ALGUNAS APLICACIONES DEL TEOREMA DE LOS CEROS DE HILBERT

DAYRA DEL ROSARIO CÓRDOBA MOLINA

SAMITH TATIANA VEGA AGREDO

Universidad del Cauca

Facultad de Ciencias Naturales, Exáctas y de la Educación

Departamento de Matemáticas

Popayán

Julio, 2009

ALGUNAS APLICACIONES DEL TEOREMA DE LOS CEROS DE HILBERT

DAYRA DEL ROSARIO CÓRDOBA MOLINA

SAMITH TATIANA VEGA AGREDO

Trabajo de grado presentado como requisito
parcial para optar al título de Matemático

CARLOS ALBERTO TRUJILLO SOLARTE
Director

Universidad del Cauca
Facultad de Ciencias Naturales, Exáctas y de la Educación
Departamento de Matemáticas
Popayán
Julio, 2009

Nota de Aceptación

_____

_____

_____

_____

Dr. Carlos Alberto Trujillo Solarte
Director

_____

Mg. Maribel Díaz Noguera
Comite de seguimiento

_____

Profesor. Wilson Martínez Flor
Comite de seguimiento

Popayán, 8 de Julio, 2009

A Dios por ser nuestra fortaleza e inspiración
para culminar esta etapa en nuestras vidas.

Agradecimientos

Agradecemos a nuestros padres por habernos apoyado durante esta etapa de nuestras vidas ya que con su cariño, concejos y enseñanzas nos motivaron para llegar a ser verdaderos profesionales. A nuestros hermanos y familia por habernos acompañado en este camino y brindarnos su apoyo incondicional.

A nuestro director Carlos Alberto Trujillo Solarte porque con su motivación y conocimiento siempre ha sido la razón para querer aprender más y tener una buena formación académica y profesional. Por su amistad y por su colaboración durante el desarrollo y la culminación del presente trabajo de grado.
A la profesora Maribel Díaz y al profesor Wilson Martínez por formar parte del comité de seguimiento, por otorgarnos un espacio para presentar los avances del trabajo y por sus valiosos aportes.
A los integrantes del grupo "Álgebra Teoría de Números y Aplicaciones E.R.M,"por habernos brindado su amistad, apoyo y conocimientos para nuestro aprendizaje.

A nuestros novios por su amor, compañía y por su constante motivación, a nuestros compañeros por que más que compañeros son nuestros amigos, a ellos queremos decirles gracias por su colaboración y por haber hecho parte de nuestras vidas en estos años y a nuestros amigos por su amistad incondicional.

DAYRA DEL ROSARIO CÓRDOBA MOLINA
SAMITH TATIANA VEGA AGREDO

Universidad del Cauca
8 de Julio, 2009

Índice general

Introducción

Muchos problemas en teoría de números aditiva se estudian en un grupo ambiente G, y se basan fundamentalmente en la estructura aditiva de G. Sin embargo, en muchos casos el grupo ambiente es un campo F, y en tal caso se cuenta con funciones especiales, en particular con polinomios sobre F. En años recientes se han logrado resolver problemas antiguos utilizando métodos algebraicos, en particular es útil la relación entre el número de raíces de polinomios y grado de los mismos.

En 1995 y 1996 Noga Alon en [1] describe una técnica algebraica denominada Combinatorial Nullstellensatz o teoremas combinatorios de los ceros de Hilbert para obtener resultados en Teoría de Números Aditiva, en Combinatoria y en Teoría de Grafos. En este trabajo pretendemos dar a conocer en que consiste esta técnica y describir algunas aplicaciones de la misma.

En cualquier campo el número de raíces de un polinomio no cero no puede exceder el grado del polinomio, una extensión a polinomios de varias variables, respecto al grado del polinomio en cada variable x_i, de este resultado es:

1. Sea $P = P(x_1, \ldots, x_n)$ un polinomio en n variables $x_1, \ldots, x_n$ sobre un campo arbitrario F, supongamos que para todo $i = 1, \ldots, n$, el grado de P como un polinomio en x_i es a lo más t_i y S_i es un subconjunto de F de cardinalidad al menos $t_i + 1$. Si $P(s_1, \ldots, s_n) = 0$ para toda n-tupla $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, entonces P es el polinomio cero.

Este hecho nos permite probar el siguiente resultado:

2. Sean F un campo arbitrario, $f = f(x_1, \ldots, x_n)$ un polinomio en $F[x_1, \ldots, x_n]$, $S_1, \ldots, S_n$ subconjuntos no vacíos de F y

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s), \text{ para todo } i = 1, \ldots, n.$$

Si f se anula sobre todos los ceros de $g_1, \ldots, g_n$, esto es, si $f(s_1, \ldots, s_n) = 0$ para toda n-tupla $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, entonces existen polinomios $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ con $grad(h_i) \leq grad(f) - grad(g_i)$ y tales que

$$f = \sum_{i=1}^{n} h_i g_i.$$

Los dos resultados anteriores son fundamentales para la prueba del siguiente enunciado:

3. Sean F un campo arbitrario y $f = f(x_1, \ldots, x_n)$ un polinomio en $F[x_1, \ldots, x_n]$. Si $grad(f) = \sum_{i=1}^{n} t_i$, donde cada t_i es un entero no negativo, si el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ en f es no cero, y si $S_1, \ldots, S_n$ son subconjuntos de F con $\mid S_i \mid > t_i$, entonces existen $s_1 \in S_1, \ldots, s_n \in S_n$ tales que

$$f(s_1, \ldots, s_n) \neq 0.$$

Los resultados enunciados anteriormente se conocen como Combinatorial Nullstellensatz o Teoremas de los ceros de Hilbert, los cuales determinan una técnica para el estudio de algunos problemas combinatorios.

Este último resultado es la base fundamental para el desarrollo de nuestro trabajo y tiene diversas aplicaciones en Teoría de Números Aditiva, en Combinatoria y en Teoría de Grafos.

En este trabajo consignamos los Teoremas denominados los ceros de Hilbert y algunas de sus aplicaciones, el cual esta organizado en cuatro capítulos.

El primer capítulo constituido por fundamentos sobre polinomios que contiene definiciones y resultados básicos para el desarrollo de este trabajo, además los Teoremas denominados los ceros de Hilbert que corresponden a los resultados 1, 2 y 3. Presentamos también dos aplicaciones de estos; la primera corresponde al Teorema de Chevalley-Warning, el cual trata sobre raíces de sistemas de polinomios con coeficientes en campos finitos y la segunda corresponde al Teorema de Cauchy-Davenport, el cual trata sobre adición de clases residuales.

En el segundo capítulo presentamos dos aplicaciones del resultado 3, la primera de ellas denominada El Método Polinomial el cual es una herramienta muy utilizada en el estudio de problemas que tienen que ver con el cardinal de conjuntos suma con restricciones y la segunda en Conjuntos Suma en Espacios Vectoriales sobre Campos Primos.

En el tercer capitulo consignamos conceptos y resultados básicos sobre Teoría de Grafos y dos aplicaciones del resultado 3. La primera trata sobre la existencia de un grafo p-regular, es decir que todos sus vértices tienen grado p. La segunda corresponde a un resultado geométrico.

En el cuarto capítulo escribimos algunas conclusiones de nuestro trabajo.

El desarrollo del trabajo se realizó como requisito parcial para optar al título de Matemático bajo la asesoría del profesor Carlos Alberto Trujillo Solarte.

Capítulo 1

Teoremas Básicos

La finalidad de este capítulo es presentar los conceptos básicos de la teoría de polinomios, mostrar en que consiste la técnica algebraica denominada los teoremas de los ceros de Hilbert y describir dos aplicaciones de la misma.

1.1. Preliminares

En álgebra elemental consideramos un polinomio sobre un anillo R como una expresión de la forma $a_0 + a_1x + \cdots + a_nx^n$, donde n es un entero no negativo y los a_i son elementos de un anillo R y usualmente son números reales o complejos; x es variable: esto es, cuando se substituye x por un elemento arbitrario $\alpha \in R$, se obtiene un elemento bien definido $a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R$.

El concepto de polinomio y las operaciones asociadas pueden generalizarse a una escena algebraica formal de manera directa.

Definición 1.1 *Sea R un anillo arbitrario. Un polinomio sobre R es una expresión de la forma*

$$f := f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1x + \cdots + a_nx^n,$$

donde n es un entero no negativo.

a. *Los elementos $a_i \in R$, para todo $0 \leq i \leq n$ y se llaman coeficientes de f y x es un símbolo que no pertenece a R, llamado una indeterminada sobre R.*

b. *Si $a_n \neq 0$ se dice que f tiene grado n y se denota por $grad(f) = n$; a_n se llama el coeficiente principal de f y a_nx^n el término principal de f. Por convenio definimos*

el grado del polinomio nulo (con todos los coeficientes cero) como $-\infty$.

c. *Los polinomios de grado* ≤ 0 *se llaman polinomios constantes.*

d. *Si* R *tiene identidad 1 y el coeficiente principal de* f *es 1, entonces* f *se llama un polinomio mónico.*

e. *Un elemento* $a \in R$ *se llama una raíz (o un cero) del polinomio* f *si y sólo si* $f(a) = 0$.

Adoptamos el convenio que:

- $0x^n = 0$
- $ax^n + 0 = ax^n$, $a \neq 0$

En particular, el polinomio $f(x)$ anterior puede entonces ser dado por la forma equivalente $f(x) = a_0 + a_1x + \ldots + a_nx^n + 0x^{n+1} + \ldots + 0x^{n+h}$; donde h es algún entero positivo. Por lo tanto, cuando comparamos dos polinomios $f(x)$ y $g(x)$ sobre R, es posible asumir que ambos involucran las mismas potencias de x.

Definición 1.2 *Sean*

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

polinomios sobre R. *Los polinomios* $f(x)$ *y* $g(x)$ *son iguales sí y sólo si* $a_i = b_i$ *para todo* $0 \leq i \leq n$.

Definimos la suma de $f(x)$ *y* $g(x)$ *como*

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

Para definir el producto de dos polinomios sobre R, *sean*

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{m} b_j x^j.$$

Así

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ donde } c_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq n;\, 0 \leq j \leq m}} a_i b_j.$$

Notemos que el conjunto de polinomios sobre R con las operaciones anteriores forma un anillo.

Definición 1.3 *El anillo formado por los polinomios sobre R con las operaciones anteriores se llama el anillo polinomial sobre R y se denota mediante $R[x]$.*

El elemento cero de $R[x]$ es el polinomio cuyos coeficientes son todos 0. Este polinomio se llama el *polinomio cero* y se denota mediante 0. En el contexto debe ser claro que 0 se establece para el elemento cero de R o para el polinomio cero.

El siguiente Teorema determina una cota superior para el grado de suma y producto de polinomios.

Teorema 1.1 ([2])*Sean R un anillo y $f, g \in R[x]$. Entonces*

$$grad(f+g) \leq \text{máx}\{grad(f), grad(g)\},$$

$$grad(fg) \leq grad(f) + grad(g).$$

Si R es un dominio entero, tenemos que

$$grad(fg) = grad(f) + grad(g).$$

En adelante, F denotará un campo arbitrario, p denotará un número primo, F_p denotará el campo de clases residuales módulo p y $F[x]$ denotará el anillo de polinomios en x sobre F.

El concepto de divisibilidad cuando se especializa el anillo $F[x]$, conduce a lo siguiente.

Definición 1.4 *Sea F un campo. Un polinomio $g \in F[x]$ divide al polinomio $f \in F[x]$ en F si existe un polinomio $h \in F[x]$ tal que $f = gh$. También decimos que g es un divisor de f, o que f es un múltiplo de g, o que f es divisible por g, o que g es un factor de f.*

Las unidades de $F[x]$ son los divisores del polinomio constante 1, que son precisamente todos los polinomios constantes no cero.

Por otra parte, dados los polinomios f y g en $F[x]$ no siempre tendremos que g es divisor de f, sin embargo tenemos una relación entre estos, conocida como el algoritmo de la división.

Teorema 1.2 (Algoritmo de la división) *Sean F un campo y g un polinomio no cero en $F[x]$. Entonces todo $f \in F[x]$ puede escribirse como:*

$$f = gq + r,$$

donde $q, r \in F[x]$ y $grad(r) < grad(g)$. Además q y r son únicos.

