UNIVERSIDAD DEL BÍO-BÍO

FACULTAD DE EDUCACIÓN Y HUMANIDADES

ESCUELA DE PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

RESULTANTE Y APLICACIONES

MEMORIA PARA OPTAR AL TÍTULO DE PROFESOR DE EDUCACIÓN MEDIA EN EDUCACIÓN MATEMÁTICA

AUTOR: PAMELA BELÉN BUSTOS VIVANCO

VICTORIA PAZ FUENTEALBA VÁSQUEZ

PROFESOR GUÍA: EDGARDO ANDRÉS RIQUELME FAÚNDEZ

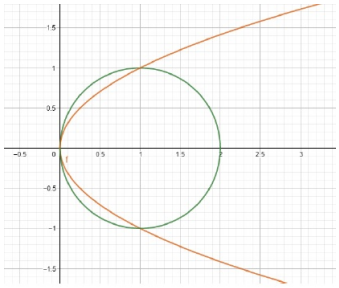
CHILLÁN

Introducción

Conocemos diferentes métodos para la resolución de sistema de dos ecuaciones lineales, ya sea por sustitución, reducción, igualación, entre otros, pero qué sucede cuando estamos en presencia de sistemas más complicados, por ejemplo, con ecuaciones no lineales. Visto desde una perspectiva geométrica, nos podemos preguntar cuáles son los puntos de intersección de dos curvas en el plano, sin la necesidad de su gráfica, como es el siguiente caso

$$\begin{aligned} f &= y^2 + x^2 - 2x \\ g &= y^2 - x \end{aligned}$$

donde podemos notar que f corresponde a una circunferencia y g corresponde a una parábola, como muestra la siguiente imagen:



Lo primero que pensamos cuando estamos frente a una resolución de este tipo de sistemas de ecuaciones es que puede ser un proceso difícil y muy extenso, sin embargo, existe un método que permite resolver este tipo de sistemas de ecuaciones con mayor facilidad, conocido como la resultante de dos polinomios, para el cual se requiere un conocimiento más amplio del álgebra abstracta. Este método consiste en eliminar una o más variables del sistema de ecuaciones polinomiales, reduciendo el problema dado a uno equivalente, pero con menos variables en juego. La versión moderna de este método se asocia a Sylvester, en el año 1853, la cual conoceremos a profundidad en esta memoria, a través

de su definición, utilidad, ejemplos y aplicaciones. Comenzaremos estudiando polinomios y luego veremos cómo la resultante es una generalización de los métodos utilizados en sistemas de ecuaciones lineales.

En cuanto al estudio de polinomios, según el Curriculum de Chile, es en primero medio donde los alumnos se familiarizan con estos, en la unidad de funciones, conociendo primero la función lineal, luego la función afín y, por último, en el curso de segundo medio, la cuadrática. Así también, conocen los productos notables en primero medio y nuevamente en segundo aprenden a factorizar estos. Posteriormente, conocen los sistemas de ecuaciones lineales, donde su solución corresponde a la intersección de dos rectas en un punto, para las cuales existen diversos procedimientos para resolverlos, es aquí donde la resultante es un nuevo método para este tipo de problemas y algunos más difíciles, como es el caso de ecuaciones distintas a las lineales, que geométricamente se pueden interpretar como la intersección de curvas.

Índice general

CAPÍTULO 1

Preliminares

Para el correcto estudio de la resultante, es importante revisar previamente algunas definiciones, como, por ejemplo, anillos, anillos de polinomios, plano proyectivo, entre otros.

1.1 Anillos

En la primera década del siglo XX existían teorías concretas de anillos conmutativos y no conmutativos y sus ideales. Sus raíces fueron principalmente en la teoría algebraica de números, geometría algebraica, y la teoría de los números hipercomplejos.

La primera definición abstracta de un anillo fue dada por Fraenkel, en un artículo de 1914 titulado "On zero divisors and the decomposition of rings". Esta definición pretendía abarcar tanto anillos conmutativos como no conmutativos y dar una teoría abstracta y completa de estos, pero con esto último no hubo éxito, pues era demasiado ambicioso.

Fraenkel, definió un anillo como "un sistema" con dos operaciones abstractas, a las que dio los nombres de adición y multiplicación.

Definición 1. *R es un anillo si tiene dos operaciones binarias, adición y multiplicación, que satisfacen las siguientes condiciones:*

1. $a + b = b + a$ para todo a en R
2. $(a + b) + c = a + (b + c)$ para todo a, b, c en R
3. Existe un elemento neutro para la suma tal que $a + 0 = a$ para todo a en R

4. Para cada elemento a en R existe un elemento inverso $-a$ tal que $a + (-a) = 0$
5. $(ab)c = a(bc)$ para todo a y b en R
6. Para a, b, c en R

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

Si existe un elemento 1 en R tal que $1 \neq 0$ y $1a = a1 = a$ para cada elemento a en R, decimos que tal anillo R es un ***anillo con unitario***. Un anillo R para el cual $ab = ba$ para todo a y b en R se llama ***anillo conmutativo***. Un anillo conmutativo R con identidad se llama ***dominio entero***, si para a, b en R tales que $ab = 0$, se cumple que $a = 0$ o $b = 0$.
Un anillo R, con identidad, en el que todo elemento distinto de cero en R es una ***unidad***, es decir, para cada a en R , existe un único elemento a^{-1} tal que $a^{-1}a = aa^{-1} = 1$, se llama ***anillo de división***.
Un anillo de división conmutativo, se llama ***cuerpo***.

1.2 Anillos de polinomios

A pesar de la definición abstracta de un anillo, como vimos anteriormente, los anillos de polinomios, anillos de enteros algebraicos y anillos de números hipercomplejos permanecieron centrales en la teoría de anillos, en las manos de los grandes algebristas Noether y Artin, en 1920.

Los ideales en anillos de polinomios y su importancia en geometría algebraica tenían sus inicios implícitos en el trabajo de M. Noether (c. 1870). Los avances importantes fueron hechos por Kronecker en la década de 1880 y especialmente por Hilbert, Lasker y Macauley en 1890, 1905 y 1913, respectivamente.

Supondremos que R es un anillo conmutativo con unitario

Definición 2. *Una expresión de la forma*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

*donde $a_i \in R$ y $a_n \neq 0$ se llama **polinomio sobre** R con indeterminada x. Los elementos $a_0, a_1, \ldots, a_n$ se llaman **coeficientes** de f. El coeficiente a_n se*

llama ***coeficiente líder****. Si el coeficiente líder de un polinomio es 1, se llama* ***mónico****. Si n es el mayor entero no negativo para el que $a_n \neq 0$, decimos que el* ***grado*** *de f es n y se escribe $gr\ f(x) = n$. Si no existe tal n, es decir, si $f = 0$, entonces el grado de f se define como $-\infty$.*

Dos polinomios son exactamete iguales cuando sus coeficientes correspondientes son iguales, es decir, si

$$p(x) = a_0 + a_1x + a_nx^n$$
$$q(x) = b_0 + b_1x + b_mx^m$$

entonces $p(x) = q(x)$ si y solo si $a_i = b_i$, para todo $i \geq 0$
Para mostrar que el conjunto de todos los polinomios forma un anillo, debemos definir adición y multiplicación. Sean dos polinomios,

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m$$

La suma de $p(x)$ y $q(x)$ se define como

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k$$

Donde $c_i = a_i + b_i$ para cada i.
El producto de $p(x)$ y $q(x)$ se define como

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$$

donde

$$c_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_i + \cdots + a_{i-1}b_1 + a_ib_0$$

para cada i. Donde algunos coeficientes pueden ser cero

Denotaremos $R[x]$ al conjunto de todos los polinomios con coeficientes en un anillo R.

Teorema 1. *El conjunto $R[x]$ de todos los polinomios en un indeterminada x, con coeficientes en un anillo R, es un anillo bajo la suma y multiplicación polinomial. Si R es conmutativo, entonces lo es $R[x]$ y si R tiene unitario 1, entonces 1 también es unitario en $R[x]$*

Si R es un anillo y x e y son indeterminadas, podemos formar el anillo $(R[x])[y]$, esto es, el anillo de polinomios en y con coeficientes que son polinomios en x. $(R[x])[y]$ es naturalmente isomorfo a $(R[y])[x]$.
Por esto consideraremos el polinomio $R[x, y]$, **el anillo de polinomios en dos indeterminadas x e y.**
Se define de manera análoga el anillo $R[x_1, \ldots, x_n]$ de polinomios en n indeterminadas x_i con coeficientes en R

1.3 Algoritmo de la división

El algoritmo de Euclides se documentó por primera vez en los "Euclid's Elements" alrededor del año 300 a. C., pero presumiblemente es bastante más antiguo. Según Knuth, podríamos llamar al algoritmo de Euclides el abuelo de todos los algoritmos, porque es el algoritmo no trivial más antiguo que ha sobrevivido hasta el día de hoy.

Conocemos las propiedades elementales del algoritmo de la división euclidiana en $\mathbb{Z}$, donde dados $a, b \in \mathbb{Z}, b \neq 0$, existen únicos números q y r en $\mathbb{Z}$ (cociente y resto), tales que $a = bq + r$ y $0 \leq r < |d|$

De manera análoga en $F[x]$, anillo de polinomios sobre un cuerpo F, existe una división euclídea de polinomios.

Teorema 2. *Sean*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$$

dos elementos de $F[x]$, con a_n y b_m ambos distintos del cero de F y $m > 0$. Entonces existen polinomios únicos $q(x)$ y $r(x)$ en $F[x]$ tales que $f(x) = g(x)q(x) + r(x)$, donde el grado de $r(x)$ es menos que m, es decir, menor que el grado de $g(x)$.

