1}$$

en caso contrario, $a_i(M) := -\infty$. Una notación también frecuente en la literatura es la de "end", en nuestro caso, escribiríamos $a_i(M) := \operatorname{end}(H^i_{\mathfrak{m}}(M))$.

Definición B.1. (Regularidad Castelnuovo-Mumford) Sea M un R-módulo graduado y sea $\ell \in \mathbb{N}_0$. Se define la regularidad de Castelnuovo-Mumford de M a nivel ℓ como

$$\operatorname{reg}^\ell(M) := \sup\{a_i(M) + i : i \geq \ell\}.$$

La regularidad de Castelnuovo-Mumford de M se define como

$$\operatorname{reg}(M) := \operatorname{reg}^0(M).$$

Obsérvese que como $\operatorname{cd}_{\mathfrak{m}}(M) < \infty$, tenemos

$$\operatorname{reg}^\ell(M) \in \mathbb{Z} \cup \{-\infty\}.$$

El máximo sobre los i positivos es también un invariante interesante:

$$\operatorname{greg}(M) := \sup_{i>0}\{a_i(M) + i\} = \operatorname{reg}(M/H^0_{\mathfrak{m}}(M)).$$

Ver Bayer y Mumford [BM93] o [Mum66].

A continuación repasamos algunos hechos simples sobre la regularidad.

Lema B.2. *Sea M un R-módulo graduado finitamente generado $\ell, k \in \mathbb{N}_0$. Luego, se tienen las siguientes afirmaciones:*

1. *Si $k \geq l$ entonces* $\operatorname{reg}^k(M) \leq \operatorname{reg}^\ell(M)$.
2. *Para todo $n \in \mathbb{Z}$ se tiene* $\operatorname{reg}^\ell(M(n)) = \operatorname{reg}^\ell(M) - n$.
3. $\operatorname{reg}(M) = \operatorname{máx}\{\operatorname{end}(\Gamma_{\mathfrak{m}}(M)), \operatorname{reg}^1(M)\}$.
4. $\operatorname{reg}(M/\Gamma_{\mathfrak{m}}(M)) = \operatorname{reg}^1(M/\Gamma_{\mathfrak{m}}(M)) = \operatorname{reg}^1(M) \leq \operatorname{reg}(M)$.
5. $M = \Gamma_{\mathfrak{m}}(M)$ *si y sólo si* $\operatorname{reg}^1(M) = -\infty$.
6. $M = 0$ *si y sólo si* $\operatorname{reg}(M) = -\infty$.

Podemos dar una caracterización alternativas de Regularidad en nivel ℓ, sin necesitar pasar por la definición de los módulos $a_i(M)$:

Para todo $\ell \in \mathbb{N}_0$ y que todo R-módulo graduado finitamente generado tiene:

$$\operatorname{reg}^\ell(M) = \operatorname{ínf}\{r \in \mathbb{Z} : H^i_{\mathfrak{m}}(M)_{r+i-\ell} = 0, \forall i \geq \ell\}. \tag{B.2}$$

A continuación damos dos resultados que son los que motivaron este apéndice sobre regularidad, por su aplicación a estas notas sobre resultantes.

Lema B.3. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), y sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R. Entonces*

$$\operatorname{reg}(R) = 0.$$

Además, $\operatorname{reg}(R) = \operatorname{reg}^\ell(R)$ *para todo* $\ell \leq n$.

Demostración. Por el Corolario A.9 se tiene que $H^i_{R_+}(R) = 0$ para todo $i \neq n$, y $H^n_{R_+}(R) \cong \frac{1}{X_1 \cdots X_n} A[X_1^{-1}, \ldots, X_n^{-1}]$. Aplicando la definición de $a_i(R)$ dada en (B.1)

$$a_n(R) := \sup\{\mu \mid H^n_{\mathfrak{m}}(R)_\mu \neq 0\}, \text{ y } a_i(R) = -\infty \text{ si } i \neq n.$$

Ahora, como $H^n_{\mathfrak{m}}(R)_\mu = \frac{1}{X_1 \cdots X_n} A[X_1^{-1}, \ldots, X_n^{-1}]_\mu$, tenemos $H^n_{\mathfrak{m}}(R)_{-n} \cong \frac{1}{X_1 \cdots X_n} A \neq 0$ y $H^n_{\mathfrak{m}}(R)_\mu = 0$ si $\mu \geq -n+1$. Luego, $a_n(R) = -n$.

Por la Definición B.1 se tiene que $\operatorname{reg}^\ell(R) := \sup\{a_i(R) + i : i \geq \ell\}$, de lo que se deduce que para todo $\ell \leq n$,

$$\operatorname{reg}(R) = \operatorname{reg}^\ell(R) = \operatorname{reg}^n(R) = a_n(R) + n = -n + n = 0. \qquad \square$$

El segundo corolario corresponde al caso $g \neq 0$.