De esta forma cada raíz a de un polinomio f determina un factor lineal de este, lo cual es consecuencia directa del algoritmo de la división.

Teorema 1.3 (Teorema del factor) *Sea F un campo. Un elemento $a \in F$ es una raíz del polinomio $f \in F[x]$ si y sólo si $x - a$ divide a f en $F[x]$.*

Prueba. Supongamos que para $a \in F$ tenemos que $f(a) = 0$. Por el algoritmo de la división existen $q(x), r(x) \in F[x]$ tales que:

$$f(x) = (x - a)q(x) + r(x),$$

donde el grado de $r(x)$ es menor que 1. Entonces debemos tener $r(x) = c$ para $c \in F$, así:

$$f(x) = (x - a)q(x) + c,$$

luego como a es raíz de f, tenemos

$$0 = f(a) = (a - a)q(a) + c.$$

De modo que $c = 0$. Entonces $f(x) = (x - a)q(x)$, así $(x - a)$ divide a $f(x)$.

Recíprocamente, si $(x - a)$ divide a $f(x)$ en $F[x]$, donde $a \in F$, entonces tenemos que

$$f(x) = (x - a)q(x),\ q(x) \in F[x]$$

y

$$f(a) = (a - a)q(a) = 0.$$

Así $f(a) = 0$, es decir a es un cero de $f \in F[x]$. $\square$

Ahora definimos los polinomios en varias variables que es el tema a estudiar.

Definición 1.5 *Un monomio en las indeterminadas $x_1, \ldots, x_n$ es un producto de la forma*

$$x_1^{t_1} \cdot x_2^{t_2} \cdots x_n^{t_n} = \prod_{i=1}^{n} x_i^{t_i},$$

donde todos los exponentes $t_1, \ldots, t_n$ son enteros no negativos. El grado total de este monomio es la suma $\sum_{i=1}^{n} t_i = t_1 + t_2 + \ldots + t_n$.

Con esto definimos un polinomio f en las indeterminadas $x_1, \ldots, x_n$ con coeficientes en F como una combinación lineal finita de monomios sobre el campo F.

Así, denotando $x^t = \prod_{i=1}^{n} x_i^{t_i}$ con $t = (t_1, \ldots, t_n)$, podemos escribir el polinomio f en la forma

$$f = \sum_t a_t x^t,$$

$a_t \in F$, donde la suma es sobre un número finito de n-tuplas $t = (t_1, \ldots, t_n)$.
Cuando $t = (0, \ldots, 0)$, tenemos que $x^t = 1$.

Finalmente definimos el grado total de un polinomio según el grado total de los monomios que lo conforman.

Definición 1.6 *Sea $f = \sum_t a_t x^t$, un polinomio en $F[x_1, \ldots, x_n]$.*

1. *Llamamos a_t el coeficiente del monomio x^t.*
2. *El grado total de f, denotado $grad(f)$, es el máximo de los grados totales de los monomios x^t cuyo coeficiente a_t es no cero.*

En forma análoga a polinomios en una variable, el siguiente lema determina el grado total de suma y producto de polinomios en varias variables.

Lema 1.1 *Sean $f, g \in F[x_1, \ldots, x_n]$. Entonces*

$$grad(f + g) \leq \text{máx}\{grad(f), grad(g)\},$$

$$grad(fg) = grad(f) + grad(g).$$

Del álgebra de polinomios en una variable sobre un campo es bien conocido que un polinomio no cero no puede tener un número de raíces mayor que su grado, de manera más precisa tenemos el siguiente resultado.

Teorema 1.4 *Un polinomio $f(x)$ no cero en $F[x]$ con coeficientes en un campo F y grado $n \geq 0$ tiene a lo más n ceros en F. Equivalentemente puede enunciarse como: Si $f(x)$ es un polinomio no cero de grado $n \geq 0$ en $F[x]$ y $f(s) = 0$, para todo $s \in S \subset F$, con $\mid S \mid > n$, entonces f es el polinomio cero.*

Prueba. Aplicamos inducción matemática sobre el grado de f.

Sean $f(x)$ un polinomio no cero en $F[x]$ y $grad(f) = n$.

- Cuando $n = 0$, f es un polinomio constante no nulo, el cual no tiene raíces. Así se garantiza la veracidad del teorema.
- Asumamos que el enunciado es cierto para todo polinomio no cero en $F[x]$ de grado $n - 1 \geq 0$, es decir todo polinomio no cero de grado $n - 1$ tiene a lo más $n - 1$ raíces.

Sea f un polinomio no cero de grado n y consideremos los siguientes casos:

Caso 1. Si f no tiene raíces en F, entonces no hay nada que probar.

Caso 2. Si f tiene raíces en F.

Supongamos que a es una raíz de f en F, por Teorema 1.3 tenemos que:

$$f(x) = q(x)(x - a),$$

donde $q \in F[x]$.

Notemos que $x - a$ tiene grado 1 y q tiene grado $n - 1$. Por hipótesis inductiva, q tiene a lo más $n - 1$ raíces en F, entonces f tiene a lo más n raíces en F. □

De forma equivalente tenemos el siguiente teorema el cual estima la cardinalidad de un conjunto, que contiene los ceros de un polinomio, mediante su grado.

Teorema 1.5 *Sea $f \in F[x]$ un polinomio no cero de grado n, en una variable sobre un campo F (así el coeficiente de x^n en f es no nulo) y sea S un subconjunto de F tal que $\mid S \mid > n$. Entonces existe $s \in S$ tal que $f(s) \neq 0$.*

En otras palabras, si un polinomio no cero de grado n se anula en todo elemento de S entonces $\mid S \mid \leq n$, dando un sentido combinatorio a un resultado algebraico.

Prueba. Argumentamos por contradicción.

Sean $f(x)$ un polinomio no cero en $F[x]$ y $grad(f) = n$.

Supongamos que S es un subconjunto de F con $\mid S \mid > n$ y para todo $s \in S$ se tiene que $f(s) = 0$, esto es; S está contenido en el conjunto de raíces de f.
Así el número de raíces de f es mayor que n, lo cual contradice el Teorema 1.4. Por lo tanto existe $s \in S$ tal que $f(s) \neq 0$. $\square$

Las extensiones de estos teoremas a varias variables se enuncian a continuación y son el pilar de la técnica algebraica que estudiaremos.

1.2. Los teoremas básicos denominados los ceros de Hilbert

En cualquier campo el número de raíces de un polinomio no cero no puede exceder el grado del polinomio, una extensión del Teorema 1.4 a polinomios de varias variables, respecto al grado del polinomio en cada variable x_i, es dado a continuación.

Teorema 1.6 *Sea $P = P(x_1, \ldots, x_n)$ un polinomio en n variables $x_1, \ldots, x_n$ sobre un campo arbitrario F, supongamos que para todo $i = 1, \ldots, n$, el grado de P como un polinomio en x_i es a lo más t_i y S_i es un subconjunto de F de cardinalidad al menos $t_i + 1$. Si $P(s_1, \ldots, s_n) = 0$ para toda n-tupla $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, entonces P es el polinomio cero.*

Prueba. Aplicamos inducción sobre el número de variables n.

- Para $n = 1$, tenemos que $P = P(x_1)$ es un polinomio en x_1 de grado a lo sumo t_1 y $S_1 \subset F$ tal que $\mid S_1 \mid \geq t_1 + 1$, luego como $P(s_1) = 0$ para todo $s_1 \in S_1$, entonces P tiene por lo menos $t_1 + 1$ raíces y por lo tanto P es el polinomio cero.

- Supongamos que el enunciado se cumple para polinomios en $n - 1$ variables, esto es, si $P(s_1, \ldots, s_{n-1}) = 0$ para toda $(n-1)$-tupla $(s_1, \ldots, s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, entonces P es el polinomio cero.

Probemos que la afirmación se cumple para polinomios en n variables.

Dado el polinomio $P = P(x_1, \ldots, x_n)$ y conjuntos $S_1, \ldots, S_n$ que satisfacen las hipótesis del teorema, escribamos P como un polinomio en la variable x_n, así:

$$P = \sum_{i=0}^{t_n} P_i(x_1, \ldots, x_{n-1}) x_n^i,$$

donde cada $P_i(x_1, \ldots, x_{n-1})$ es un polinomio en $n-1$ variables $x_1, \ldots, x_{n-1}$ y de grado a lo más t_j en cada variable x_j, para $1 \leq j \leq n-1$. Fijando la $(n-1)$-tupla $(s_1, \ldots, s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, el polinomio

$$Q(x_n) = P(s_1, \ldots, s_{n-1}, x_n) = \sum_{i=0}^{t_n} P_i(s_1, \ldots, s_{n-1}) x_n^i,$$

tiene grado a lo más t_n en x_n y es tal que:

$$Q(s_n) = P(s_1, \ldots, s_{n-1}, s_n) = 0, \text{ para todo } s_n \in S_n.$$

Como $Q(x_n)$ tiene a lo más t_n raíces y $\mid S_n \mid \geq t_n + 1$, entonces $Q(x_n)$ es el polinomio cero, y así

$$P_i(s_1, \ldots, s_{n-1}) = 0, \text{ para todo } (s_1, \ldots, s_{n-1}) \in S_1 \times \cdots \times S_{n-1}.$$

Luego de la hipótesis de inducción tenemos que:

$$P_i(x_1, \ldots, x_{n-1}) \text{ es el polinomio cero para todo } i.$$

Por lo tanto, P es el polinomio cero. □

Para dar una generalización de Teorema 1.5, necesitamos de un paso intermedio que es el Teorema 1.7, para ello se recurre a resultados de la Geometría algebraica, como es el Teorema de los ceros de Hilbert que afirma: si F es un campo algebraicamente cerrado y $f, g_1, \ldots, g_m$ son polinomios en el anillo $F[x_1, \ldots, x_n]$, tales que f se anula sobre todos los ceros de $g_1, \ldots, g_m$, entonces existe un entero k y existen polinomios $h_1, \ldots, h_m$ en $F[x_1, \ldots, x_n]$ tal que:

$$f^k = \sum_{i=1}^{m} h_i g_i.$$

En el caso especial $m = n$, donde cada g_i es un polinomio en una variable de la forma $\prod_{s \in S_i} (x_i - s)$, es válida una conclusión más fuerte que enunciamos a continuación.

Teorema 1.7 *Sean F un campo arbitrario, $f = f(x_1, \ldots, x_n)$ un polinomio en $F[x_1, \ldots, x_n]$, $S_1, \ldots, S_n$ subconjuntos no vacíos de F y*

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s), \text{ para cada } i = 1, \ldots, n.$$

Si f se anula sobre todos los ceros de $g_1, \ldots, g_n$, esto es, si $f(s_1, \ldots, s_n) = 0$ para toda n-tupla $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, entonces existen polinomios $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ con $grad(h_i) \leq grad(f) - grad(g_i)$ y tales que

$$f = \sum_{i=1}^{n} h_i g_i.$$

Prueba. Definamos $t_i = \mid S_i \mid -1$ para todo i. Por hipótesis tenemos que:

$$f(s_1, \ldots, s_n) = 0, \text{ para toda } n\text{-tupla } (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n \tag{1.1}$$

y

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s);$$

expandiendo la productoria se tiene que:

$$g_i(x_i) = x_i^{t_i+1} - \alpha_i(x_i),$$

donde $\alpha_i(x_i)$ es el polinomio restante con términos de grado $\leq t_i$. Así;

$$x_i^{t_i+1} = g_i(x_i) + \alpha_i(x_i). \tag{1.2}$$

Escribamos f como una combinación lineal de monomios y sustituyamos cada $x_i^{k_i}$, donde $k_i > t_i, 1 \leq i \leq n$, usando la relación (1.2) repetidamente.

Organizando términos respecto a los g_i, $1 \leq i \leq n$ tenemos que:

$$\begin{aligned} f(x_1, \ldots, x_n) \;=\; & h_1(x_1, \ldots, x_n) g_1(x_1) + h_2(x_1, \ldots, x_n) g_2(x_2) + \cdots \\ & + h_n(x_1, \ldots, x_n) g_n(x_n) + \bar{f}(x_1, \ldots, x_n), \end{aligned} \tag{1.3}$$

donde $\bar{f}$ resulta directamente de sustituir repetidamente $x_i^{k_i}$ por $\alpha_i(x_i)$ en f, $1 \leq i \leq n$, donde $k_i > t_i$, el cual tiene grado a lo sumo t_i en x_i para $1 \leq i \leq n$.

