LA CONJETURA DE SNEVILY

Lady Catherine Cadena Betancourt
Angélica María Dulcey Sánchez

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
Mayo 2013

LA CONJETURA DE SNEVILY

Autoras

Lady Catherine Cadena Betancourt

Angélica María Dulcey Sánchez

Trabajo de grado como requisito

parcial para optar el título de

Licenciadas en Matemáticas

Director: M.Cs. Carlos Arturo Rodriguez Palma

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga

Mayo 2013

Agradecimientos

Expresamos nuestra más sincera gratitud al profesor Carlos Arturo Rodríguez por haber aceptado ser nuestro director en este trabajo. Gracias a su amplio conocimiento en Teoría de Números y Álgebra Moderna, a su dedicación, asesoría, amistad y esfuerzo la realización de este trabajo se desarrolló en forma exitosa. Del mismo modo reconocemos que su apoyo fue incondicional en la participación del evento ALTENCOA5 (Álgebra, Teoría de Números y sus Aplicaciones), al cual asistimos en calidad de ponentes, mostrando la investigación elaborada sobre la Conjetura de Snevily.

A la Universidad Industrial de Santander, especialmente a la escuela de Matemáticas, por permitirnos hacer parte de sus estudiantes y formarnos bajo la tutoría de sus profesores, a ellos queremos decirles gracias por compartir su conocimiento y amor hacia las Matemáticas, por inculcarnos siempre el compromiso formativo con las futuras generaciones, en especial a los docentes Gabriel Yañez y Edilberto Reyes.

Finalmente a nuestras familias, por su apoyo incondicional, esfuerzo y manifestaciones de cariño que nos permitieron superar la adversidad.

Dedicatoria

A nuestros abuelos que nos dieron las bases de nuestra formación...

A todos los amantes y estudiosos de la Matemática...

Resumen

Título: La Conjetura de Snevily. [1]

Autoras: Catherine Cadena, Angélica Dulcey.[2]

Palabras Claves: Transversal Latina, Tabla de Adición de Cayley, Grupo Abeliano, Combinatoria de Nulltellensatz, Caracteres, Función Multilineal, Conjetura de Snevily.

Contenido: Una transversal de una matriz $n \times n$ es una colección de n celdas, dos de las cuales no se encuentran en la misma fila o columna; si, los elementos de la transversal son distintos se denomina latina. Un resultado alrededor de la tabla de adición de Cayley conjeturado por Hunter S. Snevily en [9], afirma que: Para cualquier n impar, toda submatriz $k \times k$ de la tabla de adición de Cayley de $\mathbb{Z}_n$ contiene una transversal latina. De manera general, Si $A = \{a_1, a_2, \cdots, a_k\}$ y $B = \{b_1, b_2, \cdots, b_k\}$ son dos subconjuntos de un grupo abeliano G de orden impar, entonces existe una permutación $\pi \in S_k$ tal que las sumas $a_i + b_{\pi(i)}$ con $1 \leq i \leq k$, son distintas dos a dos. Alon mostró en [1] la conjetura para grupos de orden primo, incluso cuando A es una secuencia de k elementos de G, con $k < |G|$. Dasgupta, Károlyi y otros en [3] demostraron la conjetura para grupos cíclicos de orden impar y, para los grupos $\mathbb{Z}_{(p^\alpha)}$ y $(\mathbb{Z}_p)^\alpha$. Finalmente en el 2009 Bodan Arzovsky demuestra en [2] la conjetura para el caso G de orden impar.

[1] Monografía.

[2] Facultad de Ciencias. Escuela de Matemáticas. Director: Carlos Arturo Rodríguez Palma, Magíster en Matemáticas.

Abstract

Title: The Snevily's Conjeture. [3]

Authors: Catherine Cadena, Angélica Dulcey.[4]

Keywords: Transversal Latin, The Cayley Addition Table, Abelian Group, Combinatorial Null-tellensatz, Characters, Multilinear Function, Snevily's Conjecture.

Subject: A transversal in an $n \times n$ matrix is a collection of n cells, no two in the same row or in the same column; if, the transversal's elements are different, it is called latin. A result about the Cayley addition table conjectured by Hunter S. Snevily in [3],states that: For any n odd, all $k \times k$ submatrix k of the Cayley addition table of Z_n contains a latin transversal. In general, if $A = \{a_1, a_2, \cdots, a_k\}$ and $B = \{b_1, b_2, \cdots, b_k\}$ are two subsets of an abelian group G of odd order , then there is a permutation $\pi \in S_k$ such that $a_i + b_{\pi(i)}$, $1 \leq i \leq k$, are pairwise distinct. Alon showed in [1] that this conjecture is true for groups of prime order , even when A is a sequence of k elements of G, with $k < |G|$. Dasgupta, Károlyi and others in [2] proved the conjecture for odd-order cyclic groups and for groups $\mathbb{Z}_{(p^\alpha)}$ and $(\mathbb{Z}_p)^\alpha$. Finally in 2009 Bodan Arzovsky proves in [2] the conjecture for the case G of odd order.

[3]Monograph.

[4]Faculty of Sciences. School of Mathematics. Director: Carlos Arturo Rodríguez Palma, Master of Mathematics.

Índice general

Índice de cuadros

Introducción

Alrededor del siglo XVII, el matemático Pierre Fermat despertó el interés por la teoría de números, dicen que retaba a otros matemáticos a resolver problemas que él mismo había resuelto o al menos conjeturado. La facilidad para formular conjeturas sencillas hacía a los problemas mucho más intrigantes. Fermat conjeturó resultados muy interesantes dentro de la teoría de números que fueron demostrados por grandes matemáticos como Euler, Kummer, Dirichlet, Legendre entre otros.