Demostración: Primero demostraremos la existencia de $q(x)$ y $r(x)$. Si $f(x)$ es un polinomio cero, entonces

$$0 = 0 \cdot g(x) + 0$$

luego, tanto q como r también son el polinomio cero. Ahora supongamos que $f(x)$ no es el polinomio cero y que $gr\ f(x) = n$ y $gr\ g(x) = m$. Si $m > n$,

entonces $q(x) = 0$ y $r(x) = f(x)$. Podemos ahora suponer que $m \leq n$ y proceder por inducción en n. Si

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

entonces el polinomio

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

tiene grado menor a n o es el polinomio cero. Por la hipótesis de inducción, existen polinomios $q'(x)$ y $r(x)$ tales que

$$f'(x) = q'(x)g(x) + r(x)$$

donde $r(x) = 0$ o el grado de $r(x)$ es menos al grado de $g(x)$. Ahora, sea

$$q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}.$$

Entonces

$$f(x) = g(x)q(x) + r(x),$$

con $r(x)$ el polinomio cero o $gr\, r(x) < gr\, g(x)$.
Para mostrar que $q(x)$ y $r(x)$ son unicos, supongamos que además existen $q_1(x)$ y $r_1(x)$ tales que $f(x) = g(x)q_1(x) + r_1(x)$ con $gr\, r_1(x) < gr\, g(x)$ o $r_1(x) = 0$, de manera que

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x).$$

y

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

Si $g(x)$ no es el polinomio cero, entonces

$$gr\,(g(x)[q(x) - q_1(x)]) = gr\,(r_1(x) - r(x)) \geq gr\, g(x).$$

Pero, los grados tanto de $r(x)$ como de $r_1(x)$ son estrictamente menores que el grado de $g(x)$; por lo tanto $r(x) = r_1(x)$ y $q(x) = q_1(x)$.

Definición 3. *Sea A un anillo conmutativo con identidad. Diremos que A es* ***dominio euclídeo*** *si existe la división euclidiana en A*

Definición 4. *Si R es un anillo conmutativo con unitario y $a \in R$, el ideal $\{ra|r \in R\}$ de todos los múltiplos de a es el ideal principal generado por a y se denota $< a >$. Un ideal N de R es un ideal principal si $N =< a >$ para alguna a en R*

Es claro que el ideal $< x >$ en $F[x]$ consta de todos los polinomios en $F[x]$ que tengan término constante cero

Definición 5. *Un dominio entero D es un Dominio de ideales principales, si todo ideal en D es un ideal principal*

Teorema 3. *Si F es un cuerpo, todo ideal en $F[x]$ es principal*

Demostración: Sea I un ideal de $F[x]$. Si I es el ideal cero, no hay nada que demostrar. Supongamos que I es un ideal no trivial en $F[x]$, y sea $p(x) \in I$ un elemnto distinto de cero de grado minimal. Si $gr\, p(x) = 0$, entonces $p(x)$ es una contante no nula y 1 está en I. Como 1 genera todo $F[x]$, $\langle 1 \rangle >= I = F[x]$ y I es un ideal principal.
Ahora supongamos que $gr\, p(x) \geq 1$ y sea $f(x)$ cualquier elemento en I. Por el algoritmo de la división existen $q(x)$ y $r(x)$ en $F[x]$ tales que $f(x) = p(x)q(x)+r(x)$ y $gr\, r(x) < gr\, p(x)$. Como $f(x), p(x) \in I$ e I es un ideal, $r(x) = f(x) - p(x)q(x)$ también está en I. Pero, como escogimos $p(x)$ de grado minimal, $r(x)$ debe ser el polinomio cero. Como podemos escribir cualquier elemento $f(x)$ en I como $p(x)q(x)$ para algun $q(x) \in F[x]$, tenemos que $I = \langle p(x) \rangle$ □

1.4 Polinomios irreducibles

Definición 6. *Un polinomio no constante $f(x) \in F[x]$ es irreducible sobre F, si $f(x)$ no puede expresarse como producto $g(x)h(x)$ de dos polinomios $g(x)$ y $h(x)$ en $F[x]$, ambos de grado menos que el grado de $f(x)$*

Cabe resaltar el concepto de irreducible sobre F y no solo irreducible, pues un polinomio puede ser irreducible en cierto cuerpo, pero puede ser no irreducible en un cuerpo mayor, que contenga a F.

Definición 7. *Un dominio entero D es un dominio de factorización única, si se satisfacen las siguientes condiciones:*

1. Todo elemento de D que no sea ni 0 ni una unidad, se puede factorizar en un numero finito de irreducibles

2. Si $p_1 \dots p_r$ y $q_1 \dots q_s$, son dos factorizaciones en irreducibles del mismo elemento de D. Entonces $r = s$ y los q_j pueden renumerarse de manera que p_i y q_i sean asociados.

Para $f(x), g(x) \in F[x]$ decimos que $g(x)$ divide $f(x)$ en $F[x]$. Si existe $q(x) \in F[x]$ tal que $f(x) = g(x)q(x)$

Teorema 4. *Si $p(x)$ es irreducible en $F[x]$ y $p(x)$ divide al producto $r_1(x) \cdots r_n(x)$ para $r_i(x) \in F[x]$, entonces $p(x)$ divide a $r_i(x)$ para al menos una i*

(*Para profundizar en su demostración Ver libro "Algebra Abstracta"de John Fraleigh*)

Teorema 5. *(Factorización única) Si F es un cuerpo, entonces todo polinomio no constante $f(x) \in F[x]$ se puede factorizar en $F[x]$ en un producto de polinomios irreducibles, los polinomios irreducibles son únicos, excepto por el orden y por factores unidad (esto es, constantes distintas de cero) en F.*

Demostración: Sea $f(x) \in F[x]$ un polinomio no constante. si $f(x)$ no es irreducible, entonces $f(x) = g(x)h(x)$ con el grado de $g(x)$ y el grado de $h(x)$, ambos menores que el grado de $f(x)$. Si $g(x)$ y $h(x)$ son irreducibles, nos detendremos aquí. De nos ser así, al menos uno de ellos se factoriza en polinomios de grado menor. Continuando este proceso (en realidad argumento de inducción), llegaremos a la factorización

$$f(x) = p_1(x)p_2(x) \cdots p_r(x),$$

donde $p_i(x)$ es irreducible.
Falta mostrar la unicidad. Supongase que

$$f(x) = p_1(x)p_2(x) \cdots p_r(x) = q_1(x)q_2 \cdots q_s(x)$$

son dos factorizaciones de $f(x)$ en polinomios irreducibles. Entonces, por el *Teorema 4*, $p_1(x)$ divide alguna $q_j(x)$, supongamos que $q_1(x)$. Como $q_1(x)$ es irreducible,

$$q_1(x) = u_1 p_1(x),$$

donde $u_1 \neq 0$, pero u_1 está en F y es, por lo tanto, una unidad. Entonces, al sustituir $q_1(x)$ por $u_1 p_1(x)$ y cancelar, obtenemos

$$p_2(x) \cdots p_r(x) = u_1 q_2(x) \cdots q_s(x).$$

Por argumento similar, digamos que $q_2(x) = u_2 p_2$, asi que

$$p_3(x) \cdots p_r(x) = u_1 u_2 q_3(x) \cdots q_s(x).$$

Al continuar así, por último se llegará a que

$$1 = u_1 u_2 \cdots u_r q_{r+1}(x) \cdots q_s(x).$$

Claramente, esto es posible solo sí $s = r$ de modo que esta ecuación es en realidad $1 = u_1 u_2 \cdots u_r$. Así los factores irreducibles de $p_i(x)$ y $q_j(x)$ fueron los mismos, exepto quizá, por el orden y por factores de unidad.

1.5 Plano proyectivo

La idea original de unir una línea recta de los puntos del infinito al plano habitual, constituyendo un plano proyectivo, se debe a Desargues. Su libro, publicado en 1639, tenía la intención de dar una base matemática a los métodos de perspectiva empleados por pintores y arquitectos. La concepción de Desargues del plan proyectivo es, en esencia, la que describiremos a continuación.

Definición 8. *Sea F un cuerpo. Sea el dos dimensional espacio proyectivo P_F^2 sobre F dado por las clases de equivalencia triples (x, y, z) con $x, y, z \in F$ con al menos uno de los x, y, z no cero.*

Definición 9. *Dos triples (x_1, y_1, z_1) y (x_2, y_2, z_2) se dicen equivalentes si existe un elemento distinto de cero $\lambda \in F$ tal que*

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$$

La clase de equivalencia de (x, y, z) es denotada por $(x : y : z)$

1. Si $z \neq 0$ estos son puntos infinitos en P_F^2
2. Si $z = 0$ son puntos llamados infinitos en P_F^2

Para evitar el problema de los representantes de clase, nosotros solo trabajaremos con polinomios homogéneos.
Si $f(x, y)$ es un polinomio en x e y, entonces nosotros podemos hacer este, homogéneo insertando apropiadas potencias de z.