Así, si $(s_1, \ldots, s_n) \in (S_1 \times \cdots \times S_n)$ de (1.3) se sigue que:

$$f(s_1, \ldots, s_n) = h_1(s_1, \ldots, s_n) g_1(s_1) + \cdots + h_n(s_1, \ldots, s_n) g_n(s_n) + \bar{f}(s_1, \ldots, s_n).$$

Como $s_i \in S_i$, entonces $g_i(s_i) = 0$ para $1 \leq i \leq n$. Entonces

$$f(s_1, \ldots, s_n) = \bar{f}(s_1, \ldots, s_n), \text{ para toda } n\text{-tupla } (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$$

por lo tanto por (1.1),

$$\bar{f}(s_1, \ldots, s_n) = 0, \text{ , para toda } n\text{-tupla } (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$$

y por Teorema 1.6, $\bar{f}$ es el polinomio cero, puesto que $\bar{f}$ tiene grado $\leq t_i$ en cada x_i y $\mid S_i \mid = t_i + 1$ que son las hipótesis del teorema. Esto implica que

$$f(x_1, \ldots, x_n) = h_1(x_1, \ldots, x_n)g_1(x_1) + \cdots + h_n(x_1, \ldots, x_n)g_n(x_n),$$

esto es

$$f = \sum_{i=1}^{n} h_i g_i.$$

Además, del Lema 1.1

$$\begin{aligned} grad(f) &= \text{máx}\{grad(h_i g_i) : i = 1, 2, \ldots, n\} \\ &\geq grad(h_i g_i) \\ &= grad(h_i) + grad(g_i), \end{aligned}$$

de donde $grad(h_i) \leq grad(f) - grad(g_i)$, lo cual completa la prueba.□.

Así, de los Teoremas 1.6 y 1.7 se tiene finalmente la generalización del Teorema 1.5.

Teorema 1.8 *Sean F un campo arbitrario y $f = f(x_1, \ldots, x_n)$ un polinomio en $F[x_1, \ldots, x_n]$. Si $grad(f) = \sum_{i=1}^{n} t_i$, donde cada t_i es un entero no negativo, si el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ en f es no cero, y si $S_1, \ldots, S_n$ son subconjuntos de F con $\mid S_i \mid > t_i$, entonces existen $s_1 \in S_1, \ldots, s_n \in S_n$ tales que*

$$f(s_1, \ldots, s_n) \neq 0.$$

Prueba. Argumentamos por contradicción.

Supongamos que $S_1, \ldots, S_n$ son subconjuntos de F con $\mid S_i \mid > t_i$ y para todo $s_1 \in S_1, \ldots, s_n \in S_n$ se tiene que

$$f(s_1, \ldots, s_n) = 0.$$

Sea $\mid S_i \mid = t_i + 1$ para todo i y definamos

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

Por Teorema 1.7 existen polinomios $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ que satisfacen

$$grad(h_i) \leq \sum_{i=1}^{n} t_i - grad(g_i),$$

y tales que

$$f = \sum_{i=1}^{n} h_i g_i. \tag{1.4}$$

Por hipótesis, el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ en el lado izquierdo de (1.4) es no cero, entonces este coeficiente es el mismo en el lado derecho de (1.4).

Por otro lado el grado de cada $h_i g_i = h_i \prod_{s \in S_i}(x_i - s)$ es a lo más $grad(f)$.
Por lo tanto si existen monomios de grado igual al grado de f en $h_i g_i$, ellos son divisibles por $x_i^{t_i+1}$, de donde se sigue que el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ en $\sum_{i=1}^{n} h_i g_i$ es cero, lo cual contradice lo anterior. Por lo tanto, existen $s_1 \in S_1, \ldots, s_n \in S_n$ tales que

$$f(s_1, \ldots, s_n) \neq 0. \square$$

Los resultados en varias variables (Teorema 1.6, Teorema 1.7 y Teorema 1.8) enunciados anteriormente se conocen como Combinatorial Nullstellensatz o teoremas de los ceros de Hilbert y determinan una técnica para el estudio de algunos problemas combinatorios.

1.3. Dos aplicaciones de los teoremas básicos

El primer teorema, conjeturado por Artín en 1934, fue probado por Chevalley en 1935 y extendido por Warning en 1935, el cual trata sobre raíces de sistemas de polinomios con coeficientes en campos finitos.

Teorema 1.9 (Chevalley-Warning) *Sean p un primo y*

$$P_1 = P_1(x_1, \ldots, x_n),\ P_2 = P_2(x_1, \ldots, x_n),\ \ldots,\ P_m = P_m(x_1, \ldots, x_n)$$

m polinomios en el anillo $\mathbb{Z}_p[x_1, \ldots, x_n]$. Si $n > \sum_{i=1}^{m} grad(P_i)$ y los polinomios P_i tienen un cero en común $(c_1, \ldots, c_n)$, entonces tienen otro cero en común.

Prueba. Argumentamos por contradicción.

Supongamos lo contrario, es decir; que $P_1, \ldots, P_m$ no tienen otro cero común distinto de $(c_1, \ldots, c_n)$ y consideremos el polinomio f en $\mathbb{Z}_p[x_1, \ldots, x_n]$.

$$f = f(x_1, \ldots, x_n) = \prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{p-1}) - \delta \prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_j}} (x_j - c),$$

donde δ se escoge en $\mathbb{Z}_p$ tal que:

$$f(c_1, \ldots, c_n) = 0.$$

Más aún δ existe y su valor es no cero.

Veamos también que:

$$f(s_1, \ldots, s_n) = 0 \text{ para todo } s_i \in \mathbb{Z}_p. \tag{1.5}$$

1. Si $(s_1, \ldots, s_n) = (c_1, \ldots, c_n)$, es trivial.

2. Si $(s_1, \ldots, s_n) \neq (c_1, \ldots, c_n)$. Tenemos:

2.1. Por hipótesis hay un polinomio P_j que no se anula en $(s_1, \ldots, s_n)$, implicando que

$$1 - P_j(s_1, \ldots, s_n)^{p-1} = 0.$$

2.2. Además si $(s_1, \ldots, s_n) \neq (c_1, \ldots, c_n)$, entonces algún $s_k \neq c_k$, para $1 \leq k \leq n$, así

$$\prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_k}} (s_k - c) = 0.$$

Luego,

$$\prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_j}} (s_j - c) = \left[\prod_{\substack{j=1 \\ j \neq k}}^{n} \prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_j}} (s_j - c) \right] \left[\prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_k}} (s_k - c) \right] = 0.$$

Por consiguiente

$$f(s_1, \ldots, s_n) = 0 \text{ para todo } s_i \in \mathbb{Z}_p.$$

Como:

- grado de $\prod_{i=1}^{m} (1 - P_i(x_1, \ldots, x_n)^{p-1})$ es $(p-1) \sum_{i=1}^{m} grad(P_i)$.

- grado de $-\delta \prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_j}} (x_j - c)$ es $(p-1)n$.

Pero por hipótesis $n > \sum_{i=1}^{m} grad(P_i)$, entonces

$$(p-1) \sum_{i=1}^{m} grad(P_i) < (p-1)n,$$

de lo cual se sigue que el grado total de f esta determinado por

$$\prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}_p \\ c \neq c_j}} (x_j - c).$$

Por lo tanto, si $t_i = p-1$ para $1 \leq i \leq n$ el grado total de $\prod_{i=1}^{n} x_i^{t_i}$ es $\sum_{i=1}^{n} t_i = (p-1)n$ y también el de f. Así el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ en f es $-\delta \neq 0$.
Finalmente, si $S_i = \mathbb{Z}_p$ para $1 \leq i \leq n$ ($\mid S_i \mid = p > p-1 = t_i$), aplicando el Teorema 1.8 a f se tiene que existen $s_1 \in S_1, \ldots, s_n \in S_n$ tales que:

$$f(s_1, \ldots, s_n) \neq 0,$$

lo cual contradice (1.5).□

El Teorema de Cauchy-Davenport es uno de los resultados, con numerosas aplicaciones en Teoría de Números Aditiva, el cual trata sobre adición de clases residuales, este teorema fue probado por Cauchy en 1813 y redescubierto por Davenport en 1935, una forma de enunciarlo es la siguiente.

Teorema 1.10 (Cauchy-Davenport) *Sean p un primo, A, B subconjuntos no vacíos de $\mathbb{Z}_p$ y $A + B = \{a + b : a \in A \ , \ b \in B\}$, entonces*

$$\mid A + B \mid \geq \text{mín}\{p, \mid A \mid + \mid B \mid -1\}.$$

Prueba. Para esta prueba consideramos dos casos:

Caso 1. $\mid A \mid + \mid B \mid > p$.

Si $\mid A \mid + \mid B \mid > p$ el resultado es trivial, ya que para todo $g \in \mathbb{Z}_p$, los dos conjuntos A y $g - B$ se intersectan, implicando que $A + B = \mathbb{Z}_p$.

Probemos que $A + B = \mathbb{Z}_p$.

- Si A y B son subconjuntos de $\mathbb{Z}_p$, claramente $A + B$ también lo es.
- Recíprocamente, dado que para cualquier $g \in \mathbb{Z}_p$, $\mid B \mid = \mid g - B \mid$, entonces

  $$\mid A \mid + \mid g - B \mid > \mid \mathbb{Z}_p \mid = p.$$

  Como $g - B$ y A son subconjuntos de $\mathbb{Z}_p$, $A \cup (g - B) \subseteq \mathbb{Z}_p$, lo cual implica que

  $$\begin{aligned} \mid \mathbb{Z}_p \mid &\geq \mid A \cup (g - B) \mid \\ &= \mid A \mid + \mid g - B \mid - \mid A \cap (g - B) \mid . \end{aligned}$$

Luego si

$$A \cap (g - B) = \phi,$$

entonces

$$| \mathbb{Z}_p | \ \geq \ | A | + | B | .$$

Lo cual contradice la hipótesis. Por lo tanto $A \cap (g - B) \neq \phi$ y en consecuencia existen $a \in A$ y $a \in (g - B)$ tales que $a = g - b$ de donde

$$g = (a + b) \in A + B$$

lo cual muestra que $\mathbb{Z}_p \subseteq A + B$.

Así $\mathbb{Z}_p = A + B$.

Por consiguiente

$$| A + B | = p = \text{mín}\{p, | A | + | B | - 1\}.$$

Caso 2. $| A | + | B | \leq p$.

Debemos probar que

$$| A + B | \geq | A | + | B | - 1.$$

Argumentamos por contradicción. Supongamos que

$$| A + B | < | A | + | B | - 1, \text{ esto es; } | A + B | \leq | A | + | B | - 2.$$

Sea C un subconjunto de $\mathbb{Z}_p$ que cumple

$$A + B \subset C \text{ y } | C | = | A | + | B | - 2.$$

Definamos $f = f(x, y) = \prod_{c \in C}(x + y - c)$ y observe que por definición de C

$$f(a, b) = 0 \text{ para todo } a \in A, b \in B. \tag{1.6}$$

Tomemos $t_1 = | A | - 1$, $t_2 = | B | - 1$ y notemos que el coeficiente de $x^{t_1} y^{t_2}$ en f es el coeficiente binomial $\binom{|A|+|B|-2}{|A|-1}$, el cual es no cero en $\mathbb{Z}_p$.
Como $grad(f) = t_1 + t_2 = | C |$ y el coeficiente de $x^{t_1} y^{t_2}$ en f es no cero, entonces por Teorema 1.8, dado que $A, B \subseteq \mathbb{Z}_p$ y $| A | > t_1$ y $| B | > t_2$, tenemos que existen $a \in A$ y $b \in B$ tales que:

$$f(a, b) \neq 0,$$

lo cual contradice (1.6). En consecuencia $| A + B | \geq | A | + | B | - 1$.
Por lo tanto

$$| A + B | \geq \text{mín}\{p, | A | + | B | - 1\}.$$

Completando así la prueba.□

Capítulo 2

Sumas Restringidas

En este capítulo presentamos una técnica algebraica para obtener resultados en Teoría de Números Aditiva y en combinatoria y describimos algunas de sus aplicaciones que pueden verse como generalizaciones del Teorema de Cauchy-Davenport.