Con el paso del tiempo la teoría de números ha cobrado importancia y muchos han sido los interesados en trabajar esta rama de la matemática, "la teoría de los números ocupa un peculiar y distinguido lugar entre las diversas ramas de las matemáticas. Que su objetivo principal sea el estudio de algo tan conocido y familiar como son los enteros, sus propiedades y sus relaciones, explica el interés que ha suscitado siempre entre muchos ciudadanos, quienes, aun careciendo de la formación matemática apropiada, se sienten fascinados por sus problemas, tan fáciles de enunciar y, sin embargo, tan difíciles a veces de resolver"(Cilleruelo,J.y Córdoba,A.(2010))

A raíz de las distintas características y propiedades que se han podido apreciar en los enteros, la teoría de números se divide en distintas ramas, una de éstas es la teoría de números aditiva, que en síntesis trata de resolver los problemas de representación de los números enteros como sumas.

La teoría de números aditiva estudia dos tipos de problemas, los problemas clásicos que se denominan problemas directos y los problemas inversos.

Un problema directo de la teoría de números aditiva es un problema en el cual dados dos conjuntos

finitos A y B de un grupo abeliano G, se trata de determinar la estructura y las propiedades del conjunto suma. Ejemplos de este tipo de problema son: el conocido Teorema de Lagrange que afirma que todo entero no negativo puede escribirse como la suma de cuatro cuadrados; el teorema Cauchy-Davenport que dice para p primo y conjuntos no vacíos $A, B \subset \mathbb{Z}_p$, se satisface $|A + B| \geq min(p, |A| + |B| - 1)$.

Un problema inverso de la teoría de números aditiva es un problema en el cual se deduce la estructura de dos conjuntos cuyo conjunto suma tiene pocos elementos. Un ejemplo característico es el teorema obtenido por Vosper en 1956, según el cual la igualdad $|A + B| = |A| + |B| - 1$ en el teorema de Cauchy-Davenport se satisface solamente si ambos conjuntos A y B son progresiones aritméticas con la misma diferencia.

A través de la tabla de adición de Cayley, podemos representar la suma de dos conjuntos; y deducir propiedades tales como la conmutatividad del conjunto suma si observamos que la tabla es simétrica respecto a su diagonal principal.

Hunter Snevily, hace observaciones sobre la tabla de Cayley y alrededor del año 1999 en [9] conjetura:

Conjetura 1: *P*ara cualquier n impar, y cualquier $k \in \{1, 2, \cdots, n\}$ toda submatriz $k \times k$ de la tabla de adición de Cayley de $\mathbb{Z}_n$ contiene una transversal latina.

Conjetura 2: *P*ara cualquier n par y cualquier $k \in \{1, 2, \cdots, n\}$, cualquier submatriz $k \times k$ de la tabla de adición de Cayley de $\mathbb{Z}_n$ contiene una transversal latina siempre que la submatriz no sea un subgrupo de orden par o una traslación de tal subgrupo.

A partir de la fecha en que se propuso la Conjetura 1 se han obtenido algunos resultados alrededor de ésta, estudiar y dar a conocer estos resultados es la tarea fundamental de esta monografía.

El trabajo está organizado en cuatro capítulos. En el primer capítulo consignamos las definiciones, las proposiciones y los teoremas necesarios para abordar y entender los principales planteamientos que han sido propuestos en busqueda de la demostración de ésta conjetura; en el segundo capítulo

estudiamos la herramienta principal que se utiliza para demostrar algunos casos particulares de la Conjetura de Snevily, en el tercer capítulo presentamos en forma ejemplificada la Conjetura y estudiamos los trabajos de Alon en [1]; Dasgupta, Károlyi, Serra y Szegedy en [3] quienes han aportado algunos resultados sobre la Conjetura, y finalmente estudiamos el planteamiento de Bodan Arzovsky en [2] quien logra demostrar el problema para grupos abelianos de orden impar; en el cuarto capítulo presentamos las conclusiones del trabajo de investigación.

Capítulo 1

Marco Teórico

En este capítulo mostraremos algunos resultados que son importantes para poder comprender el contenido de este trabajo monográfico.[1] Presentaremos algunos resultados sobre grupos abelianos, campos y anillos finitos, extensiones, anillos de polinomios, raíces de la unidad, polinomios ciclótomicos y caracteres.

1.1. Teoremas Importantes sobre Grupos Abelianos

Los siguientes conceptos y resultados fueron tomados de [4], [6] y [11] en donde se pueden encontrar en detalle las respectivas demostraciones.

Definición 1.1. Un grupo es un conjunto G con una operación binaria $*$ en G tal que se cumplen las siguientes propiedades:

1. Asociativa; esto es, para todo $a, b, c \in G$

$$a * (b * c) = (a * b) * c$$

[1] Como no es nuestro interés profundizar en los conceptos básicos de cualquier curso de álgebra moderna, mostraremos explícitamente los resultados; si el lector está interesado en la demostración de alguno de ellos, le invitamos a consultar la bibliografía.

2. Existe una identidad (ó unicidad) $e \in G$ tal que para todo $a \in G$

$$a * e = e * a = a$$

3. Para cada $a \in G$, existe un único elemento inverso $a^{-1} \in G$ tal que:

$$a * a^{-1} = a^{-1} * a = e$$

   Si el grupo tambien satisface

4. Para todo $a, b \in G$

$$a * b = b * a$$

   El grupo se llama abeliano ó conmutativo.

Definición 1.2. Un grupo es finito si contiene un número finito de elementos. Al número de elementos de un grupo finito se le llama su orden. Escribimos $|G|$ para denotar el orden del grupo finito G.

Definición 1.3. Un grupo multiplicativo G se denomina cíclico, si existe algún elemento $g \in G$ tal que para todo $b \in G$ existe algún y con $b = g^y$. El elemento g se llama un **Generador** del grupo cíclico y escribimos $G = \langle g \rangle$.

