Sección de Matemáticas
Universidad de La Laguna

Fernando León Delgado

Introducción a los ideales de Fitting y a las resultantes

Introduction to the Fitting ideals and the resultants

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, marzo de 2024

Dirigido por
Evelia Rosa García Barroso

Evelia Rosa García Barroso
Departamento de Matemáticas,
Estadística e Investigación
Operativa.
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A mis padres por ayudarme y apoyarme en todo momento.

A mi hermana Sandra por apoyarme.

A mi abuela Aurora por preguntarme siempre que venía de la universidad cómo me había ido o si me había mojado por la lluvia.

Y a Evelia García, matemática increíble. Gracias por ayudarme y aguantarme.

Fernando León Delgado
La Laguna, 6 de marzo de 2024

Resumen · Abstract

Resumen

Este trabajo tiene cuatro objetivos. El primero es introducir el concepto de los ideales de Fitting y mostrar algunas de sus propiedades, para ello, se emplearán herramientas de álgebra conmutativa. El segundo es definir la resultante de dos polinomios con coeficientes en un anillo conmutativo unitario y demostrar algunas de sus propiedades más relevantes. El tercero es mostrar la relación que existe entre los ideales de Fitting y las resultantes y las aplicaciones de esta relación, como pueden ser hallar la ecuación implícita de una curva parametrizada o la resolución de un sistema de dos ecuaciones polinómicas. Por último el cuarto objetivo es dar una prueba del Teorema de Bézout haciendo uso de resultantes. Para la prueba de dicho teorema estudiamos el concepto de multiplicidad de intersección.

Palabras clave: *Presentación – Módulos – Ideales de Fitting – Resultantes – Ecuación implícita – Raíces comunes – Teorema de Bézout.*

Abstract

This project has four objectives. The first one is to introduce the concept of Fitting ideals and demonstrate some of their properties, for which tools from commutative algebra will be employed. The second one is to define the resultant of two polynomials with coefficients in a unitary commutative ring and prove some of its most relevant properties. The third one is to show the relationship between Fitting ideals and resultants and the applications of this relationship, such as finding the implicit equation of a parametrized curve or solving a system of two polynomial equations. The last goal is to provide a proof of Bézout's Theorem using the resultants. For the proof of this theorem, we study the concept of intersection number.

Keywords: *Presentation – Modules – Fitting ideals – Resultants – Implicit equation – Common roots – Bézout Theorem.*

Contenido

Introducción

Hans Fitting fue un matemático alemán que nació el 13 de noviembre de 1906 en Mönchengladbach, Alemania y falleció el 6 de junio de 1938 en Königsberg. De 1925 a 1932, Fitting estudió Matemáticas, Física y Filosofía en las universidades de Tübingen y Göttingen, donde se doctoró en 1932 por sus trabajos sobre teoría de grupos. Su directora de tesis en Göttingen fue Emmy Noether. Tras su doctorado, Fitting continuó sus investigaciones en los Institutos Matemáticos de las Universidades de Göttingen y Leipzig. Además, de realizar aportaciones fundamentales a la Teoría de Grupos, se dedicó a investigar los ideales de anillos no conmutativos y a estudiar los ideales determinantes de módulos finitamente generados sobre un anillo conmutativo. En su artículo de 33 páginas [4], Fitting introdujo lo que a día de hoy se denominan ideales de Fitting.

Los ideales de Fitting son una herramienta de gran ayuda en el contexto de la teoría de Iwasawa, una interesante área de estudio dentro de la Teoría de números (ver [8, Section 2]). Además, estos pueden usarse para computar los denominados polinomios de Alexander, importantes en Teoría de nudos (ver [7]). Además, los ideales de Fitting también son de gran ayuda para hallar soluciones de un sistema de ecuaciones polinómicas o calcular la ecuación implícita de una curva o una superficie parametrizada.

La resultante de dos polinomios con coeficientes en un anillo conmutativo unitario R es un elemento de R y relaciona las raíces de dichos dos polinomios. Las resultantes se utilizan para resolver sistemas de ecuaciones polinómicas, para determinar si existen o no soluciones o para reducir un sistema dado a uno con menos variables y/o menos ecuaciones.

Esta memoria de fin de Grado está estructurada en tres capítulos. Para el desarrollo del primero hemos seguido, fundamentalmente, la referencia [1],

mientras que el segundo se basa mayormente en [9] y el último en [6].

En el Capítulo 1 se introduce la definición de presentación de un módulo y se justifica la existencia de un tipo de presentación en concreto para $R-$módulos finitamente generados donde R es un anillo noetheriano. Luego, demostramos algunas propiedades de los ideales generados por los menores de una matriz. Más adelante, mostramos las propiedades necesarias para poder probar la buena definición de los ideales de Fitting. Finalmente, demostraremos algunas propiedades de estos ideales.

En el Capítulo 2 primero mostramos algunas propiedades de los determinantes. Luego, introducimos el concepto de resultante y ayudándonos de las propiedades antes vistas, demostramos propiedades de la resultante. Luego relacionamos lo probado en el Capítulo 1 con las resultantes. Por último, damos algunas aplicaciones de la resultante.

Finalmente, en el Capítulo 3 empezamos demostrando algunos resultados sobre polinomios homogéneos haciendo uso de resultantes. Luego damos una definición de la multiplicidad de intersección de dos curvas proyectivas en un punto que generaliza la existente para una curva y una recta, que hace uso de una parametrización de la recta. Terminamos el capítulo probando el Teorema de Bézout y dando un ejemplo de cómo hallar los puntos de intersección de dos curvas proyectivas complejas usando la resultante.

1

Introducción a los ideales de Fitting

En este capítulo haremos una introducción a los ideales de Fitting y mostraremos algunas de sus propiedades. En buena parte de lo que sigue nos hemos basado en el libro [1].

1.1. Presentación de módulos

En esta sección estudiaremos las presentaciones de módulos, fundamentales para dar luego la definición de los ideales de Fitting.

Definición 1.1.1 *Sean R un anillo conmutativo unitario y M un $R-$módulo, entonces una presentación (libre) de M es una sucesión exacta de la forma*

$$G \xrightarrow{\phi} F \xrightarrow{\psi} M \longrightarrow 0$$

con G y F $R-$módulos libres. Si además, G y F son libres de rango finito, entonces la presentación se dice que es finita. Si M tiene una presentación finita, entonces diremos que M está finitamente presentado.

Proposición 1.1.2 *Sean R un anillo conmutativo unitario, M un $R-$módulo y $\{m_\lambda\}_{\lambda\in\Lambda}$ generadores de M. Entonces existe una sucesión exacta de $R-$módulos libres*

$$0 \longrightarrow K \longrightarrow \bigoplus_{\lambda\in\Lambda} R \xrightarrow{\alpha} M \longrightarrow 0$$

tal que $\alpha(e_\lambda) = m_\lambda$, para todo $\lambda \in \Lambda$, donde $\{e_\lambda\}_{\lambda\in\Lambda}$ es la base canónica de $\bigoplus_{\lambda\in\Lambda} R$, y además, hay una presentación de M de la forma

$$\bigoplus_{\sigma\in\Sigma} R \longrightarrow \bigoplus_{\lambda\in\Lambda} R \xrightarrow{\alpha} M \longrightarrow 0. \tag{PS}$$

para cierto Σ conjunto de índices.

Demostración. Definimos $\alpha : \bigoplus_{\lambda\in\Lambda} R \longrightarrow M$ teniendo en cuenta que, para todo $x \in \bigoplus_{\lambda\in\Lambda} R$, existe un único $\{\mu_\lambda\}_{\lambda\in\Lambda} \subseteq R$ tal que $x = \sum_{\lambda\in\Lambda} \mu_\lambda e_\lambda$ porque $\{e_\lambda\}_{\lambda\in\Lambda}$ es una base libre del $R-$módulo libre $\bigoplus_{\lambda\in\Lambda} R$. Luego definimos $\alpha(x) := \sum_{\lambda\in\Lambda} \mu_\lambda m_\lambda$. Además como M es un $R-$módulo $\alpha(x) \in M$, para cualquier $x \in \bigoplus_{\lambda\in\Lambda} R$ y si $x = x' \in \bigoplus_{\lambda\in\Lambda} R$ entonces $\alpha(x) = \alpha(x')$ porque existe un único $\{\mu_\lambda\}_{\lambda\in\Lambda} \subseteq R$ tal que $x = \sum_{\lambda\in\Lambda} \mu_\lambda e_\lambda = x'$. Por tanto α es aplicación. Además, α es un homomorfismo de $R-$módulos. En efecto, sean $r_1, r_2 \in R$ y $x, y \in \bigoplus_{\lambda\in\Lambda} R$, entonces, existen unos únicos $\{\mu_\lambda\}_{\lambda\in\Lambda}, \{\eta_\lambda\}_{\lambda\in\Lambda} \subseteq R$ tales que $x = \sum_{\lambda\in\Lambda} \mu_\lambda e_\lambda, y = \sum_{\lambda\in\Lambda} \eta_\lambda e_\lambda$. Luego se tiene que

$$\alpha(r_1x + r_2y) = \alpha\left(r_1 \sum_{\lambda\in\Lambda} \mu_\lambda e_\lambda + r_2 \sum_{\lambda\in\Lambda} \eta_\lambda e_\lambda\right) = \alpha\left(\sum_{\lambda\in\Lambda} (r_1\mu_\lambda + r_2\eta_\lambda)e_\lambda\right)$$

$$= \sum_{\lambda\in\Lambda} (r_1\mu_\lambda + r_2\eta_\lambda)m_\lambda$$

por definición de α y además,

$$r_1\alpha(x) + r_2\alpha(y) = r_1 \sum_{\lambda\in\Lambda} \mu_\lambda m_\lambda + r_2 \sum_{\lambda\in\Lambda} \eta_\lambda m_\lambda = \sum_{\lambda\in\Lambda} (r_1\mu_\lambda + r_2\eta_\lambda)m_\lambda.$$

Por tanto, $\alpha(r_1x + r_2y) = r_1\alpha(x) + r_2\alpha(y)$, para cualesquiera $r_1, r_2 \in R$, y x, y en $\bigoplus_{\lambda\in\Lambda} R$. Tenemos entonces que α es homomorfismo. Además como el conjunto $\{m_\lambda\}_{\lambda\in\Lambda}$ genera a M, entonces α es sobreyectiva pues dado $m \in M$, existe $\{\theta_\lambda\}_{\lambda\in\Lambda} \subseteq R$ tal que $m = \sum_{\lambda\in\Lambda} \theta_\lambda m_\lambda$, tomamos $x := \sum_{\lambda\in\Lambda} \theta_\lambda e_\lambda \in \bigoplus_{\lambda\in\Lambda} R$ y se tiene que $\alpha(x) = m$. Sea ahora $K := Ker(\alpha)$ que es un submódulo del $R-$módulo $\bigoplus_{\lambda\in\Lambda} R$. Consideramos,

$$0 \longrightarrow K \xrightarrow{i_K} \bigoplus_{\lambda\in\Lambda} R \xrightarrow{\alpha} M \longrightarrow 0, \tag{SE}$$

donde $i_K : K \longrightarrow \bigoplus_{\lambda\in\Lambda} R$ denota la inclusión de K en $\bigoplus_{\lambda\in\Lambda} R$. La sucesión (SE) es exacta pues α es sobreyectiva, $Ker(\alpha) = Im(i_K) = K$ y la inclusión i_K es inyectiva. Ahora, determinaremos una presentación de M. Sea $\{k_\sigma\}_{\sigma\in\Sigma}$ un conjunto

de generadores de K y definimos $\beta : \bigoplus_{\sigma\in\Sigma} R \longrightarrow K$ como sigue: como $\bigoplus_{\sigma\in\Sigma} R$ es un $R-$módulo libre, para cualquier $y \in \bigoplus_{\sigma\in\Sigma} R$, existe un único $\{w_\sigma\}_{\sigma\in\Sigma} \subseteq R$ tal que $y = \sum_{\sigma\in\Sigma} w_\sigma e'_\sigma$, donde $\{e'_\sigma\}_{\sigma\in\Sigma}$ es la base canónica de $\bigoplus_{\sigma\in\Sigma} R$. Entonces definimos $\beta(y) := \sum_{\sigma\in\Sigma} w_\sigma k_\sigma$. Además β es un epimorfismo, se demuestra de forma similar a lo hecho para α. Así, obtenemos el siguiente diagrama de $R-$módulos

$$\begin{array}{ccccccc} \bigoplus_{\sigma\in\Sigma} R & \xrightarrow{i_K\circ\beta} & \bigoplus_{\lambda\in\Lambda} R & \xrightarrow{\alpha} & M & \longrightarrow & 0 \\ {\scriptstyle\beta}\downarrow & \nearrow_{i_K} & & & & & \\ K & & & & & & \end{array}$$

donde la fila superior es una presentación de M ya que α es epimorfismo e $Im(i_K \circ \beta) = Im(\beta) = K = Ker(\alpha)$. □

Corolario 1.1.3 *Sean R un anillo conmutativo unitario noetheriano y M un $R-$módulo finitamente generado, entonces existe una presentación de M de la forma*

$$R^q \longrightarrow R^n \longrightarrow M \longrightarrow 0 \tag{PF}$$

para ciertos $n, q \in \mathbb{N}$.

Demostración. Por la Proposición 1.1.2, sabemos que M tiene una presentación del tipo (PS). Siguiendo la notación de la demostración de la Proposición 1.1.2, se tiene que cada $\lambda \in \Lambda$ y cada $\sigma \in \Sigma$ se corresponden con un generador de M y K respectivamente. Además, por hipótesis tenemos que M está finitamente generado. Luego consideramos $\{m_i\}_{i=1}^n$ ($n \in \mathbb{N}\setminus\{0\}$), un conjunto de generadores de M. De este modo, Λ es un conjunto finito y

$$K = \left\{ (r_1, r_2, \ldots, r_n) \in R^n : \sum_{i=1}^{n} r_i m_i = 0 \right\}$$

es un submódulo del $R-$módulo R^n. Por último, por ser R un anillo noetheriano, aplicando [10, Corollary 7.22 i)] se tiene que R^n es un $R-$módulo noetheriano y por tanto, K está finitamente generado. Luego, podemos tomar Σ finito. □

Para más información acerca de módulos se puede consultar [10, Chapters 6, 7, 9 and 10].

Nota: Como para cualquier $n \in \mathbb{N}\setminus\{0\}$, $R \oplus \overset{n)}{\cdots} \oplus R \cong R^n$, en el caso finito se puede definir una presentación como (PF).

Ejemplo 1.1.4 *(Construcción de una presentación finita) Sea el $\mathbb{Z}-$módulo $M := \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Para construir una presentación como en la prueba de la Proposición 1.1.2, primero tomamos un conjunto de generadores de M, consideramos por ejemplo, $\{e_i\}_{i=1}^3$ donde $e_1 = ([1]_2, [0]_3, [0]_5)$, $e_2 = ([0]_2, [1]_3, [0]_5)$ y $e_3 = ([0]_2, [0]_3, [1]_5)$. Definimos $\alpha : \mathbb{Z}^3 \longrightarrow M$ con $\alpha(1,0,0) = e_1$, $\alpha(0,1,0) = e_2$, $\alpha(0,0,1) = e_3$ y lo extendemos por linealidad. Para β, primero calculamos $Ker(\alpha) = K$ (siguiendo la notación de la Proposición 1.1.2):*

$$\begin{aligned} K &= \{(a,b,c) \in \mathbb{Z}^3 : \alpha(a,b,c) = 0_M\} = \{(a,b,c) \in \mathbb{Z}^3 : ae_1 + be_2 + ce_3 = 0_M\} \\ &= \{(a,b,c) \in \mathbb{Z}^3 : [a]_2 = [0]_2 \ \wedge \ [b]_3 = [0]_3 \ \wedge \ [c]_5 = [0]_5\} \\ &= \{(a,b,c) \in \mathbb{Z}^3 : a = 2k_1, b = 3k_2, c = 5k_3;\ k_1,k_2,k_3 \in \mathbb{Z}\} \\ &= \{(2k_1, 3k_2, 5k_3) \in \mathbb{Z}^3 : k_1,k_2,k_3 \in \mathbb{Z}\} = \langle (2,0,0), (0,3,0), (0,0,5)\rangle\,. \end{aligned}$$

La relación $(2,0,0)$ se corresponde con la ecuación $2e_1 = 0_M$, así como $(0,3,0)$ se corresponde con $3e_2 = 0_M$ y $(0,0,5)$ con $5e_3 = 0_M$. Luego, definimos

$$\begin{aligned} \beta: \quad \mathbb{Z}^3 &\longrightarrow K \\ (a,b,c) &\longmapsto \beta(a,b,c) := (2a, 3b, 5c) \end{aligned}$$

y la extendemos a $\mathbb{Z}^3$, $i_K \circ \beta : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$. De forma matricial,

$$(i_K \circ \beta)(a,b,c) = \begin{pmatrix} a & b & c \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}.$$

Así, tenemos la presentación de M

$$\mathbb{Z}^3 \xrightarrow{i_K \circ \beta} \mathbb{Z}^3 \xrightarrow{\alpha} M \longrightarrow 0. \tag{P1}$$

Obsérvese que una presentación de un $R-$módulo finitamente generado no tiene por qué ser única: para construir (P1) elegimos como generadores de K a $(2,0,0), (0,3,0)$ y $(0,0,5)$ pero podríamos haber añadido el elemento $(4,0,0)$. De este modo tendríamos otra presentación de M,

$$\mathbb{Z}^4 \xrightarrow{i_K \circ \beta'} \mathbb{Z}^3 \xrightarrow{\alpha} M \longrightarrow 0$$

donde $i_K \circ \beta'$ tiene por matriz asociada a $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \\ 4 & 0 & 0 \end{pmatrix}$.

1.2. El ideal generado por los menores de una matriz

En esta sección estudiaremos el ideal generado por los menores de una matriz y mostraremos algunas de sus propiedades, que nos serán de utilidad más adelante.

Sean R un anillo conmutativo unitario, $A \in \mathcal{M}_{m,n}(R)$ y $r \in \mathbb{Z}$. Denotamos por $I_r(A)$ al ideal de R generado por los menores de orden r de A. Por convenio, tenemos que

$$I_r(A) = \begin{cases} \langle 0 \rangle \text{ , } si\ r > min\{m,n\} \\ R, \ \ si\ r \leq 0 \text{ .} \end{cases}$$

Propiedad 1.2.1 *Sea R un anillo conmutativo y unitario y $A \in \mathcal{M}_{m,n}(R)$. Se tiene que*

i) $R = I_0(A) \supseteq I_1(A) \supseteq I_2(A) \supseteq \cdots$
ii) Si $U \in (\mathcal{M}_m(R))^*$ entonces $I_r(U) = R$, para todo $r \leq m$.

Demostración. Demostraremos *i)*. Si $B = (b_{ij})_{i,j=1}^{r} \in \mathcal{M}_r(R)$ es submatriz de A de tamaño $r \times r, r \geq 1$, y denotamos por B_{ij} la submatriz de B que resulta al quitar a B la i-ésima fila y la j-ésima columna para cualesquiera $i, j \in \{1, \ldots, r\}$, se tiene que, calculando el determinante de B por la i-ésima fila,

$$det(B) = \sum_{j=1}^{r} (-1)^{i+j} b_{ij} det(B_{ij}) \in I_{r-1}(A)$$

pues $det(B_{ij}) \in I_{r-1}(A)$ para todo $j = 1, \ldots, r$. Pero por definición, sabemos que $I_r(A) = \langle \{det(B) : \text{B submatriz de A de tamaño } r \times r\} \rangle$, luego se sigue que $I_r(A) \subseteq I_{r-1}(A)$, para todo $r \in \mathbb{Z}$, y de este modo se deduce *i)*. Ahora, demostraremos *ii)*. Si $U \in \mathcal{M}_m(R)$ es una matriz inversible entonces existe $U^{-1} \in \mathcal{M}_m(R)$ tal que $UU^{-1} = U^{-1}U \overset{(*)}{=} \mathrm{I}_m$ donde I_m denota la matriz identidad de orden m. Entonces por $(*)$, se sigue que $det(U^{-1}U) = det(\mathrm{I}_m)$ luego, $det(U^{-1})det(U) = det(\mathrm{I}_m) = 1$ y por tanto, $det(U) \in R^*$ y $\langle det(U) \rangle = R$. Concluimos que, $I_m(U) = R$ y se deduce aplicando *i)* que $I_r(U) = R$ pues $R = I_0(U) \supseteq I_1(U) \supseteq I_2(U) \supseteq \cdots \supseteq I_m(U) \supseteq \cdots$ para todo $r \leq m$. □

Dada una matriz de tamaño $p \times q$, $q \geq n, X := (x_{ij})$, denotamos su j-ésima columna por X^j. Si $I = (i_1, \ldots, i_r)$ y $J := (j_1, \ldots, j_r)$ son dos tuplas con $1 \leq i_1 < i_2 < \cdots < i_r \leq p$ y $1 \leq j_1 < j_2 < \cdots < jr \leq q$, llamamos

$$X_{IJ} := \begin{pmatrix} x_{i_1 j_1} & \cdots & x_{i_1 j_r} \\ \vdots & & \vdots \\ x_{i_r j_1} & \cdots & x_{i_r j_r} \end{pmatrix} \text{ y } X_I := \begin{pmatrix} x_{i_1 1} & \cdots & x_{i_1 n} \\ \vdots & & \vdots \\ x_{i_r 1} & \cdots & x_{i_r n} \end{pmatrix}.$$

Así, $X_{IJ} \in \mathcal{M}_r(R)$ y $X_I \in \mathcal{M}_{r,n}(R)$.

Lema 1.2.2 *Sean R un anillo conmutativo unitario, y las siguientes matrices $A \in \mathcal{M}_{m,n}(R), B \in \mathcal{M}_{n,p}(R), U \in (\mathcal{M}_m(R))^*, V \in (\mathcal{M}_n(R))^*$. Entonces, para cualquier $r \in \mathbb{Z}$, se tiene*

i) $I_r(AB) \subseteq I_r(A) I_r(B)$.

ii) $I_r(UAV) = I_r(A)$.