2.1. El Método Polinomial

Definición 2.1 *Sea p un primo. Para un polinomio $h = h(x_0, \ldots, x_k)$ sobre $\mathbb{Z}_p$ y para subconjuntos $A_0, \ldots, A_k$ de $\mathbb{Z}_p$, definamos:*

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0 + \ldots + a_k : a_i \in A_i,\ h(a_0, \ldots, a_k) \neq 0\}.$$

Ejemplo 2.1 *Sean $p = 5$, $A_0 = \{0, 1\}, A_1 = \{2, 3, 4\}, A_2 = \{1, 2\}$ subconjuntos de $\mathbb{Z}_5$ y $h(x_0, x_1, x_2) = x_0 + x_1 + x_2 \in \mathbb{Z}_5[x_0, x_1, x_2]$.*
Luego

$$\begin{aligned} A_0 + A_1 + A_2 &= \left\{ \begin{array}{cccc} 0+2+1, & 0+2+2, & 0+3+1, & 0+3+2, \\ 0+4+1, & 0+4+2, & 1+2+1, & 1+2+2, \\ 1+3+1, & 1+3+2, & 1+4+1, & 1+4+2 \end{array} \right\} \\ &= \{3, 4, 4, 0, 0, 1, 4, 0, 0, 1, 1, 2\} \\ &= \{0, 1, 2, 3, 4\} \end{aligned}$$

y notemos que

$$h(0, 2, 1) = 3, \quad h(0, 2, 2) = 4, \quad h(0, 3, 1) = 4, \quad h(0, 3, 2) = 0,$$

$h(0,4,1)=0, \quad h(0,4,2)=1, \quad h(1,2,1)=4, \quad h(1,2,2)=0,$
$h(1,3,1)=0, \quad h(1,3,2)=1, \quad h(1,4,1)=1, \quad h(1,4,2)=2.$

Así

$$\begin{aligned}\oplus_h \sum_{i=0}^{2} A_i =& \left\{ \begin{array}{cccc} 0+2+1, & 0+2+2, & 0+3+1, & 0+4+2, \\ 1+2+1, & 1+3+2, & 1+4+1, & 1+4+2 \end{array} \right\} \\ =&\{1,2,3,4\}.\end{aligned}$$

Ejemplo 2.2 *Sean $p=3$, $A_0=\{0,2\}, A_1=\{0,1\}$ subconjuntos de $\mathbb{Z}_3$ y $h(x_0,x_1)=x_0^2+2x_1+2 \in \mathbb{Z}_3[x_0,x_1]$.*
Luego

$$\begin{aligned}A_0+A_1 =&\{0+0,0+1,2+0,2+1\} \\ =&\{0,1,2,0\} \\ =&\{0,1,2\}.\end{aligned}$$

y notemos que

$h(0,0)=2, \quad h(0,1)=1, \quad h(2,0)=0, \quad h(2,1)=2.$

Así

$$\oplus_h \sum_{i=0}^{1} A_i = \{0+0,0+1,2+1\} = \{0,1\}.$$

Definición 2.2 *Sean p un primo y $A_0,\ldots,A_k$ subconjuntos no vacíos del grupo cíclico $\mathbb{Z}_p$, definamos:*

$$\oplus_{i=0}^{k} A_i = \{a_0+\ldots+a_k : a_i \in A_i, a_i \neq a_j \ \forall\, i \neq j\}.$$

Ejemplo 2.3 *Sean $p=5$, $A_0=\{0,1\}, A_1=\{2,3,4\}, A_2=\{1,2\}$ subconjuntos de $\mathbb{Z}_5$.*
Luego

$$\begin{aligned}A_0+A_1+A_2 =& \left\{ \begin{array}{cccc} 0+2+1, & 0+2+2, & 0+3+1, & 0+3+2, \\ 0+4+1, & 0+4+2, & 1+2+1, & 1+2+2, \\ 1+3+1, & 1+3+2, & 1+4+1, & 1+4+2 \end{array} \right\} \\ =&\{3,4,4,0,0,1,4,0,0,1,1,2\} \\ =&\{0,1,2,3,4\}.\end{aligned}$$

Así

$$\begin{aligned}\oplus_{i=0}^{2}A_i =&\{0+2+1, 0+3+1, 0+3+2, 0+4+1, 0+4+2, 1+3+2, 1+4+2\}\\ =&\{0,1,2,3,4\}.\end{aligned}$$

Notemos que para el polinomio $h(x_0,\ldots,x_k)=\prod_{0\leq j<i\leq k}(x_i-x_j)$ sobre $\mathbb{Z}_p$ tenemos que la suma $\oplus_{i=0}^{k}A_i$ es igual a la suma $\oplus_h \sum_{i=0}^{k} A_i$.

El siguiente teorema de esta sección se conoce como Polinomial y es una aplicación del Teorema 1.8, el cual es una herramienta muy utilizada en el estudio de problemas que tienen que ver con el cardinal de conjuntos suma con restricciones.
Este método tiene diversas aplicaciones en Teoría de Números Aditiva y fue formulado por Noga Alon, Melvyn Nathanson e Imre Ruzsa.

Teorema 2.1 (El método polinomial) *Sean p un primo, $h=h(x_0,\ldots,x_k)$ un polinomio sobre $\mathbb{Z}_p$ y $A_0,\ldots,A_k$ subconjuntos no vacíos de $\mathbb{Z}_p$, donde $\mid A_i \mid = c_i+1$ y definamos $m=(\sum_{i=0}^{k}c_i)-grad(h)$. Si el coeficiente de $\prod_{i=0}^{k}x_i^{c_i}$ en*

$$(x_0+\ldots+x_k)^m h(x_0,\ldots,x_k)$$

es no cero en $\mathbb{Z}_p$ entonces

$$\mid \oplus_h \sum_{i=0}^{k} A_i \mid \geq m+1$$

(y así $m<p$).

Prueba. Notemos que:

- Si $m<0$ la conclusión es trivial.
- Si $m=0$ tenemos que: $\sum_{i=0}^{k}c_i = grad(h)$ y se tiene que cumplir que:

$$\mid \oplus_h \sum_{i=0}^{k} A_i \mid \geq 1,$$

lo cual no es posible puesto que si $h(a_0,\ldots,a_k)=0$ para toda $(k+1)$-tupla $(a_0,\ldots,a_k)\in(A_0\times\cdots\times A_k)$ entonces

$$\mid \oplus_h \sum_{i=0}^{k} A_i \mid = 0,$$

y además $grad(h) < \sum_{i=0}^{k} \mid A_i \mid$ y $\mid A_i \mid = c_i + 1$, es decir que hay mas raíces que el grado del polinomio. Por lo tanto h es el polinomio cero.

Para $m > 0$, argumentamos por contradicción.
Supongamos que el coeficiente de $\prod_{i=0}^{k} x_i^{c_i}$ en $(x_0 + \ldots + x_k)^m h(x_0, x_1, \ldots, x_k)$ es no cero en $\mathbb{Z}_p$ y $\mid \oplus_h \sum_{i=0}^{k} A_i \mid < m + 1$.

Sea E un conjunto de m elementos de $\mathbb{Z}_p$ que contiene al conjunto $\oplus_h \sum_{i=0}^{k} A_i$.

Sea $Q = Q(x_0, \ldots, x_k)$ un polinomio definido como sigue:

$$Q(x_0, \ldots, x_k) = h(x_0, \ldots, x_k) \cdot \prod_{e \in E} (x_0 + \ldots + x_k - e).$$

Entonces:

1. $Q(a_0, \ldots, a_k) = 0$ para toda $(k+1)$-tupla $(a_0, \ldots, a_k) \in (A_0 \times \cdots \times A_k)$ ya que $h(a_0, \ldots, a_k) = 0$ ó $a_0 + \ldots + a_k \in E$.

2. Del Lema 1.1,

$$\begin{aligned} grad(Q) &= grad(h) + grad\left(\prod_{e \in E} (x_0 + \ldots + x_k - e)\right) \\ &= grad(h) + \mid E \mid \\ &= grad(h) + m \\ &= grad(h) + \left(\sum_{i=0}^{k} c_i\right) - grad(h) \\ &= \sum_{i=0}^{k} c_i. \end{aligned}$$

3. El coeficiente del monomio $\prod_{i=0}^{k} x_i^{c_i}$ en Q es el mismo coeficiente que el de este monomio en el polinomio

$$(x_0 + \ldots + x_k)^m h(x_0, \ldots, x_k)$$

ya que $Q(x_0, \ldots, x_k) = h(x_0, \ldots, x_k)(x_0 + \ldots + x_k)^m$ + términos de menor orden, el cual es no cero en $\mathbb{Z}_p$ por hipótesis.

En virtud de que $A_i \subseteq \mathbb{Z}_p$ para todo $0 \leq i \leq k$, $\mid A_i \mid > c_i$ y por el Teorema 1.8, existen $a_0 \in A_0, \ldots, a_k \in A_k$ tales que:

$$Q(a_0, \ldots, a_k) \neq 0,$$

lo cual contradice 1.
Por lo tanto

$$\mid \oplus_h \sum_{i=0}^{k} A_i \mid \geq m + 1$$

y así $m < p$. $\square$

A continuación presentamos dos aplicaciones que se derivan del Método Polinomial.

2.2. Aplicaciones del método polinomial

Para la prueba de la primera aplicación recurrimos al siguiente lema, el cual es un resultado combinatorio que se utilizará para calcular el coeficiente requerido.

Lema 2.1 *Sean $c_0, \ldots, c_k$ enteros no negativos y supongamos que*

$$\sum_{i=0}^{k} c_i = m + \binom{k+1}{2},$$

donde m es un entero no negativo. Entonces el coeficiente de $\prod_{i=0}^{k} x_i^{c_i}$ en el polinomio

$$(x_0 + \ldots + x_k)^m \prod_{0 \leq j < i \leq k} (x_i - x_j)$$

es

$$\frac{m!}{c_0! \ldots c_k!} \prod_{0 \leq j < i \leq k} (c_i - c_j).$$

Para la prueba ver [11], referenciado en [1].

Primera aplicación

Proposición 2.1 *Sean p un primo y $A_0, \ldots, A_k$ subconjuntos no vacíos del grupo cíclico $\mathbb{Z}_p$.*
Si $\mid A_i \mid \neq \mid A_j \mid$ para todo $0 \leq i < j \leq k$ y $\sum_{i=0}^{k} \mid A_i \mid \leq p + \binom{k+2}{2} - 1$, entonces

$$\mid \{a_0 + \ldots + a_k : a_i \in A_i, a_i \neq a_j \ \forall \ i \neq j\} \mid \geq \sum_{i=0}^{k} \mid A_i \mid - \binom{k+2}{2} + 1.$$

Prueba. Definamos el polinomio h sobre $\mathbb{Z}_p$ así:

$$h(x_0, \ldots, x_k) = \prod_{0 \leq j < i \leq k} (x_i - x_j)$$

Supongamos que $\mid A_i \mid = c_i + 1$, donde los c_i son enteros no negativos distintos dos a dos y tomemos $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$, luego

$$\begin{aligned} m &= \sum_{i=0}^{k} (\mid A_i \mid -1) - \binom{k+1}{2} \\ &= \sum_{i=0}^{k} \mid A_i \mid -(k+1) - \binom{k+1}{2} \\ &= \sum_{i=0}^{k} \mid A_i \mid -\binom{k+2}{2} \\ &\leq p + \binom{k+2}{2} - 1 - \binom{k+2}{2} \\ &= p - 1 \\ &< p. \end{aligned}$$

Luego, por Lema 2.1 el coeficiente de $\prod_{i=0}^{k} x_i^{c_i}$ en el polinomio

$$h \cdot (x_0 + \ldots + x_k)^m$$

es

$$\frac{m!}{c_0! \ldots c_k!} \prod_{0 \leq j < i \leq k} (c_i - c_j),$$

que no es cero módulo p, ya que $m < p$ y los c_i son distintos por pares.
Por lo tanto por Teorema 2.1

$$\mid \oplus_h \sum_{i=0}^{k} A_i \mid = \mid \oplus_{i=0}^{k} A_i \mid \geq m + 1 = \sum_{i=0}^{k} \mid A_i \mid - \binom{k+2}{2} + 1. \; \square$$

Observemos que:

- En la notación de la Definición 2.2, la afirmación de la Proposición 2.1, es: si $\mid A_i \mid \neq \mid A_j \mid$ para todo $0 \leq i < j \leq k$ y

$$\sum_{i=0}^{k} \mid A_i \mid \leq p + \binom{k+2}{2} - 1,$$

entonces

$$| \oplus_{i=0}^{k} A_i | \geq \sum_{i=0}^{k} | A_i | - \binom{k+2}{2} + 1.$$

- En el caso especial de esta proposición en el cual $k = 1, A_0 = A$ y $A_1 = A - \{a\}$ para un elemento arbitrario $a \in A$ implica que si $A \subset \mathbb{Z}_p$ y $2 \mid A \mid -1 \leq p + 2$, entonces el número de sumas $a_1 + a_2$ con $a_1, a_2 \in A$ y $a_1 \neq a_2$ es al menos $2 \mid A \mid -3$.