Teorema 1.1. *i. Cada subgrupo de un grupo cíclico es cíclico.*

ii. En un grupo cíclico finito $\langle g \rangle$ de orden m, el elemento g^t genera un subgrupo de orden $\frac{m}{gcd(t,m)}$.

iii. Sea d un divisor positivo del orden del grupo cíclico finito $\langle g \rangle$. Entonces $\langle g \rangle$ contiene $\phi(d)$ elementos de orden d. (ϕ es la función de Euler)

iv. Un grupo cíclico finito $\langle g \rangle$ de orden m contiene $\phi(m)$ generadores; es decir, elementos g^r tales que $\langle g^r \rangle = \langle g \rangle$. Los generadores son las potencias g^r con $gcd(r, m) = 1$.

Teorema 1.2. *(Unicidad de los Grupos Cíclicos de Orden n) Si n es un entero positivo, tenemos que el grupo cíclico de orden n es el único grupo de este orden si y sólo si n y su función de Euler son coprimos, es decir, $(\phi(n), n) = 1$.*

1.2. Anillos y Campos

El segundo objeto algebraico que consideraremos se denomina *Anillo*. Para cualquier persona le es familiar el hecho de que en muchos sistemas numéricos se nos muestren dos operaciones binarias distintas: adición y producto. Ahora se definirá un tipo de estructura algebráica conocida como Anillo, el cual comparte algunas de las propiedades básicas de esos sistemas numéricos. Estos resultados fueron tomados de [8],[6] y [11] donde se pueden encontrar las respectivas demostraciones.

Definición 1.4. Un anillo $(R, +, \cdot)$ es un conjunto R, que junto con dos operaciones binarias denotadas por + y ·, tales que:

i. R es un grupo abeliano con respecto a +.

ii. $\cdot$ es asociativo, esto es, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in R$

iii. Se cumplen las dos leyes distributivas, es decir, para todo $a, b, c \in R$ se tiene que

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

y

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Los anillos se clasifican de acuerdo a la siguiente definición:

Definición 1.5. Se dice que:

i. Un anillo es llamado Anillo con Identidad si el anillo tiene identidad multiplicativa, es decir, si existe un elemento e tal que $ae = ea = a$ para todo $a \in R$.

ii. Un anillo es llamado Conmutativo si $\cdot$ es conmutativo.

iii. Un anillo es llamado un Dominio Integral si éste es un Anillo conmutativo con identidad $e \neq 0$ en el cual $ab = 0$ implica que $a = 0$ ó $b = 0$.

iv. Un anillo es llamado Anillo con División si los elementos de R distintos de cero bajo $\cdot$ forman un grupo.

v. Un anillo conmutativo con división es llamado un Campo.

El último concepto es de gran importancia en nuestro trabajo, por tal razón haremos énfasis especial en éste, así, podemos decir que un Campo es un conjunto F que junto con dos operaciones binarias llamadas, adición y producto, están definidas y el cual contiene dos elementos distintos 0 y e con $0 \neq e$, por tanto F es un grupo abeliano respecto a la adición, con 0 como elemento identidad, y los elementos distintos de cero forman un grupo abeliano respecto a la multiplicación con e como elemento identidad. Las dos operaciones, se relacionan mediante las leyes distributivas $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$. El elemento 0 es llamado el elemento cero y e es el elemento identidad multiplicativo o simplemente identidad. Un Campo no tiene divisores de cero, esto es si $ab = 0$ y $a = 0$ entonces multiplicando por a^{-1} obtenemos $b = a^{-1}0 = 0$.

Definición 1.6. Se llama característica de un anillo unitario al menor número natural n tal que $na = 0$ para todo $a \in R$, si no existe tal número se dice que el anillo es de característica nula.

Teorema 1.3. *Todo Dominio Integral Finito es un Campo.*

Teorema 1.4. *Un anillo $R \neq 0$ de característica positiva, con identidad y sin divisores de cero tiene característica prima.*

Corolario 1.4.1. *Un campo finito tiene característica prima.*

Para cada primo p el anillo de clases residuales $\mathbb{Z}/[p]$ forma un campo con p elementos, que puede ser identificado con el campo F_p de orden p; esto se resume en el siguiente resultado:

Definición 1.7. Para un primo p, sea F_p el conjunto de enteros $\{0, 1, ..., p-1\}$ y sea $\varphi : \mathbb{Z}/p \longrightarrow F_p$ la función definida por $\varphi([a]) = a$ para $a = 0, 1, ...p - 1$. Entones F_p dotado con la estructura de campo inducida por φ, es un campo finito.

El campo F_p desempeña un papel importante en la teoría de cuerpos, puesto que cada campo de característica p contiene una copia isomorfa de F_p. Esta observación junto con el hecho de que

cada campo finito tiene característica prima son fundamentales para la clasificación de campos finitos.

Teorema 1.5. *Sea F un campo finito. Entonces F tiene p^n elementos donde el primo p es la característica de F y n es el grado de F sobre su subcampo primo.*

Lema 1.1. *Si F es un campo finito con q elementos, entonces cada $f \in F$ satisface $f^q = f$*

Lema 1.2. *Si F es un campo finito con q elementos, y K es un subcampo de F, entonces el polinomio $x^q - x$ en $K[x]$ se factoriza en $F[x]$ como:*

$$x^q - x = \prod_{a \in F} (x - a)$$

y F es el campo de ruptura (división) de $x^q - x$ sobre K.

Teorema 1.6. *Para cada primo p y cada $n \in N$ existe un campo finito con p^n elementos. Todo campo finito con $q = p^n$ elementos es isomorfo al campo de ruptura de $x^q - x$ sobre F_p.*

Teorema 1.7. *Sea F_q un campo finito con $q = p^n$ elementos. Entonces cada subcampo de F_q tiene orden p^m donde m es un divisor positivo de n. Reciprocamente si m es un divisor de n, existe exactamente un subcampo de F_q de orden p^m.*

Teorema 1.8. *Para cada campo finito F_q el grupo multiplicativo $F_q^\times$ es ciclíco.*

Definición 1.8. Un generador de $F_q^\times$ se llama elemento primitivo de F_q.