Demostración. Para demostrar *i)*, pongamos que $A = (a_{ij})$ y $B = (b_{ij})$. Sea $C := AB$. Dado $I = (1_1, \ldots, i_r)$ con $1 \leq i_1 < i_2 < \cdots < i_r \leq m$ y $K = (k_1, \ldots, k_r)$ con $1 \leq k_1 < k_2 < \cdots < k_r \leq p$, tenemos que $det(C_{IK}) = det(C^1_{IK} \ldots, C^r_{IK})$, pero $C^\alpha_{IK} = \sum_{j_\alpha=1}^{n} A^{j_\alpha} b_{j_\alpha k_\alpha}$, para cualquier $\alpha \in \{1, 2 \ldots, r\}$, pues en general, si $C = (c_{ij})_{i=1,\ldots,m;\ j=1,\ldots,p}$, dado $\beta \in \{1, \ldots, p\}$, se sigue que $c_{j\beta} = a_{j1}b_{1\beta} + \cdots + a_{jn}b_{n\beta}$ con $1 \leq j \leq m$. Luego,

$$C^\beta = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} b_{1\beta} + \cdots + \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} b_{n\beta} = A^1 b_{1\beta} + \cdots + A^n b_{n\beta} = \sum_{j=1}^{n} A^j b_{j\beta}.$$

Por tanto, se tiene que

$$det(C_{IK}) = det\left(\sum_{j_1=1}^{n} A_I^{j_1} b_{j_1 k_1}, \ldots, \sum_{j_r=1}^{n} A_I^{j_r} b_{j_r k_r} \right) = \sum_{J}^{n} det(A_I^{j_1}, \ldots, A_I^{j_r}) b_{j_1 k_1} \cdots b_{j_r k_r}.$$

En la última suma cada sumando se corresponde con $J = (j_1, \ldots, j_r)$ donde $1 \leq j_i \leq n$. Además, si hay dos j_i iguales, entonces se tiene que $det(A_I^{j_1}, \ldots, A_I^{j_r}) = 0$ pues dos columnas son iguales, pero si en J no hay elementos repetidos entonces J es una permutación de algún $H = (h_1, \ldots, h_r)$ con $1 \leq h_1 < \cdots < h_r \leq q$, así, $j_i = \sigma(h_i)$, con σ una permutación. Si denotamos el signo de la permutación σ por $(-1)^\sigma$, se tiene que

$$det(A_I^{j_1}, \ldots, A_I^{j_r}) = (-1)^\sigma det(A_{IH})$$

porque cada vez que permutamos dos columnas de una matriz cuadrada, su determinante cambia de signo. Pero desarrollando el determinante por filas, obtenemos

$$det(B_{HK}) = \sum_{\sigma} (-1)^\sigma b_{\sigma(h_1)k_1} \cdots b_{\sigma(h_r)k_r}.$$

Por tanto, $det(C_{IK}) = \sum_{H} det(A_{IH}) det(B_{HK}) \in I_r(A) I_r(B)$ ya que para cualquier H, $det(A_{IH}) \in I_r(A)$ y $det(B_{HK}) \in I_r(B)$. Luego, para toda $C' \in \mathcal{M}_r(R)$ submatriz de AB, $det(C') \in I_r(A) I_r(B)$ y por tanto, $I_r(AB) \subseteq I_r(A) I_r(B)$ y así queda demostrado *i)*.

Ahora para demostrar *ii)*, sabemos por la Propiedad 1.2.1 *ii)* que $I_r(W) \overset{*}{=} R$, para $W = U, U^{-1}, V, V^{-1}$. Tenemos además que

$$I_r(A) = I_r(U^{-1}UAVV^{-1}) \overset{i)\ 2\ \text{veces}}{\subseteq} I_r(U^{-1}) I_r(UAV) I_r(V^{-1}) \overset{*}{=} R I_r(UAV) R$$

$$= I_r(UAV) \overset{i)\ 2\ \text{veces}}{\subseteq} I_r(U)I_r(A)I_r(V) \overset{*}{=} RI_r(A)R = I_r(A).$$

Luego, se sigue que $I_r(A) \subseteq I_r(UAV) \subseteq I_r(A)$ y que $I_r(UAV) = I_r(A)$. □

Propiedad 1.2.3 *Sea R un anillo conmutativo unitario y la matriz por bloques $A = \left(\begin{array}{c|c} B & \boldsymbol{O} \\ \hline \boldsymbol{O} & C \end{array}\right)$ con coeficientes en R y donde $\boldsymbol{O}$ denota una matriz nula, entonces se tiene que para todo $r \in \mathbb{Z}$*

$$I_r(A) = \sum_{s+t=r} I_s(B)I_t(C).$$

Demostración. La prueba es consecuencia de desarrollar el determinante de A por filas o columnas y fijándonos en cómo son los menores de A. □

1.3. Versión débil del Lema de Schanuel

En esta sección introduciremos el concepto de módulo proyectivo y daremos una prueba de una versión simplificada del Lema de Schanuel que nos servirá para demostrar el Lema de Fitting. Para quien esté interesado, la versión completa del Lema de Schanuel se encuentra en la página 35 del libro [1].

Definición 1.3.1 *Sean R un anillo conmutativo unitario y M un $R-$módulo. Se dice que M es proyectivo si dado cualquier diagrama de homomorfismos de R-módulos de la forma*

$$\begin{array}{ccccc} & & M & & \\ & & \downarrow{\scriptstyle f} & & \\ M'' & \xrightarrow[g]{} & M' & \longrightarrow & 0 \end{array}$$

donde la fila inferior es una sucesión exacta (g epimorfismo), existe un homomorfismo de R-módulos $h : M \longrightarrow M''$ tal que el siguiente diagrama es conmutativo

$$\begin{array}{ccccc} & & M & & \\ & \overset{h}{\swarrow} & \downarrow{\scriptstyle f} & & \\ M'' & \xrightarrow[g]{} & M' & \longrightarrow & 0 \end{array}$$

es decir, $f = g \circ h$.

Proposición 1.3.2 *Todo módulo libre es proyectivo.*

Demostración. Sean R anillo conmutativo unitario y los homomorfismos de R-módulos $f : M \longrightarrow M'$, $g : M'' \longrightarrow M'$ con g sobreyectiva y M libre. Como M es libre, podemos considerar una base $\{e_i\}_{i\in I}$ de M. Usando que g es sobreyectiva

se tiene que para todo $i \in I$, existe $m_i'' \in M''$ tal que $f(e_i) \overset{(*)}{=} g(m_i'')$. Luego, podemos definir $h : M \longrightarrow M''$ tal que si $m \in M$, existe un único $\{r_i\}_{i\in I} \subseteq R$ con $m = \sum_{i\in I} r_i e_i$; $h(m) := \sum_{i\in I} r_i m_i''$. Primero, tenemos que probar que h es aplicación. Para cualquier $m \in M, h(m) = \sum_{i\in I} r_i m_i'' \in M''$ y para cualesquiera $m_1, m_2 \in M$ tales que $m_1 = m_2$ existe un único $\{r_i\}_{i\in I} \subseteq R$ donde $m_1 = m_2 = \sum_{i\in I} r_i e_i$. Luego, $h(m_1) = \sum_{i\in I} r_i m_i'' = h(m_2)$. Por tanto, h es aplicación. Además, h es homomorfismo. En efecto, sean $r_1, r_2 \in R$ y $m_1, m_2 \in M$, entonces existen unos únicos $\{\lambda_i\}_{i\in I}, \{\mu_i\}_{i\in I} \subseteq R$ tales que $m_1 = \sum_{i\in I} \lambda_i e_i, m_2 = \sum_{i\in I} \mu_i e_i$. Luego,

$$\begin{aligned} h(r_1 m_1 + r_2 m_2) &= h\left(\sum_{i\in I} (r_1\lambda_i + r_2\mu_i)e_i\right) = \sum_{i\in I} (r_1\lambda_i + r_2\mu_i)m_i'' \\ &= r_1 \sum_{i\in I} \lambda_i m_i'' + r_2 \sum_{i\in I} \mu_i m_i'' = r_1 h(m_1) + r_2 h(m_2). \end{aligned}$$

También, $h(e_i) = m_i''$, para todo $i \in I$ y aplicando g, se sigue que $g(h(e_i)) = g(m_i'')$, para cualquier $i \in I$ y por $(*)$ se tiene que $g(h(e_i)) = (g\circ h)(e_i) = f(e_i)$, para todo $i \in I$. Luego, por ser $\{e_i\}_{i\in I}$ una base de M, se sigue que $g \circ h = f$ y que M es proyectivo. □

Corolario 1.3.3 *Para cualquier $n \in \mathbb{N}\setminus\{0\}$ y para cualquier anillo conmutativo unitario R, R^n es proyectivo.*

Demostración. Para todo $n \in \mathbb{N}\setminus\{0\}$ y para todo anillo conmutativo unitario R, R^n es libre y por la Proposición 1.3.2 proyectivo. □

Si tenemos un anillo conmutativo unitario R y M y N dos R-módulos, denotamos por $M \oplus N = \{m + n : m \in M \ \wedge \ n \in N\}$. Si ahora consideramos $f : M_1 \longrightarrow M_2$ y $g : M_3 \longrightarrow M_4$ homomorfismos de módulos denotamos por $f \oplus g : M_1 \oplus M_3 \longrightarrow M_2 \oplus M_4$ al homomorfismo tal que si $x = m_1 + m_3$ con $m_i \in M_i$, $i \in \{1, 3\}$, entonces, $(f \oplus g)(x) := f(m_1) + g(m_3)$. Además si $f : M_1 \longrightarrow M$, $g : M_2 \longrightarrow M$ son homomorfismos de módulos, entonces $f + g : M_1 \oplus M_2 \longrightarrow M$ se define como $(f + g)(x) := f(m_1) + g(m_2)$ para cualquier $x = m_1 + m_2$ donde $m_i \in M_i$, $1 \leq i \leq 2$.

Lema 1.3.4 (Schanuel débil) *Sean R un anillo conmutativo unitario y $L \xrightarrow{i} P \xrightarrow{\alpha} M \longrightarrow 0$, $L' \xrightarrow{i'} P' \xrightarrow{\alpha'} M \longrightarrow 0$ sucesiones exactas de $R-$módulos con P y P' proyectivos. Entonces el siguiente diagrama*

$$\begin{array}{ccccccc} L \oplus P' & \xrightarrow{i\oplus 1_{P'}} & P \oplus P' & \xrightarrow{\alpha+0} & M & \longrightarrow & 0 \\ & & \cong\downarrow \gamma & & \downarrow 1_M & & \\ P \oplus L' & \xrightarrow[1_P\oplus i']{} & P \oplus P' & \xrightarrow[0+\alpha']{} & M & \longrightarrow & 0 \end{array} \tag{SD}$$

es conmutativo, donde γ es un isomorfismo.

Demostración. Primero, tenemos los siguientes diagramas

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \alpha & & \\ P' & \xrightarrow[\alpha']{} & M & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccc} & & P' & & \\ & & \downarrow \alpha' & & \\ P & \xrightarrow[\alpha]{} & M & \longrightarrow & 0 \end{array}$$

donde las filas inferiores son sucesiones exactas por hipótesis y P y P' son proyectivos. Luego, existen $h : P \longrightarrow P'$, $h' : P' \longrightarrow P$ homomorfismos tales que $\alpha = \alpha' \circ h$ y $\alpha' = \alpha \circ h'$. Consideramos H y H' las matrices asociadas a h y h' respectivamente. Ahora, construimos el siguiente diagrama

$$\begin{array}{ccccccc} L \oplus P' & \xrightarrow{i\oplus 1_{P'}} & P \oplus P' & \xrightarrow{\alpha+0} & M & \longrightarrow & 0 \\ & & \uparrow \delta & & \downarrow 1_M & & \\ & & P \oplus P' & \xrightarrow{\alpha+\alpha'} & M & \longrightarrow & 0 \\ & & \downarrow \tau & & \downarrow 1_M & & \\ P \oplus L' & \xrightarrow[1_P\oplus i']{} & P \oplus P' & \xrightarrow[0+\alpha']{} & M & \longrightarrow & 0 \end{array}$$

donde τ y δ son los homomorfismos de módulos con matrices asociadas

$$T = \left(\begin{array}{c|c} \mathbf{I} & H \\ \hline \mathbf{O} & \mathbf{I} \end{array}\right) \text{ y } \Delta = \left(\begin{array}{c|c} \mathbf{I} & \mathbf{O} \\ \hline H' & \mathbf{I} \end{array}\right)$$

respectivamente, donde $\mathbf{I}$ es la matriz identidad y $\mathbf{O}$ es una matriz nula de los órdenes que corresponda. Ambas matrices tienen inversas y por tanto, τ y δ son isomorfismos. De hecho, las matrices asociadas a τ^{-1} y δ^{-1} son $T^{-1} = \left(\begin{array}{c|c} \mathbf{I} & -H \\ \hline \mathbf{O} & \mathbf{I} \end{array}\right)$ y $\Delta^{-1} = \left(\begin{array}{c|c} \mathbf{I} & \mathbf{O} \\ \hline -H' & \mathbf{I} \end{array}\right)$. Tenemos que la matriz asociada a $\gamma := \tau \circ \delta^{-1}$ es

$$\Gamma = \Delta^{-1}T = \left(\begin{array}{c|c} \mathbf{I} & \mathbf{O} \\ \hline -H' & \mathbf{I} \end{array}\right)\left(\begin{array}{c|c} \mathbf{I} & H \\ \hline \mathbf{O} & \mathbf{I} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{I} & H \\ \hline -H' & -H'H + \mathbf{I} \end{array}\right).$$

Si denotamos por A y A' las matrices asociadas a α y α', respectivamente, se sigue que la matriz asociada al homomorfismo $(0 + \alpha') \circ \gamma$ es

$$\Gamma\left(\frac{\mathbf{O}}{A'}\right) = \left(\begin{array}{c|c} \mathbf{I} & H \\ \hline -H' & -H'H+\mathbf{I} \end{array}\right)\left(\frac{\mathbf{O}}{A'}\right) = \left(\frac{HA'}{-H'(HA')+A'}\right).$$

Como $\alpha = \alpha' \circ h$ y $\alpha' = \alpha \circ h'$ se deduce que $A \overset{(*_1)}{=} HA'$ y $A' \overset{(*_2)}{=} H'A$, luego, la matriz asociada a $(0+\alpha') \circ h$ es

$$\left(\frac{HA'}{-H'(HA')+A'}\right) \overset{(*_1)}{=} \left(\frac{A}{-H'A+A'}\right) \overset{(*_2)}{=} \left(\frac{A}{-A'+A'}\right) = \left(\frac{A}{\mathbf{O}}\right).$$

Por tanto, la matriz asociada a $(\alpha+0)$, que es $\left(\frac{A}{\mathbf{O}}\right)$, es la misma que la matriz asociada a $(0+\alpha') \circ \gamma$. Luego, se tiene que $(\alpha+0) = (0+\alpha') \circ \gamma$, $(0+\alpha') \circ \gamma = 1_M \circ (\alpha+0)$ y el cuadrado de (SD) es conmutativo como queríamos demostrar. Faltaría por probar que las dos filas del diagrama (SD) son sucesiones exactas.

- Para fila superior. Observamos que, $(\alpha+0)$ es sobreyectiva puesto que por exactitud α lo es (para todo $m \in M$, existe $p \in P$ tal que $\alpha(p) = m$, luego, para cualquier $m \in M$, existe $x := p + 0_{P'} \in P \oplus P'$ tal que $(\alpha+0)(x) = \alpha(p) = m$). Y por exactitud también, sabemos que $Ker(\alpha) \overset{(*)}{=} Im(i)$, y se tiene que

$$\begin{aligned} Ker(\alpha+0) &= \{p+p' \in P \oplus P' : (\alpha+0)(p+p') = 0\} \\ &= \{p+p' \in P \oplus P' : \alpha(p) = 0\} = \{p+p' \in P \oplus P' : p \in Ker(\alpha)\} \\ &\overset{(*)}{=} \{p+p' \in P \oplus P' : p \in Im(i)\} = Im(i \oplus 1_{P'}). \end{aligned}$$

- Para la fila inferior razonamos de forma similar. Primero, $(0+\alpha')$ es sobreyectiva puesto que por exactitud α' lo es (para todo $m \in M$, existe $p' \in P'$ tal que $\alpha'(p') = m$ luego, para cualquier $m \in M$, existe $x := 0_P + p' \in P \oplus P'$ tal que $(0+\alpha')(x) = \alpha'(p') = m$). También por exactitud, sabemos que $Ker(\alpha') \overset{(*)}{=} Im(i')$, y se tiene que

$$\begin{aligned} Ker(0+\alpha') &= \{p+p' \in P \oplus P' : (0+\alpha')(p+p') = 0\} \\ &= \{p+p' \in P \oplus P' : \alpha'(p') = 0\} = \{p+p' \in P \oplus P' : p' \in Ker(\alpha')\} \\ &\overset{(*)}{=} \{p+p' \in P \oplus P' : p' \in Im(i')\} = Im(1_P \oplus i'). \end{aligned}$$

□

1.4. El lema de Fitting

En las siguientes páginas daremos la prueba del Lema de Fitting que encontramos en [1, Lemma 5.34]. Gracias a este y a lo probado en las tres secciones anteriores podremos justificar la buena definición de los ideales de Fitting.

Lema 1.4.1 (Fitting) *Sean R un anillo conmutativo unitario, M un R-módulo, $r \in \mathbb{Z}$ y $R^n \xrightarrow{\alpha} R^m \xrightarrow{\mu} M \longrightarrow 0$, $R^q \xrightarrow{\beta} R^p \xrightarrow{\pi} M \longrightarrow 0$ dos presentaciones de M con A y B matrices asociadas a α y β respectivamente. Entonces,*

$$I_{m-r}(A) = I_{p-r}(B).$$

Demostración. Distinguiremos varios casos:
Caso 1: Si $m = p$ y $\mu = \pi$. Sea $K := Ker(\mu)$, se tiene por exactitud que $Im(\alpha) = K$ y que $Im(\beta) = K$, por tanto, $Im(\alpha) = Im(\beta)$. Pero $Im(\alpha)$ es el módulo generado por las filas de A, luego, se deduce que cada fila de B es una combinación lineal de las filas de A. Por tanto, hay una matriz C tal que $CA \overset{(*)}{=} B$. Sea $s := m - r$. Dado k, denotaremos por $\mathbf{I}_k$ a la matriz identidad de orden k. También denotaremos por $\mathbf{O}_{mq}$ la matriz nula de tamaño $m \times q$. Tomando $V := \left(\begin{array}{c|c} \mathbf{I}_n & \mathbf{O}_{nq} \\ \hline -C & \mathbf{I}_q \end{array}\right)$ la matriz de bloques, se tiene que

$$V\left(\frac{A}{B}\right) = \left(\begin{array}{c|c} \mathbf{I}_n & \mathbf{O}_{nq} \\ \hline -C & \mathbf{I}_q \end{array}\right)\left(\frac{A}{B}\right) = \left(\frac{A}{-CA+B}\right) \overset{(*)}{=} \left(\frac{A}{\mathbf{O}_{qp}}\right).$$

Luego, se deduce que

$$I_s\left(V\left(\frac{A}{B}\right)\right) = I_s\left(\left(\frac{A}{\mathbf{O}_{qp}}\right)\right).$$

Además, V es inversible, de hecho, $det(V) = 1$. Por tanto, aplicando el Lema 1.2.2 *ii)* se sigue que

$$I_s\left(\left(\frac{A}{B}\right)\right) = I_s\left(\left(\frac{A}{\mathbf{O}_{qp}}\right)\right).$$

Pero $I_s\left(\left(\frac{A}{\mathbf{O}_{qp}}\right)\right) = I_s(A)$, luego, $I_s\left(\left(\frac{A}{B}\right)\right) = I_s(A)$. De manera similar se puede probar que $I_s\left(\left(\frac{A}{B}\right)\right) = I_s(B)$. Para ello, haciendo el mismo razonamiento que cuando empezamos la prueba de este caso, se tiene que existe una matriz D tal que $DB = A$. Tomando $W := \left(\begin{array}{c|c} \mathbf{I}_q & -D \\ \hline \mathbf{O}_{nq} & \mathbf{I}_n \end{array}\right)$ se sigue que $W\left(\frac{A}{B}\right) = \left(\frac{\mathbf{O}}{B}\right)$. Por el mismo razonamiento que antes se llega a lo que queríamos y se deduce que

$$I_s(A) = I_s\left(\left(\frac{A}{B}\right)\right) = I_s(B).$$

Caso 2: Si $m = p$ y hay un isomorfismo $\gamma : R^m \longrightarrow R^p$ tal que $\pi \circ \gamma \overset{(*)}{=} \mu$. Digamos que γ está representado por la matriz G. Luego,

$$R^n \xrightarrow{\gamma\circ\alpha} R^p \xrightarrow{\pi} M \longrightarrow 0 \tag{SuEx}$$

es una presentación de M pues π es sobreyectiva (ya lo sabíamos) y $Ker(\pi) = Im(\gamma \circ \alpha)$. En efecto, tenemos primero que,

$$Im(\gamma \circ \alpha) = \gamma(Im(\alpha)) = \gamma(Ker(\mu))$$

porque por exactitud, $Im(\alpha) = Ker(\mu)$, luego, probar que $Ker(\pi) = Im(\gamma \circ \alpha)$ es equivalente a demostrar que $Ker(\pi) = \gamma(Ker(\mu))$. Primero, sea $x \in Ker(\pi)$, entonces $\pi(x) = 0$ y aplicando $(*)$, se sigue que $(\mu \circ \gamma^{-1})(x) = 0$. Por tanto, $\mu(\gamma^{-1}(x)) = 0$, luego, $\gamma^{-1}(x) \in Ker(\mu)$ y $\gamma(\gamma^{-1}(x)) = x \in \gamma(Ker(\mu))$. De este modo, se deduce que $Ker(\pi) \subseteq \gamma(Ker(\mu))$.

Ahora, para el otro contenido, sea $x \in \gamma(Ker(\mu))$. Entonces existe y en R^m tal que $x = \gamma(y)$ con $\mu(y) = 0$. Además,

$$\pi(x) = \pi(\gamma(y)) = (\pi \circ \gamma)(y) \overset{(*)}{=} \mu(y) = 0.$$

Por tanto, $x \in Ker(\pi)$ y $\gamma(Ker(\mu)) \subseteq Ker(\pi)$. Por ambos contenidos se deduce que $Ker(\pi) = Im(\gamma \circ \alpha)$, que (SuEx) es exacta y que estamos por tanto ante una presentación de M. Aplicando el caso 1 a las presentaciones

$$R^q \xrightarrow{\beta} R^p \xrightarrow{\pi} M \longrightarrow 0 \ \text{ y } \ R^n \xrightarrow{\gamma\circ\alpha} R^p \xrightarrow{\pi} M \longrightarrow 0$$

se tiene que $I_s(B) = I_s(GA)$. Como G es la matriz asociada a γ, que es isomorfismo, sabemos que G es inversible, luego por el Lema 1.2.2 *ii)* se sigue que $I_s(GA) = I_s(A)$ y por tanto, $I_s(B) = I_s(A)$ como queríamos.