A partir de los anteriores resultados se tiene el siguiente teorema conjeturado por Erdös y Heilbronn en 1964 y probado 30 años después por Dias Da Silva y Hamidoune usando algunas herramientas de Álgebra Lineal y la Teoría de Representaciones del grupo simétrico.

Teorema 2.2 (Conjetura de Erdös-Heilbronn) *Si p es un primo y A es un subconjunto no vacío de $\mathbb{Z}_p$, entonces*

$$| \{a + a' : a, a' \in A, a \neq a'\} | \geq \text{mín}\{p, 2 \mid A \mid -3\}.$$

Prueba. Para esta prueba aplicamos la Proposición 2.1 con $k = 1$, $A_0 = A$ y $A_1 = A - \{a\}$ para $a \in A$ fijo. Como $A \subseteq \mathbb{Z}_p$ y $| A_0 | \neq | A_1 |$, entonces:

Si $2 \mid A \mid -3 \leq p$, es decir $2 \mid A \mid -1 \leq p + 2$ lo cual es equivalente a

$$| A_0 | + | A_1 | \leq p + \binom{3}{2} - 1 = p + 2,$$

y dado que

$$\{a_0 + a_1 : a_0 \in A_0, a_1 \in A_1, a_0 \neq a_1\} = \{a + a' : a, a' \in A, a \neq a'\},$$

entonces

$$| \{a + a' : a, a' \in A, a \neq a'\} | \geq | A_0 | + | A_1 | - \binom{3}{2} + 1 = 2 \mid A \mid -3.$$

En este caso el mínimo es $2 \mid A \mid -3$.

Ahora, si $2 \mid A \mid -3 > p$ o sea $| A_0 | + | A_1 | - 2 > p$, escogemos $A_1' \subseteq A_1$ tal

que $\mid A_0 \mid + \mid A_1' \mid -2 = p$ y por lo tanto el teorema se cumple para A_0 y A_1', luego como

$$\{a_0 + a_1 : a_0 \in A_0, a_1 \in A_1', a_0 \neq a_1\} \subseteq \{a_0 + a_1 : a_0 \in A_0, a_1 \in A_1, a_0 \neq a_1\},$$

entonces

$$\mid \{a_0 + a_1 : a_0 \in A_0, a_1 \in A_1, a_0 \neq a_1\} \mid \geq \mid \{a_0 + a_1 : a_0 \in A_0, a_1 \in A_1', a_0 \neq a_1\} \mid > p.$$

En este caso el mínimo es p. Por lo tanto

$$\mid \{a + a' : a, a' \in A, a \neq a'\} \mid \geq \text{mín}\{p, 2 \mid A \mid -3\}. \square$$

Una consecuencia de la Proposición 2.1 es la siguiente.

Teorema 2.3 *Sean p un primo y $A_0, \ldots, A_k$ subconjuntos no vacíos de $\mathbb{Z}_p$, donde $\mid A_i \mid = b_i$, y supongamos $b_0 \geq b_1 \geq \ldots \geq b_k$. Definamos $b_0', \ldots, b_k'$ por*

$$b_0' = b_0 \ \ y \ \ b_i' = \text{mín}\{b_{i-1}' - 1, b_i\}, \ \ para \ \ 1 \leq i \leq k.$$

Si $b_k' > 0$ entonces

$$\mid \oplus_{i=0}^{k} A_i \mid \geq \text{mín}\left\{p, \sum_{i=0}^{k} b_i' - \binom{k+2}{2} + 1\right\}.$$

Para la prueba ver [11], referenciado en [1].

El siguiente resultado de Dias Da Silva y Hamidoune es una consecuencia simple de un caso especial del teorema anterior.

Teorema 2.4 (Dias Da Silva y Hamidoune) *Sean p un primo, A un subconjunto no vacío de $\mathbb{Z}_p$ y*

$$s^{\wedge}A = \{a_0 + \ldots + a_{s-1} : a_i \in A_i \, y \, a_i \neq a_j \ \ \forall \, i \neq j\}$$

el conjunto de todas las sumas de s elementos distintos de A, entonces

$$\mid s^{\wedge}A \mid \geq \text{mín}\{p, s \mid A \mid -s^2 + 1\}.$$

Prueba. Consideremos los siguientes casos.

Caso 1. Si $\mid A \mid < s$ no tenemos nada que probar ya que no tiene sentido hablar del conjunto $s^{\wedge}A$.

Caso 2. Si $\mid A \mid \geq s$ tomemos $s = k+1$ y apliquemos el Teorema 2.3 con $A_i = A$, $b'_i = \mid A \mid -i$ para todo i, $0 \leq i \leq k$.

Como $b'_k = \mid A \mid -k = \mid A \mid -s+1 \geq s-s+1 = 1 > 0$ y además

$$s^{\wedge}A = \{a_0 + \ldots + a_k : a_i \in A_i \text{ y } a_i \neq a_j \ \forall\, i \neq j\},$$

entonces:

$$\begin{aligned}
\mid s^{\wedge}A \mid &= \mid (k+1)^{\wedge}A \mid \\
&\geq \text{mín}\left\{p, \sum_{i=0}^{k} b'_i - \binom{k+2}{2} + 1\right\} \\
&= \text{mín}\left\{p, \sum_{i=0}^{k} (\mid A \mid -i) - \frac{(k+1)(k+2)}{2} + 1\right\} \\
&= \text{mín}\left\{p, (k+1) \mid A \mid -\frac{k(k+1)}{2} - \frac{(k+1)(k+2)}{2} + 1\right\} \\
&= \text{mín}\{p, (k+1) \mid A \mid -(k+1)^2 + 1\} \\
&= \text{mín}\{p, s \mid A \mid -s^2 + 1\}.
\end{aligned}$$

Por lo tanto

$$\mid s^{\wedge}A \mid \geq \text{mín}\{p, s \mid A \mid -s^2 + 1\}. \square$$

Notemos que el teorema anterior es una generalización de Teorema 2.2, pues si hacemos $s = 2$ se obtiene que

$$\mid 2^{\wedge}A \mid = \mid \{a_0 + a_1 : a_i \in A_i \text{ y } a_i \neq a_j \ \forall\, i \neq j\} \geq \text{mín}\{p, 2 \mid A \mid -3\}.$$

Segunda aplicación

Proposición 2.2 *Si p es un primo y A, B son dos subconjuntos no vacíos de $\mathbb{Z}_p$, entonces*

$$\mid \{a+b : a \in A, b \in B \text{ y } ab \neq 1\} \mid \geq \text{mín}\{p, \mid A \mid + \mid B \mid -3\}.$$

Prueba. Definamos $h(x_0, x_1) = x_0x_1 - 1$ sobre $\mathbb{Z}_p$ y sean $A_0 = A$ y $A_1 = B$, donde $\mid A \mid = c_0 + 1$, $\mid B \mid = c_1 + 1$ y $m = c_0 + c_1 - grad(h) = \mid A \mid + \mid B \mid -4$.
Como

$$\{a + b : a \in A, b \in B \ y \ ab \neq 1\} = \{a_0 + a_1 : a_i \in A_i \ y \ h(a_0, a_1) \neq 0\}$$

y dado que el coeficiente del monomio $x_0^{c_0}x_1^{c_1}$ en el polinomio

$$(x_0 + x_1)^{|A|+|B|-4}(x_0x_1 - 1)$$

es

$$C = \binom{\mid A \mid + \mid B \mid -4}{\mid B \mid -2} = \frac{(\mid A \mid + \mid B \mid -4)!}{(\mid B \mid -2)!(\mid A \mid -2)!},$$

entonces si $m = \mid A \mid + \mid B \mid -4 < p$, es decir, si $\mid A \mid + \mid B \mid -3 \leq p$, tenemos que C es distinto de cero módulo p y en este caso del Teorema 2.1

$$\mid \{a + b : a \in A, b \in B \, y \, ab \neq 1\} \mid \geq m + 1 = \mid A \mid + \mid B \mid -3.$$

Así el mínimo es $\mid A \mid + \mid B \mid -3$.

Por otro lado, si $m = \mid A \mid + \mid B \mid -4 \geq p$, es decir, si $\mid A \mid + \mid B \mid -3 > p$, escogemos $B' \subseteq B$ tal que $\mid A \mid + \mid B' \mid -3 = p$ y así el teorema se cumple para A y B'. Luego

$$\mid \{a + b : a \in A, b \in B' \, y \, ab \neq 1\} \mid \geq \mid A \mid + \mid B' \mid -3 = p$$

además, ya que

$$\{a + b : a \in A, b \in B' \, y \, ab \neq 1\} \subseteq \{a + b : a \in A, b \in B \, y \, ab \neq 1\}$$

entonces

$$\mid \{a + b : a \in A, b \in B \, y \, ab \neq 1\} \mid \geq \mid \{a + b : a \in A, b \in B' \, y \, ab \neq 1\} \mid \geq p.$$

En este caso el mínimo es p y por lo tanto

$$\mid \{a + b : a \in A, b \in B \, y \, ab \neq 1\} \mid \geq \text{mín}\{p, \mid A \mid + \mid B \mid -3\}. \square$$

2.3. Conjuntos suma en espacios vectoriales sobre campos primos

En esta sección presentamos otra aplicación del Teorema 1.8, el cual es una extensión del Teorema de Cauchy-Davenport.

Definición 2.3 *Una terna (r, s, n) de enteros positivos satisface la condición Hopf-Stiefel si*

$$\binom{n}{k} \text{ es par para cada entero } k, \text{ satisfaciendo } n - r < k < s.$$

Ejemplo 2.4 *Consideremos la terna $(1, 4, 3)$ y veamos si satisface la condición Hopf-Stiefel.*

$$\binom{3}{k} \text{ es par para todo } k,\ 2 < k < 4,$$

tomando $k = 3$ tenemos

$$\binom{3}{3} = 1, \quad \text{no es par.}$$

Por lo tanto la terna $(1, 4, 3)$ no satisface la condición Hopf-Stiefel.

Ejemplo 2.5 *Consideremos la terna $(3, 4, 5)$ y veamos si satisface la condición Hopf-Stiefel.*

$$\binom{5}{k} \text{ es par para todo } k,\ 2 < k < 4,$$

tomando $k = 3$ tenemos

$$\binom{5}{3} = 10, \text{ es par.}$$

Por lo tanto la terna $(3, 4, 5)$ satisface la condición Hopf-Stiefel.

Yuzvinsky [59] (Referenciado en [1]) probó que en un espacio vectorial de dimensión infinita sobre F_2, existen dos subconjuntos $A, B \subset V$ satisfaciendo $\mid A \mid = r, \mid B \mid = s$ y $\mid A + B \mid \leq n$ si y sólo si la terna (r, s, n) satisfacen la condición Hopf-Stiefel.

Eliahou y Keivaire [23] demostraron que esto puede probarse usando la técnica algebraica de [10], [11] y generalizaron este resultado para un primo p arbitrario, obteniendo así una generalización del Teorema de Cauchy Davenport y el resultado de Yuzvinsky. ([23], [10] y [11] Referenciados en [1]).