Lema B.4. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R y $f_1, \ldots, f_n$ n polinomios homogéneos de R, con $\deg(f_i) = d_i$, que forman una sucesión regular en R. Escribamos $B := R/(f_1, \ldots, f_n)$. Entonces*

$$\operatorname{reg}(B) = \sum_i (d_i - 1).$$

Además, $\operatorname{reg}^\ell(R) = -\infty$ *para todo* $\ell \geq 1$.

Demostración. Por el Corolario A.10 se tiene que $H^i_{R_+}(B) = 0$ para todo $i \neq 0$, y $H^0_{R_+}(B) \cong R/(X_1^{d_1}, \ldots, X_n^{d_n})$. Aplicando la definición de $a_i(R)$ dada en (B.1)

$$a_0(R) := \sup\{\mu \mid H^0_{\mathfrak{m}}(R)_\mu \neq 0\}, \text{ y } a_i(R) = -\infty \text{ si } i \neq 0.$$

Sea $\mu_0 := \sum_i (d_i - 1)$. Como $H^0_{R_+}(B) : \mu \cong R/(X_1^{d_1}, \ldots, X_n^{d_n})_\mu$, tenemos que $H^0_{\mathfrak{m}}(B)_{\mu_0}$ es isomorfo al A-módulo $X_1^{d_1-1} \cdots X_n^{d_n-1} A \neq 0$ y $H^0_{\mathfrak{m}}(B)_\mu = 0$ si $\mu \geq \mu_0$. Luego, $a_0(B) = \mu_0$.

Por la Definición B.1 se tiene que $\operatorname{reg}^\ell(B) - \infty$ si $\ell \geq 1$, y que

$$\operatorname{reg}(B) = \operatorname{reg}^0(B) = a_0(B) + 0 = \mu_0. \qquad \square$$

Este resultado demuestra que $H^0_{\mathfrak{m}}(B)_\nu = 0$ si $\nu \geq \nu_0 := \sum_i (d_i - 1) + 1$, y que además, este valor es óptimo.

Ejercicios.

1. Probar que $\Gamma_I(-)$ es un funtor aditivo exacto a izquierda
2. Probar el Corolario A.9.
3. Probar el Corolario A.10.
4. Extender el Corolario A.10 al caso de $r < n$ polinomios homogéneos de $R = A[X_1, \ldots, X_n]$, con $\deg(f_i) = d_i$, que forman una sucesión regular en R.
5. Probar el Lema B.2.

Referencias

[BBD12] Nicolás Botbol, Laurent Busé, and Manuel Dubinsky. Package for elimination theory. *Available on Macaulay2 website*, 2012.

[BH93] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[BM93] Dave Bayer and David Mumford. What can be computed in algebraic geometry? In *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, Sympos. Math., XXXIV, pages 1–48. Cambridge Univ. Press, Cambridge, 1993.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Dem84] Michel Demazure. Une définition constructive du resultant. *Centre de Mathématiques de l'Ecole Polytechnique*, 2(Notes informelles du calcul formel 1984-1994):0–23, May 1984.

[EG84] David Eisenbud and Shiro Goto. Linear free resolutions and minimal multiplicity. *J. Algebra*, 88(1):89–133, 1984.

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes*. Graduate Texts in Mathematics. 197. New York, NY: Springer. x, 294 p., 2000.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[GKZ94] Israel M Gel′fand, Mikhail M Kapranov, and Andrei V Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc, Boston, MA, 1994.

[GS] Daniel R Grayson and Michael E Stillman. Macaulay 2, a software system for research in algebraic geometry. *http://www.math.uiuc.edu/Macaulay2/*.

[Har67] Robin Hartshorne. *Local cohomology*, volume 1961 of *A seminar given by A. Grothendieck, Harvard University, Fall*. Springer-Verlag, Berlin, 1967.

[Hun07] Craig Huneke. Lectures on local cohomology. In *Interactions between homotopy theory and algebra*, volume 436 of *Contemp. Math*, pages 51–99. Amer. Math. Soc, Providence, RI, 2007. Appendix 1 by Amelia Taylor.

[Hur13] Hurwitz. Uber die tragheitsformen eines algebraischen moduls. 3:20, 1913.

[Jou91] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math*, 90(2):117–263, 1991.

[Mac65] Robert E MacRae. On an application of the Fitting invariants. *J. Algebra*, 2:153–169, 1965.

[Mum66] David Mumford. *Lectures on curves on an algebraic surface*. With a section by G. M. Bergman. Annals of Mathematics Studies, No. 59. Princeton University Press, Princeton, N.J., 1966.

[Nor76] D. G. Northcott. *Finite free resolutions*. Cambridge University Press, Cambridge, 1976. Cambridge Tracts in Mathematics, No. 71.

[Ooi82] Akira Ooishi. Castelnuovo's regularity of graded rings and modules. *Hiroshima Math. J.*, 12:627–644, 1982.

Departamento de Matemática, FCEN, Universidad de Buenos Aires, Argentina
E-mail address: nbotbol@dm.uba.ar