Finalmente, en general, como R^n es proyectivo, para todo $n \in \mathbb{N}\setminus\{0\}$ por el Corolario 1.3.3, aplicando el Lema 1.3.4 a las presentaciones del enunciado del lema, se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccccccc}
R^n \oplus R^p & \xrightarrow{\alpha\oplus 1_{R^p}} & R^m \oplus R^p & \xrightarrow{\mu+0} & M & \longrightarrow & 0 \\
 & & \cong\downarrow\gamma & & \downarrow 1_M & & \\
R^m \oplus R^q & \xrightarrow[1_{R^m}\oplus\beta]{} & R^m \oplus R^p & \xrightarrow[0+\pi]{} & M & \longrightarrow & 0
\end{array}$$

o equivalentemente,

$$\begin{array}{ccccccc}
R^{n+p} & \xrightarrow{\alpha\oplus 1_{R^p}} & R^{m+p} & \xrightarrow{\mu+0} & M & \longrightarrow & 0 \\
 & & \cong\downarrow\gamma & & \downarrow 1_M & & \\
R^{m+q} & \xrightarrow[1_{R^m}\oplus\beta]{} & R^{m+p} & \xrightarrow[0+\pi]{} & M & \longrightarrow & 0.
\end{array} \tag{PC2}$$

Las matrices asociadas a $(\alpha\oplus 1_{R^p})$ y $(1_{R^m}\oplus\beta)$ son $\left(\begin{array}{c|c} A & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I}_p \end{array}\right)$ y $\left(\begin{array}{c|c} \mathbf{I}_m & \mathbf{O} \\ \hline \mathbf{O} & B \end{array}\right)$, matrices que tienen tamaños $(n+p)\times(m+p)$ y $(q+p)\times(m+p)$ respectivamente. Nos

damos cuenta que en (PC2) estamos en las hipotésis del caso 2, luego se tiene que

$$I_{(m+p)-r}\left(\left(\begin{array}{c|c} A & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I}_p \end{array}\right)\right) = I_{(m+p)-r}\left(\left(\begin{array}{c|c} \mathbf{I}_m & \mathbf{O} \\ \hline \mathbf{O} & B \end{array}\right)\right).$$

Además aplicando la Propiedad 1.2.3 a $\left(\begin{array}{c|c} A & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I}_p \end{array}\right)$ y $\left(\begin{array}{c|c} \mathbf{I}_m & \mathbf{O} \\ \hline \mathbf{O} & B \end{array}\right)$ se tiene que

$$I_{(m+p)-r}\left(\left(\begin{array}{c|c} A & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I}_p \end{array}\right)\right) = I_{m-r}(A) \quad \text{e} \quad I_{(m+p)-r}\left(\left(\begin{array}{c|c} \mathbf{I}_m & \mathbf{O} \\ \hline \mathbf{O} & B \end{array}\right)\right) = I_{p-r}(B).$$

Por tanto, $I_{m-r}(A) = I_{p-r}(B)$. □

Definición 1.4.2 (Ideales de Fitting) *Sean R un anillo conmutativo unitario, M un R-módulo finitamente presentado y $r \in \mathbb{Z}$. Tomamos cualquier presentación de M de la forma $R^n \xrightarrow{\alpha} R^m \longrightarrow M \longrightarrow 0$, si denotamos por A la matriz asociada a α (a esta matriz de la conoce como la matriz de la presentación), definimos el r-ésimo ideal de Fitting de M, $Fitt_r(M)$ por*

$$Fitt_r(M) := I_{m-r}(A).$$

Nótese que por el Lema 1.4.1 la definición de los ideales de Fitting no depende de la presentación que se tome y que para que un $R-$módulo M esté finitamente presentado basta con que M sea finitamente generado y R sea noetheriano por la Propiedad 1.1.3.

En lo que sigue, si no se especifica, al referirnos a un módulo M asumiremos que está finitamente presentado.

1.5. Propiedades de los ideales de Fitting

En esta sección presentaremos algunas de las propiedades de los ideales de Fitting. Las tres siguientes propiedades se encuentran en [1, páginas 40 y 42].

Propiedad 1.5.1 *Sea R un anillo conmutativo unitario y M un R-módulo entonces, se tiene que para cualquier $r \in \mathbb{Z}$, $Fitt_r(M)$ es finitamente generado,*

$$\langle 0\rangle = Fitt_{-1}(M) \subseteq Fitt_0(M) \subseteq Fitt_1(M) \subseteq \cdots \subseteq Fitt_m(M) = R,$$

$Fitt_k(M) = \langle 0\rangle$, para todo $k < 0$ y $Fitt_w(M) = R$, para cualquier $w \geq m$.

Demostración. Por la definición de los ideales de Fitting está claro que son finitamente generados y la segunda parte se tiene de la Propiedad 1.2.1 *i)*. □

Propiedad 1.5.2 *Sean R un anillo conmutativo unitario, $a_1, a_2, \ldots, a_m \in R$ con $\langle a_1\rangle \supseteq \langle a_2\rangle \supseteq \cdots \supseteq \langle a_m\rangle$ y el R-módulo $M = (R/\langle a_1\rangle) \oplus \cdots \oplus (R/\langle a_m\rangle)$. Entonces se tiene que,*

$$Fitt_r(M) = \langle a_1 \cdots a_{m-r}\rangle, \text{ para todo } 0 \leq r \leq m-1.$$

Demostración. Tenemos que $\{e_i\}_{i=1}^m$ es una base de M donde $e_i = (0 + \langle a_1\rangle) + \cdots + (0 + \langle a_{i-1}\rangle) + (1 + \langle a_i\rangle) + (0 + \langle a_{i+1}\rangle) + \cdots + (0 + \langle a_m\rangle)$. Las relaciones no redundantes en los $\{e_i\}_{i=1}^m$ son las correspondientes a $a_i e_i = 0$, para todo $i = 1, \ldots, m$. Podemos tomar como presentación de M, $R^m \xrightarrow{\alpha} R^m \xrightarrow{\beta} M \longrightarrow 0$ donde α es el homomorfismo con matriz asociada

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix},$$

y $\beta : R^m \longrightarrow M$ está definido por $\beta(0, 0, \ldots, 0, \overset{-i-}{1}, 0, \ldots, 0) = e_i$, para cualquier $i = 1, \ldots, m$. Si tomamos una submatriz A' de A de tamaño $(m-r) \times (m-r)$ con determinante no nulo, se tiene que A' es una matriz diagonal de la forma $A' = diag(a_{j_i})_{i=1}^{m-r}$ con $j_{i+1} = j_i + 1$, para todo $i \in \{1, \ldots, m-r-1\}$. Puesto que si hay partes de columnas de A juntas que en A no están juntas entonces habría una columna llena de ceros y por tanto, el determinante de A' sería cero. Como $\langle a_{k'}\rangle \subseteq \langle a_k\rangle$, para cualquier $k' \geq k$ y $j_i \geq i$, para todo $i \in \{1, \ldots, m-r\}$ entonces, $\langle a_{j_i}\rangle \subseteq \langle a_i\rangle$, para cualquier $i \in \{1, \ldots, m-r\}$. Por tanto, para todo $i \in \{1, \ldots, m-r\}$, existe $h_i \in R$ tal que $a_{j_i} = h_i a_i$. Luego,

$$det(A') = a_{j_1} a_{j_2} \cdots a_{j_{m-r}} = (h_1 a_1) \cdots (h_{m-r} a_{m-r}) = \left(\prod_{i=1}^{m-r} h_i\right)(a_1 \cdots a_{m-r}).$$

Y así queda probado que $det(A') \in \langle a_1 a_2 \cdots a_{m-r}\rangle$, para cualquier A' submatriz A de tamaño $(m-r) \times (m-r)$. Por tanto, $I_{m-r}(A) \subseteq \langle a_1 a_2 \cdots a_{m-r}\rangle$, lo que equivale a que $Fitt_r(M) \subseteq \langle a_1 a_2 \cdots a_{m-r}\rangle$. Pero además, como $\langle a_1 a_2 \cdots a_{m-r}\rangle \subseteq Fitt_r(M)$ puesto que $a_1 a_2 \cdots a_{m-r} \in Fitt_r(M)$ ya que si consideramos la submatriz diagonal $A' = diag(a_i)_{i=1}^{m-r}$ de A de orden $m-r$, $det(A') = a_1 a_2 \cdots a_{m-r}$. Por tanto, $a_1 a_2 \cdots a_{m-r} \in I_{m-r}(A) = Fitt_r(M)$. De este modo, queda demostrado que $Fitt_r(M) = \langle a_1 a_2 \cdots a_{m-r}\rangle$, para todo $0 \leq r \leq m-1$. □

Propiedad 1.5.3 *Sean R un anillo conmutativo unitario y M un R-módulo finitamente generado con $\{e_i\}_{i=1}^m$ conjunto de generadores de M. Si denotamos por $\mathfrak{a} := Ann(M)$ al anulador de M, entonces se tiene que*

i) $\mathfrak{a} Fitt_r(M) \subseteq Fitt_{r-1}(M)$, *para todo* $r > 0$.

ii) $\mathfrak{a}^m \subseteq Fitt_0(M) \subseteq \mathfrak{a}$.

Demostración. Como M puede generarse por m elementos $\{e_i\}_{i=1}^m$, podemos construir una presentación de M de la forma $R^n \xrightarrow{\alpha} R^m \xrightarrow{\mu} M \longrightarrow 0$ como en la Proposición 1.1.3, donde α es un homomorfismo con matriz asociada A. Cada una de las filas de A se corresponde con una relación de los $\{e_i\}_{i=1}^m$. Probemos *i)* distinguiendo dos casos para r.

- Si $r > m$, entonces $r - 1 \geq m$, $Fitt_r(M) = Fitt_{r-1}(M) = R$ y trivialmente se tiene que $\mathfrak{a} \subseteq R$. Luego,

$$\mathfrak{a}Fitt_r(M) = \mathfrak{a}R = a \subseteq R = Fitt_{r-1}(M)$$

  y por tanto, $\mathfrak{a}Fitt_r(M) \subseteq Fitt_{r-1}(M)$.
- Si $r \leq m$, entonces sea $s := m - r + 1 \geq 1$. Para cualquier $x \in \mathfrak{a}$, formamos la sucesión

$$R^{n+m} \xrightarrow{\beta_x} R^m \xrightarrow{\mu} M \longrightarrow 0, \tag{S1}$$

  con $\beta := \alpha + x1_{R^m}$, es decir si $y = (y_1, \ldots, y_n, z_1, \ldots, z_m)$ para ciertos $y_1, \ldots, y_n, z_1, \ldots, z_m \in R$, entonces

$$\beta_x(y) = (\alpha + x1_{R^m}) = \alpha(y_1, \ldots, y_n) + (xz_1, \ldots, xz_m).$$

  Hecha esta aclaración, probemos que la sucesión (S1) es exacta. Para ello, es suficiente con demostrar que $Ker(\mu) = Im(\beta_x)$ o lo que es equivalente por exactitud, $Im(\alpha) = Im(\beta_x)$ (que μ es sobreyectiva ya lo tenemos de antes). Primero, sea $x' \in Im(\alpha)$, entonces existe $z = (z_1, \ldots, z_n) \in R^n$ tal que $x' = \alpha(z)$. Tomamos $z' := (z_1, \ldots, z_n, 0, \overset{m)}{\ldots}, 0) \in R^{n+m}$ tenemos que

$$\beta_x(z') = \alpha(z_1, \ldots, z_n) + (x \cdot 0, \overset{m)}{\ldots}, x \cdot 0) = \alpha(z_1, \ldots, z_n) = \alpha(z) = x'.$$

  Por tanto, $x' \in Im(\beta_x)$, para cualquier $x' \in Im(\alpha)$ e $Im(\alpha) \subseteq Im(\beta_x)$. Ahora para el otro contenido, sea $x' \in Im(\beta_x)$ entonces existe

$$z = (z_1, \ldots, z_n, z'_1, \ldots, z'_m) \in R^{n+m}$$

  tal que $x' = \beta(z) = \alpha(z_1, \ldots, z_n) + x(z'_1, \ldots, z'_m)$. Luego,

$$\begin{aligned}\mu(x') &= \mu(\alpha(z_1, \ldots, z_n) + x(z'_1, \ldots, z'_m)) = \mu(\alpha(z_1, \ldots, z_n)) + x\mu(z'_1, \ldots, z'_m) \\ &= (\mu \circ \alpha)(z_1, \ldots, z_n) + x\mu(z'_1, \ldots, z'm).\end{aligned}$$

  Pero $\mu \circ \alpha = 0$ por exactitud y $x\mu(z'_1, \ldots, z'_m) = 0$ porque $\mu(z'_1, \ldots, z'_m) \in M$ y $x \in \mathfrak{a} = Ann(M)$ y por tanto, $\mu(x') = 0 + 0 = 0$ y $x' \in Ker(\mu)$. Entonces, para todo $x' \in Im(\beta_x), x' \in Ker(\mu)$ y de este modo queda probado que $Im(\beta_x) \subseteq Ker(\mu) = Im(\alpha)$. Luego, por los dos contenidos tenemos que $Im(\beta_x) = Ker(\mu)$ y que (S1) es una presentación de M para cualquier $x \in \mathfrak{a}$.

Dado un $x \in \mathfrak{a}$ la matriz asociada a β_x es $\left(\frac{A}{x\mathbf{I}_m}\right)$. Dada una $(s-1)\times(s-1)$ submatriz B de A (aquí $s>1$), podemos construir una submatriz B' de A de tamaño $s\times s$ de este modo: pongamos que no aparece parte de la i-ésima fila de A en B para cierto i; formamos la $m\times s$ submatriz B'' de $\left(\frac{A}{x\mathbf{I}_m}\right)$ con las mismas columnas de B pero completándolas con los elementos de A de esas columnas, más la i-ésima columna de $x\mathbf{I}_m$ al final. Finalmente, formamos B' como la submatriz $s\times s$ de B con las mismas filas que B más la i-ésima fila en la posición apropiada. Desarrollando $det(B')$ por la última columna, se tiene que

$$det(B') \in \{xdet(B), -xdet(B)\}.$$

Por construcción, $det(B') \in I_s\left(\left(\frac{A}{x\mathbf{I}_m}\right)\right) = I_s(A)$, luego, $det(B') \in I_s(A)$. Por lo tanto, $xdet(B) \in I_s(A)$ y como además, $x \in \mathfrak{a}$ es arbitrario e $I_{s-1}(A)$ está generado por todos los posibles $det(B)$ con B submatriz $(s-1)\times(s-1)$ de A, se tiene que $\mathfrak{a}Fitt_r(M) \subseteq Fitt_{r-1}(M)$ y así, queda probado *i)*.

Ahora, para demostrar *ii)*, primero, aplicando varias veces *i)* se deduce que

$$\mathfrak{a}^k Fitt_r(M) \subseteq \mathfrak{a}^{k-1}Fitt_{r-1}(M) \subseteq \cdots \subseteq Fitt_{r-k}(M).$$

Por tanto, $\mathfrak{a}^k Fitt_r(M) \subseteq Fitt_{r-k}(M)$, para cualesquiera $r,k>0$. Luego, en particular, se tiene que $\mathfrak{a}^m Fitt_m(M) \subseteq Fitt_0(M)$, y teniendo en cuenta que $Fitt_m(M)=R$, se sigue que

$$\mathfrak{a}^m R = \mathfrak{a}^m \subseteq Fitt_0(M).$$

Para el segundo contenido de *ii)*, dada B una submatriz $m\times m$ cualquiera de A con determinante no nulo, pongamos $B=(b_{ij})_{i,j=1,\ldots,m}$. Si denotamos por $\{e'_i\}_{i=1}^m$ la base canónica de R^m, entonces, $e_i=\mu(e'_i)$, para todo $i\in\{1,\ldots,m\}$. Como cada fila de A se corresponde con una relación de los $\{e_i\}_{i=1}^m$ y las filas de B son filas de A, se deduce que $\sum_{j=1}^m b_{ij}e_j = 0$, para cualquier $i\in\{1,\ldots,m\}$ o matricialmente,

$$B\begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \qquad (*_1)$$

Sea ahora $C := Adj(B)^t$ la traspuesta de la matriz adjunta de B, entonces por la regla de Cramer (RC), se tiene que $det(B)\mathbf{I}_m \overset{(*_2)}{=} CB$. Multiplicando por la derecha en ambos lados de la igualdad $(*_2)$ por $\begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix}$ se tiene que:

$$det(B)\mathbf{I}_m \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} = (CB) \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} = C \left[B \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} \right] \overset{(*_1)}{=} C \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Por tanto,

$$\begin{pmatrix} det(B) & 0 & 0 \cdots & 0 \\ 0 & det(B) & 0 \cdots & 0 \\ \vdots & \vdots & \vdots \ddots & \vdots \\ 0 & 0 & 0 \cdots & det(B) \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = \begin{pmatrix} det(B)e_1 \\ det(B)e_2 \\ \vdots \\ det(B)e_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Luego, $det(B)e_i = 0$, para todo $i = 1, \ldots, m$. Además, como $\{e_i\}_{i=1}^m$ genera M, es claro que $det(B)m' = 0$, para cualquier $m' \in M$. Así, de la definición de anulador se deduce que $det(B) \in Ann(M) = \mathfrak{a}$. Luego, $det(B) \in \mathfrak{a}$, para toda B submatriz $m \times m$ de A. Por tanto, se deduce que $Fitt_0(M) = I_m(A) \subseteq \mathfrak{a}$. Queda así probado el segundo contenido de *ii)*. □

Propiedad 1.5.4 *Los ideales de Fitting conmutan con la localización, es decir, si tenemos R un anillo conmutativo unitario, M un R-módulo finitamente generado y S una parte multiplicativamente cerrada de R, entonces dado $r \in \mathbb{Z}$,*

$$Fitt_r(S^{-1}M) = S^{-1}Fitt_r(M).$$

Demostración. Podemos considerar $R^n \xrightarrow{\alpha} R^m \xrightarrow{\beta} M \longrightarrow 0$ una presentación de M cualquiera, a partir de ella podemos construir una presentación del $(S^{-1}R)$-módulo $S^{-1}M$. Definimos $\alpha_* : (S^{-1}R)^n \longrightarrow (S^{-1}R)^m$ con

$$\begin{cases} \alpha_*(\frac{1}{1}, \frac{0}{1}, \ldots, \frac{0}{1}) = \left(\frac{\alpha_1(1,0,\ldots,0)}{1}, \ldots, \frac{\alpha_m(1,0,\ldots,0)}{1} \right) \\ \alpha_*(\frac{0}{1}, \frac{1}{1}, \ldots, \frac{0}{1}) = \left(\frac{\alpha_1(0,1,\ldots,0)}{1}, \ldots, \frac{\alpha_m(0,1,\ldots,0)}{1} \right) \\ \qquad\qquad \vdots \\ \alpha_*(\frac{0}{1}, \frac{0}{1}, \ldots, \frac{1}{1}) = \left(\frac{\alpha_1(0,0,\ldots,1)}{1}, \ldots, \frac{\alpha_m(0,0,\ldots,1)}{1} \right) \end{cases}$$

donde $(\alpha_1, \alpha_2, \ldots, \alpha_m) = \alpha$. De este modo, extendiendo α_* por linealidad se tiene que α_* es un homomorfismo. Ahora definimos $\beta_* : (S^{-1}R)^m \longrightarrow S^{-1}M$ como, $\beta_*(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}) = \frac{r_1}{s_1} \frac{\beta(1,0,\ldots,0)}{1} + \cdots + \frac{r_m}{s_m} \frac{\beta(0,0,\ldots,1)}{1}$. Es un simple ejercicio de escritura ver que β_* es un homomorfismo de $(S^{-1}R)$-módulos. Construimos así la sucesión de $(S^{-1}R)$-módulos

$$(S^{-1}R)^n \xrightarrow{\alpha_*} (S^{-1}R)^m \xrightarrow{\beta_*} S^{-1}M \longrightarrow 0. \qquad (S^{-1}P)$$

Para demostrar que $(S^{-1}P)$ es una presentación de $S^{-1}M$, hay que probar que es exacta, es decir, dos cosas:

i) $Im(\alpha_*) = Ker(\beta_*)$.
ii) $Im(\beta_*) = S^{-1}M$ ($\equiv \beta_*$ epimorfismo).

Demostremos primero *i)*. Sea $(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}) \in Im(\alpha_*)$, entonces existe $(\frac{r'_1}{s'_1}, \ldots, \frac{r'_n}{s'_n})$ en $(S^{-1}R)^n$ tal que

$$\left(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}\right) = \alpha_* \left(\frac{r'_1}{s'_1}, \ldots, \frac{r'_n}{s'_n}\right) = \frac{r'_1}{s'_1}\left(\frac{\alpha_1(1,0,\ldots,0)}{1}, \ldots, \frac{\alpha_m(1,0,\ldots,0)}{1}\right) + \cdots + \frac{r'_n}{s'_n}\left(\frac{\alpha_1(0,0,\ldots,1)}{1}, \ldots, \frac{\alpha_m(0,0,\ldots,1)}{1}\right).$$

Por tanto, se tiene que

$$\beta_* \left(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}\right) = \frac{r'_1}{s'_1}\left(\frac{\beta(\alpha_1(1,0,\ldots,0), \ldots, \alpha_m(1,0,\ldots,0))}{1}\right) + \cdots + \frac{r'_n}{s'_n}\left(\frac{\beta(\alpha_1(0,0,\ldots,1), \ldots, \alpha_m(0,0,\ldots,1))}{1}\right),$$

luego,

$$\beta_* \left(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}\right) = \frac{r'_1}{s'_1}\,\frac{\beta(\alpha(e_1))}{1} + \cdots + \frac{r'_n}{s'_n}\,\frac{\beta(\alpha(e_n))}{1}$$

donde $\{e_i\}_{i=1}^n$ es la base canónica de R^n. Teniendo en cuenta que por exactitud, $Ker(\beta) = Im(\alpha)$, se deduce que

$$\beta_* \left(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}\right) = \frac{r'_1}{s'_1}\,\frac{0}{1} + \cdots + \frac{r'_n}{s'_n}\frac{0}{1} = \frac{0}{1}.$$

Por tanto, $(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}) \in Ker(\beta_*)$ e $Im(\alpha_*) \subseteq Ker(\beta_*)$. Ahora, para el otro contenido, sea $(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}) \in Ker(\beta_*)$, entonces,

$$\beta_* \left(\frac{r_1}{s_1}, \ldots, \frac{r_m}{s_m}\right) = \frac{r_1}{s_1}\,\frac{\beta(1,0,\ldots,0)}{1} + \cdots + \frac{r_m}{s_m}\,\frac{\beta(0,0,\ldots,1)}{1} = \frac{0}{1}.$$

Luego,

$$\frac{\beta(s_2s_3\cdots s_m r_1, s_1s_3\cdots s_m r_2, \ldots, s_1s_2\cdots s_{m-1}r_m)}{s_1s_2\cdots s_{m-1}s_m} = \frac{0}{1}$$

si y solo si, existe $u \in S$ tal que $u\beta(s_2s_3\cdots s_m r_1, s_1s_3\cdots s_m r_2, \ldots, s_1s_2\cdots s_{m-1}r_m) = 0$ y por tanto, $(us_2s_3\cdots s_m r_1, us_1s_3\cdots s_m r_2, \ldots, us_1s_2\cdots s_{m-1}r_m) \in Ker(\beta)$. Pero por exactitud, $Ker(\beta) = Im(\alpha)$, luego se tiene que

$$(us_2s_3\cdots s_m r_1, us_1s_3\cdots s_m r_2, \ldots, us_1s_2\cdots s_{m-1}r_m) \in Im(\alpha).$$

Por tanto, existe $(t_1, t_2, \ldots, t_n) \in R^n$ tal que

$$\alpha(t_1, t_2, \ldots, t_n) = (us_2s_3 \cdots s_m r_1, us_1s_3 \cdots s_m r_2, \ldots, s_1s_2 \cdots s_{m-1} r_m). \qquad (\star)$$

Además como S es una parte multiplicativamente cerrada de R y $u, s_1, s_2, \ldots, s_m \in S$, podemos tomar $(\frac{t_1}{us_1s_2\cdots s_m}, \frac{t_2}{us_1s_2\cdots s_m}, \cdots, \frac{t_n}{us_1s_2\cdots s_m}) \in (S^{-1}R)^n$ y se tiene que

$$\alpha_* \left(\frac{t_1}{us_1s_2 \cdots s_m}, \frac{t_2}{us_1s_2 \cdots s_m}, \ldots, \frac{t_n}{us_1s_2 \cdots s_m} \right) = \frac{1}{us_1s_2 \cdots s_m} \alpha_* \left(\frac{t_1}{1}, \frac{t_2}{1}, \ldots, \frac{t_n}{1} \right),$$

que por $(\star)$, es igual a

$$\frac{1}{us_1s_2 \cdots s_m} \left(\frac{us_2 \cdots s_m r_1}{1}, \ldots, \frac{us_1s_2 \cdots s_{m-1} r_m}{1} \right) = \left(\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_m}{s_m} \right).$$

Por tanto, $(\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_m}{s_m}) \in Im(\alpha_*)$ y $Ker(\beta_*) \subseteq Im(\alpha_*)$. De estos dos contenidos, se deduce *i)*.