Definición 2.4 *Una terna (r, s, n) de enteros positivos satisface la condición Hopf-Stiefel respecto a un primo p si*

$$\binom{n}{k} \text{ es divisible por } p \text{ para cada entero } k, \text{ satisfaciendo } n - r < k < s.$$

Definición 2.5 *Sea $\beta_p(r,s)$ denotando el menor entero n, para el cual la terna (r,s,n) satisface la condición Hopf-Stiefel con respecto a un primo p; esto es,*

$$\beta_p(r,s) = \text{mín}\left\{ \begin{array}{c} n \in \mathbb{Z}^+ : (r,s,n) \text{ satisface la condición Hopf-Stiefel} \\ \text{respecto a un primo } p \end{array} \right\},$$

$$\beta_p(r,s) = \text{mín}\left\{ n \in \mathbb{Z}^+ : p \Big| \binom{n}{k} \text{ para todo entero } k,\ n-r < k < s \right\}. \tag{2.1}$$

Ejemplo 2.6 *Sean $p = 2$ y $(3,4,n)$ una terna de enteros positivos.*
Encontremos el menor entero n para el cual la terna satisface (2.1).
Tenemos que:

$$\beta_2(3,4) = \text{mín}\left\{ n \in \mathbb{Z}^+ : 2 \Big| \binom{n}{k}\ \forall\, k,\ n-2 \leq k \leq 3 \right\}.$$

Como $k > 0$, entonces $n - 2 > 0$, es decir, $n > 2$. Luego

- *$\beta_2(3,4) = 3$?. No, puesto que:*

  Tomando $k = 1$ tenemos que $\binom{3}{1} = 3$ y $2 \nmid 3$.
  Así para $n = 3$ no se cumple.

- *$\beta_2(3,4) = 4$?. Si, puesto que:*

  Tomando $k = 2$ tenemos que $\binom{4}{2} = 6$ y $2 \big| 6$

  Tomando $k = 3$ tenemos que $\binom{4}{3} = 4$ y $2 \big| 4$.
  Así para $n = 4$ se cumple.

Por lo tanto el menor entero n para el cual la terna $(3,4,n)$ satisface (2.1) es $n = 4$.

Ejemplo 2.7 *Sean $p = 2$ y $(5,6,n)$ una terna de enteros positivos.*
Encontremos el menor entero n para el cual la terna satisface (2.1).
Tenemos que:

$$\beta_2(5,6) = \text{mín}\left\{ n \in \mathbb{Z}^+ : 2 \Big| \binom{n}{k}\ \forall\, k,\ n-4 \leq k \leq 5 \right\}.$$

Como $k > 0$, entonces $n - 4 > 0$, es decir, $n > 4$. Luego

- *$\beta_2(5,6) = 5$?. No, puesto que:*

  Tomando $k = 1$ tenemos que $\binom{5}{1} = 5$ y $2 \nmid 5$.
  Así para $n = 5$ no se cumple.

- $\beta_2(5,6) = 6$?. *No, puesto que:*

  Tomando $k = 2$ *tenemos que* $\binom{6}{2} = 15$ *y* $2 \nmid 15$.
  Así para $n = 6$ *no se cumple.*

- $\beta_2(5,6) = 7$?. *No, puesto que:*

  Tomando $k = 3$ *tenemos que* $\binom{7}{3} = 35$ *y* $2 \nmid 35$.
  Así para $n = 7$ *no se cumple.*

- $\beta_2(5,6) = 8$?. *Si, puesto que:*

  Tomando $k = 4$ *tenemos que* $\binom{8}{4} = 70$ *y* $2 \mid 70$.

  Tomando $k = 5$ *tenemos que* $\binom{8}{5} = 56$ *y* $2 \mid 56$.
  Así para $n = 8$ *se cumple.*

Por lo tanto el menor entero n *para el cual la terna* $(5,6,n)$ *satisface* (2.1) *es* $n = 8$.

Recordemos que en el Teorema de Cauchy-Davenport consideramos A y B subconjuntos no vacíos de $\mathbb{Z}_p$, en el siguiente teorema consideramos A y B conjuntos finitos no vacíos de un espacio vectorial V sobre F_p.

Teorema 2.5 *Si* A *y* B *son dos subconjuntos finitos no vacíos de un espacio vectorial* V *sobre* F_p *y* $\mid A \mid = r$, $\mid B \mid = s$, *entonces*

$$\mid A + B \mid \geq \beta_p(r,s).$$

Prueba. Argumentamos por contradicción.

Sean A, B conjuntos de V sobre F_p con $\mid A \mid = r$, $\mid B \mid = s$ y

$$\mid A + B \mid < \beta_p(r,s).$$

Supongamos que V es finito e identifiquemoslo con el campo finito F_q, donde $q = p^d$ para algún entero positivo d, de la misma cardinalidad sobre F_p. Tomemos A y B subconjuntos de F_q y definamos $C = A + B$ con $\mid C \mid = n$;
es decir,

$$n < \beta_p(r,s).$$

Definamos el polinomio Q sobre F_q así

$$Q(x,y) = \prod_{c \in C}(x + y - c),$$

y observemos que por definición de C

$$Q(a,b) = 0 \text{ para todo } a \in A, b \in B. \tag{2.2}$$

Por definición de $\beta_p(r,s)$ hay algún entero k satisfaciendo $n - r < k < s$ tal que $\binom{n}{k}$ no es divisible por p, así el coeficiente de $x^{t_1}y^{t_2}$ en Q es $\binom{n}{k}$ que no es cero módulo p.

Tomando $t_1 = n - k$ y $t_2 = k$ tenemos que $grad(Q) = t_1 + t_2 =\mid C \mid$, entonces por Teorema 1.8 dado que $A, B \subset F_q$ con $\mid A \mid = r > t_1$ y $\mid B \mid = s > t_2$ existen $a \in A$ y $b \in B$ tales que

$$Q(a,b) \neq 0.$$

Lo cual contradice (2.2). Por lo tanto $\mid C \mid = n \geq \beta_p(r,s)$. $\square$

Capítulo 3

Teoría de Grafos

Finalizamos este trabajo con dos aplicaciones del Teorema de los ceros de Hilbert en teoría de grafos y presentamos algunos conceptos y resultados necesarios para el desarrollo de este capítulo.

3.1. Conceptos y resultados básicos

Sea V un conjunto no vacío y k un número natural, se denota mediante $V^{[k]}$ al conjunto de todos los subconjuntos de V con k elementos, es decir:

$$V^{[k]} := \{X \subseteq V \ : \mid X \mid = k\},$$

donde $\mid X \mid$ es el cardinal del conjunto X.

Definición 3.1 *Un **grafo simple** (sobre V) es un par ordenado*

$$G = (V, A), \text{ donde } A \subseteq V^{[2]},$$

*V se llama el conjunto de **vértices** de G y A el conjunto de **aristas** de G. $\mid V \mid$ y $\mid A \mid$ se llaman el **orden** y el **tamaño** del grafo G, respectivamente.*

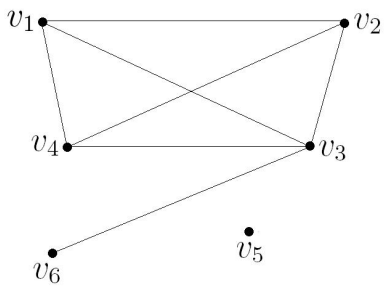
En este capítulo cuando se haga referencia a un grafo, este será un grafo simple y cuando sea necesario denotaremos un grafo $G = (V, A)$ mediante $G = (V(G), A(G))$, para hacer énfasis en que los conjuntos $V(G)$ y $A(G)$, son los conjuntos de vértices y aristas respectivamente del grafo G.

Si $\mid V \mid$ es finito, también lo es $\mid A \mid$ y el grafo G se dice **finito**. El tamaño de un grafo finito G es al menos 0 y a lo sumo $\binom{|V|}{2}$. Si $\mid V \mid$ es infinito y $\mid A \mid$ es infinito el

grafo $G = (V, A)$ se dice **infinito**. A menos que se diga lo contrario, los grafos que se estudian en este capítulo serán finitos.

Generalmente un grafo se representa gráficamente en forma tal que cada vértice queda representado por un punto en el plano y cada arista por una curva de Jordan que une los representantes de sus extremos, es decir una curva continua entre los extremos que no se cruza a si misma.

Ejemplo 3.1



Grafo G, con $\mid V \mid = 6$ y $\mid A \mid = 7$

Definición 3.2 *Si $a = \{u, v\} \in A$, los vértices u y v se llaman **adyacentes** o **extremos** de la arista a. Si $u \in V$ y para todo $v \in V$, $\{u, v\} \notin A$, entonces u es un **vértice aislado**. $\{u, v\}$ y $\{v, u\}$ denotan la misma arista para todo $u, v \in V$.*

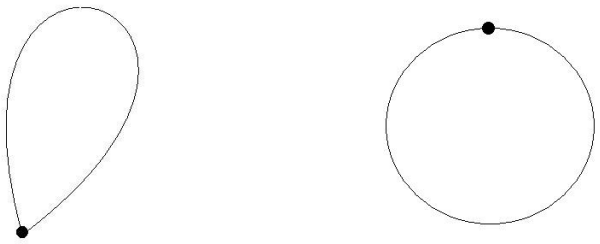
Notemos que en el ejemplo anterior

- $V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$.
- $A = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}, \{v_3, v_6\}\}$.
- v_1 y v_2, v_1 y v_3, v_1 y v_4, v_2 y v_3, v_2 y v_4, v_3 y v_4, v_3 y v_6 son vértices adyacentes.
- v_5 es un vértice aislado.

Casos especiales.

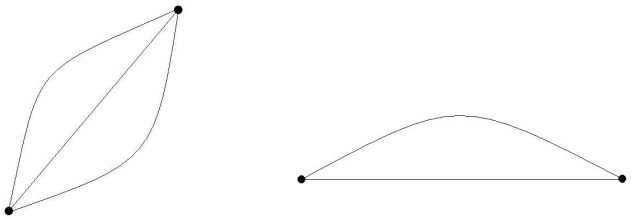
- **Un lazo, rizo o bucle (loop)** es una arista en que sus dos extremos son el mismo vértice.

Ejemplo 3.2



- Si varias aristas tienen los mismos extremos, decimos que son **aristas múltiples**.