Finalmente, mostraremos que significa que dos rectas se cortan en el punto del infinito.

$$y = mx + b_1$$
$$y = mx + b_2$$

Estas dos rectas oblicuas paralelas con $b_1 \neq b_2$. Ellas tienen sus formas homogéneas

$$y = mx + b_1 z$$
$$y = mx + b_2 z$$

Buscando la intersección de ambas rectas obtenemos los siguientes resultados

$$z = 0 \quad \text{y} \quad y = mx$$

no podemos tener x, y, z, todos cero, por lo cual obtenemos un $x \neq 0$. Luego nosotros podemos reescribir realizando el cociente por x y finalmente obtenemos

$$(x : mx : 0) = (1 : m : 0)$$
$$z = 0 \quad \text{punto infinito}$$

CAPÍTULO 2

La resultante

La resultante de dos polinomios univariados se remonta a Leibniz y Bezout. Su presentación moderna se debe a Sylvester en 1853. La resultante tiene una gran importancia en diversas ramas de la matemática, es utilizada en una gran cantidad de demostraciones, tiene una gran importancia algorítmica, por lo cual es muy reconocida actualmente. También estuvo muy latente hasta los años 50, siendo un elemento fundamental de la Teoría de la eliminación y renació en los años 60 con la necesidad de realizar cálculos, hasta entonces impensados, los cuales fueron posible con el desarrollo de la tecnología.

En cuanto a sus precursores, la historia nos dice que Leibniz redactó una carta a Tschirnahaus, la cual nunca envió. Esta describía cómo calcular la resultante de dos polinomios de grado cinco mediante el algoritmo de Euclides, explicando que su desaparición significa que los dos polinomios tienen MCD no trivial.

En Europa aparece el término de determinante en el año 1683 en una carta enviada por Gottfried Wilhelm von Leibniz a Guillaume de l'Hopital, donde explicaba que un sistema de ecuaciones lineales tiene solución, en esta época los determinantes se conocían por el nombre de resultantes.

Después de trabajos anteriores, Bezout introdujo el término de resultante, nombre que proviene de su propia ecuación "resultante de la eliminación", la cual se obtiene como determinante de una matriz. Bezout, en una memoria presentada a la Academia de París en 1764, mostró un sistema de procedimientos para resolver sistemas de n ecuaciones lineales con n incógnitas. Siendo conocido por la generalización de la resultante al caso de un sistema de ecuaciones con más de una incógnita.

Además, fue el primero que dio una demostración satisfactoria del teorema de que dos curvas algebraicas m y n grados respectivamente, se cortan en general

en $m \cdot n$ puntos, y así este teorema se suele conocer como "teorema de Bezout".

La resultante aparece cuando se busca una condición para que los sistemas de ecuaciones de polinomios de distinto grado tengan una solución

Sylvester hizo una gran contribución al campo de las matrices, y es por esto por lo que el "método dialítico de Sylvester", para eliminar una incógnita entre dos ecuaciones de polinomios, lleva su nombre. La idea de este matemático era la siguiente:

Ejemplo 1. *Consideremos como ejemplo dos ecuaciones, de grado 2 y grado 3 respectivamente, así, para eliminar x del par de ecuaciones*

$$\begin{aligned} x^2 + ax + b &= 0 \\ x^3 + cx^2 + dx + e &= 0 \end{aligned}$$

hay que multiplicar la primera ecuación por x y de nuevo la ecuación resultante por x, y la segunda ecuación también por x. Entonces, consderando a cada una de las cinco potencias $x^4, x^3, x^2, x, x^0 = 1$ de la incógnita x como una incógnita distinta, la condición necesaria y suficiente para que un sistema lineal homogéneo tenga solución no trivial ($x^0 = 1$).

$$\begin{aligned} x^2 + ax + b &= 0 \\ x^3 + ax^2 + bx &= 0 \\ x^4 + ax^3 + bx^2 &= 0 \\ x^3 + cx^2 + dx + e &= 0 \\ x^4 + cx^3 + dx^2 + ex &= 0 \end{aligned}$$

ordenando las ecuaciones convenientemente, obtenemos la siguiente matriz,

$$\begin{pmatrix} 1 & a & b & 0 & 0 \\ 0 & 1 & a & b & 0 \\ 0 & 0 & 1 & a & b \\ 1 & c & d & e & 0 \\ 0 & 1 & c & d & e \end{pmatrix}$$

de la cual tomaremos su traspuesta,

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ a & 1 & 0 & c & 1 \\ b & a & 1 & d & c \\ 0 & b & a & e & d \\ 0 & 0 & b & 0 & e \end{pmatrix}$$

lo que hace que el determinante conocido como la resultante en el método de

Sylvester, igualado a cero, dé el resultado de la eliminación.
Las resultantes en varias variables fueron principalmente introducidas por Macaulay luego de trabajo previo por Euler, Sylvester y A.L. Cauchy.

De lo mencionado anteriormente, se motiva la sigueinte definición.

Definición 10. *Sean $f(x)$ y $g(x)$ polinomios de grado m y n respectivamente, y sea S la $m+n$ por $m+n$ matriz de Sylvester de estos polinomios. Entonces la resultante de $f(x)$ y $g(x)$ es $Res_x(f,g) = det(S)$,*

$$S = \begin{pmatrix} a_m & 0 & \cdots & 0 & 0 & b_n & 0 & \cdots & 0 & 0 \\ a_{m-1} & a_m & \cdots & 0 & 0 & b_{n-1} & b_n & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_1 & a_2 & 0 & 0 & \cdots & b_1 & b_2 \\ 0 & 0 & \cdots & a_0 & a_1 & 0 & 0 & \cdots & b_0 & b_1 \\ 0 & 0 & \cdots & 0 & a_0 & 0 & 0 & \cdots & 0 & b_0 \end{pmatrix}$$

Ejemplo 2. *Sean*

$$f = y^2 + x^2 - 2x$$
$$g = y^2 - x$$

Entonces

$$Res(f,g) = det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ x^2 - 2x & 0 & -x & 0 \\ 0 & x^2 - 2x & 0 & -x \end{pmatrix} = x^2(x-1)^2$$

Teorema 6. *Sean $f, g \in F[x]$. Entonces*

$$Res(f,g) = 0 \Leftrightarrow gr(mcd(f,g)) \geq 1 \Leftrightarrow \exists \alpha \in \overline{F} \text{ tal que } f(\alpha) = g(\alpha) = 0$$

Demostración: La segunda equivalencia es bien conocida *(Ver capitulo 3 del libro "Ideals, Varieties, and Algorithms"de David Cox.)*. Para demostrar entonces la primera igualdad, debemos considerar la transformación lineal Φ entre los F-espacios vectoriales de polinomios.

$$F[x]_{<n} \times F[x]_{<m} := \{(s,t) : s,t \in F[x], s = 0 \text{ o } gr(s) < n \text{ y } t = 0 \text{ o } gr(t) < m\}$$
$$\text{y} \quad F[x]_{<m+n} := \{h \in k[x] : h = 0 \text{ o } gr(h) < m+n\},$$

dada por

$$\Phi : F[x]_{<n} \times F[x]_{<m} \to F[x]_{<m+n}$$
$$(s,t) \mapsto s\,f + t\,g,$$

que está bien definida dado que $gr(s\ f), gr(t\ g) < m+n$ cuando $gr(s) < n$ y $gr(t) < m$.

Como los dos espacios vectoriales tienen dimensión $m+n$

Φ es un isomorfismo $\Leftrightarrow$ es un monomorfismo $\Leftrightarrow$ es un epimorfismo $\Leftrightarrow$ su matriz en cualquier par de bases es invertible.

Considerando las siguientes bases canónicas ordenadas de $F[x]_{<n}\times$ y $F[x]_{<m+n}$ respectivamente,

$$\mathcal{B} := ((x^{n-1},0),\ldots,(1,0);(0,x^{m-1}),\ldots,(0,1)) \quad \text{y} \quad \mathcal{B}' := (x^{m+n-1},\ldots,1),$$

La matriz $[\Phi]_{\mathcal{B},\mathcal{B}'}$ de Φ en las bases $\mathcal{B}$ de $F[x]_{<n}\times F[x]_{<m}$ y $\mathcal{B}'$ de $F[x]_{<n+m}$ resulta ser

$$[\Phi]_{\mathcal{B},\mathcal{B}'} = \left(\begin{array}{c|c|c|c} \uparrow & \uparrow & \uparrow & \\ [x^{n-1}f]_{\mathcal{B}'} & \ldots [f]_{\mathcal{B}'} & \ldots [x^{m-1}g]_{\mathcal{B}'} & \ldots [g]_{\mathcal{B}'} \\ \downarrow & \downarrow & \downarrow & \downarrow \end{array}\right)$$

$$\begin{pmatrix} a_m & 0 & \cdots & 0 & 0 & b_n & 0 & \cdots & 0 & 0 \\ a_{m-1} & a_m & \cdots & 0 & 0 & b_{n-1} & b_n & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_1 & a_2 & 0 & 0 & \cdots & b_1 & b_2 \\ 0 & 0 & \cdots & a_0 & a_1 & 0 & 0 & \cdots & b_0 & b_1 \\ 0 & 0 & \cdots & 0 & a_0 & 0 & 0 & \cdots & 0 & b_0 \end{pmatrix} = S(f,g)$$

Por lo tanto Φ es un isomorfismo si y solo sí $S(f,g)$ es invertible si y solo sí $Res(f,g) \neq 0$.

Probemos ahora:

$(\Rightarrow)$: $Res(f,g) = 0$ implica que Φ no es isomorfismo, es decir no es monomorfismo por ser espacios de la misma dimensión, y por lo tanto existe $(s,t) \in F[x]_n \times F[x]_m$ no nulo tal que $s\ f + t\ g = 0$. Es decir $s\ f = -t\ g$ pero en este caso no pueden ser f y g coprimos ya que sería $f|t$ y $g|s$, lo que contradice los grados de s y t y que no sean ambos nulos.