Probemos ahora *ii)*. Primero, que $Im(\beta_*) \subseteq S^{-1}M$ se tiene pues β_* está bien definida. Ahora, para el otro contenido, por exactitud tenemos que $M = Im(\beta)$. Luego, para cualquier $m \in M$, existe $(r_1, \ldots, r_m) \in R^m$ tal que $m = \beta(r_1, \ldots, r_m)$ y por tanto, para todo $\frac{m}{s} \in S^{-1}M$,

$$\begin{aligned} \frac{m}{s} &= \frac{\beta(r_1, \ldots, r_m)}{s} = \frac{r_1\beta(1, 0, \ldots, 0) + \cdots + r_m\beta(0, 0, \ldots, 1)}{s} \\ &= \frac{r_1}{s} \frac{\beta(1, 0, \ldots, 0)}{1} + \cdots + \frac{r_m}{s} \frac{\beta(0, 0, \ldots, 1)}{1} = \beta_* \left(\frac{r_1}{s}, \ldots, \frac{r_m}{s} \right). \end{aligned}$$

Entonces, para cualquier $\frac{m}{s} \in S^{-1}M$, $\frac{m}{s} \in Im(\beta_*)$ y por tanto, $S^{-1}M \subseteq Im(\beta_*)$. Luego, se tiene *ii)* y que $(S^{-1}P)$ es una presentación de $S^{-1}M$. Ahora, por como hemos construido nuestra presentación se sigue que si $(\alpha_{ij})_{i\leq n,\, j\leq m}$ es la matriz asociada a α entonces $\left(\frac{\alpha_{ij}}{1}\right)_{i\leq n,\, j\leq m}$ es la matriz asociada a α_*. Así, para cualquier $r \in \mathbb{Z}$, si $Fitt_r(M) = \langle a_1, \ldots, a_k \rangle$, para ciertos $a_1, \ldots, a_k \in R$, entonces

$$Fitt_r(S^{-1}M) = \left\langle \frac{a_1}{1}, \ldots, \frac{a_k}{1} \right\rangle$$

y

$$\begin{aligned} S^{-1}Fitt_r(M) = S^{-1} \langle a_1, \ldots, a_k \rangle &= \left\{ \frac{b}{s} : s \in S \wedge b \in \langle a_1, \ldots, a_k \rangle \right\} \\ &= \left\{ \frac{r_1a_1 + \cdots + r_ka_k}{s} : s \in S \wedge r_1, \ldots, r_k \in R \right\} \\ &= \left\{ \frac{r_1}{s} \frac{a_1}{1} + \cdots + \frac{r_k}{s} \frac{a_k}{1} : s \in S \wedge r_1, \ldots, r_k \in R \right\} \subseteq Fitt_r(S^{-1}M). \end{aligned}$$

Luego, $S^{-1}Fitt_r(M) \subseteq Fitt_r(S^{-1}M)$ y el otro contenido se tiene pues para todo $i \in \{1, \ldots, k\}$, $\frac{a_i}{1} \in \left\{ \frac{b}{s} : s \in S \wedge b \in \langle a_1, \ldots, a_k \rangle \right\} = S^{-1}Fitt_r(M)$ y por tanto, $\left\langle \frac{a_1}{1}, \ldots, \frac{a_k}{1} \right\rangle = Fitt_r(S^{-1}M) \subseteq S^{-1}Fitt_r(M)$. De ambos contenidos queda demostrado lo que queríamos. □

Propiedad 1.5.5 *Sean R un anillo conmutativo y unitario y M y M' dos R-módulos isomorfos finitamente generados. Entonces, para cualquier $r \in \mathbb{Z}$*

$$Fitt_r(M) = Fitt_r(M').$$

Demostración. Primero, como M es isomorfo a M', existe $f : M \longrightarrow M'$ isomorfismo. Ahora, si tomamos $R^n \xrightarrow{\alpha} R^m \xrightarrow{\beta} M \longrightarrow 0$ una presentación cualquiera de M, podemos considerar la sucesión $R^n \xrightarrow{\alpha} R^m \xrightarrow{f\circ\beta} M' \longrightarrow 0$. Demostremos que esta es una presentación de M'. Tenemos primero por exactitud que $Ker(\beta) = Im(\alpha)$. Si tomamos $x \in Ker(f \circ \beta)$, entonces, $f(\beta(x)) = 0$ y por tanto, $\beta(x) \in Ker(f)$. Pero $Ker(f) = \{0\}$ pues f en particular es un monomorfismo. Luego, $\beta(x) = 0$ y $x \in Ker(\beta) = Im(\alpha)$. Entonces, se sigue que $Ker(f \circ \beta) \subseteq Im(\alpha)$. Recíprocamente, sea $x \in Im(\alpha) = Ker(\beta)$, se tiene que $\beta(x) = 0$ y por tanto,

$$(f \circ \beta)(x) = f(\beta(x)) = f(0) = 0$$

y $x \in Ker(f \circ \beta)$. Luego, $Im(\alpha) \subseteq Ker(f \circ \beta)$ y con el otro contenido se deduce que $Im(\alpha) = Ker(f \circ \beta)$. Ahora, que $Im(f \circ \beta) \subseteq M'$ es trivial y para el otro contenido, consideramos un $m' \in M'$ cualquiera. Por ser f en particular sobreyectiva, existe $m \in M$ tal que $m' = f(m)$. Además, como por exactitud, β es sobreyectiva, sabemos que existe $x \in R^m$ tal que $\beta(x) = m$. Luego,

$$m' = f(m) = f(\beta(x)) = (f \circ \beta)(x).$$

De este modo, se deduce que $m' \in Im(f \circ \beta)$ y que $M' = Im(f \circ \beta)$. Queda así probado que $R^n \xrightarrow{\alpha} R^m \xrightarrow{f\circ\beta} M' \longrightarrow 0$ es una presentación de M'. Por último, para cualquier $r \in \mathbb{Z}$, $Fitt_r(M) = Fitt_r(M')$ pues si A es la matriz de α, $Fitt_r(M) = I_{m-r}(A) = Fitt_r(M')$. □

Que dos módulos tengan los mismos ideales de Fitting no implica que sean isomorfos como ilustra el siguiente ejemplo extraído de [3, Example A2.57.].

Ejemplo 1.5.6 *Sea K un cuerpo, y consideramos los $K[x, y]$-módulos M y M' con matrices de presentación*

$$A = \begin{pmatrix} x & 0 \\ y & x \\ 0 & y \end{pmatrix} \quad y \quad A' = \begin{pmatrix} x & 0 \\ y & 0 \\ 0 & x \\ 0 & y \end{pmatrix}$$

respectivamente. Tenemos que

$$\begin{array}{lll} Fitt_0(M) = I_2(A) = \langle x^2, xy, y^2 \rangle & y & Fitt_0(M') = I_2(A') = \langle x^2, xy, y^2 \rangle . \\ Fitt_1(M) = I_1(A) = \langle x, y \rangle & y & Fitt_1(M') = I_1(A') = \langle x, y \rangle . \end{array}$$

Además, $Fitt_k(M) = Fitt_k(M') = K[x,y]$, para todo $k \geq 2$. En resumen, $Fitt_r(M) = Fitt_r(M')$ para todo $r \in \mathbb{Z}$. Probemos ahora que M y M' no son isomorfos. Primero, por la Propiedad 1.5.3 i) con $r = 2$ se tiene que $Ann(M), Ann(M') \subseteq \langle x,y\rangle$. Además por cómo es la matriz A', se sigue que $x, y \in Ann(M')$ y por tanto, $\langle x,y\rangle \subseteq Ann(M')$. De este modo, se deduce que $Ann(M') = \langle x,y\rangle$. Pero, ni x ni y están en $Ann(M)$, es más, si lo estuvieran la matriz A tendría que ser igual a A', por lo que $Ann(M) \neq Ann(M')$ y M y M' no pueden ser isomorfos.

Propiedad 1.5.7 *[12, Lemma 15.8.4. (2)]. Sean R un anillo conmutativo y unitario, M y M' dos $R-$módulos, entonces para todo $r \in \mathbb{Z}$, se tiene que*

$$Fitt_r(M \oplus M') = \sum_{r_1+r_2=r} Fitt_{r_1}(M) Fitt_{r_2}(M').$$

Demostración. Si $R^n \xrightarrow{\alpha} R^m \xrightarrow{\beta} M \longrightarrow 0$ y $R^{n'} \xrightarrow{\alpha'} R^{m'} \xrightarrow{\beta'} M' \longrightarrow 0$ son dos presentaciones de M y M' respectivamente y A es la matriz de α y A' es la matriz de α', podemos construir $R^{n+n'} \xrightarrow{\alpha\oplus\alpha'} R^{m+m'} \xrightarrow{\beta\oplus\beta'} M \oplus M' \longrightarrow 0$ presentación de $M \oplus M'$ con matriz de presentación $B = \left(\begin{array}{c|c} A & \mathbf{O} \\ \hline \mathbf{O} & A' \end{array}\right)$. Por tanto, para cualquier $r \in \mathbb{Z}$, $Fitt_r(M \oplus M') = I_{(m+m')-r}(B)$ y si aplicamos la Propiedad 1.2.3, se sigue que

$$\begin{aligned} Fitt_r(M \oplus M') &= \sum_{r_1+r_2=m+m'-r} I_{r_1}(A) I_{r_2}(A') \\ &= \sum_{r_1+r_2=m+m'-r} Fitt_{m-r_1}(M) Fitt_{m'-r_2}(M') \\ &= \sum_{(m-r_1)+(m'-r_2)=r} Fitt_{m-r_1}(M) Fitt_{m'-r_2}(M') \\ &= \sum_{k_1+k_2=r} Fitt_{k_1}(M) Fitt_{k_2}(M'). \end{aligned}$$

□

Propiedad 1.5.8 *[12, Lemma 15.8.7.]. Sean R un anillo conmutativo unitario y M un $R-$módulo. Entonces, si M puede ser generado por r elementos, $Fitt_r(M) = R$ y además si R es local el recíproco es cierto.*

Demostración. Si M puede ser generado por r elementos, podemos encontrar una presentación de M de la forma $R^q \xrightarrow{\alpha} R^r \xrightarrow{\beta} M \longrightarrow 0$. Si llamamos A a la matriz de α, se tiene que A tiene r columnas. Luego, $Fitt_r(M) = I_0(A) = R$. Recíprocamente, supongamos que R es local y $Fitt_r(M) = R$. Primero, $\mathfrak{m} := R \setminus R^*$ es un ideal (maximal) de R. Si consideramos $R^n \xrightarrow{\alpha} R^q \xrightarrow{\beta} M \longrightarrow 0$

una presentación cualquiera de M, se tiene que M puede ser generado por q elementos. Denotamos por $A \in \mathcal{M}_{n,q}(R)$ la matriz de α. Supongamos ahora que $q = r + 1$, entonces

$$I_{q-r}(A) = I_1(A) = Fitt_r(M) = R,$$

luego, A tiene una entrada que no está en $\mathfrak{m}$, porque si A tuviera todas sus entradas en $\mathfrak{m}$, $I_1(A) \subseteq \mathfrak{m} \neq R$. Como A tiene una entrada $a \in R^*$, hay un generador que se puede poner como combinación lineal de los demás y por tanto sobra, ya que si $\{e_j\}_{j=1}^{r+1} \subseteq M$ es el conjunto de generadores de M y la fila en la que está a es $\begin{pmatrix} r_{i,1} & r_{i,2} & \cdots & r_{i,j-1} & a & r_{i,j+1} & \cdots & r_{i,r+1} \end{pmatrix}$; entonces

$$r_{i,1}e_1 + \cdots + r_{i,j-1}e_{j-1} + ae_j + r_{i,j+1}e_{j+1} + \cdots + r_{i,r+1}e_{r+1} = 0.$$

Luego, $ae_j = -\sum_{k \neq j} r_{i,k}e_k$ y $a^{-1}ae_j = e_j = \sum_{k \neq j}(-a^{-1}r_{i,k})e_k$. Ahora, si tenemos que $q = r + k$, para cierto $k \geq 1$, aplicando el mismo razonamiento, podemos ir quitando generadores de uno en uno hasta quedarnos con r. □

Ejemplo 1.5.9 *Sean el anillo local* $\mathbb{Z}_{(2)} = \left\{\frac{r}{s} \in \mathbb{Q} : 2 \nmid s\right\} \subseteq \mathbb{Q}$ *y el* $\mathbb{Z}_{(2)}-$*módulo* $M = \left\{\left(\frac{[r_1]_2}{s_1}, \frac{[r_2]_3}{s_2}, \frac{[r_3]_7}{s_3}\right) : s_1, s_2, s_3 \in \mathbb{Z} \setminus \{0\}\right\}$.

Tomamos como generadores de M *a* $e_1 = \left(\frac{[1]_2}{1}, \frac{[0]_3}{1}, \frac{[0]_7}{1}\right), e_2 = \left(\frac{[0]_2}{1}, \frac{[1]_3}{1}, \frac{[0]_7}{1}\right)$ *y* $e_3 = \left(\frac{[0]_2}{1}, \frac{[0]_3}{1}, \frac{[1]_7}{1}\right)$. *Una matriz de presentación de* M *sería*

$$A = \begin{pmatrix} \frac{2}{1} & \frac{0}{1} & \frac{0}{1} \\ \\ \frac{0}{1} & \frac{3}{1} & \frac{0}{1} \\ \\ \frac{0}{1} & \frac{0}{1} & \frac{7}{1} \end{pmatrix}.$$

Así, $Fitt_0(M) = \left\langle \frac{42}{1} \right\rangle = \left\langle \frac{2}{1} \right\rangle$ *pues* $\frac{2}{1} \in \left\langle \frac{42}{1} \right\rangle$ *ya que* $\frac{2}{1} = \frac{1}{21}\frac{42}{1}$ *(*$\frac{1}{21} \in \mathbb{Z}_{(2)}$, $21 \nmid 2$*) y* $\frac{42}{1} \in \left\langle \frac{2}{1} \right\rangle$ *porque* $\frac{42}{1} = \frac{21}{1}\frac{2}{1}$. *Además,* $Fitt_1(M) = \left\langle \frac{6}{1}, \frac{21}{1}, \frac{14}{1} \right\rangle \subseteq \mathbb{Z}_{(2)}$ *y* $\left\langle \frac{21}{1} \right\rangle \subseteq Fitt_1(M)$ *pero* $\left\langle \frac{21}{1} \right\rangle = \mathbb{Z}_{(2)}$ *ya que* $\frac{1}{21}\frac{21}{1} = \frac{1}{1} \in \left\langle \frac{21}{1} \right\rangle$. *De este modo, es claro que* $Fitt_1(M) = \mathbb{Z}_{(2)}$ *y que*

$$Fitt_k(M) = \begin{cases} \left\langle \frac{0}{1} \right\rangle \text{ si } k \leq 0 \\ \left\langle \frac{2}{1} \right\rangle \text{ si } k = 0 \\ \mathbb{Z}_{(2)} \text{ si } k \geq 1 \end{cases}.$$

Aplicando la Propiedad 1.5.8, como $Fitt_1(M) = \mathbb{Z}_{(2)}$ *y* $\mathbb{Z}_{(2)}$ *es local, se tiene que* M *puede ser generado por un único elemento. De otra manera,* $\mathfrak{m} = \mathbb{Z}_{(2)} \setminus \mathbb{Z}_{(2)}{}^*$ $= \left\{\frac{2h}{s} \in \mathbb{Q} : 2 \nmid s\right\}$. *Luego, se deduce que* $\frac{3}{1}, \frac{7}{1} \notin \mathfrak{m}$ *y de hecho,* $e_2, e_3 = 0_M$ *pues como* $\frac{3}{1}e_2 = 0_M$ *y* $\frac{7}{1}e_3 = 0_M$ *se tiene que* $\frac{1}{3}\frac{3}{1}e_2 = e_2 = 0_M$ *y* $\frac{1}{7}\frac{7}{1}e_3 = e_3 = 0_M$. *Por tanto, podemos quitar del conjunto de generadores a* e_2 *y* e_3 *y tomar como matriz de presentación de* M *a* $A' = \begin{pmatrix} \frac{2}{1} \end{pmatrix}$.

2

La resultante

En este capítulo estudiaremos la resultante de dos polinomios y mostraremos la relación que tienen con los ideales de Fitting que estudiamos en el Capítulo 1. En gran parte de lo que sigue nos hemos basado en las notas [9].

2.1. Notación y propiedades

Sea A una matriz cuadrada, entonces, denotamos por $A^\wedge := Adj(A)^t$ la traspuesta de la matriz adjunta de A. Tenemos además la regla de Cramer

$$AA^\wedge = A^\wedge A = (det(A))I. \tag{RC}$$

Sea R un anillo conmutativo unitario, denotamos por $R[T]$ al anillo de polinomios en una variable T y coeficientes en R. Para cualquier $N > 0$, denotamos por $R[T]^{(N)}$ al conjunto de polinomios de grado menor que N. De este modo,

$$R[T]^{(N)} = \{r_1T^{N-1} + r_2T^{N-2} + \cdots + r_N : r_j \in R, \text{para todo } j \in \{1, \ldots, N\}\}.$$

Así, $R[T]^{(N)}$ es un R-módulo libre de rango N y una base es $\{1, T, \ldots, T^{N-1}\}$. Para cualquier sucesión de N polinomios en $R[T]^{(N)}$ de la forma

$$f_i = r_{i1}T^{N-1} + f_{i2}T^{N-2} + \cdots + r_{iN},\ i = 1, \ldots, N$$

consideramos la matriz

$$A(f_1, \ldots, f_N) := \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1N} \\ r_{21} & r_{22} & \cdots & r_{2N} \\ \vdots & \vdots & & \vdots \\ r_{N1} & r_{N2} & \cdots & r_{NN} \end{pmatrix} = (r_{ij})_{i,\, j=1,\ldots,N}$$

y su determinante

$$det(f_1, \ldots, f_N) := det(A(f_1, \ldots, f_N)).$$

De las propiedades de los determinantes se tiene que

Propiedad 2.1.1 *Sea $i \in \{1, \ldots, N\}$, entonces existe $\varphi : R[T]^{(N)} \longrightarrow R$ lineal con $\varphi(f_i) = det(f_1, \ldots, f_N)$.*

Demostración. Si $det(f_1 \ldots, f_N) = 0$, podemos tomar $\varphi = 0$. Supongamos que $det(f_1 \ldots, f_N) \neq 0$. Entonces $\{f_1, \ldots, f_N\}$ es un conjunto linealmente independiente en $R[T]^{(N)}$ y como el rango del R-módulo libre $R[T]^{(N)}$ es N, entonces, $\{f_i\}_{i=1}^N$ es base de $R[T]^{(N)}$. Por tanto, para todo $r \in R[T]^{(N)}$, existe un único $\{r_i\}_{i=1}^N$ tal que $r = \sum_{i=1}^{N} r_i f_i$ y definimos

$$\varphi(r) := \sum_{i=1}^{N} r_i \; det(f_1, \ldots, f_N) = det(f_1, \ldots, f_N) \sum_{i=1}^{N} r_i$$

que es lineal. □

Propiedad 2.1.2 *Sea S_N el conjunto de todas las permutaciones de $\{1, \ldots, N\}$. Entonces para cualquier $\sigma \in S_N$, se tiene que*

$$det(f_{\sigma(1)}, \ldots, f_{\sigma(N)}) = (sgn(\sigma)) \; det(f_1, \ldots, f_N),$$

donde $sgn(\sigma)$ denota el signo de σ.

Demostración. Cada vez que se permutan dos filas (o columnas) de una matriz cuadrada su determinante cambia de signo. □

Propiedad 2.1.3 *Se tiene que $det(T^{N-1}, T^{N-2}, \ldots, 1) = 1$.*

Demostración. Obsérvese que $A(T^{N-1}, \ldots, 1) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = I_N.$ □

Propiedad 2.1.4 *Si $f_i \in R[T]^{(N)}$ es de grado menor estrictamente que $N-1$, para todo $i \in \{1, \ldots, N\}$ entonces $det(f_1, \ldots, f_N) = 0$.*

Demostración. Como $deg(f_i) < N - 1$, para todo $i \in \{1, \ldots, N\}$ entonces $f_i = 0T^{N-1} + r_{i2}T^{N-2} + \cdots + r_{in}$, para todo $i \in \{1, \ldots, N\}$ y para ciertos $r_{ij} \in R$. Luego,

$$A(f_1, \ldots, f_N) = \begin{pmatrix} 0 & r_{12} & \cdots & r_{1N} \\ 0 & r_{22} & \cdots & r_{2N} \\ \vdots & \vdots & & \vdots \\ 0 & r_{N2} & \cdots & r_{NN} \end{pmatrix}$$

cuya primera columna es nula y concluímos la propiedad. □

Propiedad 2.1.5 *Si R es un dominio de integridad, entonces $det(f_1, \ldots, f_N) = 0$ si y sólo si, existen $r_1, r_2, \ldots, r_N \in R$ no todos nulos tales que $r_1 f_1 + r_2 f_2 + \cdots + r_N f_N = 0$.*

Demostración. Supongamos en primer lugar que $det(f_1, \ldots, f_N) = 0$, entonces hay una fila de la matriz $A(f_1, \ldots, f_N)$ que es combinación lineal de las demás, y por tanto, existe un $i \in \{1, \ldots, N\}$ tal que $f_i = \sum_{j \in \{1,\ldots,N\} \setminus \{i\}} r_j f_j$ para ciertos $r_j \in R$. Entonces, $0 = \sum_{j \in \{1,\ldots,N\} \setminus \{i\}} r_j f_j - f_i$ es decir, $0 = r_1 f_1 + \cdots + r_i f_i + \cdots + r_N f_N$, donde $r_i := -1$.