Definición 1.9. F_q contiene $\varphi(q-1)$ elementos primitivos donde φ es la función Phi de Euler.

1.3. Anillos de Polinomios

Definición 1.10. Se define la adición y el producto de polinomios como:

i. La adición de $f(x)$ y $g(x)$, $f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i$.

ii. El producto de $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{j=0}^{n} b_j x^j$ es

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k$$

donde $c_k = \sum_{\substack{i+j=k, \\ 0\leq i\leq n, \\ 0\leq j\leq m}} a_i b_j$.

Así el anillo formado por los polinomios sobre R, con las operaciones descritas, es llamado el Anillo de los Polinomios sobre R y se denota por $R[x]$.

El elemento cero de $R[x]$ es el polinomio cuyos coeficientes son todos cero, es llamado el polinomio cero y se denota por 0.[2]

Definición 1.11. Sea $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio sobre R que no es el polinomio cero. Podemos suponer que $a_n \neq 0$, entonces a_n es llamado el *coeficiente principal* de $f(x)$ y a_0 el *término constante* mientras que n es llamado el grado de $f(x)$, denotado por $n = deg(f(x)) = deg(f)$. Por notación designaremos $deg(0) = -\infty$.

Polinomios de grado menor o igual a cero son llamados *polinomios constantes*. Si R tiene la identidad 1 y el coeficiente principal de $f(x)$ es 1, entonces $f(x)$ es llamado *Polinomio Mónico*.

Definición 1.12. Sea K un subcampo de F y $\alpha \in F$. Si α satisface una ecuación polinomial no trivial con coeficientes en K, esto es, si $a_n\alpha^n + \cdots + a_1\alpha + a_0 =$ con $a_i \in K$ no todos ceros, entonces α es llamado *algebraico* sobre K.

Definición 1.13. Si $\alpha \in F$ es *algebraico* sobre K, entonces el único polinomio mónico determinado $g \in K[x]$ que genera el ideal $J = \{f \in K[x] : f(\alpha) = 0\}$ de $K[x]$ es llamado el *polinomio minimal* de α sobre K.

Teorema 1.9. *Sea R un anillo, entonces*

i. $R[x]$ *es conmutativo sí y sólo sí R es conmutativo.*

ii. $R[x]$ *es un anillo con identidad sí y sólo sí R tiene una identidad.*

[2]Debe ser claro si el 0 representa el elemento cero o el polinomio cero.

iii. $R[x]$ es un dominio integral sí y sólo sí R es un dominio integral.

Teorema 1.10. *Sean $f_1, f_2, \cdots, f_n$ polinomios en $F[x]$ los cuales no son todos cero. Entonces existe un único polinomio mónico $d \in F[x]$ con las siguientes propiedades:*

1. *d divide a cada f_j con $1 \leq j \leq n$,*
2. *Todo polinomio $c \in F[x]$ divisor de cada f_j, $1 \leq j \leq n$, divide a d. Además, d puede ser expresado en la forma*

$$d = b_1 f_1 + \cdots + b_n f_n$$

con $b_1, b_2, \cdots, b_n \in F[x]$

Definición 1.14. Un polinomio $p \in F[x]$ es llamado *irreducible sobre F* (o irreducible en $F[x]$ o primo en $F[x]$) si p tiene grado positivo y $p = bc$ con $b, c \in F[x]$ implica que uno de los dos b o c es una constante polinomial.

Lema 1.3. *Si un polinomio irreducible p en $F[x]$ divide a un producto de polinomios $f_1 f_2 \cdots f_m$ en $F[x]$, entonces al menos uno de los factores f_j es divisible por p.*

Teorema 1.11. *(Factorización Única en $F[x]$) Cualquier polinomio $f \in F[x]$ de grado positivo puede escribirse de la forma*

$$f = a p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

donde $a \in F$, $p_1, p_2, \cdots, p_k$ son polinomios mónicos irreducibles en $F[x]$, y $r_1, r_2, \cdots, r_k$ son enteros positivos. Por otra parte esta factorización es única salvo el orden de los factores.

Existe un resultado importante que relaciona las raíces de un polinomio con el concepto de divisibilidad, se resume en el siguiente teorema:

Teorema 1.12. *Un elemento $b \in F$ es una raiz de un polinomio $f \in F[x]$ sí y sólo sí $x - b$ es divisible por $f(x)$.*

1.4. Extensiones de Campos

Definición 1.15. Decimos que el cuerpo L es una extensión de K, si K es un subcuerpo de L, es decir, $K \subset L$ y las operaciones $+$ y $\cdot$ en K coinciden con las de L.

Definición 1.16. Se dice que una extensión, L/K, es:

1. simple, si $L = K(a)$ con $a \in L$.
2. algebraica, si todo $a \in L$ es algebraico sobre K, es decir, existe un polinomio $P \in K[x]$ tal que $P(a) = 0$.
3. trascendente, si no es algebraica. En particular existirá algún $a \in L$ que es trascendente, es decir, que no es no algebraico sobre k.

Si L/K es una extensión de K, entonces L es un espacio vectorial sobre K.

Definición 1.17. A la dimensión de L como espacio vectorial sobre K se le llama grado de L/K y se escribe $[L : K]$. Si el grado es finito se dice que la extensión es finita, en caso contrario se dice que es infinita.

Definición 1.18. Si a es algebraico sobre K, se dice que $p \in K[x]$ es el polinomio mínimo de a si p es mónico, a es un cero de p y no hay otro polinomio de grado menor con estas características.