$(\Leftarrow)$: Probemos la contrarecíproca, $Res(f,g) \neq 0 \Rightarrow mcd(f,g) = 1$. Al ser Φ isomorfismo, es decir epimorfismo, existe $(s,t) \in F[x]_n \times F[x]_m$ tal que $sf+tg = 1$, es decir f y g son coprimos.

Como corolario se obtiene

Corolario 1. *sea R un DFU y $f,g \in R[x]$ no ambos nulos. Entonces mcd (f,g) es no constante en $R[x]$ si y solo si $res(f,g) = 0$ en R*

(Para profundizar en la diferencia entre el teorema y el corolario antes mencionado ver libro "Modern computer algebra"de von Zur Gathen)

Proposición 1. *Sean*

$$f = a_d(X)Y^d + \cdots + a_o(X)$$
$$g = b_e(X)Y^e + \cdots + b_0(X)$$

donde a_i, b_j *son polinomios en las variables* $x_1, x_2, \ldots$ *con coeficientes en un cuerpo* F

Entonces para cada $x = (x_1, x_2, \ldots)$ *tenemos* $Res_Y(X) = 0$ *si y solo sí* $a_d(x) = b_e(x) = 0$ *o* $f(x, Y), g(x, Y)$ *admiten un factor común no constante.*

Demostración: Para cada x, la resultante de $f(x, Y)$ y $g(x, Y)$ es $R(x)$. Por otro lado $f(x, Y)$ y $g(x, Y)$ admiten una raíz común si y solo sí admiten un factor y no constante.

Cuando $f, g \in F[x, y]$, escribimos $res_x(f, g)$ para la resultante en $F[y]$ con respecto a x. Simétricamente, hay un polinomio $res_y(f, g)$ en $F[x]$. Tenemos la siguiente relación en $\mathrm{gr}_y res_x(f, g)$, donde gr_y denota el grado con respecto a la variable y

Teorema 7. *Sea* $f, g \in F[x, y]$ *con* $m = gr_x f = gr_x g$, *y* $gr_y f, gr_y g \leq d$. *Entonces*

$$gr_y res_x(f, g) \leq (m + n)d$$

(para profundizar en la demostracióon de este teorema, ver libro "Modern computer algebra"de Joachim von zur Gathen)

2.1 La resultante es una combinación polinomial de f y g

Proposición 2. *Existen polinomios* $s, t \in F[x]$ *no ambos nulos con* $gr(S) < n$ *y* $gr(t) < m$ *que satisfacen la identidad de Bézout*

$$Res(f, g) = s\, f + t\, g.$$

Demostración: Tanto para $Res(f, g) = 0$ como para $Res(f, g) \neq 0$. Podemos identificar los polinomios s y t por la igualdad que se obtiene a través de una pequeña modificacion a la matriz de Sylvester, le sumamos a la última fila x por la penúltima, $+x^2$ por la antepenúltima y así sucesivamente hasta sumarte

x^{m+n-1} por la primera, con lo cual no se modifica el determinante.

$$Res(f,g) = det \left(\begin{array}{cccccccccc} a_m & 0 & \cdots & 0 & 0 & b_n & 0 & \cdots & 0 & 0 \\ a_{m-1} & a_m & \cdots & 0 & 0 & b_{n-1} & b_n & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_1 & a_2 & 0 & 0 & \cdots & b_1 & b_2 \\ 0 & 0 & \cdots & a_0 & a_1 & 0 & 0 & \cdots & b_0 & b_1 \\ \hline x^{n-1}f & x^{n-2}f & \cdots & xf & f & x^{m-1}g & x^{m-2}g & \cdots & xg & g \end{array} \right)$$

Luego se divide este determinante como la suma de dos determinantes escribiendo la última fila como

$$(x^{n-1}f, \ldots, f, x^{m-1}g, \ldots, g) = (x^{n-1}f, \ldots, f, 0, \ldots, 0) + (0, \ldots, 0, x^{m-1}g, \ldots, g),$$

y sacando luego f en factor común del primer determinante y g del segundo, se obtiene $Res(f,g) = s\,f + t\,g$ con

$$s = det \begin{pmatrix} a_m & 0 & \cdots & 0 & 0 & b_n & 0 & \cdots & 0 & 0 \\ a_{m-1} & a_m & \cdots & 0 & 0 & b_{n-1} & b_n & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_1 & a_2 & 0 & 0 & \cdots & b_1 & b_2 \\ 0 & 0 & \cdots & a_0 & a_1 & 0 & 0 & \cdots & b_0 & b_1 \\ x^{m-1} & x^{m-2} & \cdots & x & 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$t = det \begin{pmatrix} a_m & 0 & \cdots & 0 & 0 & b_n & 0 & \cdots & 0 & 0 \\ a_{m-1} & a_m & \cdots & 0 & 0 & b_{n-1} & b_n & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_1 & a_2 & 0 & 0 & \cdots & b_1 & b_2 \\ 0 & 0 & \cdots & a_0 & a_1 & 0 & 0 & \cdots & b_0 & b_1 \\ 0 & 0 & \cdots & 0 & 0 & x^{n-1} & x^{n-2} & \cdots & x & 1 \end{pmatrix}$$

las que cumplen las condiciones de grado requeridas, desarrollando por la última fila, y son la única solución con esos grados.

2.2 La fórmula de Poisson

La resultante es nula si y solo sí f y g comparten una raíz en $\overline{F}$.
Esto queda de manifiesto en la siguiente descripción de la resultante como producto de diferencias de raíces de f y g.

Proposición 3. *Sea*

$$f = a_m(x-\alpha_1)\cdots(x-\alpha_m), g = b_n(x-\beta_1)\cdots(x-\beta_n) \in \overline{F}[x].$$

Entonces

$$Res(f,g) = a_m^n \prod_{1\leq i\leq m} g(\alpha_i) = a_m^n b_n^m \prod_{1\leq i\leq m, \leq j\leq n} (\alpha_i - \beta_j).$$

La segunda igualdad se obtiene desarrollando $g(\alpha_i)$ para $1 \leq i \leq m$. Por lo tanto mostremos la validez de la primera igualdad. Lo hacemos aquí para el caso en que f tiene todas sus raíces simples, es decir $\alpha_i \neq \alpha_j$ si $i \neq j$, recordando para ello el determinante de Vandermonde definido como

$$\mathcal{V}(a_1,\ldots,a_m) = det \begin{pmatrix} a_1^{m-1} & \cdots & a_m^{m-1} \\ \vdots & \cdots & \vdots \\ a_1 & \cdots & a_m \\ 1 & \cdots & 1 \end{pmatrix} = \prod_{1\leq i<j\leq m} (\alpha_i - \alpha_j)$$

que es no nulo cuando $\alpha_i \neq \alpha_j$ para $i \neq j$. Consideremos entonces el siguiente producto de matrices

$$\begin{pmatrix} & Id_n & & & 0 & \\ & & & & & \\ a_1^{m+n-1} & \cdots & a_1^m & a_1^{m-1} & \cdots & 1 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ a_m^{m+n-1} & \cdots & a_m^m & a_m^{m-1} & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\ a_{m-1} & a_m & \cdots & 0 & b_{n-1} & b_n & \cdots & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \cdots & a_1 & 0 & 0 & \cdots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

$$= \begin{pmatrix} a_m & 0 & 0 & & & & \\ \vdots & \ddots & 0 & & & * & \\ * & \cdots & a_m & & & & \\ & & & & & & \\ & & & a_1^{m-1}g(\alpha_1) & \cdots & g(\alpha_1) \\ & 0 & & \vdots & \cdots & \vdots \\ & & & a_m^{m-1}g(\alpha_1) & \cdots & g(\alpha_1) \end{pmatrix}$$

Calculando determinantes, quedan las siguientes matrices triangulares en bloques,

$$\mathcal{V}(\alpha_1,\ldots,\alpha_m)Res(f,g) = a_m^n g(\alpha_1)\cdots g(\alpha_m)\mathcal{V}(\alpha_1,\ldots,\alpha_m),$$

y el enunciado se obtiene simplificando $V(\alpha_1, \ldots, \alpha_m)$, que es no nulo en el caso considerado. El caso general se obtiene por un argumento de continuidad, o bien haciendo la misma construcción de producto de matrices, pero en lugar de considerar la matriz de Vandermonde de ($\alpha_1, \ldots, \alpha_m$)se considera la matriz de Vandermonde generalizada que tiene en cuenta la estructura de multiplicidades de las raíces de f. Existen tales matrices, y su relación con la interpolación de Hermite, así como la matriz de Vandermonde clásica se corresponde con la interpolación de Lagrange. La fórmula de Poisson tiene una consecuencia inmediata con respecto al algoritmo de división, de los tiempos de Euclides: Sea $f = q\, g + r$, con $k := gr(r) < n = gr(g)$, entonces

$$Res(f, g) = (-1)^{mn} b_n^{m-k} Resp(g, r),$$

ya que $f(\beta_i) = r(\beta_i), 1 \leq i \leq n$, implica

$$Res(g, f) = b_n^m \prod_{1 \leq i \leq n} f(\beta_i) = b_n^{m-k} b_n^k \prod_{1 \leq i \leq n} r(\beta_i) = b_n^{m-k} Resp(g, r).$$

.