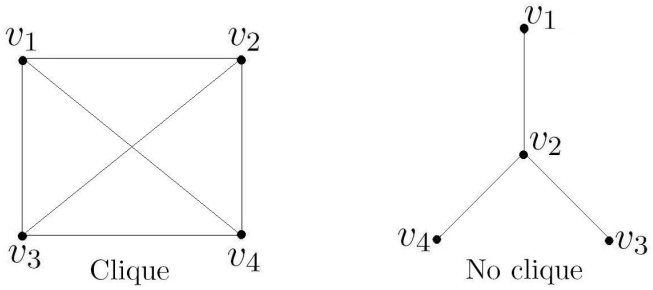
Ejemplo 3.3



Definición 3.3 *Un **multigrafo** es un grafo con aristas múltiples.*

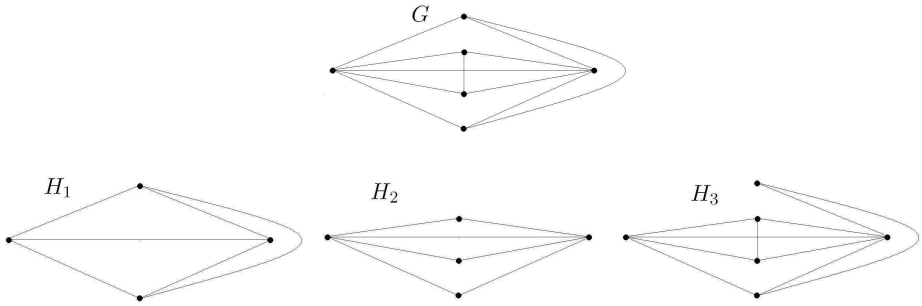
Definición 3.4 *Un **clique** en un grafo es un conjunto de vértices mutuamente adyacentes.*

Ejemplo 3.4



Definición 3.5 *Sean $G = (V(G), A(G))$ y $H = (V(H), A(H))$ dos grafos, H es **subgrafo** de G si $V(H) \subseteq V(G)$ y $A(H) \subseteq A(G)$, donde cada arista en $A(H)$ tiene sus extremos en $V(H)$. Si H es subgrafo de G, se escribe $H \subseteq G$ y se dice que G contiene a H.*

Ejemplo 3.5



H_1, H_2, H_3 subgrafos del grafo G

Definición 3.6 *Sea $G = (V, A)$ un grafo. Definimos el* ***grado de un vértice*** *como el número de aristas que inciden en el vértice; dado un vértice $v \in V$ su grado se denota $gr(v)$.*

El ***máximo grado*** *de G (según vértices) es el máximo grado de los vértices y se denota mediante $\Delta(G)$; es decir:*

$$\Delta(G) = \text{máx}\{gr(v) : v \in V(G)\}.$$

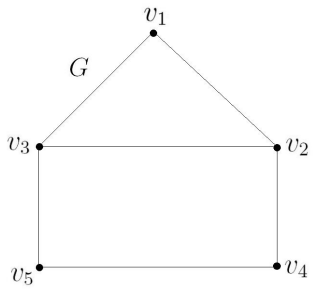
El ***mínimo grado*** *de G (según vértices) es el mínimo grado de los vértices y se denota mediante $\delta(G)$; es decir:*

$$\delta(G) = \text{mín}\{gr(v) : v \in V(G)\}.$$

El ***grado promedio*** *de G se define como la suma de los grados de los vértices de G sobre el número de vértices de G y se denota mediante $\Omega(G)$; es decir:*

$$\Omega(G) = \frac{\sum_{v \in V} gr(v)}{\mid V \mid}.$$

Ejemplo 3.6



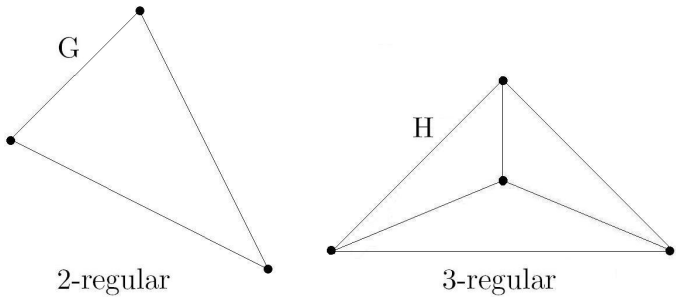
Notemos que:

- $gr(v_1) = 2$, $gr(v_2) = 3$, $gr(v_3) = 3$, $gr(v_4) = 2$ *y* $gr(v_5) = 2$.
- $\Delta(G) = 3$, $\delta(G) = 2$ *y* $\Omega(G) = \frac{12}{5}$.

Un grafo es ***k-regular*** *cuando el grado de todos los vértices de* G *es igual a* k*; es decir:*

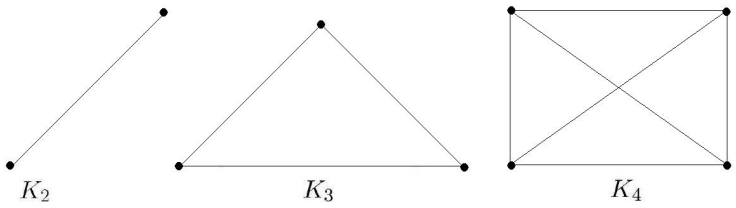
$$\Delta(G) = \delta(G) = k.$$

Ejemplo 3.7



Definición 3.7 *Si* $A = V^{[2]}$*, es decir* $\mid A \mid = \binom{|V|}{2}$ *el grafo* G *se llama* ***grafo completo*** *sobre* V *y se denota* $K_{|V|} = (V, A)$*.* K_n *denota el grafo completo sobre* n *vértices. Todo grafo completo con* n *vértices es* $(n-1)$*-regular.*

Ejemplo 3.8

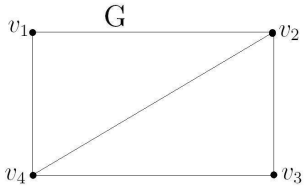


Definición 3.8 *Sea* $G = (V, A)$ *un grafo con* $V = \{v_1, \ldots, v_n\}$ *y* $A = \{a_1, \ldots, a_m\}$ *sus conjuntos de vértices y aristas respectivamente. Definimos:*

- *La* ***matriz de adyacencia*** *de* G *de orden* $n \times n$ *denotada* $M_A = (m_{ij})$ *cuyas entradas son* 1 *o* 0 *se define de la siguiente manera:*

$$(m_{ij}) = \begin{cases} 1, & si\ \{v_i, v_j\} \in A \\ 0, & si\ \{v_i, v_j\} \notin A. \end{cases}$$

Ejemplo 3.9 *Dado el siguiente grafo G, encontremos su matriz de adyacencia respecto a los vértices v_1, v_2, v_3 y v_4.*



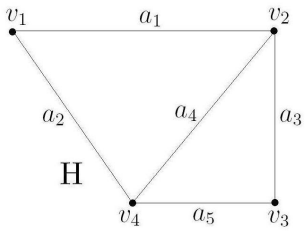
$$M_A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Notemos que M_A es una matriz simétrica.

- *La **matriz de incidencia** de G de orden $n \times m$ denotada $M_I = (m'_{ij})$ se define así:*

$$(m'_{ij}) = \begin{cases} 1, & \text{si } v_i \text{ es extremo de } a_j \\ 0, & \text{en otro caso.} \end{cases}$$

Ejemplo 3.10 *Dado el siguiente grafo H, encontremos su matriz de incidencia.*



$$M_I = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} a_1 & a_2 & a_3 & a_4 & a_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Las matrices definidas anteriormente dependen del orden en que tomemos los vértices y las aristas; en otras palabras, dependen de los nombres que les demos a los vértices y aristas del grafo correspondiente.

Lema 3.1 *En todo grafo $G = (V, A)$ se cumple la siguiente igualdad:*

$$2 \mid A \mid = \sum_{v \in V} gr(v).$$

Prueba. El resultado es inmediato, ya que cuando se suman los grados de los vértices de un grafo, cada arista de G se cuenta dos veces, porque a tiene dos vértices como extremos. □

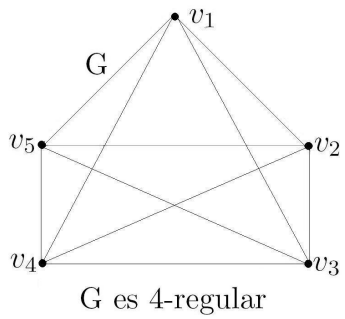
3.2. Dos Aplicaciones del Teorema 1.8

Procedemos a describir dos aplicaciones en teoría de grafos.

Notemos que:

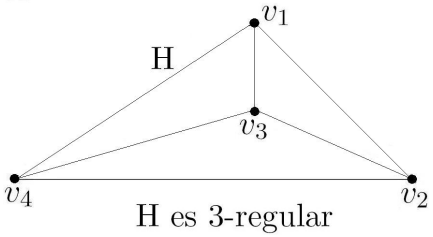
- Una conjetura bien conocida de Berge y Sauer, probada por Taskinov [53] (Referenciado en [1]), asegura que cualquier grafo 4-regular contiene un subgrafo 3-regular.

  Ejemplo 3.11 *Construyamos un grafo G 4-regular así:*



G es 4-regular

  Sea H un subgrafo 3-regular construido de la siguiente manera:

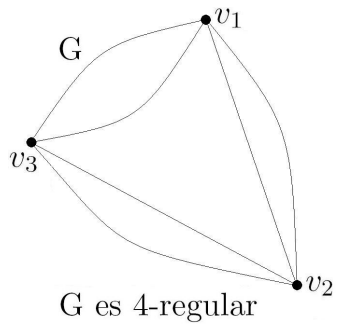


H es 3-regular

  Es claro que $H \subseteq G$ puesto que $V_H \subseteq V_G$ y $A_H \subseteq A_G$, donde cada arista en A_H tiene sus extremos en V_H.

  Presentamos el siguiente ejemplo para observar que la afirmación anterior es falsa para grafos con aristas múltiples.

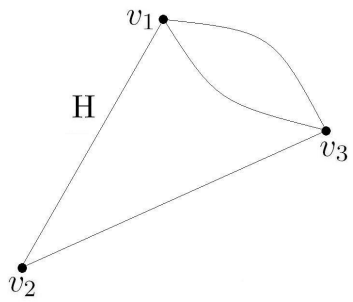
Ejemplo 3.12 *Construyamos un grafo 4-regular con aristas múltiples.*



G es 4-regular

Ahora tenemos que construir un subgrafo H 3-regular tal que $H \subseteq G$.

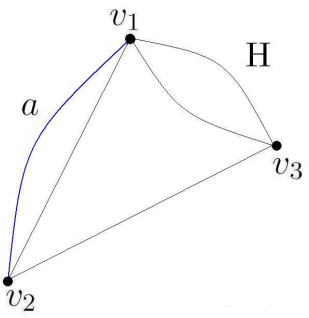
Si construimos H de la siguiente manera:



tenemos que H no es 3-regular puesto que:

$$gr(v_1) = 3,\ gr(v_2) = 2 \ \ y \ \ gr(v_3) = 3.$$

Si trazamos una arista extra a en H de la siguiente manera:



tenemos que:

$$gr(v_1) = 4,\ gr(v_2) = 3 \ \ y \ \ gr(v_3) = 3.$$

Por lo tanto H no es 3-regular, así G no contiene un 3-regular.

Primera Aplicación.

Teorema 3.1 *Para todo primo p, cualquier grafo $G = (V, A)$ con grado promedio mayor que $2p-2$ y grado máximo a lo sumo $2p-1$ contiene un subgrafo p-regular.*

Prueba. Sea $(M_{v,a})_{v\in V, a\in A}$ la matriz de incidencia de G definida así:

$$M_{v,a} = \begin{cases} 1, & \text{si } v \in a \\ 0, & \text{en otro caso.} \end{cases}$$

Asociemos cada arista a de G con una variable x_a y consideremos el polinomio

$$F = \prod_{v\in V} \left[1 - \left(\sum_{a\in A} M_{v,a} x_a \right)^{p-1} \right] - \prod_{a\in A} (1 - x_a),$$

sobre F_p.

Como:

- grado de $\prod_{v\in V} \left[1 - \left(\sum_{a\in A} M_{v,a}x_a\right)^{p-1}\right]$ es a lo sumo $(p-1) \mid V \mid$ y
- grado de $\prod_{a\in A}(1-x_a)$ es $\mid A \mid$,

entonces el grado total de F es $\mid A \mid$, puesto que $(p-1) \mid V \mid < \mid A \mid$, esto se da por hipótesis del grado promedio de G. En efecto;
por Lema 3.1 tenemos que

$$2 \mid A \mid = \sum_{v\in V} gr(v) \Rightarrow \mid A \mid = \frac{1}{2} \sum_{v\in V} gr(v)$$

luego

$$\begin{aligned} \Omega(G) = \frac{\sum_{v\in V} gr(v)}{\mid V \mid} > 2p-2 &\Rightarrow \sum_{v\in V} gr(v) > (2p-2) \mid V \mid \\ &\Rightarrow \sum_{v\in V} gr(v) > 2(p-1) \mid V \mid \\ &\Rightarrow \frac{1}{2} \sum_{v\in V} gr(v) > (p-1) \mid V \mid \\ &\Rightarrow \mid A \mid > (p-1) \mid V \mid . \end{aligned}$$

Como el grado de F esta determinado por $\prod_{a\in A}(1-x_a)$ entonces el coeficiente de $\prod_{a\in A} x_a$ en F es $(-1)^{|A|+1} \neq 0$.
Por lo tanto si $t_a = 1$, $a \in A$, el grado de F es $\sum_{a\in A} t_a =\mid A \mid$.

Finalmente si $S_a = \{0, 1\}$, $S_a \subseteq F_p$. Por Teorema 1.8, existen valores $x_a \in \{0, 1\} = S_a$ tales que:

$$F(x_a : a \in A) \neq 0.$$

Por la definición de F, el vector anterior $(x_a : a \in A)$ no es el vector cero, ya que para este vector $F = 0$. Además para este vector $\sum_{a\in A} M_{v,a}x_a$ es cero módulo p para cada v porque de lo contrario F debería anularse en este punto.