Ahora, supongamos que existen $r_1, \ldots, r_N \in R$ con $(r_1, \ldots, r_N) \neq (0, \ldots, 0)$ tales que $r_1 f_1 + \cdots + r_N f_N = 0$, entonces existe al menos un $i \in \{1, \ldots, N\}$ tal que $r_i \neq 0$ y

$$r_i f_i = \sum_{j \in \{1,\ldots,N\} \setminus \{i\}} (-r_j) f_j. \qquad (*_1)$$

Por propiedades de los determinantes tenemos que

$$det(f_1, \ldots, f_{i-1}, r_i f_i, f_{i+1}, \ldots, f_N) = r_i \; det(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_N).$$

Pero $det(f_1, \ldots, f_{i-1}, r_i f_i, f_{i+1}, \ldots, f_N) = 0$ porque, por $(*_1)$, la fila i-ésima es combinación lineal de las otras. Por tanto, $r_i \; det(f_1, \ldots, f_N) = 0$ y como R es dominio de integridad y $r_i \neq 0$, se sigue que $det(f_1, \ldots, f_N) = 0$. □

Propiedad 2.1.6 *Se tiene que*

$$det(f_1, \ldots, f_N) \begin{pmatrix} T^{N-1} \\ \vdots \\ 1 \end{pmatrix} = (A(f_1, \ldots, f_N))^{\wedge} \begin{pmatrix} f_1 \\ \vdots \\ f_N \end{pmatrix}.$$

Demostración. Por la definición de $A(f_1, \ldots, f_N)$ tenemos que

$$\begin{pmatrix} f_1 \\ \vdots \\ f_N \end{pmatrix} = A(f_1, \ldots, f_N) \begin{pmatrix} T^{N-1} \\ \vdots \\ 1 \end{pmatrix} \qquad (*_2)$$

luego, multiplicando por $(A(f_1, \ldots, f_N))^{\wedge}$ por la izquierda en ambos lados de $(*_2)$, se sigue que

$$(A(f_1, \ldots, f_N))^{\wedge} \begin{pmatrix} f_1 \\ \vdots \\ f_N \end{pmatrix} = (A(f_1, \ldots, f_N))^{\wedge} A(f_1, \ldots, f_N) \begin{pmatrix} T^{N-1} \\ \vdots \\ 1 \end{pmatrix}$$

y aplicando la regla de Cramer (RC), se tiene que

$$(A(f_1,\dots,f_N))^{\wedge}A(f_1,\dots,f_N) = det(A(f_1,\dots,f_N)) = det(f_1,\dots,f_N),$$

lo que concluye la propiedad. □

Propiedad 2.1.7 *Para cualquier polinomio $h \in R[T]^{(N)}$, existen $r_1,\dots,r_N \in R$ tales que $det(f_1,\dots,f_N)h = r_1f_1 + \cdots + r_Nf_N$.*

Demostración. Sea $h = h_1T^{N-1} + \cdots + h_N \in R[T]^{(N)}$. Por la Propiedad 2.1.6 y multiplicando por la matriz fila $\begin{pmatrix} h_1 \cdots & h_N \end{pmatrix}$ por la izquierda, se tiene que

$$\begin{pmatrix} h_1 \cdots & h_N \end{pmatrix} \begin{pmatrix} det(f_1,\dots,f_N)T^{N-1} \\ \vdots \\ det(f_1,\dots,f_N) \end{pmatrix} = \begin{pmatrix} h_1 \cdots & h_N \end{pmatrix} (A(f_1,\dots,f_N))^{\wedge} \begin{pmatrix} f_1 \\ \vdots \\ f_N \end{pmatrix}.$$

Entonces $\begin{pmatrix} det(f_1,\dots,f_N)(h_1T^{N-1} + \cdots + h_N) \end{pmatrix} = \begin{pmatrix} r_1 \, r_2 \cdots & r_N \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_N \end{pmatrix}$ donde $\begin{pmatrix} r_1 \, r_2 \cdots & r_N \end{pmatrix} = \begin{pmatrix} h_1 \cdots h_N \end{pmatrix} (A(f_1,\dots,f_N))^{\wedge}$. Luego, se sigue que

$$\begin{pmatrix} det(f_1,\dots,f_N)h \end{pmatrix} = \begin{pmatrix} r_1f_1 + \cdots + r_Nf_N \end{pmatrix}$$

y por tanto, $det(f_1,\dots,f_N)h = r_1f_1 + \cdots + r_Nf_N$. □

2.2. Primeras propiedades de la resultante

En esta sección mostraremos algunas de las propiedades de la resultante.

Definición 2.2.1 (Resultante) *Sean n, m enteros no negativos tales que $n > 0$ o $m > 0$. Entonces para cualquier par de polinomios*

$$f(T) = a_0T^n + a_1T^{n-1} + \cdots + a_n,\ g(T) = b_0T^m + b_1T^{m-1} + \cdots + b_m \in R[T] \quad \text{(D)}$$

definimos la matriz de Sylvester de f y g

$$Syl_{n,m}(f,g) := A(T^{m-1}f, T^{m-2}f, \dots, f, T^{n-1}g, T^{n-2}g, \dots, g)$$

y la resultante de f y g,

$$Res_{n,m}(f,g) := det(Syl_{n,m}(f,g)) \in R.$$

La matriz de Sylvester es una matriz cuadrada de orden $n+m$ y

$$Syl_{0,m}(f,g) = A(T^{m-1}f, T^{m-2}f, \dots, f),\ Syl_{n,0}(f,g) = A(T^{n-1}g, T^{n-2}g, \dots, g).$$

Proposición 2.2.2 *Sean $a, b \in R$, y f y g como en (D). Se tiene*

i) $Res_{n,m}(af, bg) = a^m b^n Res_{n,m}(f, g)$.
ii) $Res_{n,m}(f, g) = (-1)^{n+m} Res_{m,n}(g, f)$.
iii) $Res_{n,0}(f, b_0) = b_0^n$, $Res_{0,m}(a_0, g) = a_0^m$.
iv) Si $f \in R[T]^{(n)}$ *y* $g \in R[T]^{(m)}$ *entonces* $Res_{n,m}(f, g) = 0$.
v) Para cualquier $h \in R[T]^{(n+m)}$ *existen polinomios* $u \in R[T]^{(n)}$ *y* $v \in R[T]^{(m)}$ *tales que* $Res_{n,m}(f, g)h = uf + vg$.

Demostración. Primero observemos que

$$\begin{aligned} Res_{n,m}(af, bg) &= det(Syl_{n,m}(af, bg)) \\ &= det(A(T^{m-1}(af), T^{m-2}(af), \ldots, af, T^{n-1}(bg), T^{n-2}(bg), \ldots, bg)). \end{aligned}$$

Por propiedades de los determinantes, si un elemento multiplica a toda una fila (o columna) se puede extraer del determinante multiplicando, luego,

$$Res_{n,m}(af, bg) = a^m b^n det(A(T^{m-1}f, \ldots, f, T^{n-1}g, \ldots, g)) = a^m b^n Res_{n,m}(f, g)$$

y concluimos *i)*. El apartado *ii)* es consecuencia de la Propiedad 2.1.2. Por otra parte, $Res_{n,0}(f, b_0) = det(Syl_{n,0}(f, b_0)) = det(A(T^{n-1}b_0, T^{n-2}b_0, \ldots, Tb_0, b_0))$. Razonando como en la prueba de *i)*, se sigue que $det(A(T^{n-1}b_0, \ldots, Tb_0, b_0)) = b_0^n det(A(T^{n-1}, \ldots, T, 1))$ que por la Propiedad 2.1.3 es igual a $b_0^n \cdot 1$. Luego, $Res_{n,0}(f, b_0) = b_0^n$. Análogamente, se tiene que

$$Res_{0,m}(a_0, g) = det(Syl_{0,m}(a_0, g)) = det(T^{m-1}a_0, \ldots, Ta_0, a_0) = a_0 det(T^{n-1}, \ldots, 1)$$

y nuevamente por la Propiedad 2.1.3 se deduce *iii)*. Ahora, si tomamos $f \in R[T]^{(n)}$ y $g \in R[T]^{(m)}$ entonces, $deg(f) < n$ y $deg(g) < m$. Luego se sigue que en $Syl_{n,m}(f, g)$ la primera columna está llena de ceros, ya que esa columna se corresponde con los coeficientes de T^{n+m-1} en $T^{m-1}f, \ldots, f, T^{n-1}g, \ldots, g$ y estos polinomios como mucho tienen grado $n + m - 2$. Luego, $det(Syl_{n,m}(f, g)) = 0$ y por tanto, $Res_{n,m}(f, g) = 0$ y queda probado *iv)*. Ahora, si consideramos $h \in R[T]^{(n+m)}$, por la Propiedad 2.1.7 sabemos que existen $c_1, \ldots, c_{m+n} \in R$ tales que

$$\begin{aligned} det(T^{m-1}f, \ldots, f, T^{n-1}g, \ldots, g)h &= \sum_{i=1}^{m} c_i(T^{m-i}f) + \sum_{i=1}^{n} c_{m+i}(T^{n-i}g) \\ &= f \sum_{i=1}^{m} c_i T^{m-i} + g \sum_{i=1}^{n} c_{m+i} T^{n-i}. \end{aligned}$$

Luego si llamamos $u := c_1 T^{m-1} + \cdots + c_m \in R[T]^{(m)}$ y $v := c_{m+1} T^{n-1} + \cdots + c_{m+n} \in R[T]^{(n)}$ se llega a que *v)* es cierto. □

Proposición 2.2.3 *Sea R un dominio de integridad. Entonces $Res_{n,m}(f,g)=0$ si y sólo si, existen polinomios $u\in R[T]^{(m)}$ y $v\in R[T]^{(n)}$ con $(u,v)\neq(0,0)$ tales que $uf+vg=0$ en $R[T]$.*

Demostración. De la definición de resultante se tiene que $Res_{n,m}(f,g)=0$ si y solo si, $det(T^{m-1}f,\dots,f,T^{n-1}g,\dots,g)=0$ y se da por la Propiedad 2.1.5 si, y solo si, existe $(a'_1,\dots,a'_m,b'_1\dots,b'_n)\in R^{n+m}\setminus\{(0,\dots,0)\}$ tal que $a'_1T^{m-1}f+\cdots+a'_mf+b'_1T^{n-1}+\cdots+b'_ng=0$. Luego, queda probado considerando $u:=a'_1T^{m-1}+\cdots+a'_m\in R[T]^{(m)}$ y $v:=b'_1T^{n-1}+\cdots+b'_n\in R[T]^{(n)}$. □

Proposición 2.2.4 *Sean R un dominio de factorización única, $f=a_0T^n+\cdots+a_n\in R[T], a_0\neq 0, n>0$ y $g=b_0T^m+\cdots+b_m\in R[T]$. Entonces, $Res_{n,m}(f,g)=0$ si, y solo si, f y g tienen al menos un divisor común de grado mayor que cero.*

Demostración. Primero, supongamos que $f=u'\phi$ y $g=v'\phi$ para ciertos $u',v',\phi\in R[T]$ con $deg(\phi)>0$, entonces $\phi\neq 0$ y como $n>0$, $f\neq 0$ y se deduce que $u'\neq 0$. Se tiene además que $v'f-u'g=v'u'\phi-u'v'\phi=0$ donde $deg(u')<deg(f)=n$ y por tanto, $-u'\in R[T]^{(n)}$ y $deg(v')<deg(g)\leq m$, entonces $v'\in R[T]^{(m)}$. Luego, como por definición todo dominio de factorización única en particular es un dominio de integridad, aplicando la Proposición 2.2.3 se deduce que $Res_{n,m}(f,g)=0$. Ahora, supongamos que $Res_{n,m}(f,g)=0$. Nuevamente, como todo dominio de factorización única es un dominio de integridad, aplicando la Proposición 2.2.3, se tiene que existen $u\in R[T]^{(m)}$ y $v\in R[T]^{(n)}$ con $u\neq 0$ o $v\neq 0$ tales que $uf+vg=0$. Tenemos que v no puede ser 0 porque si $v=0$ entonces se tendría que $u\neq 0$ y $uf+vg=uf=0$ con $u\neq 0$ y $f\neq 0$, lo cual es absurdo porque estamos en un dominio de integridad. Luego, $v\neq 0$ y $uf=-vg$. Como además, $a_0\neq 0$ entonces $deg(f)=n$, y por tanto, uno de los factores irreducibles de f debe dividir a g porque $R[T]$ es un dominio de factorización única y $deg(v)<n=deg(f)$. □

2.3. La resultante $Res_{n,m}(f,g)$ como polinomio en coeficientes de f y g

Continuamos con más propiedades de la resultante.

Propiedad 2.3.1 *Sean $f=a_0T^n+\cdots+a_n, g=b_0T^m+\cdots+b_m\in R[T]$, con $n,m>0$. Si $Syl_{n,m}(f,g)=(c_{ij})_{i,j=1,\dots,n+m}$, entonces se tiene que*

I) Si $i\in\{1,\dots,m\}$, $c_{ij}=\begin{cases} a_{j-i}, \text{ si } j\in\{i,\dots,i+n\} \\ 0, \quad \text{si } j\notin\{i,\dots,i+n\}. \end{cases}$

$$II)\, Si\ i \notin \{1,\dots,m\},\ c_{ij} = \begin{cases} b_{j-i+m},\ si\ \ j \in \{i-m,\dots,i\} \\ \\ 0, \qquad\quad si\ j \notin \{i-m,\dots,i\}. \end{cases}$$

Demostración. Es consecuencia de la Definición 2.2.1. □

Definición 2.3.2 *Sea $S_{n,m}$ el conjunto de permutaciones de S_{n+m} definido como sigue:*

$$S_{n,m} = \left\{ \sigma \in S_{n+m} : \begin{array}{c} i \le \sigma(i) \le i+n, \text{para todo } i \in \{1,\dots,m\} \\ \wedge \\ k \le \sigma(k+m) \le k+m, \text{para todo } k \in \{1,\dots,n\} \end{array} \right\}.$$

Propiedad 2.3.3 *Tomando f y g como en la Propiedad 2.3.1, tenemos*

$$Res_{n,m}(f,g) = \sum_{\sigma \in S_{n,m}} (sgn(\sigma)) a_{\sigma(1)-1} \cdots a_{\sigma(m)-m} b_{\sigma(m+1)-1} \cdots b_{\sigma(m+n)-n}.$$

Demostración. Por la definición clásica de determinante y usando la Propiedad 2.3.1 se tiene que

$$\begin{aligned} Res_{n,m}(f,g) &= \sum_{\sigma \in S_{n+m}} (sgn(\sigma)) c_{1,\sigma(1)} \cdots c_{m+n,\sigma(m+n)} \\ &= \sum_{\sigma \in S_{n,m}} (sgn(\sigma)) a_{\sigma(1)-1} \cdots a_{\sigma(m)-m} b_{\sigma(m+1)-1} \cdots b_{\sigma(m+n)-n}. \end{aligned}$$

Nótese que si $\sigma \in S_{n+m} \setminus S_{n,m}$, por la Propiedad 2.3.1 existe $\alpha \in \{1,\dots,m+n\}$ tal que $c_{\alpha,\sigma(\alpha)} = 0$ y por tanto $sgn(\sigma) c_{1,\sigma(1)} \cdots c_{n+m,\sigma(n+m)} = 0$ y si además $\sigma \in S_{n,m}$ entonces nuevamente por la Propiedad 2.3.1, $c_{1,\sigma(1)} = a_{\sigma(1)-1}$, $\dots$, $c_{m,\sigma(m)} = a_{\sigma(m)-m}$, $c_{m+1,\sigma(m+1)} = b_{\sigma(m+1)-1}$, $\dots$, $c_{m+n,\sigma(m+n)} = b_{\sigma(m+n)-n}$. □

Definición 2.3.4 *Sean $\vec{A} = (A_0, A_1, \dots, A_n)$ y $\vec{B} = (B_0, B_1, \dots, B_m)$ variables y consideremos*

$$F(\vec{A},T) = A_0T^n + A_1T^{n-1} + \cdots + An,\ G(\vec{B},T) = B_0T^m + B_1T^{m-1} + \cdots + B_m$$

con coeficientes en $\mathbb{Z}[\vec{A},\vec{B}] := \mathbb{Z}[A_0, A_1, \dots, An, B_0, B_1, \dots, B_m]$. Definimos la resultante de $\vec{A}$ y $\vec{B}$ como $Res(\vec{A},\vec{B}) := Res_{n,m}(F,G)$. Ahora bien, por la Propiedad 2.3.3 podemos escribir

$$Res(\vec{A},\vec{B}) = \sum_{\sigma \in S_{n,m}} (sgn(\sigma)) A_{\sigma(1)-1} \cdots A_{\sigma(m)-m} B_{\sigma(m+1)-1} \cdots B_{\sigma(m+n)-n}. \quad (*_3)$$

Propiedad 2.3.5 *Considerando $\vec{A}, \vec{B}$ como en la Definición 2.3.4, la resultante $Res(\vec{A},\vec{B})$ es un polinomio homogéneo en $\vec{A}$ de grado m y también es un polinomio homogéneo en $\vec{B}$ de grado n.*

Demostración. Es consecuencia de $(*_3)$. □

Propiedad 2.3.6 *Tomando $\vec{A}, \vec{B}$ como en la Definición 2.3.4, si ponemos que $peso(A_i) = i$, para todo $i \in \{0, 1, \ldots, n\}$ y $peso(B_j) = j$, para cualquier $j \in \{0, 1, \ldots, m\}$, entonces el peso de cualquier término de $Res(\vec{A}, \vec{B})$ es igual a mn.*

Demostración. Sea $\sigma \in S_{n,m} \subseteq S_{n+m}$. Como el peso de un producto es la suma de los pesos de los factores, entonces

$$peso(A_{\sigma(1)-1} \cdots A_{\sigma(m)-n} B_{\sigma(m+1)-1} \cdots B_{\sigma(m+n)-n}) = \sum_{i=1}^{m} peso(A_{\sigma(i)-i})$$

$$+ \sum_{j=1}^{n} peso(B_{\sigma(m+j)-j}) = \sum_{i=1}^{m} (\sigma(i) - i) + \sum_{j=1}^{n} (\sigma(m+j) - j) = \sum_{i=1}^{m+n} \sigma(i) - \sum_{i=1}^{m} i$$

$$- \sum_{j=1}^{n} j \overset{(*_4)}{=} \sum_{i=1}^{m+n} i - \sum_{i=1}^{m} i - \sum_{j=1}^{n} j = \frac{(m+n)(m+n+1)}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2}$$

$$= \frac{\cancel{m(m+1)} + mn + \cancel{n(n+1)} + nm - \cancel{m(m+1)} - \cancel{n(n+1)}}{2} = \frac{2mn}{2} = mn,$$

donde la igualdad $(*_4)$ es cierta ya que $\alpha \in S_{n+m}$. □

Propiedad 2.3.7 *Considerando $\vec{A}, \vec{B}$ como en la Definición 2.3.4, se tiene que la resultante $Res(\vec{A}, \vec{B})$ es una $\mathbb{Z}$-combinación lineal de monomios de la forma $A_0^{i_0} A_1^{i_1} \cdots A_n^{i_n} B_0^{j_0} B_1^{j_1} \cdots B_m^{j_m}$ donde $i_0 + \cdots + i_n = m$, $j_0 + \cdots + j_m = n$, $i_1 + 2i_2 + \cdots + ni_n + j_1 + 2j_2 + \cdots + mj_m = mn$. Además, $Res(\vec{A}, \vec{B}) = A_0^m B_m^n + \cdots + (-1)^{mn} A_n^m B_0^n$.*

Demostración. Por la Propiedad 2.3.5 como $Res(\vec{A}, \vec{B})$ es un polinomio homogéneo en $\vec{A}$ de grado m, es claro que $i_0 + \cdots + i_n = m$ y nuevamente, por la Propiedad 2.3.5, como $Res(\vec{A}, \vec{B})$ es un polinomio homogéneo en $\vec{B}$ de grado n, es claro que, $j_0 + j_1 + \cdots + j_m = n$. Ahora, poniendo pesos como en la Propiedad 2.3.6, se sigue que, $peso(A_0^{i_0} A_1^{i_1} \cdots A_n^{i_n} B_0^{j_0} B_1^{j_1} \cdots B_m^{j_m}) = mn$, pero $peso(A_0^{i_0} A_1^{i_1} \cdots A_n^{i_n} B_0^{j_0} B_1^{j_1} \cdots B_m^{j_m}) = 0i_0 + 1i_1 + \cdots + ni_n + 0j_0 + 1j_1 + \cdots + mj_m$. Luego, $i_1 + 2i_2 + \cdots + ni_n + j_1 + 2j_2 + \cdots + mj_m = mn$. Por último, los términos $A_0^m B_m^n$, $(-1)^{mn} A_n^m B_0^n$ se corresponden con las permutaciones $(1, 2, \ldots, m + n), (n+1, n+2, \ldots, n+m, 1, 2, \ldots, n) \in S_{n,m}$ respectivamente. □

2.4. La resultante en función de las raíces

Sean $\vec{X} = (X_1, \ldots, X_n), \vec{Y} = (Y_1, \ldots, Y_m)$ variables y consideremos

$$f = \prod_{i=1}^{n} (T - X_i) = T^n + a_1(\vec{X}) T^{n-1} + \cdots + a_n(\vec{X}) \in \mathbb{Z}[\vec{X}][T],$$

y

$$g = \prod_{j=1}^{m}(T - Y_j) = T^m + b_1(\vec{Y})T^{m-1} + \cdots + b_m(\vec{Y}) \in \mathbb{Z}[\vec{Y}][T].$$

Lema 2.4.1 *Sea* $Res(\vec{X}, \vec{Y}) := Res_{n,m}(f, g)$. *Entonces*

i) $Res(\vec{X}, \vec{Y}) \in \mathbb{Z}[\vec{X}, \vec{Y}]$ *es un polinomio homogéneo de grado* mn.
ii) $Res(\vec{X}, 0) = b_m(\vec{Y})^n = (-1)^{mn}(Y_1 \cdots Y_m)^n$.
iii) Para todo $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$, $X_i - Y_j$ *divide a* $Res(\vec{X}, \vec{Y})$ *en* $\mathbb{Z}[\vec{X}, \vec{Y}]$.