2.3 El plano proyectivo como marco correcto

El marco correcto para considerar la resultante no es"polinomios en $F[x]$ con raices en $\overline{F}$"sino más bien "polinomios homogéneos en $F[x, y]$ con raíces en el espacio proyectivo $\mathbb{P}^1(\overline{F})$": Sean

$$\begin{aligned} F(\mathbf{A}, x) &:= A_m x^m + A_{m-1} x^{m-1} + \cdots + A_1 x + A_0 \\ G(\mathbf{B}, x) &:= B_n x^n + B_{n-1} x^{n-1} + \cdots + B_1 x + B_0 \quad \in \mathbb{Z}[\mathbf{A,B}][x] \end{aligned}$$

Así,

$$\begin{aligned} F^h(\mathbf{A}, x, y) &:= A_m x^m + A_{m-1} x^{m-1} y + \cdots + A_1 x y^{m-1} + A_0 y^m \\ G^h(\mathbf{B}, x, y) &:= B_n x^n + B_{n-1} x^{n-1} y + \cdots + B_1 x y^{n-1} + B_0 y^n \quad \in \mathbb{Z}[\mathbf{A,B}][x, y] \end{aligned}$$

son las homogeneizaciones de los polinomios F, G y definamos

$$Res(F^h G^h) := Res(F, G) \in \mathbb{Z}[\mathbf{A},\ \mathbf{B}].$$

Entonces existen $S, T \in \mathbb{Z}[\mathbf{A,B}][x, y]$ tales que $Res(F, G) = SF + TG$

El caso $a_m = 0$ y $b_n = 0$ se corresponde con la raíz al infinito $(1 : 0) \in \mathbb{P}^1(\overline{F})$.

CAPÍTULO 3

Subresultante

Al igual que la resultante, la sub-resultante de dos polinomios univariados se remonta a Leibniz y Bezout. Volvieron a aparecer a fines de los 60 para dar un algoritmo eficiente y paralelizable para el cálculo del máximo común divisor de dos polinomios y más recientemente son también utilizadas en computación simbólica-numérica.
La primera generalización de subresultantes a varias variables apareció en los libros de Laureano González-Vega, siendo la versión de Marc Chardin.

3.1 La subresultante escalar

Definición 11. *Para $0 \leq k < n$, el determinante $(\sigma_k(f,g))$ de la matriz $(m+n-2k) \times (m+n-2k)$*

$$S_k(f,g) = \begin{pmatrix}
a_m & 0 & 0 & 0 & b_n & 0 & 0 & 0 & 0 & 0 \\
a_{m-1} & a_m & 0 & 0 & b_{n-1} & b_n & 0 & 0 & 0 & 0 \\
\vdots & & \ddots & 0 & \vdots & & \ddots & 0 & 0 & 0 \\
a_{m-n+k+1} & \cdots & \cdots & a_m & b_{k+1} & \cdots & \cdots & b_n & 0 & 0 \\
\vdots & & & \vdots & \vdots & & & & \ddots & 0 \\
a_{k+1} & \cdots & \cdots & a_n & b_{n-m+k+1} & \cdots & \cdots & \cdots & \cdots & b_n \\
\vdots & & & \vdots & \vdots & & & & & \vdots \\
\vdots & & & \vdots & \vdots & & & & & \vdots \\
a_{2k-n+1} & \cdots & \cdots & a_k & b_{2k-m+1} & \cdots & \cdots & \cdots & \cdots & b_k
\end{pmatrix}$$

Es llamada la k-ésima subresultante escalar de f y g.
Según Von Zur Gathen (2003) Householder en uno de sus libros los llama *bigra-*

dients y los usan en el problema de Routh-Hurwitz de determinar si cada raíz compleja de un polinomio dado tiene parte real negativa. Este problema está íntimamente relacionado con la estabilidad sistemas dinámicos. En Habicht llama a este determinante *Nebenresultante* (resultado menor) para los polinomios f y g de grados n y n-1.

Observación

- $S_0 = Syl(f, g)$ y por lo tanto, su determinante es la resultante.
- $\sigma_n = g_n^{m-n}$
- S_k es la matriz obtenida de Sylvester al eliminar las últimas $2k$ filas, las últimas k columnas con coeficientes de f y las últimas k columnas con coeficientes de g
- S_k es una submatriz de S_i si $k \geq i$

3.2 El polinomio subresultante

Mencionaremos dos descripciones de este tipo de subresultantes con unas ligeras diferencias.
Gathen (2003) alude la primera es a Collin y la segunda a Brown y Treub y también a Zippel.

Definición 12. *Sea $M_{ik} = M_{ik}(f, g)$ la submatriz $(m+n-2k) \times (m+n-2k)$ de $Syl(f, g)$ obtenida eliminando las úlimas k de las n columnas de coeficientes de f, las últimas k de las m columnas de coeficientes de g y las últimas $2k+1$ filas, a excepción de la fila $(m+n-i-k)$, para $0 \leq k \leq n$ y $0 \leq i \leq m$:*

$$M_{ik} = \begin{pmatrix} a_m & 0 & 0 & 0 & b_n & 0 & 0 & 0 & 0 \\ a_{m-1} & a_m & 0 & 0 & b_{n-2} & b_n & 0 & 0 & 0 \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 & 0 \\ \vdots & & & a_m & \vdots & & & \ddots & 0 \\ \vdots & & & \vdots & \vdots & & & & b_n \\ \vdots & & & \vdots & \vdots & & & & \vdots \\ a_{2k-n+2} & \cdots & \cdots & a_k & b_{2k-m+2} & \cdots & \cdots & \cdots & b_{k+1} \\ a_{i+k-n+1} & \cdots & \cdots & a_i & b_{i+k-m+1} & \cdots & \cdots & \cdots & b_i \end{pmatrix}$$

El polinomio $R_k(f, g) = \sum_{0 \leq i \leq m} det(M_{ik}) x^i \in F[x]$ se denomina el k-ésimo polinomio subresultante de f y g. (En realidad, Collins lo define a través de la matriz traspuesta)

Observación

- $M_{00} = Syl(f, g)$ y por lo tanto, $R_0 = det(M_{00})$ es la resultante

Definición 13. *Consideraremos ahora el determinante* $Z_k(f, g) = det(M_k^*)$ *de la matriz* $(m + n - 2k) \times (m + n - 2k)$

$$M_k^* = \begin{pmatrix} a_m & 0 & 0 & 0 & b_n & 0 & 0 & 0 & 0 \\ a_{m-1} & a_m & 0 & 0 & b_{n-2} & b_n & 0 & 0 & 0 \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 & 0 \\ \vdots & & & a_m & \vdots & & & \ddots & 0 \\ \vdots & & & \vdots & \vdots & & & & b_n \\ \vdots & & & \vdots & \vdots & & & & \vdots \\ a_{2k-n+2} & \cdots & \cdots & a_k & b_{2k-m+2} & \cdots & \cdots & \cdots & b_{k+1} \\ x^{n-k-1}f & \cdots & \cdots & f & x^{m-k-1}g & \cdots & \cdots & \cdots & g \end{pmatrix}$$

Observamos que M_k^* es una submatriz de la matriz de Sylvester presente en la demostración de la *Proposición 1* antes vista.
El siguiente teorema muestra que las definiciones Collins y Brown y Traub describen el mismo polinomio.

Teorema 8. *Sea* $1 \leq k \leq l$.

- *Si* $\sigma_k \neq 0$, *entonces* σ_k *es el coeficiente principal de* R_k. *De lo contrario* $gr(R_k) < k$.
- $R_k = Z_k$

(para profundizar en la demostración de este teorema, ver apunte *"Subresultants revisited"* de Joachim von zur Gathen)
Con el siguiente ejemplo, mostraremos la validez de ambas definiciones:

Ejemplo 3.

$$S = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ a & 1 & 0 & c & 1 \\ b & a & 1 & d & c \\ 0 & b & a & e & d \\ 0 & 0 & b & 0 & e \end{pmatrix}$$

Calcularemos el polinomio subresultante con $k = 1$.

Comenzaremos con la definición de Collins

$$det(M_{01}) = det\begin{pmatrix} 1 & 0 & 1 \\ a & 1 & c \\ 0 & b & e \end{pmatrix} = ab - bc + e$$

$$det(M_{11}) = det\begin{pmatrix} 1 & 0 & 1 \\ a & 1 & c \\ b & a & d \end{pmatrix} = a^2 - ac - b + d$$

$$R_1(f,g) = det(M_{01}) + det(M_{11})x = (ab - bc + e) + (a^2 - ac - b + d)x$$

El polinomio subresultante obtenido a través de la ***definición 12:***

$$R_1 = (ab - bc + e) + (a^2 - ac - b + d)x$$

Continuamos con la definición de Brown y Traub

$$det(M_1^*) = det\begin{pmatrix} 1 & 0 & 1 \\ a & 1 & c \\ xf & f & g \end{pmatrix}$$

$$= det\begin{pmatrix} 1 & 0 & 1 \\ a & 1 & c \\ x^3 + ax^2 + bx & x^2 + ax + b & x^3 + cx^2 + dx + e \end{pmatrix} = a^2x - acx - bx + dx + ab - bc + e$$

El polinomio subresultante obtenido a través de la ***definición 13:***

$$\begin{aligned} Z_1 &= a^2x - acx - bx + dx + ab - bc + e \\ &= (ab - bc + e) + (a^2 - ac - b + d)x \end{aligned}$$

Con el ejemplo, queda en evidencia que $R_k = Z_k$.