Como $\sum_{\substack{a\in A\\ x_a=1}} M_{v,a} = gr(v)$ para todo $v \in V$ tenemos que en el subgrafo consistente de todas la aristas $a \in A$ para las cuales $x_a = 1$ todos los grados son divisibles por p, y como el máximo grado es menor que $2p$ todos los grados positivos de los vértices son precisamente p. Lo cual completa la prueba. □

A continuación presentamos un ejemplo del teorema anterior.

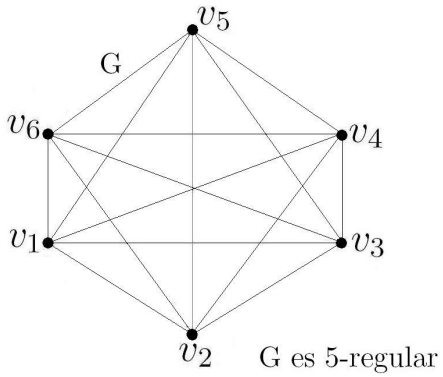
Ejemplo 3.13

i) *Consideremos un grafo regular.*
Tomando $p = 3$ tenemos que:

$$\Omega(G) > 2(3) - 2 = 4,$$

$$\Delta(G) \leq 2(3) - 1 = 5.$$

Construyamos el grafo G de la siguiente manera:



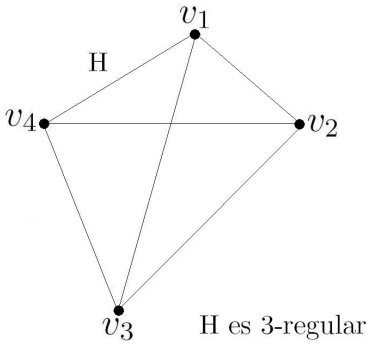
G es 5-regular

Notemos que:

$gr(v_i) = 5$, $1 \leq i \leq 6$ *por ser* G *un grafo* 5*-regular. Luego*

$$\Omega(G) = \frac{6(5)}{6} = 5 \ \ y \ \ \Delta(G) = 5.$$

Por lo tanto; G *con las condiciones anteriores contiene un subgrafo* 3*-regular, por ejemplo:*

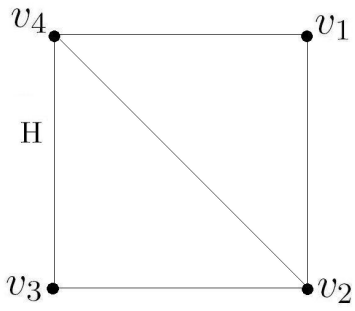


Así $H \subseteq G$.

ii) *Consideremos un grafo no regular.*
Tomando $p = 2$ *tenemos que:*

$$\Omega(H) > 2(2) - 2 = 2,$$
$$\Delta(H) \leq 2(2) - 1 = 3.$$

Construyamos el grafo H *de la siguiente manera:*



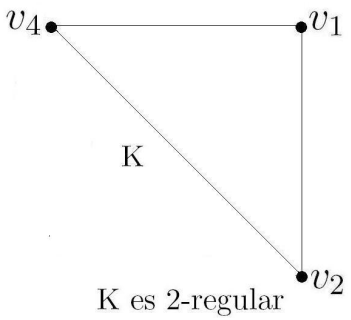
Notemos que:

$gr(v_1) = 2 \quad gr(v_2) = 3$
$gr(v_3) = 2 \quad gr(v_4) = 3.$

Además

$\Omega(H) = \frac{2+3+2+3}{4} = \frac{10}{4} = 2{,}5 > 2 \quad y \quad \Delta(H) = 3.$

Luego H con las condiciones anteriores contiene un subgrafo 2-regular, por ejemplo:



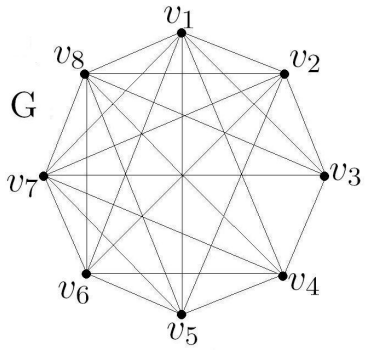
Notemos que:

- La afirmación del Teorema 3.1 es válida también para potencias primas p (ver [6], referenciado en [1]), pero no se conoce si es válido para todo entero p.

Ejemplo 3.14 *Tomando $p = 4 = 2^2$ tenemos*

$$\Omega(G) > 2(4) - 2 = 6 \;\; y \;\; \Delta(G) \leq 2(4) - 1 = 7.$$

Construyamos G de la siguiente manera:



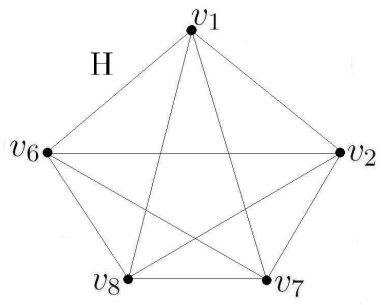
Notemos que:

$gr(v_1) = 7 \quad gr(v_2) = 6 \quad gr(v_3) = 5 \quad gr(v_4) = 6$
$gr(v_5) = 6 \quad gr(v_6) = 6 \quad gr(v_7) = 7 \quad gr(v_8) = 7.$

Además

$\Omega(G) = \frac{7+6+5+6+6+6+7+7}{8} = \frac{50}{8} = 6{,}25 > 6$ *y* $\Delta(G) = 7.$

Luego G con las condiciones anteriores contiene un subgrafo 4-regular, por ejemplo:



H es 4-regular

- Observemos que en los ejemplos anteriores los subgrafos construidos no son únicos.
- Combinando la observación anterior con algunos argumentos combinatorios adicionales, se puede demostrar que: Para todo $k \geq 4r$, todo grafo k-regular contiene un subgrafo r-regular.

Finalizamos esta sección con un resultado geométrico, el cual es una consecuencia del Teorema 1.8.

Segunda Aplicación.

Teorema 3.2 *Sean $H_1, \ldots, H_m$ una familia de hiperplanos en $\mathbb{R}^n$ que cubre todos los vértices del cubo unidad $\{0,1\}^n$ excepto uno. Entonces $m \geq n$.*

Prueba. Argumentamos por contradicción.

Supongamos que $m < n$. Sea C el conjunto de vértices del cubo unidad $\{0,1\}^n$ definido así:

$$C = \{0,1\}^n = \{(x_1, \ldots, x_n) : x_k \in \{0,1\} \text{ para } k = 1, \ldots, n\}.$$

Por hipótesis $H_1, \ldots, H_m \in \mathbb{R}^n$ cubren todos los vértices del cubo unidad $\{0,1\}^n$ excepto uno, entonces supongamos que el vértice no cubierto es el vector cero.

Sea $(a_i, x) = b_i$ la ecuación definiendo a H_i, donde $x = (x_1, \ldots, x_n)$ y (a, b) denota el producto interno entre los vectores a y b, esto es:

$$H_i = \{x : (a_i, x) = b_i,\ a_i \text{ vector normal al plano}\}.$$

Notemos que para todo i, $b_i \neq 0$, ya que H_i no cubre el origen.

Consideremos el polinomio

$$P(x) = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) - \prod_{i=1}^{m} [(a_i, x) - b_i].$$

Como:

- grado de $\prod_{i=1}^{n}(x_i - 1)$ es n y
- grado de $\prod_{i=1}^{m}[(a_i, x) - b_i]$ es $-\infty$,

entonces $grad(P) = n$ y claramente el coeficiente de $\prod_{i=1}^{n} x_i$ en P es

$$(-1)^{n+m+1} \prod_{j=1}^{m} b_j \neq 0.$$

Por consiguiente por Teorema 1.8 existe un punto $s \in \{0,1\}^n$ tal que

$$P(s) \neq 0. \tag{3.1}$$

Luego s no es el vector cero, puesto que $s \in \{0,1\}^n$ ya que P se anula sobre él, es decir, cuando s es el vector cero, $P(s) = 0$.

Como s no es el vector cero, es algún otro vértice del cubo unidad $\{0,1\}^n$ cubierto por algún hiperplano H_i, esto es, $s \in H_i$ así se cumple que $(a_i, s) = b_i$, es decir, $(a_i, s) - b_i = 0$ para algún i. Entonces tenemos:

i) $\prod_{i=1}^{n}(s_i - 1) = 0$ implicando que $(-1)^{n+m+1}\prod_{j=1}^{m} b_j \prod_{i=1}^{n}(s_i - 1) = 0$ y

ii) $\prod_{i=1}^{m}[(a_i, s) - b_i] = 0$.

Luego de i) y ii) tenemos que P se anula sobre este punto, esto es;

$$P(s) = 0.$$

lo cual contradice (3.1). Por lo tanto $m \geq n$. $\square$

Capítulo 4

Conclusiones

En este capítulo presentamos algunas conclusiones obtenidas del desarrollo de este trabajo de grado denominado "Algunas Aplicaciones del Teorema de los Ceros de Hilbert".

1. La mayoría de pruebas presentadas en este trabajo se basan en los teoremas denominados los ceros de Hilbert, probados en el capítulo 1, cuyas pruebas son algebraicas y determinan una técnica para el estudio de algunos problemas combinatorios; es decir tienen diversas aplicaciones en Teoría de Números Aditiva, en Combinatoria y en Teoría de Grafos.

2. En la mayoría de las pruebas realizadas en este trabajo utilizamos la misma técnica denominada Combinatorial Nullstellensatz (ver Teorema 1.8), donde se define un polinomio P sobre un campo arbitrario F, el cual en muchas ocasiones no es fácil deducirlo ya que este debe satisfacer que $P(s_1, \ldots, s_n) = 0$ para toda n-tupla $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, así siguiendo las hipótesis de esta técnica podemos establecer una contradicción y obtener el resultado deseado.

3. La prueba del Teorema de Chevalley-Warning la presentamos en el caso de campos finitos primos, aunque la prueba se extiende fácilmente a campos finitos arbitrarios.

4. La mayoría de los resultados presentados en el capítulo 2 son aplicaciones del Método Polinomial, pero el principal problema de este método en su aplicación consiste en determinar el polinomio y el coeficiente requerido.

5. En el Teorema de Cauchy-Davenport consideramos A y B subconjuntos no vacíos de $\mathbb{Z}_p$, pero este resultado se extiende si consideramos A y B conjuntos finitos no vacíos de un espacio vectorial V sobre F_p.

6. Para las aplicaciones en teoría de grafos es importante destacar la relación que existe entre grafos y polinomios ya que podemos asociar cada arista a de un grafo G con una variable x_a y de esta manera definir un polinomio adecuado para la aplicación del Teorema 1.8.

Bibliografía

[1] Alon Noga, *Combinatorial Nullstellensatz*. Http://www.math.tau.ac.il/~nogaa/

[2] Alon Noga , Nathanson Melvyn , Ruzsa Imre, *The polymomial method and restricted sums of congruence classes, J. Number Theory 56 (1996), 404-417.*

[3] Bollobas Bela, *Modern Graph Theory*. Springer, 1998.

[4] Cerón Samin , Martínez Wilson , Palechor Liliana, *Fundamentos de Coloreado de Grafos y Teoría de Ramsey*. Tesis Universidad del Cauca, 2005.

[5] Cox David , Little John , O'Shea Donal, *Ideals, Varieties, and Algorithms*. Springer, 1997,1992.

[6] Dissett Luis, *MLM 2070 Teoría de Grafos*. Página web: http:// www.mat.puc.cl/~ldissett/mlm2070.

[7] Gross Jonathan, Yellen Jay, *Graph Theory and Its Applications*. Chapman & Hall/CRC, 2006.

[8] Lidl Rudolf, Niedereitr Harald, *Finite Fields*. Cambridge University Press, 1997.

[9] Nathanson Melvyn, *Additive Number Theory*. Springer, 1996.

[10] Tao Terence , Vu Van H, *Additive Combinatorics*. Cambridge University Press, 2006.