Demostración. En primer lugar, consideramos $\vec{X}' = (1, a_1(\vec{X}), \ldots, a_n(\vec{X}))$, $\vec{Y}' = (1, b_1(\vec{Y}), \ldots, b_m(\vec{Y}))$. Por la Propiedad 2.3.7, sabemos que $Res(\vec{X}', \vec{Y}')$ es una $\mathbb{Z}$-combinación lineal de monomios $a_1(\vec{X})^{i_1}a_2(\vec{X})^{i_2} \cdots a_n(\vec{X})^{i_n}b_1(\vec{Y})^{j_1} \cdots b_m(\vec{Y})^{j_m}$ con $i_1 + 2i_2 + \cdots + ni_n + j_1 + 2j_2 + \cdots + mj_m \overset{(*_5)}{=} mn$ y $Res(\vec{X}', \vec{Y}') = Res_{n,m}(f, g) = Res(\vec{X}, \vec{Y})$ por definición. Ahora, como $f = \prod_{i=1}^{n}(T - X_i) = T^n + a_1(\vec{X})T^{n-1} + \cdots + a_n(\vec{X})$ es claro que f es el producto de n polinomios homogéneos $(T - X_i)$ de grado 1 y por tanto, f es homogéneo de grado n, luego es claro que $deg(a_i(\vec{X})T^{n-i}) = n$, para todo $i \in \{1, \ldots, n\}$ y por tanto,

$$deg(a_i(\vec{X})) = i, \text{ para cualquier } i \in \{1, \ldots, n\}. \qquad (*_6)$$

Del mismo modo, se tiene que

$$deg(b_j(\vec{Y})) = j, \text{ para todo } j \in \{1, \ldots, m\}. \qquad (*_7)$$

Como los términos de $Res(\vec{X}, \vec{Y})$ son de la forma $a_1(\vec{X})^{i_1}a_2(\vec{X})^{i_2} \cdots a_n(\vec{X})^{i_n}$ $b_1(\vec{Y})^{j_1} \cdots b_m(\vec{Y})^{j_m}$, su grado es $deg(a_1(\vec{X}))i_1 + \cdots + deg(a_n(\vec{X}))i_n + deg(b_1(\vec{Y}))j_1$ $+ \cdots + deg(b_m(\vec{Y}))j_m \overset{(*_6),(*_7)}{=} i_1 + 2i_2 + \cdots + ni_n + j_1 + 2j_2 + \cdots + mj_m \overset{(*_5)}{=} mn$, y de este modo, queda demostrado *i)*. Ahora por definición, $Res(\vec{X}, 0) = Res_{n,m}(f, b_m(\vec{Y}))$ y aplicando la Proposición 2.2.2 *iii)* se tiene que

$$Res(\vec{X}, 0) = b_m(\vec{Y})^n = [(-1)^m Y_1 \cdots Y_m]^n = (-1)^{mn}(Y_1 \cdots Y_m)^n,$$

y $b_m(\vec{Y}) = (-1)^m Y_1 \cdots Y_m$ puesto que como $\prod_{j=1}^{m}(T - Y_j) = T^m + b_1(\vec{Y})T^{m-1}$ $+ \cdots + b_m(\vec{Y})$, se sigue que $b_m(\vec{Y}) = (-Y_1)(-Y_2) \cdots (-Y_m) = (-1)^m Y_1 \cdots Y_m$, y queda así probado *ii)*. Por último, por la Proposición 2.2.2 *v)* (tomando $h = 1 \in R[T]$) sabemos que existen $u \in R[\vec{X}, \vec{Y}][T]^{(m)}$ y $v \in R[\vec{X}, \vec{Y}][T]^{(n)}$ tales que $Res_{n,m}(f, g) = Res(\vec{X}, \vec{Y}) = uf + vg$, es decir, $Res(\vec{X}, \vec{Y}) = u\prod_{i=1}^{n}(T - X_i)$

$+ v\prod_{j=1}^{m}(T - Y_j)$. Sustituyendo ahora X_i por T $(i = 1, \ldots, n)$ llegamos a que $X_i - Y_j$ divide a $Res(\vec{X}, \vec{Y})$, para todo $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$, y queda así demostrado *iii)*. □

Proposición 2.4.2 *Con la notación anterior se tiene que*

i) $Res_{n,m}(f, g) = \prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j)$.

ii) $Res_{n,m}(f, B_0T^m + B_1T^{m-1} + \cdots + B_m) = \prod_{i=1}^{n}(B_0X_i^m + B_1X_i^{m-1} + \cdots + B_m)$.

Demostración. El polinomio $(X_i - Y_j)$ es primo en $\mathbb{Z}[\vec{X}, \vec{Y}]$, para todo (i, j) $\in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$ y divide a $Res(\vec{X}, \vec{Y}) = Res_{n,m}(f, g)$ por el Lema 2.4.1 *iii)*. Hay en total, mn y $deg(Res(\vec{X}, \vec{Y})) = mn$, por tanto, podemos escribir $Res(\vec{X}, \vec{Y}) = a\prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j)$ en $\mathbb{Z}[\vec{X}, \vec{Y}]$ para cierto $a \in \mathbb{Z}$. Sustituyendo 0 por $Y_1, \ldots, Y_m$ se tiene que $Res(\vec{X}, 0) = a\prod_{i=1}^{n}\prod_{j=1}^{m}(-Y_j) = a(-1)^{mn}(Y_1 \cdots Y_m)^n$, pero por el Lema 2.4.1 *ii)*, necesariamente a tiene que ser 1 y por tanto, se deduce *i)*. Ahora, para probar *ii)*, nótese que en ambos lados de la igualdad son polinomios homogéneos en $\vec{B}$ de grado n ($deg(B_0X_i^m + B_1X_i^{m-1} + \cdots + B_m) = 1$ y $deg(B_jX_i^{\alpha}) = 1$, para todo i, j, α). Por tanto, es suficiente ver *ii)* para polinomios mónicos $T^m + B_1T^{m-1} + \cdots + B_m$. Ahora por *i)* se tiene que

$$Res_{n,m}\left(\prod_{i=1}^{n}(T - X_i), \prod_{j=1}^{m}(T - Y_j)\right) = Res_{n,m}\left(\prod_{i=1}^{n}(T - X_i), T^m + \cdots + b_m(\vec{Y})\right)$$

$$= \prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j) = \prod_{i=1}^{n}(X_i^m + b_1(\vec{Y})X_i^{m-1} + \cdots + b_m(\vec{Y})),$$

con $b_j(\vec{Y}) := (-1)^j e_j(\vec{Y})$ y $e_j(\vec{Y}) = \sum_{1 \le k_1 < k_2 < \cdots < k_j \le m} Y_{k_1} \cdots Y_{k_j}$, para cualquier $j \in \{1, \ldots, m\}$. Estos polinomios son polinomios simétricos elementales y cumplen que si tenemos un polinomio mónico factorizado de la forma $p(\lambda) = \prod_{\alpha=1}^{N}(\lambda - Z_\alpha)$ entonces, $p(\lambda) = \lambda^N + b_1(Z_1, \ldots, Z_N)\lambda^{N-1} + \cdots + b_N(Z_1, \ldots, Z_N)$ (ver [2] para más información). Se deduce que

$$Res_{n,m}\left(\prod_{i=1}^{n}(T - X_i), T^m + B_1T^{m-1} + \cdots + B_m\right) = \prod_{i=1}^{n}(X_i^m + B_1X_i^{m-1} + \cdots + B_m)$$

como queríamos demostrar. □

Corolario 2.4.3 *Sean* $f(T) = a_0(T - c_1)\cdots(T - c_n)$ *y* $g(T) \in R[T]$ *con* $deg(g) \leq m$. *Entonces*

$$Res_{n,m}(f, g) = a_0^m \prod_{i=1}^{n} g(c_i).$$

Demostración. Sea $f^*(T) := (T - c_1)\cdots(T - c_n)$. Entonces se tiene que $Res_{n,m}(f, g) = Res_{n,m}(a_0 f^*, g)$, que por la Proposición 2.2.2 *i)*, es igual a $a_0^m Res_{n,m}(f^*, g)$ y aplicando la Proposición 2.4.2 *i)* se concluye el corolario. □

Corolario 2.4.4 *Sean* $f(T) = a_0(T - c_1)\cdots(T - c_n)$ *y* $g(T) = b_0(T - d_1)\cdots(T - d_m) \in R[T]$. *Entonces,*

$$Res_{n,m}(f, g) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(c_i - d_j).$$

Demostración. Sean $f^*(T) = (T-c_1)\cdots(T-c_n)$ y $g^*(T) = (T-d_1)\cdots(T-d_m)$. Aplicando la Proposición 2.2.2 *i)* se tiene que $Res_{n,m}(f, g) = Res_{n,m}(a_0 f^*, b_0 g^*) = a_0^m b_0^n Res_{n,m}(f^*, g^*)$ y usando la Proposición 2.4.2 *i)*, se deduce lo que queríamos pues $X_i = c_i$, para todo $i = 1, \ldots, n$ e $Y_j = d_j$, para cualquier $j = 1, \ldots, m$. □

2.5. Relación de la resultante con los ideales de Fitting

En esta sección relacionaremos la resultante con los ideales de Fitting. Esta relación la usaremos en la siguiente sección.

Proposición 2.5.1 *Sean* R *un anillo conmutativo unitario,* $f = a_0T^n + a_1T^{n-1} + \cdots + a_n, g = b_oT^m + \cdots + b_m \in R[T]$ *y* $a_0 \in R^*$ *o* $b_0 \in R^*$. *Entonces si consideramos el* R*-módulo* $M := R[T]/\langle f, g\rangle$, *se tiene que*

$$Fitt_0(M) = \langle Res_{n,m}(f, g)\rangle .$$

Demostración. Basta con encontrar una presentación de M de la siguiente forma

$$R^{n+m} \xrightarrow{\psi} R^{n+m} \xrightarrow{\pi} M \longrightarrow 0 \qquad \text{(PM)}$$

donde la matriz de ψ sea $Syl_{n,m}(f, g)$. Si definimos ψ como queremos y la aplicación $\pi : R^{n+m} \longrightarrow M$ tal que $\pi(e_i) = T^{n+m-i} + \langle f, g\rangle$, para todo $i \in \{1, \ldots, n + m\}$, donde $\{e_i\}_{i=1}^{n+m}$ es la base canónica de R^{n+m}, es claro que ψ y π son homomorfismos de R-módulos. Veamos que la sucesión (PM) es exacta, para ello, falta por demostrar

i) $Im(\psi) = Ker(\pi)$.

ii) $Im(\pi) = M$ (π es epimorfismo).

Como ψ tiene por matriz asociada a $Syl(f,g)$ se sigue que

$$\begin{cases} \psi(e_1) & = (a_0, a_1, \ldots, a_n, 0, \ldots, 0) & (T^{m-1}f) \\ \psi(e_2) & = (0, a_0, a_1, \ldots, a_n, 0 \ldots, 0) & (T^{m-2}f) \\ & \vdots & \\ \psi(e_m) & = (0, \ldots, 0, \overset{-m-}{a_0}, a_1, \ldots, a_n) & (f) \\ \psi(e_{m+1}) & = (b_0, b_1, \ldots, b_m, 0 \ldots, 0) & (T^{n-1}g) \\ \psi(e_{m+2}) & = (0, b_0, b_1, \ldots, b_m, 0 \ldots, 0) & (T^{n-2}g) \\ & \vdots & \\ \psi(e_{m+n}) & = (0, 0, \ldots, 0, \overset{-n-}{b_0}, b_1, \ldots, b_m) & (g) \end{cases} . \qquad (*_8)$$

Demostremos primero *i*). Tenemos $Im(\psi) \subseteq Ker(\pi)$ pues por ($*_8$), para todo $i = 1, \ldots, n+m$,

$$\pi(\psi(e_i)) \in \{T^j f + \langle f, g\rangle : j = 0, 1, \ldots, m-1\} \cup \{T^j g + \langle f, g\rangle : j = 0, 1, \ldots, n-1\}$$

y $T^j f, T^j g \in \langle f, g\rangle$, para cualquier $j \in \mathbb{Z}^+ \cup \{0\}$. Luego se tiene que,

$$T^j f + \langle f, g\rangle = T^j g + \langle f, g\rangle = 0 + \langle f, g\rangle ,$$

para todo $j \in \mathbb{Z}^+ \cup \{0\}$, y por tanto, $\pi(\psi(e_i)) = 0 + \langle f, g\rangle$, para cualquier $i \in \{1, \ldots, n+m\}$. Luego $\psi(e_i) \in Ker(\pi)$, para todo $i \in \{1, \ldots, n+m\}$ y por tanto, $Im(\psi) \subseteq Ker(\pi)$. Ahora, para demostrar el otro contenido, sea $(r_1, r_2, \ldots, r_{n+m}) \in Ker(\pi)$. Se tiene que $\pi(r_1, \ldots, r_{n+m}) = 0 + \langle f, g\rangle$, es decir, $\sum_{i=1}^{n+m} r_i T^{n+m-i} + \langle f, g\rangle = 0 + \langle f, g\rangle$ entonces $\sum_{i=1}^{n+m} r_i T^{n+m-i} \in \langle f, g\rangle$ y por lo tanto, existen $h, k \in R[T]$ tales que $\sum_{i=1}^{n+m} r_i T^{n+m-i} = hf + kg$. Como $h, k \in R[T]$ son de la forma $h = \sum_{i=0}^{N_1} h_i T^i$, $k = \sum_{i=0}^{N_2} k_i T^i$, para ciertos $N_1, N_2 \geq 0$, $\{h_i\}_{i=0}^{N_1}, \{k_i\}_{i=0}^{N_2} \subseteq R$. No sabemos el grado de h ni de k, pero podemos suponer que N_1 y N_2 son mayores o iguales que $m-1$ y $n-1$ respectivamente (en caso de que no lo sean, habrían h_i o k_i nulos). Pero teníamos que

$$\begin{aligned} \sum_{i=1}^{n+m} r_i T^{n+m-i} &= hf + kg \\ &= h_{m-1}T^{m-1}f + \cdots + h_0 f + k_{n-1}T^{n-1}g + \cdots + k_0 g. \end{aligned} \qquad (2.1)$$

Como $deg\left(\sum_{i=1}^{n+m} r_i T^{n+m-i}\right) \leq n+m-1$, $deg(f) = n$ y $deg(g) = m$, en (2.1) no aparecen h_{m+s} ni k_{n+s}, $s \geq 0$. Ahora, aplicando

$$p\colon \begin{array}{l} R[T]^{(n+m)}_{n+m-1} \longrightarrow R^{n+m} \\ \displaystyle\sum_{i=0} s_i T^i \longmapsto (s_{n+m-1}, s_{n+m-2}, \ldots, s_1, s_0) \end{array}$$

a (2.1) se sigue que

$$\begin{aligned}(r_1, \ldots, r_{n+m}) = {} & (h_{m-1}a_0, \ldots, h_{m-1}a_n, 0, \ldots, 0) \\ & + (h_m \cdot 0, h_{m-2}a_0, \ldots, h_{m-2}a_n, 0, \ldots, 0) \\ & + \cdots + (h_0 \cdot 0, \ldots, h_0 \cdot 0, h_0a_0, h_0a_1, \ldots, h_0a_n) \\ & + (k_{n-1}b_0, k_{n-1}b_1, \ldots, k_{n-1}b_m, 0, \ldots, 0) \\ & + \cdots + (0, \ldots, 0, k_0b_0, k_0b_1, \ldots, k_0b_m).\end{aligned}$$

Además, por ($*_8$) y como ψ es homomorfismo se tiene que

$$\begin{aligned}(r_1, \ldots, r_{n+m}) &= h_{m-1}\psi(e_1) + \cdots + h_0\psi(e_m) + k_{n-1}\psi(e_{m+1}) + \cdots + k_0\psi(e_{m+n}) \\ &= \psi(h_{m-1}e_1 + h_{m-2}e_2 + \cdots + h_0e_m + k_{n-1}e_{m+1} + \cdots + k_0e_{m+n}).\end{aligned}$$

Por tanto, existe $r' := h_{m-1}e_1 + \cdots + h_0e_m + k_{n-1}e_{m+1} + \cdots + k_0e_{m+n} \in R^{n+m}$ tal que $\psi(r') = (r_1, \ldots, r_{n+m})$. Luego, $(r_1, \ldots, r_{n+m}) \in Im(\psi)$ y para todo $(r_1, \ldots, r_{n+m}) \in Ker(\pi)$, $r \in Im(\psi)$. Por tanto, $Ker(\pi) \subseteq Im(\psi)$ y queda así de ambos contenidos probado $i)$.

Demostremos ahora $ii)$. Que $Im(\pi) \subseteq M$ es consecuencia de la buena definición de π. Para el otro contenido, sea $r_0 + r_1T + \cdots + r_NT^N + \langle f, g\rangle \in M$. Podemos suponer que $N \leq m + n - 1$ pues de no ser así, como en f o g su coeficiente de mayor grado es una unidad ($a_0 \in R^*$ o $b_0 \in R^*$) se pueden encontrar polinomios h, h' o g, g' con $deg(h') < n$ ($deg(h') \leq n-1$) o $deg(k') < m$ ($deg(k') \leq m-1$) tales que $r_0+\cdots+r_NT^N = hf+h'$ o $r_0+\cdots+r_NT^N = kg+k'$, lo que equivale a que $r_0+\cdots+r_NT^N+\langle f, g\rangle = h'+\langle f, g\rangle$ o $r_0+\cdots+r_NT^N+\langle f, g\rangle = k' + \langle f, g\rangle$. Hecha esta aclaración, se tiene que

$$\pi(0, \ldots, 0, r_N, r_{N-1}, \ldots, r_1, r_0) = r_0 + \cdots + r_NT^N + \langle f, g\rangle\,.$$

Ahora, se sigue que para todo $r(T) + \langle f, g\rangle \in M$, existe $r' \in R^{n+m}$ tal que $\pi(r') = r(T) + \langle f, g\rangle$, y por tanto, $M \subseteq Im(\pi)$. Luego se tiene $ii)$ y que (PM) es una presentación de M como queríamos demostrar. □

Corolario 2.5.2 *En las hipótesis de la Proposición 2.5.1, $Fitt_0(M)$ es un ideal principal.*

Proposición 2.5.3 *Sean R un anillo conmutativo unitario, $f = a_0T^n + \cdots + a_n$, $g = b_0T^m + \cdots + b_m$ con $a_0 \in R^*$, $m \geq n$, entonces si $M := R[T]/\langle f, g\rangle$ existe*

$$R^n \xrightarrow{G} R^n \xrightarrow{\pi} M \longrightarrow 0$$

presentación de M.

Demostración. Si $\{e_i\}_{i=1}^n$ es la base canónica de R^n entonces definimos el homomorfismo $\pi : R^n \longrightarrow M$ con $\pi(e_i) = T^{n-i} + \langle f, g\rangle$, para todo $i \in \{1, \ldots, n\}$ y para definir G, inicialmente, dividimos g entre f (lo podemos hacer pues $a_0 \in R^*$ y $m \geq n$) y nos quedamos con el resto (estaríamos buscando un representante de menor grado de la clase $g + \langle f\rangle$), ese resto es un polinomio de la forma

$$r_1(T) = r_{11}T^{n-1} + r_{12}T^{n-2} + \cdots + r_{1n} \in R[T]$$

con $\{r_{1j}\}_{j=1}^n \subseteq R$. Tomamos como la primera fila de nuestra matriz $\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n}\end{pmatrix}$. Ahora, dividimos Tg o Tr_1 entre f y nos quedamos nuevamente con el resto (estaríamos buscando un representante de menor grado de la clase $Tg + \langle f\rangle$ $= Tr_1 + \langle f\rangle$). Ese resto es un polinomio de la forma

$$r_2(T) = r_{21}T^{n-1} + r_{22}T^{n-2} + \cdots + r_{2n} \in R[T]$$

con $\{r_{2j}\}_{j=1}^n \subseteq R$. Consideramos como segunda fila de nuestra matriz $\begin{pmatrix} r_{21} & r_{22} & \cdots & r_{2n}\end{pmatrix}$. Así sucesivamente repetimos el proceso hasta hallar $r_n(T) = r_{n1}T^{n-1} + r_{n2}T^{n-2}$ $+ \cdots + r_{nn} \in R[T]$ y quedando la matriz asociada a G de la siguiente forma:

$$M_G = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix}.$$

Ahora, veamos que la sucesión $R^n \xrightarrow{G} R^n \xrightarrow{\pi} M \longrightarrow 0$ es exacta y por tanto, una presentación de M. Tenemos que probar dos cosas:
i) $Im(G) = Ker(\pi)$.
ii) $Im(\pi) = M$ (π es epimorfismo).
Probemos primero *i*), sea $i \in \{1, \ldots, n\}$, tenemos que $G(e_i) = (r_{i1}, \ldots, r_{in})$ luego, $\pi(G(e_i)) = \pi(r_{i1}, \ldots, r_{in}) = r_{i1}T^{n-1} + r_{i2}T^{n-2} + \cdots + r_{in} + \langle f, g\rangle$. Pero por construcción, $r_{i1}T^{n-1} + r_{i2}T^{n-2} + \cdots + r_{in} = hf + (T^{i-1}g)$ para cierto $h \in R[T]$, luego, $r_{i1}T^{n-1} + r_{i2}T^{n-2} + \cdots + r_{in} \in \langle f, g\rangle$ y por tanto, se sigue que

$$r_{i1}T^{n-1} + r_{i2}T^{n-2} + \cdots + r_{in} + \langle f, g\rangle = 0 + \langle f, g\rangle.$$

Luego, $\pi(G(e_i)) = 0 + \langle f, g\rangle$ y $G(e_i) \in Ker(\pi)$. Además, como $G(e_i) \in Ker(\pi)$ para todo $i \in \{1, \ldots, n\}$, se deduce que $Im(G) \subseteq Ker(\pi)$. Ahora para el otro contenido, sea $(r_1' \ldots, r_n') \in Ker(\pi)$, luego, $\pi(r_1', \ldots, r_n') = 0 + \langle f, g\rangle$ y por tanto, $r_1'T^{n-1} + \cdots + r_n' \in \langle f, g\rangle$, es decir, existen $\alpha, \beta \in R[T]$ tales que $r_1'T^{n-1} + \cdots + r_n'$ $= \alpha f + \beta g$. Podemos suponer que $deg(\beta) \leq n - 1$, porque si $deg(\beta) > n - 1$, $deg(\beta) \geq n$, entonces, podemos encontrar $q_\beta, r_\beta \in R[T]$ con $deg(r_\beta) < n$ tales que $\beta = q_\beta f + r_\beta$, luego,

$$\alpha f + \beta g = \alpha f + (q_\beta f + r_\beta)g = (\alpha + q_\beta g)f + r_\beta g.$$

Podemos poner que $\beta = \beta_0 + \beta_1 T + \cdots + \beta_{n-1}T^{n-1}$ con $\beta_0, \beta_1, \ldots, \beta_{n-1} \in R$. Luego,

$$\alpha f + \beta g = \alpha f + (\beta_0 + \beta_1 T + \cdots + \beta_{n-1}T^{n-1})g = \alpha f + \beta_0(g) + \beta_1(Tg) + \cdots + \beta_{n-1}(T^{n-1}g).$$

Pero por construcción, tenemos que $T^{i-1}g = q_i f + r_i$, para cualquier i en $\{1, \ldots, n\}$ para ciertos $q_1, q_2, \ldots, q_{n-1} \in R[T]$. Luego

$$\begin{aligned} \alpha f + \beta g &= \alpha f + \beta_0(q_1 f + r_1) + \cdots + \beta_{n-1}(q_n f + r_n) \\ &= (\alpha + \beta_0 q_1 + \beta_1 q_2 + \cdots + \beta_{n-1} q_n) f + \beta_0 r_1 + \beta_1 r_2 + \cdots + \beta_{n-1} r_n. \end{aligned}$$

Ahora, como $\alpha f + \beta g = r_1' T^{n-1} + \cdots + r_n'$ tiene grado menor o igual que $n-1$, el coeficiente de mayor grado a_0 de f es una unidad, $deg(f) = n$ y $deg(\beta_0 r_1 + \ldots + \beta_{n-1} r_n) \leq n-1$ pues $deg(r_i) \leq n-1$, para todo $i \in \{1, \ldots, n\}$. Se sigue que $\alpha + \beta_0 q_1 + \beta_1 q_2 + \cdots + \beta_{n-1} q_n = 0$ y por tanto,

$$r_1' T^{n-1} + \cdots + r'n = \beta_0 r_1 + \beta_1 r_2 + \cdots + \beta_{n-1} r_n.$$

De este modo, si definimos $p : R[T]^{(n)} \longrightarrow R^n$ como $p(s_1 T^{n-1} + \ldots + s_n) = (s_1, \ldots, s_n)$ se tiene que p es un homomorfismo de anillos. Además se sigue que $p(r_1' T^{n-1} + \cdots + r_n') = p(\beta_0 r_1 + \cdots + \beta_{n-1} r_n)$ y por tanto, $(r'1, \ldots, r_n')$ $= \beta_0 p(r_1) + \cdots + \beta_{n-1} p(r_n)$. Pero por construcción, se tiene que $p(r_i) = \psi(e_i)$ para todo $i \in \{1, \ldots, n\}$. Luego,

$$(r_1', \ldots, r_n') = \beta_0 \psi(e_1) + \cdots + \beta_{n-1}\psi(e_n) = \psi(\beta_0 e_1 + \beta_1 e_2 + \cdots + \beta_{n-1} e_n).$$

Por tanto, $(r_1', \ldots, r_n') \in Im(\psi)$ y $Ker(\pi) \subseteq Im(\psi)$. Así de los dos contenidos anteriores queda probado i).