Para terminar el capitulo daremos una tabla de equivalencia de las definiciones antes mencionadas

Concepto	Referencias
$\sigma_k(f,g) = det(S_k) \in R$	Sylvester, Trudi, Kronecker, Gordan, Habicht, Householder, von zur Gathen, Uteshev y Cherkasov, von zur Gathen y Gerhard
$R_k(f,g) = \sum_{0 \leq i \leq n} det(M_{ik}) x^i$	Jacobi, Collins, Loos, Geddes et al., Ho y Yap, Winkler, Lombardi et al., Yap
$Z_k(f,g) = det(M_k^*) \in R[x]$	Brown, Brown y Traub, Zippel, Lickteig y Roy, Reischert

Cuadro 3.1: Referencias: *Von zur Gathen, Theoretical Computer Science 297 (2003)*

CAPÍTULO 4

Aplicaciones

4.1 El discriminante

Una de las aplicaciones de la resultante es el discriminante, el cual es un objeto fundamental en matemática, en particular en la teoría de números y en geometría abstracta, que indica cuando un polinomio tiene raíces múltiples.
Uno de los ejemplos más conocidos, el cual es utilizado en la enseñanza media, es el discriminante de la función cuadrática:
Si $f = ax^2 + bx + c$ se tiene que $\text{Disc}(f) = b^2 - 4ac$.
Que se puede obtener a través de la aplicación de Resultante

Ejemplo 4. *Sean*

$$f = ax^2 + bx + c \quad y \quad f' = 2ax + b$$

$$Res(f,g) = det \begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix} = ab^2 + 4a^2c - 2ab^2 = -a(b^2 - 4ac)$$

Otro ejemplo, si $f = x^3 + px + q$, $\text{Disc}(f) = -4p^3 - 27q^2$.
De la misma forma podemos verlo con resultante:

Ejemplo 5. *Sean*

$$f = x^3 + px + q \quad y \quad f' = 3x^2 + p$$

$$Res(f,g) = det \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ p & 0 & p & 0 & 1 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{pmatrix} = 4p^3 + 27q^2 = -(-4p^3 - 27q^2)$$

Mencionaremos además, el discriminante de una función de grado 4, obtenido a través de la resultante por medio de un software matemático:
Si $f = x^4 + px^2 + qx + r$ se obtiene que
$Disc(f) = 16p^4 - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$

Sabemos que f tiene una raíz múltiple si y solo sí f y f' tienen una raíz en común, es decir, cuando $\text{Res}(f, f') = 0$.
Se define para$f = a_m x^m + \cdots + a_0 = a_m \prod_{1 \leq j \leq m}(x - \alpha_j)$ con $a_m \neq 0$,

$$\text{Disc}(f) := (-1)^{\frac{m(m-1)}{2}} \frac{1}{a_m} \text{Res}(f, f') = a_m^{2m-2} \prod_{1 \leq i \leq j \leq m} (\alpha_i - \alpha_j),$$

donde la última igualdad equivale a la fórmula de Poisson y la identidad

$$f' = a_m \sum_{1 \leq i \leq m} \prod_{j \neq i} (x - \alpha_j).$$

Se obtiene entonces

$$\text{Disc}(f) = 0 \Leftrightarrow f \text{ tiene una raíz multiple}$$

4.2 Determinar raices comunes de dos polinomios

A continuación veremos cómo encontrar las raíces comunes de dos polinomios o bien, la intersección de dos curvas planas, utilizando resultantes.
Suponga $f, g \in F[x, y]$ donde F es un cuerpo y se quiere intersectar ambas curvas.

$$X = \{(a, b) \in F^2 : f(a, b) = 0\}, \quad Y = \{(a, b) \in F^2 : g(a, b) = 0\}$$

Eliminamos la variable, considerando la resultante $r = res_y(f, g) \in F[x]$ con respecto a y. Asumimos que F es algebraicamente cerrado, de modo que cada polinomio univariado tenga raíz en F.
Sea Z la proyección de la intersección de X e Y en el eje x. Si $a \in F$ y $lc_y(f), lc_y(g)$ ambos no nulos en $x = a$, entonces:

$$\begin{aligned} a \in Z \Leftrightarrow & \quad \exists b \in F (a, b) \in X \cap Y \Leftrightarrow \exists b \in F f(a, b) = g(a, b) = 0 \\ \Leftrightarrow & \quad mcd(f(a, y), g(a, y) \neq 1 \\ \Leftrightarrow & \quad r(a) = res_y(f, g)(a) = 0 \end{aligned}$$

Asi, para determinar $X \cap Y$, primero debemos calcular el $(d + e) \times (d + e)$ determinante sobre $F[x]$ con $r \in F[x]$, donde d y e son los grados de y en f y g, respectivamente, luego encontrar todas las raíces de r y para cada raíz a

entontramos todas las raíces $b \in F$ de $mcd(f(a,y), g(a,y)) \in F[y]$. Si $r(a) = 0$ garantiza que aquellas b's existen si no ambos coeficientes principales con respecto a y desaparecen en $x = a$. En otras palabras, Z está contenido en el conjunto de raíces de r.

Ejemplo 6. *Como un ejemplo, buscaremos la solución del sistema de ecuaciones formado por* $f = 2x + 3y - 1 = 0, g = -5x + 2y + 1 = 0$.
La resultante correspondiente es

$$\begin{aligned} res_y(f,g) = & \begin{pmatrix} 3 & 2 \\ 2x-1 & -5x+1 \end{pmatrix} \\ = & -19x + 5 \in F[x] \end{aligned}$$

Donde la solución es $\left\{\frac{5}{19}, \frac{3}{19}\right\}$

Este tipo de polinomios lineal tiene una raíz si y solo sí, el coeficiente principal sea distinto de cero (entonces $X \cap Y$ consiste en un punto)

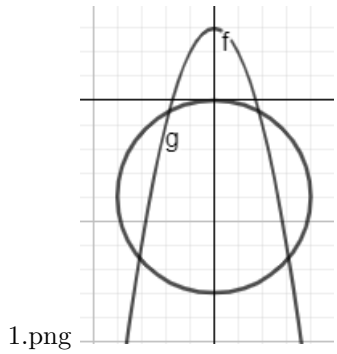
La teoría general del álgebra lineal generaliza este criterio conocido por la solubilidad simultánea de dos ecuaciones lineales en dos variables. De un modo similar, la teoría de eliminación geométrica trata de generalizar este método de intersección de curvas a dimensiones más altas. Este es un problema mucho más difícil, y los métodos algorítmicos corrientes son factibles sólo para un bastante pequeño número de variables.

Ejemplo 7. *Ejemplificaremos la intersección entre una circuenferencia y una parábola en conjunto de los reales. O bien, la solución al siguiente sistema de ecuaciones*

$$\begin{aligned} f &= y + x^2 - 2 \\ g &= x^2 + y^2 + 8y \end{aligned}$$

Nosotros buscaremos esas soluciones a través de la resultante. Tenemos

$$res_y(f,g) = det \begin{pmatrix} 1 & 0 & 1 \\ x^2-2 & 1 & 8 \\ 0 & x^2-2 & x^2 \end{pmatrix} = x^4 - 11x^2 - 20$$



1.png

Figura 4.1: intersección de la parábola f y la circunferencia g

y la proyección Z de $X \cap Y$ en el eje x consiste en cuatro ceros

$$Z = \{\frac{1}{2}\sqrt{22-2\sqrt{41}}, -\frac{1}{2}\sqrt{22-2\sqrt{41}}, \frac{1}{2}\sqrt{22+2\sqrt{41}}, -\frac{1}{2}\sqrt{22+2\sqrt{41}}\}$$

obtenidos de $res_y(f,g)$
Obtenemos los valores correspondientes para y tomando mcd :

$$\begin{aligned} & mcd\left(f\left(\frac{1}{2}\sqrt{22-2\sqrt{41}}, y\right), g\left(\frac{1}{2}\sqrt{22-2\sqrt{41}}, y\right)\right) \\ = \quad & mcd\left(\frac{7}{2}-\frac{1}{2}\sqrt{41}+y, \frac{11}{2}-\frac{1}{2}\sqrt{41}+y^2+8y\right) \quad = \quad \frac{7}{2}-\frac{1}{2}\sqrt{41}+y, \end{aligned}$$

$$\begin{aligned} & mcd\left(f\left(-\frac{1}{2}\sqrt{22-2\sqrt{41}}, y\right), g\left(-\frac{1}{2}\sqrt{22-2\sqrt{41}}, y\right)\right) \\ = \quad & mcd\left(\frac{7}{2}-\frac{1}{2}\sqrt{41}+y, \frac{11}{2}-\frac{1}{2}\sqrt{41}+y^2+8y\right) \quad = \quad \frac{7}{2}-\frac{1}{2}\sqrt{41}+y, \end{aligned}$$

$$\begin{aligned} & mcd\left(f\left(\frac{1}{2}\sqrt{22+2\sqrt{41}}, y\right), g\left(\frac{1}{2}\sqrt{22+2\sqrt{41}}, y\right)\right) \\ = \quad & mcd\left(\frac{7}{2}+\frac{1}{2}\sqrt{41}+y, \frac{11}{2}+\frac{1}{2}\sqrt{41}+y^2+8y\right) \quad = \quad \frac{7}{2}+\frac{1}{2}\sqrt{41}+y, \end{aligned}$$

$$\begin{aligned} & mcd\left(f\left(-\frac{1}{2}\sqrt{22+2\sqrt{41}}, y\right), g\left(-\frac{1}{2}\sqrt{22+2\sqrt{41}}, y\right)\right) \\ = \quad & mcd\left(\frac{7}{2}+\frac{1}{2}\sqrt{41}+y, \frac{11}{2}+\frac{1}{2}\sqrt{41}+y^2+8y\right) \quad = \quad \frac{7}{2}+\frac{1}{2}\sqrt{41}+y, \end{aligned}$$