Teorema 1.13. *Si L/K y M/L son extensiones de campos, entonces* $[M : K] = [M : L][L : K]$ *De hecho, si L/K y M/L son finitas, viéndolas como espacios vectoriales, tienen como bases* $\{x_1, x_2, \cdots, x_r\}$, $\{y_1, y_2, \cdots, y_s\}$ *respectivamente, entonces* $\{x_1y_1, x_2y_2, \cdots, x_ry_s\}$ *es una base de M/K.*

Teorema 1.14. *Toda extensión finita es algebraica.*

1.5. Raíces de Polinomios Irreducibles

Lema 1.4. *Sea $f \in F_q[x]$ un polinomio irreducible sobre el campo finito F_q y sea α una raíz de f en una extensión de F_q. Entonces para un polinomio $h \in F_q[x]$ tenemos: $h(\alpha) = 0$ sí y solo sí f/h.*

Lema 1.5. *Si $f \in F_q[x]$ un polinomio irreducible sobre el campo finito F_q de grado m, entonces $f(x)$ divide a $x^{q^n} - x$ sí y solo sí m/n.*

Teorema 1.15. *Si $f \in F_q[x]$ es un polinomio irreducible sobre F_q de grado m, entonces f tiene una raíz α en F_{q^m}. Mas aún, todas las raíces de f son simples y son los m elementos distintos $\alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$.*

Corolario 1.15.1. *Sea f un polinomio irreducible en $F_q[x]$ de grado m, entonces el campo de ruptura de f sobre F_q es F_{q^m}.*

Corolario 1.15.2. *Cualesquiera dos polinomios irreducibles en $F_q[x]$ del mismo grado, tienen campos de ruptura isomorfos.*

Definición 1.19. Sea F_{q^m} una extención de F_q y sea $\alpha \in F_{q^m}$, entonces los elementos α, α^q, α^{q^2}, $\cdots$, $\alpha^{q^{m-1}}$ se denominan conjugados de α respecto a F_q.

Nota: los conjugados de $\alpha \in F_{q^m}$ respecto a F_q son distintos sí y sólo sí el polinomio minimal de α sobre F_q tiene grado m. Por otra parte, si el grado d de este polinomio minimal es un divisor de m, entonces los conjugados de α respecto F_q son los d elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}$, cada uno repetido d/m veces.

1.6. Raíces de la Unidad y Polinomios Ciclotómicos

En esta sección se muestra el campo de ruptura del polinomio $x^n - 1$ sobre un campo K.

Definición 1.20. Sea $n \in \mathbb{Z}^+$. El campo de ruptura de $x^n - 1$ sobre K se llama $n - th$ Campo Ciclótomico sobre K, denotado por K^n. La raíces de $x^n - 1$ son llamadas $n - th$ raíces de la unidad sobre K y el conjunto de todas las raíces se denota por E^n.

Teorema 1.16. *Sea $n \in \mathbb{Z}^+$ y K un campo de característica p. Entonces:*

i. Si $p \nmid n$ entonces E^n es un grupo cíclico de orden n respecto a la multiplicación en K^n.

ii. Si p/n, tenemos que $n = mp^b$ con $m, b \in \mathbb{Z}^+$ y con $p \nmid m$. Entonces $K^n = K^m$; $E^n = E^m$ y las raíces de $x^n - 1$ en K^n son los m elementos de E^m, cada uno con multiplicidad p^b.

Definición 1.21. Sea K un campo de característica p y $n \in \mathbb{Z}^+$ tal que $p \nmid n$, entonces un generador de E^n se llama $n - th$ raíz de la unidad primitiva sobre K.

Sabemos que existen $\varphi(n)$, $n - th$ raíces de la unidad primitivas. Si ε es una de ellas, las demás son de la forma ε^s; donde $1 \leq s \leq n$ y $gcd(n, s) = 1$.

Definición 1.22. Sea K un campo de característica p, $n \in \mathbb{Z}^+$ tal que $p \nmid n$, y ε una $n - th$ raíz de la unidad primitiva sobre K. Entonces el polinomio:

$$Q_n(x) = \prod_{(1 \leq s \leq n)} (x - \varepsilon^s)$$

donde $gcd(n, s) = 1$, se llama $n - th$ polinomio ciclotómico sobre K.

Teorema 1.17. *Sea K un campo de característica p y $p \nmid n$, entonces:*

i. $x^n - 1 = \prod_{d/n} \mathbb{Q}_d(x)$

ii. Los coeficientes de $\mathbb{Q}_n(x)$ pertenecen al subcampo primo de K. En particular a $\mathbb{Z}$ si el subcampo de K es el campo de los números racionales $\mathbb{Q}$.

Teorema 1.18. *El campo ciclotómico K^n es una extensión algebraica simple de K, mas aún:*

i. Si $K = \mathbb{Q}$, entonces el polinomio ciclótomico $Q_n(x)$ es irreducible sobre $\mathbb{Q}$ y $[K^n : Q] = \varphi(n)$.

ii. Si $K = F_q$ con $gcd(q, n) = 1$, entonces $Q_n(x)$ factoriza en $\varphi(n)/d$ polinomios mónicos irreducibles distintos en $F_q[x]$ del mismo grado d, F_{q^n} es el campo de ruptura de cualquiera de tales factores irreducibles sobre K, y $[F_{q^n} : F_q] = d$ donde d es el menor entero positivo tal que $q^d \equiv 1(mdn)$

Teorema 1.19. *El campo finito F_q es el $(q-1)$st campo ciclótomico sobre cualquiera de sus subcampos.*

1.7. Teoría de Caracteres

En esta sección estudiaremos algunos conceptos del álgebra lineal y la teoría de números, estos resultados fueron tomados de [10] y [12].

Definición 1.23. Sea G un grupo abeliano finito. Un caracter χ de G es un homomorfismo $\chi : G \to U$, donde U es el grupo multiplicativo de números complejos de norma 1.