Demostremos ahora ii). Primero, $Im(\pi) \subseteq M$ es consecuencia de la buena definición de π. Por último, el otro contenido es parecido a la última parte de la prueba de la Proposición 2.5.1. Por el mismo razonamiento que en ella, todos los elementos de M se pueden poner como $a_1 T^{n-1} + a_2 T^{n-2} + \cdots + a_n + \langle f, g \rangle$. Luego, $\pi(a_1, a_2, \ldots, a_n) = a_1 T^{n-1} + \cdots + a_n + \langle f, g \rangle$ y por tanto, $M \subseteq Im(\pi)$. Queda así visto ii) y demostrado que $R^n \xrightarrow{G} R^n \xrightarrow{\pi} M \longrightarrow 0$ es una presentación de M como queríamos. □

2.6. Aplicaciones

Finalizamos este capítulo con algunas aplicaciones de lo estudiado hasta ahora.

2.6.1. Cálculo de la ecuación implícita de una curva parametrizada por polinomios

Sean R un cuerpo y la curva parametrizada $\mathscr{C} \equiv \begin{cases} x(\lambda) = a_o\lambda^n + \cdots + a_n \\ y(\lambda) = b_0\lambda^m + \cdots + b_m \end{cases}$ con $a_0\lambda^n + \cdots + a_n, b_0\lambda^m + \cdots + b_m \in R[\lambda]$. Podemos considerar los polinomios $f := a_0\lambda^n + a_1\lambda^{n-1} + \cdots + (a_n - x), g := b_0\lambda^m + \cdots + (b_m - y) \in R[x,y][\lambda]$. Por la Proposición 2.2.4, es claro que una ecuación de $\mathscr{C}$ es $Res_{n,m}(f,g) = 0$.

Ejemplo 2.6.1.1 *Sean* $R = \mathbb{R}$ *y*

$$\mathscr{C} \equiv \begin{cases} x(\lambda) = \lambda^2 - 3\lambda + 5 \\ y(\lambda) = \lambda - 1, \end{cases}$$

entonces $f := \lambda^2 - 3\lambda + (5 - x)$ *y* $g := \lambda + (-1 - y)$. *Tenemos*

$$Syl_{2,1}(f,g) = \begin{pmatrix} 1 & -3 & 5-x \\ 1 & -1-y & 0 \\ 0 & 1 & -1-y \end{pmatrix} \text{ y } Res_{2,1}(f,g) = \begin{vmatrix} 1 & -3 & 5-x \\ 1 & -1-y & 0 \\ 0 & 1 & -1-y \end{vmatrix}$$

$$= \begin{vmatrix} -1-y & 0 \\ 1 & -1-y \end{vmatrix} - \begin{vmatrix} -3 & 5-x \\ 1 & -1-y \end{vmatrix} = (-1-y)^2 - (-3(-1-y) - 5 + x)$$
$$= (-1-y)[-1-y+3] + 5 - x = (-1-y)(2-y) + 5 - x = -2 + y + y^2$$
$$-2y + 5 - x = y^2 - y + 3 - x.$$

Luego, la ecuación implícita de $\mathscr{C}$ *es* $y^2 - y + 3 - x = 0$. *Observamos en este ejemplo que* $y(\lambda)$ *tiene grado* 1 *y la ecuación obtenida coincide con despejar* λ *de* $y(\lambda)$ y *luego sustituirla en la expresión de* x.

Ejemplo 2.6.1.2 *Sean* $R = \mathbb{R}$ *y*

$$\mathscr{C} \equiv \begin{cases} x(\lambda) = \lambda^5 - 3\lambda^4 + 2\lambda^3 + \lambda - 3 \\ y(\lambda) = \lambda^3 + \lambda^2 - 4\lambda + 1. \end{cases}$$

Entonces $f := \lambda^5 - 3\lambda^4 + 2\lambda^3 + \lambda + (-3 - x), g := \lambda^3 + \lambda^2 - 4\lambda + (1 - y)$, *así,*

$$Syl_{5,3}(f,g) = \begin{pmatrix} 1 & -3 & 2 & 0 & 1 & -3-x & 0 & 0 \\ 0 & 1 & -3 & 2 & 0 & 1 & -3-x & 0 \\ 0 & 0 & 1 & -3 & 2 & 0 & 1 & -3-x \\ 1 & 1 & -4 & 1-y & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -4 & 1-y & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & -4 & 1-y & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & -4 & 1-y & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -4 & 1-y \end{pmatrix}.$$

Podemos calcular el determinante de una matriz de orden 8, *pero tenemos una alternativa usando la Proposición 2.5.1: si* $M = R[\lambda]/\langle f, g\rangle$, *entonces*

$Fitt_0(M) = \langle Res_{5,3}(f,g)\rangle$ (aquí, $R = \mathbb{R}[x,y]$). Vamos a calcular $Fitt_0(M)$, y para ello, lo que podemos hacer es buscar la matriz de presentación (de G) de la Proposición 2.5.3 ($m \leftrightarrow n$ en este caso). Para ello, primero tenemos que hacer tres divisiones.

$$\begin{array}{llll|l} \lambda^5 & -3\lambda^4 & +2\lambda^3 & +0\lambda^2 \quad +\lambda \quad +(-3-x) & \lambda^3+\lambda^2-4\lambda+(1-y) \\ \hline -4\lambda^4 & +6\lambda^3 & +(y-1)\lambda^2 & +\lambda & \lambda^2-4\lambda+10 \\ & 10\lambda^3 & +(y-17)\lambda^2 & +(5-4y)\lambda \quad +(-3-x) & \\ & & (y-27)\lambda^2 & +(45-4y)\lambda \quad +(10y-13-x) & \end{array}$$

luego, $r_1(\lambda) = (y-27)\lambda^2 + (45-4y)\lambda + (10y-13-x)$,

$$\begin{array}{llll|l} (y-27)\lambda^3 & +(45-4y)\lambda^2 & +(10y-13-x)\lambda & +0 & \lambda^3+\lambda^2-4\lambda+(1-y) \\ \hline (-5y+72)\lambda^2 & +(14y-121-x)\lambda & +(y^2-28y+27) & & (y-27) \end{array}$$

así, $r_2(\lambda) = (-5y+72)\lambda^2 + (14y-121-x)\lambda + (y^2-28y+27)$,

$$\begin{array}{llll|l} (-5y+72)\lambda^3 & +(14y-121-x)\lambda^2 & +(y^2-28y+27)\lambda & +0 & \lambda^3+\lambda^2-4\lambda+(1-y) \\ \hline (19y-193-x)\lambda^2 & +(y^2-48y+315)\lambda & +(-5y^2+77y-72) & & (-5y+72) \end{array}$$

y $r_3(\lambda) = (19y-193-x)\lambda^2 + (y^2-48y+315)\lambda + (-5y^2+77y-72)$. Por tanto, la matriz asociada a G es

$$M_G = \begin{pmatrix} y-27 & 45-4y & 10y-13-x \\ -5y+72 & 14y-x-121 & y^2-28y+27 \\ 19y-193-x & y^2-48y+315 & -5y^2+77y-72 \end{pmatrix}$$

y operando, se tiene que $det(M_G) = x^3 - 43x^2y + 327x^2 + 14xy^3 - 85xy^2 - 20xy + 1596x - y^5 + 7y^4 + 10y^3 - 178y^2 + 203y + 1945$. Luego, como $Fitt_0(M) = \langle det(M_G)\rangle = \langle Res_{5,3}(f,g)\rangle$, la ecuación de $\mathscr{C}$ es $det(M_G) = 0$.

2.6.2. Cálculo de la ecuación implícita de una curva racional

Sean R un cuerpo y $\mathscr{C} \equiv \begin{cases} x(\lambda) = \frac{p_1(\lambda)}{q_1(\lambda)} \\ y(\lambda) = \frac{p_2(\lambda)}{q_2(\lambda)} \end{cases}$ una curva racional con $p_1(\lambda), q_1(\lambda), p_2(\lambda), q_2(\lambda) \in R[\lambda]$. Definimos los polinomios $f := p_1 - q_1 x \in R[x]^{(n)}[\lambda] \subseteq R[x,y][\lambda]$ para cierto $n \in \mathbb{N}$ y $g := p_2 - q_2 y \in R[y]^{(m)}[\lambda] \subseteq R[x,y][\lambda]$ para cierto $m \in \mathbb{N}$. Entonces nuevamente, por la Proposición 2.2.4, una ecuación implícita de $\mathscr{C}$ es $Res_{n,m}(f,g) = 0$. Además, como por la Propiedad 2.2.2 i),

$$Res_{n,m}(f,g) = s_1 Res_{n,m}(-f,-g) = s_2 Res_{n,m}(-f,g) = s_3 Res_{n,m}(-f,-g)$$

para ciertos $s_1, s_2, s_3 \in \{1,-1\}$, podemos tomar indistintamente f y g o $-f$ y $-g$, o f y $-g$ o $-f$ y g.

Ejemplo 2.6.2.1 *Tomamos $R = \mathbb{R}$.*

a) *Sea* $\mathscr{C} \equiv \begin{cases} x(\lambda) = \frac{\lambda^2}{1+\lambda+\lambda^2} \\ y(\lambda) = \frac{\lambda^2}{1+2\lambda^2+\lambda^4} \end{cases}$

Tenemos $f := (1-x)\lambda^2 - x\lambda - x$ *y* $g := -y\lambda^4 + (1-2y)\lambda^2 - y$. *No podemos usar la Proposición 2.5.3 pues* $(1-x) \notin (\mathbb{R}[x,y])^*$. *Para hallar la ecuación implícita de* $\mathscr{C}$ *calculamos simplemente* $Res_{2,4}(f,g)$. *Se tiene que*

$$Syl_{2,4}(f,g) = \begin{pmatrix} 1-x & -x & -x & 0 & 0 & 0 \\ 0 & 1-x & -x & -x & 0 & 0 \\ 0 & 0 & 1-x & -x & -x & 0 \\ 0 & 0 & 0 & 1-x & -x & -x \\ -y & 0 & 1-2y & 0 & -y & 0 \\ 0 & -y & 0 & 1-2y & 0 & -y \end{pmatrix} y$$

$Res_{2,4}(f,g) = det(Syl_{2,4}(f,g)) = x^4y^2 - 2x^4y + x^4 + 2x^3y - 2x^3 + 2x^2y^2 + x^2y + x^2 - 2xy + y^2$, *y así, una ecuación implícita de* $\mathscr{C}$ *es* $Res_{2,4}(f,g) = 0$.

b) *Sea* $\mathscr{C} \equiv \begin{cases} x(\lambda) = \frac{\lambda^2}{\lambda-1} \\ y(\lambda) = \frac{\lambda^2}{1+2\lambda^2+\lambda^4} \end{cases}$

Tenemos $f := -\lambda^2 + x\lambda - x$ *y* $g := -y\lambda^4 + (1-2y)\lambda^2 - y$. *Aquí, como* $deg(\lambda - 1) = 1 < 2 = deg(\lambda^2)$, $a_0 = -1 \in (\mathbb{R}[x,y])^*$, *podemos usar la Proposición 2.5.3 para no tener que calcular un determinante de orden* 6*:*

$$\begin{array}{llll|l} -y\lambda^4 & +0\lambda^3 & (1-2y)\lambda^2 & +0\lambda & -y & -\lambda^2 + x\lambda - x \\ & -xy\lambda^3 & +(1-2y+xy)\lambda^2 & +0\lambda & -y & y\lambda^2 + xy\lambda + (-1+2y-xy+x^2y) \\ & & (1-2y+xy-x^2y)\lambda^2 & +x^2y\lambda & -y & \\ & & & (-x^3y+2x^2y-2xy+x)\lambda & +(x^3y-x^2y+2xy-x-y) & \end{array}$$

$r_1(\lambda) = (-x^3y + 2x^2y - 2xy + x)\lambda + (x^3y - x^2y + 2xy - x - y)$

$$\begin{array}{llll|l} (-x^3y+2x^2y-2xy+x)\lambda^2 & +(x^3y-x^2y+2xy-x-y)\lambda & +0 & & -\lambda^2 + x\lambda - x \\ & (-x^4y+3x^3y-3x^2y+x^2+2xy-x-y)\lambda & +(x^4y-2x^3y+2x^2y-x^2) & (x^3y-2x^2y+2xy-x) & \end{array}$$

$y\, r_2(\lambda) = (-x^4y + 3x^3y - 3x^2y + x^2 + 2xy - x - y)\lambda + (x^4y - 2x^3y + 2x^2y - x^2)$.
Luego la matriz asociada a G *es:*

$$M_G = \begin{pmatrix} -x^3y + 2x^2y - 2xy + x & x^3y - x^2y + 2xy - x - y \\ -x^4y + 3x^3y - 3x^2y + x^2 + 2xy - x - y & x^4y - 2x^3y + 2x^2y - x^2 \end{pmatrix},$$

$det(M_G) = -x^2 - 4x^4y^2 + 8x^3y^2 - 8x^2y^2 + 4xy^2 - y^2 + x^4y - 2x^3y + 5x^2y - 2xy$, *y la ecuación implícita de* $\mathscr{C}$ *es* $det(M_G) = 0$.

2.6.3. Resolver sistemas de dos ecuaciones polinómicas

Sean K un cuerpo y $f := p(x,y), g := q(x,y) \in K[x,y]$, entonces para resolver el sistema de ecuaciones $\begin{cases} f = 0 \\ g = 0 \end{cases}$ por la Proposición 2.2.4, calculamos

$Res_{n,m}(f,g)$ como polinomio en y (aquí, $deg_y(f) = n$ y $deg_y(g) = m$) o como polinomio en x (aquí, $deg_x(f) = n$ y $deg_x(g) = m$). Con la primera opción, nos queda un polinomio en x y con la segunda un polinomio en y. Luego ese polinomio tendrá sus raíces en $\overline{K}$, donde $\overline{K}$ denota la clausura algebraica de K, pues nos quedamos con raíces de ese polinomio que estén en K, y luego sustituímos en f y g esos valores de x o y dependiendo de qué opción hayamos elegido y nos quedarán dos polinomios en la otra variable y los pares formados por las correspondientes raíces de $Res_{n,m}(f,g)$ y las raíces comunes de estos dos polinomios mencionados antes son las soluciones del sistema.

Ejemplo 2.6.3.1 *Consideramos en* $\mathbb{R}^2$ *el sistema* $\begin{cases} x^2+y^3-1=0 \\ x^2+y^2-1=0 \end{cases}$, *así,* $f := x^2+y^3-1$ y $g := x^2+y^2-1$, *veámoslos como polinomios en* x *por ejemplo. Tenemos que* $\langle f,g\rangle = \langle f, f-g\rangle$. *Entonces* $\langle f,g\rangle = \langle x^2+y^3-1, y^3-y^2\rangle$. *Como vimos en la Proposición 2.5.1 la relación que hay entre la resultante y* $Fitt_0(M)$ *con* $M = \mathbb{R}[y][x]/\langle f,g\rangle$ *y* $\langle f,g\rangle = \langle x^2+y^3-1, y^3-y^2\rangle$, *es claro que para resolver el sistema es suficiente con calcular primero*

$$Res_{2,0}(f, f-g) = \begin{vmatrix} y^3-y^2 & 0 \\ 0 & y^3-y^2 \end{vmatrix} = (y^3-y^2)^2 = [y^2(y-1)]^2.$$

Además $y^4(y-1)^2 = 0$ *si y sólo si,* $y \in \{0,1\}$. *Ahora, aquí no podemos sustituir los valores de* y *en* $f-g$ *porque al no aparecer* x, *no determinará ningún valor para esta. Sustituyendo en* f, *se tiene que*

- *Si* $y = 0$; $f(x,y) = f(x,0) = x^2-1 = 0$ *si y sólo si,* $x \in \{1,-1\}$. *De aquí, obtenemos las soluciones* $(1,0),(-1,0)$.
- *Si* $y = 1$; $f(x,y) = f(x,1) = x^2 = 0$ *si y sólo si,* $x = 0$. *Luego, obtenemos la solución* $(0,1)$.

Por tanto, el conjunto de soluciones del sistema es $\{(1,0),(-1,0),(0,1)\}$.

Ejemplo 2.6.3.2 *Sean* $f(x,y) = y^2+(a_{11}x^2+a_{12}x+a_{13})y+(a_{21}x^2+a_{22}x+a_{23})$ *y* $g(x,y) = y^2+(b_{11}x^2+b_{12}x+b_{13})y+(b_{21}x^2+b_{22}x+b_{23}) \in \mathbb{R}[x,y]$ *sin factores en común, entonces el sistema*

$$\begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases} \tag{2.6.3.2}$$

admite un sistema de ecuaciones equivalente de la forma

$$\begin{cases} p_1(x)y + p_2(x) = 0 \\ q_1(x)y + q_2(x) = 0. \end{cases}$$

En efecto, usando la Proposición 2.5.1 y la Proposición 2.5.3 podemos calcular un múltiplo de $Res_{2,2}(f,g)$, *considerando* f *y* g *polinomios en* $\mathbb{R}[x][y]$ *como sigue,*

$$\begin{array}{l|l} f & g \\ \hline [(a_{11}-b_{11})x^2+(a_{12}-b_{12})x+(a_{13}-b_{13})]y+[(a_{21}-b_{21})x^2+(a_{22}-b_{22})x+(a_{23}-b_{23})] & 1 \end{array}$$

$r_1(y) = [(a_{11}-b_{11})x^2+(a_{12}-b_{12})x+(a_{13}-b_{13})]y+[(a_{21}-b_{21})x^2+(a_{22}-b_{22})x+(a_{23}-b_{23})]$. *Ahora, dividimos* $yr_1(y)$ *entre* g, *el cociente es* $[(a_{11}-b_{11})x^2+(a_{12}-b_{12})x+(a_{13}-b_{13})]$, *y el coeficiente de* y *en el resto* $r_2(y)$ *es*

$$\begin{aligned} p_1(x) &:= [(a_{21}-b_{21})x^2+(a_{22}-b_{22})x+(a_{23}-b_{23})] \\ &- [(a_{11}-b_{11})x^2+(a_{12}-b_{12})x+(a_{13}-b_{13})](b_{11}x^2+b_{12}x+b_{13}) \\ &= (b_{11}^2-a_{11}b_{11})x^4+(-a_{11}b_{12}+2b_{11}b_{12}-b_{11}a_{12})x^3 \\ &+ (a_{21}-b_{21}+b_{12}^2-a_{11}b_{13}+2b_{11}b_{13}-a_{12}b_{12}-b_{11}a_{13})x^2 \\ &+ (a_{22}-b_{22}-a_{12}b_{13}+2b_{12}b_{13}-b_{12}a_{13})x+(a_{23}-b_{23}-a_{13}b_{13}+b_{13}^2). \end{aligned}$$

Además, el término independiente de $r_2(y)$ *es*

$$\begin{aligned} p_2(x) &:= 0-[(a_{11}-b_{11})x^2+(a_{12}-b_{12})x+(a_{13}-b_{13})](b_{21}x^2+b_{22}x+b_{23}) \\ &= (-a_{11}b_{21}+b_{11}b_{21})x^4+(-a_{11}b_{22}+b_{11}b_{22}-a_{12}b_{21}+b_{12}b_{21})x^3 \\ &+ (-a_{11}b_{23}+b_{11}b_{23}-a_{12}b_{22}+b_{12}b_{22}-a_{13}b_{21}+b_{13}b_{21})x^2 \\ &+ (-a_{12}b_{23}+b_{12}b_{23}-a_{13}b_{22}+b_{13}b_{22})x+(-a_{13}b_{23}+b_{13}b_{23}). \end{aligned}$$

Si llamamos $q_i(x) := (a_{i1}-b_{i1})x^2+(a_{i2}-b_{i2})x+(a_{i3}-b_{i3})$ *con* $i \in \{1,2\}$, *entonces tenemos que* $r_1 = q_1y+q_2$ y $r_2 = p_1y+p_2$. *Un múltiplo de* $Res_{2,2}(f,g)$ *es* $\begin{vmatrix} q_1 & q_2 \\ p_1 & p_2 \end{vmatrix}$, *pero* $\begin{vmatrix} q_1 & q_2 \\ p_1 & p_2 \end{vmatrix} = Res_{1,1}(r_1,r_2)$. *Luego anular* $Res_{2,2}(f,g)$ *es equivalente a anular* $Res_{1,1}(r_1,r_2)$ *y el sistema* (2.6.3.2) *equivale a* $\begin{cases} r_1=0 \\ r_2=0 \end{cases}$ *que se resuelve hallando las raíces del polinomio* $\begin{vmatrix} q_1 & q_2 \\ p_1 & p_2 \end{vmatrix}(x)$ *y sustituyendo en* r_1 *o en* r_2. *Es claro que si* α *es una raíz de* $\begin{vmatrix} q_1 & q_2 \\ p_1 & p_2 \end{vmatrix}(x)$ *entonces el par* $\left(\alpha, \frac{-q_2(\alpha)}{q_1(\alpha)}\right)$ *es solución de ambos sistemas mientras* α *sea real y no anule a* q_1.

En este enlace https://www.geogebra.org/calculator/dhhnwvfg *se accede a un archivo de GeoGebra que ilustra este ejemplo. (Ver Figura 2.1).*

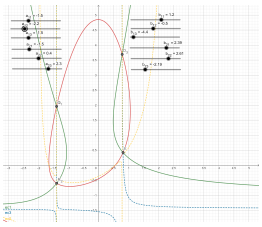


Figura 2.1.

3

El Teorema de Bézout

El objetivo de este capítulo es dar una prueba del Teorema de Bézout usando resultantes. En la mayor parte de lo que sigue nos hemos basado en [6].

3.1. Preliminares

En esta sección mostraremos una serie de definiciones y resultados que nos llevarán a la prueba del Teorema de Bézout.

Lema 3.1.1 *Sean K cuerpo, F y G dos polinomios homogéneos en $K[x,y,z]$ de grados m y n respectivamente, sin componentes en común. Entonces se tiene que*

a) $\mathscr{C}_F$ y $\mathscr{C}_G$ se intersecan en un número finito de puntos.
b) $\mathscr{C}_F$ y $\mathscr{C}_G$ se intersecan en a lo sumo en mn puntos distintos.