Notamos que el MCD entre una ecuación cuadrática y una lineal es, efectiva-

mente, la lineal y de allí las soluciones son:

$$\{\left(\frac{1}{2}\sqrt{22-2\sqrt{41}},-\frac{7}{2}+\frac{1}{2}\sqrt{41}\right);\left(-\frac{1}{2}\sqrt{22-2\sqrt{41}},-\frac{7}{2}+\frac{1}{2}\sqrt{41}\right);$$
$$\left(\frac{1}{2}\sqrt{22-2\sqrt{41}},-\frac{7}{2}-\frac{1}{2}\sqrt{41}\right);\left(-\frac{1}{2}\sqrt{22-2\sqrt{41}},-\frac{7}{2}-\frac{1}{2}\sqrt{41}\right)\}$$

4.3 Teorema de Bezout

La intersección de dos curvas planas se reduce al descubrimiento de raíces de polinomios univariados, lo que significa una tarea no muy extensa. Si m es el grado del polinomio f y n el grado del polinomio g y $mcd(f,g)=1$ en $F[x,y]$, entonces $X\cap Y$ tiene, en la mayoría de los casos, mn puntos. Este es el llamado teorema de Bezout por el geómetra francés Etienne Bezout. El cual es válido para variedades algebráicas arbitrarias, proveyó un conteo de puntos " en el infinito" y "puntos multiples y pomponentes" adecuadamente y todos los componentes de la intersección tienen la dimensión "correcta"
Si $mcd(f,g)=h$ para algún $h\in F[x,y]$ no constante, entonces todos los puntos de la curva $h=0$ pertenecen a $X\cap Y$, y la intersección es el infinito. Un ejemplo trivial es cuando $f=h=g$

Ejemplo 8. *Consideremos, ahora, dos curvas en el plano $X,Y\subseteq C^2$ dado por los polinomios f y g*

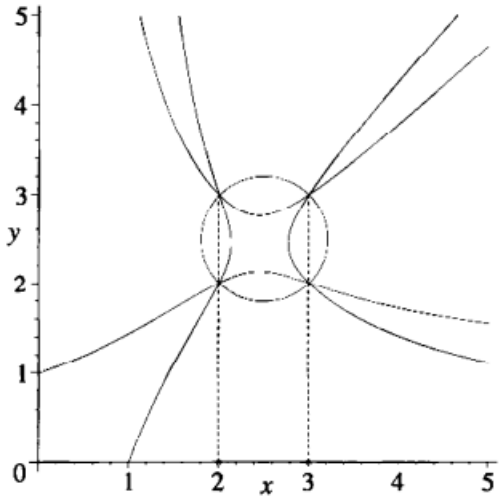
$$\begin{aligned} f =&(y^2+6)(x^2+1)-y(x^2+1)\\ g =&(x^2+6)(y^2+1)-x(y^2+1) \quad \in\mathbb{Z}[x,y]\end{aligned}$$

Para el simplificar el desarrollo de este ejemplo se utilizó un software matemático llamado MAPLE, de donde obtuvimos la siguiente resultante

$$\begin{aligned} res_y(f,g) = &\quad 2x^6-22x^5+102x^4-274x^3+488x^2-552x+188\\ = &\quad 2(x-2)^2(x-3)^2(x^2-x+4)\end{aligned}$$

Tiene las cuatro raíces distintas $\{2,3,(1\mp\sqrt{15i}/2\}$, donde $i=\sqrt{-1}$. Para cada uno de estos valores de x calculamos los valores correspondientes para y :

$$\begin{aligned} mcd(f(2,y),g(2,y)) = &\quad mcd(y^2-5y+6,-2y^2+10y-12)\\ = &\quad y^2-5y+6=(y-2)(y-3),\\ mcd((2,y),g(2,y)) = &\quad mcd(2y^2-10y+12,-3y^2+15y-18)\\ = &\quad y^2-5y+6=(y-2)(y-3)\end{aligned}$$



2.png

Figura 4.2: intersección de curvas planas

$$mcd\left(f\left(\frac{1\pm\sqrt{15}i}{2},y\right),g\left(\frac{1\pm\sqrt{15}i}{2},y\right)\right)=\left(y-\frac{1\mp\sqrt{15}i}{2}\right)$$

Así $X\cap Y$ consiste en los seis puntos

$$\left\{(2,2),(2,3),(3,2),(3,3),\left(\frac{1+\sqrt{15}i}{2},\frac{1-\sqrt{15}i}{2}\right),\left(\frac{1-\sqrt{15}i}{2},\frac{1+\sqrt{15}i}{2}\right)\right\}$$

Notamos que, solo los 4 puntos reales son visibles en la Figura 3.2. Mirando las ecuaciones, podemos observar que en $f+g$ los términos de grado 3 se anulan. El teorema de Bézout dice que $X\cap Y$ consiste en $3\cdot 3=9$ puntos, sin embargo, solo encontramos 6 de ellos en el cuerpo en el que trabajamos.
(ejemplo del libro "Modern Computer algebra"de von Zur Gathen)

4.4 Resolución de sistemas bivariados usando subresultante

En esta sección estaremos pensando en F como el cuerpo finito F_p.
Sean ahora f y g dos polinomios en $F[X,Y]$, y sean d_f = gr(f,Y) y d_g gr (g,Y), asumimos que $d_f>d_g$ (de no ser así, debemos cambiar los roles de estos polinomios). A tal sistema, asociamos la resultante y la subresultante de grado 1 de f y g con respecto a Y, escrito $R=res(f,g,Y)$ y $S=sres(f,g,Y)$.
Siguiendo la definición de Reischert, las combinaciones de filas elementales muestran que R está en $F[X]$ y S en F $[X,Y]$, de la forma $S=S_0(X)+S_1(X)Y$.

Los polinomios R y S serán nuestra herramienta básica para resolver el sistema $f = g = 0$. Cualquier solución de $f = g = 0$ es una solución de $R = S = 0$. Recíprocamente, cualquier solución (x, y) de $R = S = 0$, con además $S_1(x)$ distinto de 0 es una solución de $f = g = 0$.

(Para detalles, ver artículo "Journal of Symbolic Computation"[7])

Ejemplo 9. *Sean f y g dos polinomios bivariados sobre el cuerpo finito $GF(127)$*

$$f = x^2 + y^3 + 8y$$
$$g = x^2 + y^2 + 9$$

La resultante entre f y g, respecto a la variable Y, la podemos calcular rápidamente con la ayuda del software matemático MAGMA, del cual obtenemos.

$$\begin{aligned} R(f, g, y) &= x^6 + 12x^4 + 19x^2 + 9 \\ &= (x + 24)(x + 103)(x^4 + 80x^2 + 125) \end{aligned}$$

Notamos dos soluciones dentro de nuestro cuerpo en estudio: $x_1 = -24$ y $x_2 = -103$
La subresultante de grado 1 entre f y g viene dada por el siguiente polinomio

$$S(f, g, y) = (126x^2 + 126)y + x^2$$

Ahora, evaluando x_1 en el polinomio subresultante podemos obtener $y_1 = 47$. Por lo tanto una solución este sistema bivariado es $(-24, 47)$, (la cual podemos comprobar al reemplazar tanto en f como en g, obteniendo en ambas 0)

CAPÍTULO 5

Magma

La Resultante de ciertos polinomios puede conllevar un cálculo bastante extenso, sin embargo, la tecnología nos brinda un gran instrumento para agilizar este proceso. Para realizar algunos cálculos utilizamos Magma, un sistema de álgebra computacional.
En este capítulo mostraremos cómo el software magma puede ser usado para resolver algunos problemas de algebra abstracta.
Para una introducción general a magma puede consultar

http://magma.maths.usyd.edu.au/magma/.

Magma es un paquete que requiere un licencia para su uso. Aunque existe una versión online nosotros vamos a transcribir partes de una sesión de la versión de computador.

5.1 Ideas básicas

Para usar Magma:

1. Tipear un comando o expresión después del prompt >.
2. No olvidar colocar una semicolon (;) al final de la linea.
3. Luego, presionar la tecla enter .

Cargar un archivo

Existe la opción para cargar el contenido de un archivo en Magma. Para esto debe tipear el nombre del archivo

```
> load "nombrearchivo''
```

Cabe mencionar que esta función no está disponible para la versión online

Para nombrar algún elemento debemos definir un nombre seguido de dos puntos (:) y el signo es igual (=) y luego el comando correspondiente.