Dado que χ es un homomorfismo tenemos que:

$$\chi(g_1g_2) = \chi(g_1)\chi(g_2) \quad \forall g_1g_2 \in G$$

En particular,

$$\chi(e) = \chi(e)\chi(e)$$

y por tanto

$$\chi(e) = 1$$

Más aún, si $m = \mid G \mid$, entonces

$$\chi^m(g) = \chi(g^m) = \chi(e) = 1$$

es decir $\chi(g)$ es una raíz m-ésima de la unidad, y además

$$\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(e) = 1$$

así

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$$

Dado un número finito de caracteres $\chi_1, \chi_2, \cdots, \chi_n$ de G, se puede definir el producto caracter $\chi_1\chi_2\cdots\chi_n$ de $G \to U$ asi:

$$(\chi_1\chi_2\cdots\chi_n)(g) = \chi_1(g)\chi_2(g)\cdots\chi_n(g)$$

para todo g en G. Si $\chi_1 = \chi_2 \cdots = \chi_n = \chi$ simbolizamos por χ^n el producto $\chi_1\chi_2 \cdots \chi_n$.

Con esta operación producto, los caracteres de G forman un grupo abeliano $\hat{G}$, denominado Grupo Dual, su elemento identidad es el caracter trivial $\chi_0(g) = 1$ para todo $g \in G$. El inverso de χ es el caracter $\overline{\chi} = \chi^{-1}$ dado por $\overline{\chi}(g) = \overline{\chi(g)}$ para todo $g \in G$.

Si G es cíclico de orden m y $G = \langle g \rangle$ entonces todos los caracteres de G son de la forma:

$$\chi_a(g^k) = e^{(2\pi\imath ak)/m}$$

, con $k = 0, 1, \cdots, m-1$, para $a = 0, 1, \cdots, m-1$. Además si χ es un caracter de G, entonces $\chi(g)$ $\forall g \in G$ es una $m-$ésima raíz de la unidad, es decir

$$\chi(g) = e^{(2\pi\imath a)/m}$$

, con $a = 0, 1, \cdots, m-1$, de donde $\chi = \chi_a$. Por lo tanto, $\hat{G}$ consiste exactamente de los caracteres $\chi_0\chi_1 \cdots \chi_{m-1}$. Luego $\hat{G} \cong G$.

Teorema 1.20. *Sea H un subgrupo del grupo abeliano finito G y sea ψ un caracter de H. Entonces ψ puede extenderse a un caracter de G; es decir, existe un caracter χ de G tal que $\chi(h) = \psi(h)$ para todo $h \in H$.*

Teorema 1.21. *Para cualesquiera dos elementos distintos $g_1, g_2 \in G$ existe un caracter χ de G tal que: $\chi(g_1) \neq \chi(g_2)$*

Teorema 1.22. *El número de caracteres de un grupo abeliano finito G es igual a $|G|$*

Teorema 1.23. *Para $b \in F_q$, la función χ_b con $\chi_b(c) = \chi_1(bc)$ para todo caracter $c \in F_q$ es un caracter aditivo de F_q, y cada caracter aditivo de F_q es obtenido de esta forma.*

Teorema 1.24. *Sea g un elemento primitivo fijo de F_q. Para cada $j = 0, 1, \cdots, q-2$ la función ψ_j con: $\psi_a(g^k) = e^{2\pi iak/(q-1)}$ para $k = 0, 1, \cdots, q-2$ define un caracter multiplicativo de F_q, y cada carácter multiplicativo de F_q se obtiene de esta manera.*

Corolario 1.24.1. *El grupo de los caracteres multiplicativos de F_q es cíclico de orden $q-1$ con elemento identidad χ_o.*

Ejemplo 1.1. Consideremos el grupo multiplicativo $F_9^\times$, el cual es un grupo cíclico con 8 elementos generado por $\alpha = 1 + i$. Los elementos del grupo se presentan en la siguiente tabla:

k	0	1	2	3	4	5	6	7
α^k	1	$1+i$	$2i$	$1+2i$	2	$2+2i$	i	$2+i$

Elegimos una 8−ésima raíz de la unidad $\varepsilon \in U$, en este caso tomaremos $\varepsilon = e^{1/8} = \frac{1+i}{\sqrt{2}}$, la siguiente tabla muestra como están definidos los caracteres χ_i de $F_9^\times$, donde la entrada (a, k) corresponde a ε^{ak}, así si queremos hallar el caracter correspondiente a la entrada (1,2), tenemos que:

$$\varepsilon^{1\cdot 2} = \left(\frac{1+i}{\sqrt{2}}\right)^2 = \frac{1}{2}(1+i)^2 = \frac{1}{2}(1+2i-1) = i$$

Por tanto:

	1	$1+i$	$2i$	$1+2i$	2	$2+2i$	i	$2+i$
χ_0	1	1	1	1	1	1	1	1
χ_1	1	$\frac{1+i}{\sqrt{2}}$	i	$\frac{-1+i}{\sqrt{2}}$	-1	$\frac{-1-i}{\sqrt{2}}$	$-i$	$\frac{1-i}{\sqrt{2}}$
χ_2	1	i	-1	$-i$	1	i	-1	$-i$
χ_3	1	$\frac{-1+i}{\sqrt{2}}$	$-i$	$\frac{1+i}{\sqrt{2}}$	-1	$\frac{1-i}{\sqrt{2}}$	i	$\frac{-1-i}{\sqrt{2}}$
χ_4	1	-1	1	-1	1	-1	1	-1
χ_5	1	$\frac{-1-i}{\sqrt{2}}$	i	$\frac{1-i}{\sqrt{2}}$	-1	$\frac{1+i}{\sqrt{2}}$	$-i$	$\frac{-1+i}{\sqrt{2}}$
χ_6	1	$-i$	-1	i	1	$-i$	-1	i
χ_7	1	$\frac{1-i}{\sqrt{2}}$	$-i$	$\frac{-1-i}{\sqrt{2}}$	-1	$\frac{-1+i}{\sqrt{2}}$	i	$\frac{1+i}{\sqrt{2}}$

como podemos notar existe una simetría en la tabla, esto se debe a que

$$\chi_a(\alpha^k) = \varepsilon^{ak} = \varepsilon^{ka} = \chi_k(\alpha^a);$$

como lo afirma el Teorema 1.24.