Demostración. Sean S un punto de $\mathbb{P}^2_K$ que no está ni en $\mathscr{C}_F$ ni en $\mathscr{C}_G$ y L una recta proyectiva que no pasa por S. Consideramos ahora para cada $Q \in \mathscr{C}_L$ la recta L_Q que pasa por Q y por S. Además, para cada L_Q hay un número finito de puntos $\{P_{j_Q}\}_{j_Q=1}^{k_Q} \subseteq \mathscr{C}_{L_Q}$ de intersección con $\mathscr{C}_F$ y con $\mathscr{C}_G$. Tomamos $\{P_i\}_{i=1}^{k} = \bigcup_{Q\in L} \{P_{j_Q}\}_{j_Q=1}^{k_Q}$.

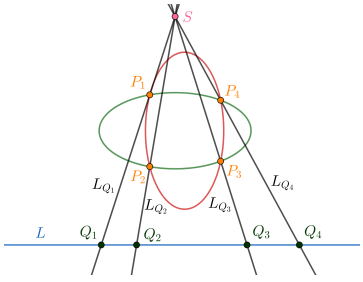


Figura 3.1.

Aplicando [6, Lemma 11.1], podemos suponer que $S = (0 : 0 : 1)$ y L es la recta $z = 0$. Tras un cambio de coordenadas, si fuera necesario, podemos escribir

$$\begin{cases} F = F_0(x,y)z^m + F_1(x,y)z^{m-1} + \cdots + F_{m-1}(x,y)z + F_m(x,y) \\ G = G_0(x,y)z^n + G_1(x,y)z^{n-1} + \cdots + G_{n-1}(x,y)z + G_n(x,y) \end{cases}$$

donde F_i y G_j son polinomios nulos u homogéneos de grado i, j; en particular, F_0 y G_0 son polinomios constantes no nulos puesto que $S \notin \mathscr{C}_F$ y $S \notin \mathscr{C}_G$. Luego un punto $Q_i = (x_i : y_i : 0) \in \mathscr{C}_L$ es la proyección de un punto de intersección $P_i \in \mathscr{C}_F \cap \mathscr{C}_G$ (ver Figura 3.1), si y solo si, existe $z_0 \in K$ tal que $F(x, y, z_0) = G(x, y, z_0) = 0$. O equivalentemente, que F y G como polinomios en z tengan una raíz común. Ahora, por la Proposición 2.2.4 sabemos que lo anterior es equivalente a que la resultante de F y G respecto de z verifica que

$$Res_z(F, G) = 0.$$

También sabemos por la Propiedad 2.3.7 que $Res_z(F, G) = 0$ o $Res_z(F, G)$ es un polinomio homogéneo de grado mn. Pero como F y G no tienen componentes en común, estamos en la segunda opción. De esta manera, los puntos $Q_i = (x_i : y_i : 0) \in \mathscr{C}_L$ se corresponden con los ceros $(x_i : y_i)$ del polinomio homogéneo $Res_z(F, G)$ de grado mn. Luego, el cardinal de $\mathscr{C}_F \cap \mathscr{C}_G$ es finito y concluímos el apartado *a)*. Ahora bien, para probar *b)* hay que tener en cuenta que un $(x_i : y_i) \in \mathbb{P}^1_K$ tal que $Res_z(F, G)(x_i, y_i) = 0$ se corresponde con los puntos $(x : y : z) \in \mathscr{C}_F \cap \mathscr{C}_G$ tales que $(x : y) = (x_i : y_i)$, y estos pueden ser varios puntos (ver Figura 3.2).

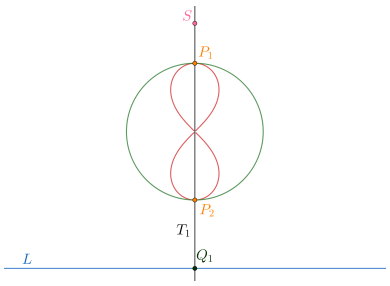


Figura 3.2.

Pero como por *a)* sabemos que $\mathscr{C}_F \cap \mathscr{C}_G$ es un conjunto finito, se tiene que existe un número finito de rectas $\{T_i\}_{i=1}^r$ que unen los puntos de $\mathscr{C}_F \cap \mathscr{C}_G$ en pares (o más). Ahora, elegimos S que no esté en ninguna de estas rectas $\{T_i\}_{i=1}^r$ y procedemos como antes para conseguir una correspondencia biyectiva entre los ceros $Q_i = (x_i : y_i)$ de $Res_z(F, G)$ con los puntos de intersección de F con G. Concluimos la prueba del lema teniendo en cuenta que $Res_z(F, G)$ es un polinomio homogéneo de grado mn, y por tanto tiene a lo sumo mn ceros distintos en $\mathbb{P}^1_K$ que se corresponden a sus factores lineales. □

Lema 3.1.2 *Sean $F, G \in \mathbb{C}[x,y,z]$ homogéneos irreducibles sin factores en común. Entonces $\mathscr{C}_F = \mathscr{C}_G$ si y solo si existe $\lambda \in \mathbb{C}\setminus\{0\}$ tal que $G = \lambda F$.*

Demostración. Primero, supongamos que los conjuntos de ceros F y G coinciden. Sabemos que el conjunto de ceros de cualquier curva en $\mathbb{P}^2_{\mathbb{C}}$ es infinito porque $\mathbb{C}$ es un cuerpo infinito. Luego, por el Lema 3.1.1 se sigue que F y G tienen una componente en común y como por hipótesis F y G son irreducibles, se deduce lo que queremos, es decir, $F = \lambda G$ para cierto $\lambda \in \mathbb{C}\setminus\{0\}$. Por último, si $G = \lambda F$ para cierto $\lambda \in \mathbb{C}\setminus\{0\}$, entonces los conjuntos de ceros de F y G coinciden. □

Definición 3.1.3 *Sean K cuerpo, $\mathscr{C}_F$, $\mathscr{C}_G$ dos curvas en $\mathbb{P}^2_K$ y $P = (x : y : z)$ un punto de $\mathbb{P}^2_K$. Diremos que $\mathscr{C}_F$ y $\mathscr{C}_G$ se intersecan adecuadamente en P si F y G no tienen ninguna componente en común T tal que $P \in \mathscr{C}_T$ y $P \in \mathscr{C}_F \cap \mathscr{C}_G$. Asumiremos que F y G no tienen factores en común. Elegimos coordenadas X, Y, Z tales que $(0 : 0 : 1)$ no está ni en $\mathscr{C}_F$ ni en $\mathscr{C}_G$ ni en ninguna de las rectas que unen los puntos de intersección de ambas curvas. Denotamos por $R(X,Y)$ a la resultante de F y G con respecto a Z ($Res_Z(F(X,Y,Z), G(X,Y,Z))$). Definimos la multiplicidad de intersección $I(P,F,G)$ para $P = (x_0 : y_0 : z_0) \in \mathbb{P}^2_K$ como la multiplicidad de $(x_0 : y_0)$ como raíz de $R(X,Y)$, es decir la multiplicidad de $yoX - x_0Y$ como factor de $R(X,Y)$.*

Esta noción no depende de la elección de coordenadas (X,Y,Z) (ver [6, Lemma 14.10]). En el caso de que G sea una recta, $I(P,F,G)$ coincide con la multiplicidad de $s_0t - t_0s$ en $F(\phi(s,t))$ con ϕ una parametrización de G y $\phi(s_0,t_0) = P$.

En efecto, por [6, Lemma 11.1] podemos suponer que $P = (1 : 0 : 0)$ y que G es la recta $z = 0$. Pongamos que

$$F(x,y,z) = F_d(x,y) + F_{d-1}(x,y)z + \cdots + F_0(x,y)z^d,$$

donde cada F_k es nulo o un polinomio homogéneo de grado k para cada $k \in \{0,1,\ldots,d-1,d\}$. Además, se tiene que por la definición de resultante,

$$R(x,y) = Res_z(F,G) = \begin{vmatrix} F_d & F_{d-1} & \ldots & F_1 & F_0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{vmatrix} = F_d.$$

Luego, $I(P,F,G)$ es la multiplicidad de $(1:0)$ como cero de $F_d(x,y)$. Pero esto coincide con la multiplicidad del punto $(1:0)$ como cero de $F(x,y,0)$ pues

$$F(x,y,0) = F_d(x,y) + F_{d-1}(x,y)\cdot 0 + \cdots + F_0(x,y)\cdot 0^d = F_d(x,y).$$

3.2. Prueba del teorema

Enunciamos y demostramos el Teorema de Bézout.

Teorema 3.2.1 (Bézout) *Sean F y G dos polinomios homogéneos en $\mathbb{C}[x,y,z]$ de grados m y n respectivamente sin factores en común. Entonces*

$$\sum_{P\in\mathscr{C}_F\cap\mathscr{C}_G} I(P,F,G) = mn.$$

Demostración. Como $Res_z(F,G) = R(x,y)$ es un polinomio homogéneo de grado mn por la Propiedad 2.3.7, la suma de las multiplicidades de los ceros de $R(x,y)$ es exactamente mn. Luego, concluimos de la definición de $I(P,F,G)$.

Ejemplo 3.2.2 *Sean $F = x^2+y^2-z^2$ y $G = xy-z^2$ en $\mathbb{C}[x,y,z]$. Entonces*

$$Res_z(F,G) = \begin{vmatrix} -1 & 0 & x^2+y^2 & 0 \\ 0 & -1 & 0 & x^2+y^2 \\ -1 & 0 & xy & 0 \\ 0 & -1 & 0 & xy \end{vmatrix} = x^4+y^4-2xy^3+3x^2y^2-2x^3y$$
$$= y^4\left(\left(\frac{x}{y}\right)^4 + 1 - 2\,\frac{x}{y} + 3\left(\frac{x}{y}\right)^2 - 2\left(\frac{x}{y}\right)^3\right).$$

Si llamamos $t = \frac{x}{y}$ y $\varphi(t) = t^4-2t^3+3t^2-2t+1$, se tiene, haciendo uso de WolframAlpha, que $\varphi(t) = (t^2-t+1)^2 = (t-\alpha)^2(t-\overline{\alpha})^2$ con $\alpha = \frac{1}{2}+\frac{\sqrt{3}}{2}i$. Luego, se deduce que

$$Res_z(F,G) = \left(x-\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)y\right)^2\left(x-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)y\right)^2.$$

Si imponemos que $Res_z(F,G)=0$, tenemos dos opciones:

- *Del primer factor no repetido de $Res_z(F,G)$ se tiene que $x = \left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)y$ y si sustituimos en $G=0$ se sigue que $\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)y^2 - z^2 = 0$ lo que equivale a que $\left(\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)y - z\right)\left(\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)y + z\right) = 0$. De este modo, obtenemos que $P_1 := \left(\frac{1}{2}+\frac{\sqrt{3}}{2}i : 1 : \frac{\sqrt{3}}{2}+\frac{1}{2}i\right)$ y $P_2 := \left(\frac{1}{2}+\frac{\sqrt{3}}{2}i : 1 : -\frac{\sqrt{3}}{2}-\frac{1}{2}i\right)$ pertenecen a $\mathscr{C}_F\cap\mathscr{C}_G$.*
- *De manera análoga con el segundo factor no repetido de $Res_z(F,G)$ se puede comprobar que $P_3 := \left(\frac{1}{2}-\frac{\sqrt{3}}{2}i : 1 : \frac{\sqrt{3}}{2}-\frac{1}{2}i\right)$ y $P_4 := \left(\frac{1}{2}-\frac{\sqrt{3}}{2}i : 1 : -\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)$ pertenecen a $\mathscr{C}_F\cap\mathscr{C}_G$.*

Por tanto, $\mathscr{C}_F\cap\mathscr{C}_G = \{P_i\}_{i=1}^4$ y por el Teorema 3.2.1 se tiene además que $\sum_{P\in\mathscr{C}_F\cap\mathscr{C}_G} I(P,F,G) = 2\cdot 2 = 4$, luego, $I(P_i,F,G) = 1$ para todo $i\in\{1,2,3,4\}$.

Conclusiones

Primero, en el Capítulo 1 en este trabajo hemos estudiado los ideales de Fitting y algunas de sus propiedades. Para llegar a probar el Lema de Fitting y la buena definición de los mismos hemos tenido que demostrar antes varias propiedades. El estudio de qué condiciones hacen falta para poder asegurar que dos módulos finitamente generados con los mismos ideales de Fitting son isomorfos, es una interesante tarea para hacer como continuación de este trabajo.

En el Capítulo 2 hemos estudiado las resultantes con el objetivo final de dar respuesta a problemas como hallar las soluciones de un sistema polinómico o calcular la ecuación implícita de una curva parametrizada y hemos relacionado la resultante con lo probado en el Capítulo 1, lo que simplifica los cálculos.

En el Capítulo 3 dimos una prueba del Teorema de Bézout por medio de la resultante apoyándonos en los resultados obtenidos en el Capítulo 2. Otra demostración de este teorema es la que da Bernard Teissier en [11] usando ideales de Fitting. Completar todos los detalles de dicha prueba podría ser un desarrollo complementario a este trabajo, tomando como punto de partida los dos primeros capítulos de esta memoria. Además para esta prueba, es imprescindible entre otras cosas, haber estudiado antes los anillos locales de $\mathbb{P}^1_{\mathbb{C}}$ en un punto $x \in \mathbb{P}^1_{\mathbb{C}}$, denotado por $\mathcal{O}_{\mathbb{P}^1_{\mathbb{C}},\, x}$ y de $\mathbb{P}^2_{\mathbb{C}}$ en un punto $y \in \mathbb{P}^2_{\mathbb{C}}$, denotado por $\mathcal{O}_{\mathbb{P}^2_{\mathbb{C}},\, y}$. Consideramos que una buena referencia para ellos es [5, Chapter 3 and 4]. Por último, a modo de ayuda decir que la valoración v_x que se considera en [11, page 577 and 578] es

$$\begin{array}{rccc} v_x\colon & \mathbb{C}(\mathbb{P}^1) & \longrightarrow & \mathbb{Z}\diagdown\{0\} \\ & uT^k & \longmapsto & k \end{array}$$

donde $\mathbb{C}(\mathbb{P}^1)$ es el anillo de fracciones de polinomios homogéneos del mismo grado, T es el generador del ideal maximal de $\mathcal{O}_{\mathbb{P}^1_{\mathbb{C}},\, x}$ y T no divide a u.

Bibliografía

[1] A. Altman, S. Kleiman. A Term of Commutative Algebra. *Worldwide Center of Mathematics, LLC.* Versión de 2017, pp. 34-42 disponible en https://www.mi.fu-berlin.de/en/math/groups/arithmetic_geometry/teaching/exercises/Altman_-Kleiman---A-term-of-commutative-algebra-_2017_.pdf.

[2] D. Cox. Galois Theory. John Wiley & Sons. 2012.

[3] D. Eisenbud. The Geometry of Syzygies. A Second Course in Algebraic Geometry and Commutative Algebra. Graduate Texts in Mathematics 229. Springer 2005. pp. 222.

[4] H. Fitting. Die Determinantenideale eines Moduls, Jahresbericht der Deutschen Mathematiker-Vereinigung 1936. pp.195-228. Disponible en https://gdz.sub.uni-goettingen.de/id/PPN37721857X_0046?tify=%7B%22pages%22%3A%5B209%5D%2C%22pan%22%3A%7B%22x%22%3A0.461%2C%22y%22%3A0.811%7D%2C%22view%22%3A%22info%22%2C%22zoom%22%3A0.344%7D

[5] W. Fulton. Algebraic curves. An Introduction to Algebraic Geometry. January 28, 2008. Disponible en https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

[6] C.G. Gibson. Elementary Geometry of Algebraic Curves: an Undergraduate Introduction. *Cambridge University Press, 1998.*

[7] E. Hironaka. Computing Alexander polynomials using monodromy. January 3, 2011. Disponible en https://www.math.fsu.edu/~hironaka/papers/AlexPoly.pdf.

[8] F.A.E. Nuccio. Fitting Ideals. Guwahati, September 22nd-29th, 2010. Disponible en: https://hal.science/hal-00947158.

[9] A. Płoski. Resultants and discriminants. Prepublicación 2016. Accesible en https://gasiull.webs.ull.es/2016-Resultants.pdf.

[10] R.Y. Sharp. Steps in Commutative Algebra. Second Edition. *London Mathematical Society Student* Texts 51. *Cambridge University Press*, 2000.

[11] B. Teissier. The hunting of invariants in the geometry of discriminants. Five lectures at the *Nordic Summer School*, pp. 566-578, 1977. Disponible en: https://webusers.imj-prg.fr/~bernard.teissier/documents/Thehunting.pdf.
[12] The Stacks project. Section 15.8 (07Z6): Fitting ideals. Disponible en: https://stacks.math.columbia.edu/tag/07Z6.

Introduction to the Fitting ideals and the resultants

Fernando León Delgado
Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu01013496888@ull.edu.es

Abstract

Fitting ideals and resultants are very helpful tools in dealing with many problems. For example, to find the solutions of a system of polynomial equations or to calculate the implicit equation of a parametric curve.

1. Fitting ideals

Definition. Let R be a unitary commutative ring and M an $R-$module, then a (free) presentation of M is an exact sequence of the form

$$G \xrightarrow{\phi} F \xrightarrow{\psi} M \longrightarrow 0$$

with G and F free $R-$modules.

Lemma. (Weak version of Schanuel's lemma). Let R be a unitary commutative ring and

$$L \xrightarrow{i} P \xrightarrow{\alpha} M \longrightarrow 0, \quad L' \xrightarrow{i'} P' \xrightarrow{\alpha'} M \longrightarrow 0$$

exact sequences of $R-$modules with P and P' projective. So the following diagram

$$\begin{array}{ccccc} L \oplus P' & \xrightarrow{i\oplus 1_{P'}} & P \oplus P' & \xrightarrow{\alpha+0} & M \longrightarrow 0 \\ \cong\downarrow\gamma & & & & \downarrow 1_M \\ P \oplus L' & \xrightarrow{1_P\oplus i'} & P \oplus P' & \xrightarrow{0+\alpha'} & M \longrightarrow 0 \end{array}$$

is commutative, where γ is an isomorphism.

Lemma. (Fitting Lemma). Let R be a unitary commutative ring, M a R-module, $r \in \mathbb{Z}$ and $R^n \xrightarrow{\alpha} R^m \xrightarrow{\mu} M \longrightarrow 0$, $R^q \xrightarrow{\beta} R^p \xrightarrow{\pi} M \longrightarrow 0$ two presentations of M with A and B matrices of α and β respectively. Then,

$$I_{m-r}(A) = I_{p-r}(B)$$

where $I_r(A)$ denotes the ideal of R generated by the r-minors of A.

Definition. (Fitting ideals). Let R be a unitary commutative ring, M a finitely presented R-module and $r \in \mathbb{Z}$. We take any presentation of M of the form $R^n \xrightarrow{\alpha} R^m \longrightarrow M \longrightarrow 0$, if we denote by A the matrix associated to α (this matrix is known as the matrix of the presentation), we define the r-th Fitting ideal of M by

$$Fitt_r(M) := I_{m-r}(A).$$

2. Resultants

Definition. Let n, m be positive integers. Then for any pair of polynomials

$$f(T) = a_0T^n + \ldots + a_n \text{ and } g(T) = b_0T^m + \ldots + b_m \in R[T]$$

we define the Sylvester's matrix of f and g

$$Syl_{n,m}(f,g) := A(T^{m-1}f, T^{m-2}f, \ldots, f, T^{n-1}g, T^{n-2}g, \ldots, g)$$

and the resultant of f and g,

$$Res_{n,m}(f,g) := det(Syl_{n,m}(f,g)) \in R.$$

Proposition. Let R be a unique factorization domain, $f = a_0T^n + \ldots + a_n \in R[T], a_0 \neq 0, n > 0$ and $g = b_0T^m + \ldots + b_m \in R[T]$. Then, $Res_{n,m}(f,g) = 0$ if, and only if, f and g have at least one common divisor of degree greater than zero.

Proposition. Let R be a unitary commutative ring, $f = a_0T^n + a_1T^{n-1} + \ldots + a_n, g = b_oT^m + \ldots + b_m \in R[T]$ and $a_0 \in R^*$ o $b_0 \in R^*$. Then, if we consider the R-module $M := R[T]/\langle f, g\rangle$, we have that

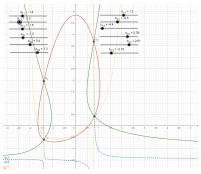
$$Fitt_0(M) = \langle Res_{n,m}(f,g)\rangle .$$

Example. Consider $f(x,y) = y^2 + (a_{11}x^2 + a_{12}x + a_{13})y + (a_{21}x^2 + a_{22}x + a_{23})$ and $g(x,y) = y^2 + (b_{11}x^2 + b_{12}x + b_{13})y + (b_{21}x^2 + b_{22}x + b_{23})$ with no common factors and $a_{ij} \in \mathbb{R}$. The system of equations

$$\begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases}$$

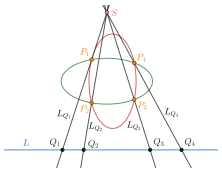
admits an equivalent system of equations of the form

$$\begin{cases} p_1(x)y + p_2(x) = 0 \\ q_1(x)y + q_2(x) = 0. \end{cases}$$



3. Bézout Theorem

Lemma. Let K be a field, F and G be two homogeneous polynomials in $K[x,y,z]$ of degrees m and n respectively, with no components in common. Then $\mathscr{C}_F$ and $\mathscr{C}_G$ intersect at most in mn different points.



Theorem. (Bézout). Let F and G be two homogeneous polynomials in $\mathbb{C}[x,y,z]$ of degrees m and n respectively without common factors. Then

$$\sum_{P \in \mathscr{C}_F \cap \mathscr{C}_G} I(P,F,G) = mn.$$

where $I(P,F,G)$ denotes the intersection number.

Example. Let $F = x^2 + y^2 - z^2$ and $G = xy - z^2$ be two homogeneous polynomials in $\mathbb{C}[x,y,z]$. Then

$$\mathscr{C}_F \cap \mathscr{C}_G = \left\{ \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i : 1 : \frac{\sqrt{3}}{2} + \frac{1}{2}i\right), \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i : 1 : -\frac{\sqrt{3}}{2} - \frac{1}{2}i\right), \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i : 1 : \frac{\sqrt{3}}{2} - \frac{1}{2}i\right), \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i : 1 : -\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) \right\}$$

and by the Bézout Theorem, $I(P,F,G) = 1$ for all $P \in \mathscr{C}_F \cap \mathscr{C}_G$.

References

[1] A. Altman, S. Kleiman. A Term of Commutative Algebra. *Worldwide Center of Mathematics, LLC*. Versión de 2017, pp. 34-42.

[2] A. Płoski. Resultants and discriminants. Prepublicación 2016. Accesible en https://gasiull.webs.ull.es/2016-Resultants.pdf.

[3] C.G. Gibson. Elementary Geometry of Algebraic Curves: an Undergraduate Introduction. Cambridge University Press 1998.