5.2 Aritmética

```
> 3+5;
8
> 5-3;
2
> 2*3;
6
```

El máximo común divisor ente "a" y "b"se puede calcular a través del comando "GCD(a,b)"

```
> GCD(124,345)
1
```

5.3 Polinomios

Ingresar polinomio

```
> p<x>:= PolynomialRing(IntegerRing());
> p;
Univariate Polynomial Ring in x over Integer Ring
```

Para introducir un polinomio debemos definir un nombre para cada uno y luego ingresarlo, debemos detacar que si queremos ingresar un número junto a una incognita se hace necesario ingresar el simbolo de multiplicación (*)

```
> f:=x^4+3*x^3-7*x^2;
> g:=x^3-3*x^2+1;
> GCD(f,g)
1
```

Factorización

Para factorizar un polinomio, debemos tener este definido y con su respectivo nombre, luego ingresar el comando (Factorization) entre paréntesis el nombre del polinomio

```
> Factorization(f)
```

```
< x,2 >
< x^2 + 3x - 7, 1 >
```

Donde el o los elementos antes de la coma representan el polinomio y el número después de la coma representa al exponente de este, por lo tanto el polinomio factorizado corresponde a

$$x^2(x^2 - 3x - 7)$$

5.4 Matrices

Para introducir una matriz debemos ingresar su comando (Matrix), luego abrir paréntesis (( )y escribir el cuerpo en el cual se desea trabajar los elementos de la matriz, continuando con una coma (,) para señalar el orden de la matriz y luego abrir corchetes ([) para escribir los elementos de esta separados por comas, finalizamos cerrando los paréntesis correspondientes( ]))

```
> M:=Matrix(RationalField(),3,[1,2,3,4,5,6,7,8,9]);
M;
[1 2 3]
[4 5 6]
[7 8 9]

> N:=Matrix(RationalField(),4,[1,2,5,4,6,7,9,7,2,3,5,6,5,6,7,5]);
N;
[1 2 5 4]
[6 7 9 7]
[2 3 5 6]
[5 6 7 5]
```

Donde M es una matriz de orden 3 y N de orden 4, sin embargo el número de filas está definido por la cantidad de elementos que ingresemos a ella.

Determinante

Para calcular el determinante de una matriz, debemos tener esta definida y nombrada, luego ingresar el comando (Determinant) y entre paréntesis el nombre de la matriz

```
> Determinante(M);
0
```

```
> Determinante(N);
-14
```

5.5 Resultante

La resultante

Magma nos ofrece una función directa para calcular la resultante de dos polinomios. Para ello debemos definir el cuerpo en el que viven los elementos, el anillo de polinomios y los polinomios en cuestión.
Una vez definidos ingresamos el comando (Resultant) y entre paréntesis el nombre de los polinomios en juego y la variable sobre la cual queremos la resultante.

```
> C:=Rationals();
> P<x,y>:=PolynomialRing(C,2);
> f:=x^2+y^2-1;
> g:=3*x+4*y;
> R:=Resultant(f,g,y);
> R;
25*x^2 - 16
```

Al tener la resultante podemos además obtener las raices de esta, con la función (Roots(UnivariatePolynomial)) y entre parenetesis, el nombre de la resultante.

```
> r:=Roots(UnivariatePolynomial(R));
> r;
[ <-4/5, 1>, <4/5, 1>]
```

Para encontrar finalmente las soluciones de esta, debemos evaluar cada solución en ambos polinomios y obtener el máximo común divisor entre ellas.

```
> r1:=C!r[1][1];
> f1:=UnivariatePolynomial(Evaluate(f,x,r1));
> g1:=UnivariatePolynomial(Evaluate(g,x,r1));
> G<x>:=Gcd(f1,g1);
> G;
x - 3/5
```

Matriz de sylvester

Magma no posee una función para calcular directamente la matriz de Sylvester, es por esto que nosotros hemos creado una función para poder calcular

esta matriz para nuestros ejemplos.
Dado un anillo de polinomios P, f, g polinomios y x la variable en la cual queremos calcular la matriz, definimos lo siguiente:

```
> SylvesterMatrix:=function(f,g,x);
m:=Degree(f,x);
n:=Degree(g,x);
M:=MatrixRing(P,m+n);
S:=Matrix(P,m+n,m+n,[]);
for j:=1 to n do
for i:=1 to (m+1) do S[j][i+j-1]:=Coefficient(f,x,m+1-i);
end for;
end for;
for j:=(n+1) to (n+m) do
for i:=1 to (n+1) do S[j][i+j-(n+1)]:=Coefficient(g,x,n+1-i);
end for;
end for;
return M!Transpose(S);
end function;
```

Para utilizar esta función debemos definir al comienzo el cuerpo en el que deseamos trabajar, debemos especificar la cantidad de variables y los polinomios a quien le deseamos calcular la matriz. Al final insertar el comando recien definido “Sylvestermatrix” y entre paréntesis los polinomios anteriormente definidos y la variable sobre la que queremos la matriz.

```
> P<x,y>:=PolynomialRing(Rationals(),2);
f:=x^2+y-2;
g:=x^2+y^2+8*y;
 > SylvesterMatrix:=function(f,g,x);
m:=Degree(f,x);
n:=Degree(g,x);
M:=MatrixRing(P,m+n);
S:=Matrix(P,m+n,m+n,[]);
for j:=1 to n do
for i:=1 to (m+1) do
S[j][i+j-1]:=Coefficient(f,x,m+1-i);
end for;
end for;
```

```
for j:=(n+1) to (n+m) do
for i:=1 to (n+1) do
S[j][i+j-(n+1)]:=Coefficient(g,x,n+1-i);
end for;
end for;
return M!S;
end function;
 > S:=SylvesterMatrix(f,g,y);
 > S;

[1              0      1]
[x^2 - 2        1      8]
[0          x^2-2    x^2]
```

Para encontrar la resultante a través de la matriz de Sylvester solo debemos calcular el deteminante de esta.

```
> Determinant(S);
x^4 - 11*x^2 + 20
```

Para calcular matrices con una sola variable solo falta modificar la función eliminando la variable sobre la cual se desea el resultado, pues solo será una.

```
> SylvesterMatrixUnivariado:=function(F,p,q);
m:=Degree(p);
n:=Degree(q);
M:=MatrixRing(F,m+n);
S:=Matrix(F,m+n,m+n,[]);
for j:=1 to n do
for i:=1 to (m+1) do
S[j][i+j-1]:=Coefficient(p,m+1-i);
end for;
end for;
for j:=(n+1) to (n+m) do
for i:=1 to (n+1) do
S[j][i+j-(n+1)]:=Coefficient(q,n+1-i);
end for;
end for;
return M!Transpose(S);
```

```
end function;
```

Y luego definir el cuerpo y los polinomios sobre los cuales trabajaremos.

```
> P<x>:=PolynomialRing(Rationals());
> f:=824*x^5 - 65*x^4 - 814*x^3 - 741*x^2 - 979*x - 764;
> g:=216*x^4 + 663*x^3 + 880*x^2 + 916*x + 617;
>  S:=SylvesterMatrixUnivariado(Rationals(),f,g);
> S;

[ 824     0     0     0     216       0      0     0       0]
[ -65   824     0     0     663     216      0     0       0]
[-814   -65   824     0     880     663    216     0       0]
[-741   -814  -65    824   916     880    663     216     0]
[-979   -741  -814  -65    617     916    880     663   216]
[-764   -979  -741  -814    0      617    916     880   663]
[ 0     -764  -979  -741    0       0     617     916   880]
[ 0       0   -764  -979    0       0      0      617   916]
[ 0      0     0    -764    0       0      0      0     617]
```

La subresultante

Para calcular la subresultante de dos polinomios, necesitamos tener definida la matriz de Sylvester de estos y luego ingresar el comando "Submatrix" y entre paréntesis nombrar la matriz que ultilizaremos, luego las filas y las columnas que deseamos dejar ambas entre corchetes [].(Si las filas o columnas que deseamos dejar son correlativas basta colocar el número de la primera, seguido de dos puntos y la última que necesitemos. Al no ser correlativos debemos mencionarlas todas)

```
> Submatrix(S,[1..7], [1,2,3,5,6,7,8])

[ 824     0     0     216       0      0       0]
[ -65   824     0     663     216      0       0]
[-814   -65   824     880     663    216       0]
[-741   -814  -65     916     880    663     216]
[-979   -741  -814   617     916    880     663]
[-764   -979  -741     0      617    916     880]
[ 0     -764  -979    0       0     617     916]
```

POLINOMIO SUBRESULTANTE

Para calcular el polinomio subresultante basta con tener las subresultantes necesarias y calcularlo a través de los determinantes es estas.
Teniendo definida la función de la matriz de Sylvester podemos calcular lo siguiente

```
> P<x>:=PolynomialRing(Rationals());
f:=x^2+3*x-5;
g:=x^3-2*x^2+7*x-8;
S:=SylvesterMatrixUnivariado(Rationals(),f,g);
M01:=Submatrix(S,[1,2,4],[1,2,4]);
M11:=Submatrix(S,[1,2,3],[1,2,4]);
M01;
M11;
Determinant(M01)+Determinant(M11)*x;
[ 1  0  1]
[ 3  1 -2]
[ 0 -5 -8]
[ 1  0  1]
[ 3  1 -2]
[-5  3  7]
27*x - 33
```

Bibliografía

[1] Bosma, W., Cannon, J. y Playoust, C. (1997), *The Magma Algebra system. I. The use lenguage*. Journal of Symbolic Computation (24).

[2] Boyer, C. (1986). *Historia de la matemática* .

[3] Cox, D., Little, J. y O'Shea, D., *Ideals, Varieties, and Algorithms.*

[4] Fraleigh, J. B. (1988). *Álgebra Abstracta*. Editorial Addison-Wesley Iberoamericana.

[5] Gathen, J. y Gerhard, J. (2012). *Modern Computer algebra.*

[6] Gathen, J. y Lücking, T. (2003) *Subresultants revisited.*

[7] Gaudry, P.y Schost, E. (2012). *Journal of Symbolic Computation.*

[8] Kleiner, I. (2007). *A History of Abstract Algebra.*

[9] Krick, T. (2015). *Resultante, subresultantes y sumas de Sylvester* .

[10] Vainsensher, I. (2017). *Curvas Algébricas planas* .

[11] Washington, L. C. (2008). *Elliptic curves, number theory and cryptography* Second edition. CRC press.