Entonces si tomamos $ak = 1$, equivalentemente $a = 1$ y $k = 1$ que corresponde al elemento número uno $1 + i$ y al caracter uno χ_1, tenemos que el conjunto

$$\{\chi_0(1+i), \chi_1(1+i), \chi_2(1+i), \chi_3(1+i), \chi_4(1+i), \chi_5(1+i), \chi_6(1+i), \chi_7(1+i)\}$$

tiene exactamente los mismos elementos que el conjunto

$$\{\chi_1(1), \chi_1(1+i), \chi_1(2i), \chi_1(1+2i), \chi_1(2), \chi_1(2+2i), \chi_1(i), \chi_1(2+i)\}$$

que corresponden a

$$\{1, \frac{1+i}{\sqrt{2}}, i, \frac{-1+i}{\sqrt{2}}, -1, \frac{-1-i}{\sqrt{2}}, -i, \frac{1-i}{\sqrt{2}}\}.$$

Capítulo 2

Combinatorial Nullstellensatz

La herramienta principal que se utiliza para demostrar algunos casos particulares de la Conjetura de Snevily, propuestos por Noga Alón en [1] y Dasgupta y otros en [3], se conoce como: *La Combinatorial Nullstellensatz*[1]. En este capítulo, damos a conocer este resultado y su demostración.

Para ello comenzaremos con una generalización del teorema fundamental del álgebra:

Lema 2.1. *Sea $p(x_1, x_2 \ldots, x_n)$ un polinomio en n variables $x_1, x_2 \ldots, x_n$ sobre un campo arbitrario $\mathbb{F}$, supongamos que para todo $i = 1, 2, \ldots, n$, el grado de p como un polinomio en x_i es a lo más c_i y A_i es un subconjunto de $\mathbb{F}$ de cardinalidad $c_i + 1$, si $p(a_1, a_2 \ldots, a_n) = 0$ para toda n−tupla $(a_1, a_2 \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, entonces p es el polinomio cero.*

Éste resultado permite demostrar un caso especial (cuando $m = n$ y $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$) del Hilberts Nullstellensatz, teorema fundamental, que afirma que si F es un campo cerrado algebraicamente, y si $f, g_1, g_2, \ldots, g_m$ son polinomios en el anillo de polinomios $F[x_1, x_2, \ldots, x_n]$, donde f se anula sobre todos los ceros comunes de $g_1, g_2, \ldots, g_m$, entonces existen, un entero k y polinomios $h_1, h_2, \ldots, h_m$ tales que

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

[1] Alón, Noga. Combinatorial Nullstellensatz.*Combinatorics, Probability and Computing* **8** (1999), 7-29. MR1684621**(2000b:05001)**

El caso especial se enuncia de la siguiente forma:

Teorema 2.1. *Sea F un campo arbitrario, y sea $f = f(x_1, x_2, \ldots, x_n)$ un polinomio en $F[x_1, x_2, \ldots, x_n]$. Sean $S_1, S_2, \ldots, S_n$ subconjuntos no vacios de $\mathbb{F}$ y definamos $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. Si f se anula sobre todos los ceros comunes de $g_1, g_2, \ldots, g_n$, entonces existen polinomios $h_1, h_2 \ldots, h_n \in F[x_1, x_2, \ldots, x_n]$ que satisfacen que $grad(h_i) \leq grad(f) - grad(g_i)$ tales que*

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

Mas aún, si $f, g_1, g_2, \ldots, g_n$ son polinomios $R[x_1, x_2, \ldots, x_n]$ para algún subanillo R de F entonces existen polinomios $h_i \in R[x_1, x_2, \ldots, x_n]$ como antes.

A partir del Teorema 2.1 se obtiene la prueba de la Combinatoria de Nullstellensatz, el cual se enuncia a continuación:

Teorema 2.2 (Combinatorial Nullstellensatz)**.** *Sea F un campo arbitrario, consideremos un polinomio $f = f(x_1, x_2, \ldots, x_n)$ en $F[x_1, x_2, \cdots, x_n]$ y supongamos que existe un monomio $x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}$ tal que $\sum_{i=1}^{n} c_i$ es igual al grado de f y cuyo coeficiente en f es distinto de cero, entonces si $S_1, S_2, \ldots, S_n$ son subconjuntos de F con $|S_i| > c_i$, existen $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ tales que:*

$$f(s_1, s_2, \ldots, s_n) \neq 0.$$

Demostración. Tomemos $|S_i| = c_i + 1$ para todo i. Supongamos que el resultado es falso, es decir:

$$f(s_1, s_2, \ldots, s_n) = 0 \text{ para toda } n\text{-tupla } (s_1, s_2 \ldots, s_n) \in S_1 \times \cdots \times S_n$$

definamos

$$g_i(x_i) = \prod_{s \in S_i}(x_i - s) = x_i^{c_i+1} - \sum_{j=0}^{c_i} g_{ij} x_i^j.$$

Por el teorema 2.1, existen polinomios $h_1, h_2, \ldots, h_n$ en $F[x_1, x_2, \ldots, x_n]$ con $grad(h_i) \leq \sum_{i=1}^{n} c_i - grad(g_i)$ tales que

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

Por lo supuesto, el coeficiente de $x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}$ en f es distinto de cero, y así el coeficiente de este monomio en $\sum_{i=1}^{n} h_i g_i$ es distinto de cero.

Por otro lado el grado de cada $h_i g_i = h_i \prod_{s \in S_i} (x_i - s)$ es a lo sumo $grad(f)$ y por tanto, si existen monomios de grado igual al $grad(f)$ en este, deben ser divisibles por $x_i^{c_i+1}$, de donde se sigue que el coeficiente de $x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}$ en $\sum_{i=1}^{n} h_i g_i$ es cero, lo cual es una contradicción. Esto concluye la prueba. □

Capítulo 3

Conjetura de Snevily

Comenzaremos este capítulo mostrando algunos ejemplos que nos ayudarán a entender en que consiste la Conjetura de Snevily y posteriormente presentaremos los resultados que se tienen alrededor de ella.

3.1. Presentación de la Conjetura

La tabla de adición de Cayley de $\mathbb{Z}_n$ puede ser considerada como un objeto matemático simple, pero guarda características que al ser demostradas podrían ser propiedades interesantes.

Por ejemplo, si consideremos el grupo aditivo $\mathbb{Z}_7$, su tabla de ***Cayley*** se representa de forma matricial como sigue:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Una submatriz 3×3 de la tabla anterior es:

+	0	2	4
1	1	**3**	5
3	3	5	**0**
4	**4**	6	1

Nóte que los elementos: $3, 0, 4$ (subrayados) no pertenenecen a una misma fila ni a una misma columna. En este caso diremos que los elementos forman una transversal de esta submatriz. Observe, además, que ellos son distintos formando así lo que denominaremos una transversal latina.

De manera general, definimos una ***transversal de una matriz*** $n \times n$ como una colección de n celdas, dos de las cuales no se encuentran en la misma fila o columna. Una *transversal de una matriz* es una ***transversal latina*** si las n celdas tienen componentes distintas.

Para $\mathbb{Z}_4$ la tabla de adición de Cayley es:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Una submatriz 2×2 de esta tabla es:

+	0	2
1	1	3
3	3	1

esta submatriz contiene sólo dos transversales: $1, 1$ y $3, 3$ ninguna de las cuales es una transversal latina.

Una submatriz 3×3 de la tabla es:

+	1	2	3
0	1	2	3
1	2	3	0
2	3	0	1

esta submatriz contiene seis transversales: $1, 3, 1$; $2, 0, 3$; $3, 3, 3$; $3, 2, 0$; $1, 0, 0$ y $2, 2, 1$ de las cuales dos son transversales latinas.

Los ejemplos anteriores nos permiten verificar las conjeturas hechas por Snevily en [9].

Conjetura 1. P*ara cualquier n impar, y cualquier* $k \in \{1, 2, \cdots, n\}$ *toda submatriz* $k \times k$ *de la tabla de adición de Cayley de* $\mathbb{Z}_n$ *contiene una transversal latina.*

Conjetura 2. P*ara cualquier n par y cualquier* $k \in \{1, 2, \cdots, n\}$*, cualquier submatriz* $k \times k$ *de la tabla de adición de Cayley de* $\mathbb{Z}_n$ *contiene una transversal latina siempre que la submatriz no sea un subgrupo de orden par o una traslación de tal subgrupo.*

Nuestro estudio se centra en una versión general de la conjetura 1, la cual afirma:

Sea $A = \{a_1, a_2, \cdots, a_k\}$ y $B = \{b_1, b_2, \cdots, b_k\}$ dos subconjuntos de un grupo abeliano G de orden impar, entonces existe una permutación $\pi \in S_k$ tal que las sumas $a_i + b_{\pi(i)}$, $1 \leq i \leq k$, son distintas dos a dos.

A continuación se presenta en orden cronológico, como se fue abordando este problema. Inicialmente presentaremos los resultados obtenidos por Noga Alon; Dasgupta y otros y finalmente concluiremos con la prueba realizada por Bodan Arzovsky.

3.2. Noga Alon

El primer resultado importante sobre la conjetura, fue mostrado por Alon en [1]; él prueba que la conjetura es cierta para grupos de orden primo, incluso cuando A es una secuencia de k elementos, con $k \leq |G|$; es decir, cuando se permite repetir elementos en A. Estos resultados se muestran a continuación:

Teorema 3.1. *Sea p un número primo de orden impar, y sean A y B dos subconjuntos cada uno de cardinalidad k del campo finito $\mathbb{Z}_p$, entonces, existe una numeración $a_1, a_2, \cdots, a_k$ de elementos de A y una numeración $b_1, b_2, \cdots, b_k$ de elementos de B tal que las sumas $a_i + b_i$ en $\mathbb{Z}_p$, son distintas dos a dos.*

Ejemplo 3.1. Consideremos los subconjuntos $A = \{2, 4, 5, 6\}$ y $B = \{0, 3, 5, 6\}$ de $\mathbb{Z}_7$ con cardinalidad $k = 4$, una ordenación de los b_i es:

$$\begin{array}{rcccc} & 2 & 4 & 5 & 6 \\ + & 0 & 3 & 5 & 6 \\ \hline & 2 & 0 & 3 & 5 \end{array}$$

Esta ordenación corresponde a la submatriz:

+	2	4	5	6
0	2	4	5	6
3	5	0	1	2
5	0	2	3	4
6	1	3	4	5

donde se verifica que los elementos $2, 0, 3, 5$ conforman una transversal latina.

El teorema anterior resuelve parcialmente el caso general de la Conjetura 1, cuando reemplazamos el grupo Abeliano G de orden impar por el campo $\mathbb{Z}_p$. Además el teorema anterior es trivial para $k = p$, esto se verifica tomando $a_i = b_i$. El caso $k < p$ se tiene a partir del siguiente teorema, cuya prueba requiere del Teorema 2.2 y de un resultado combinatorio denominado la ***Conjetura de Dyson***, la cuál se establece a continuación. Su prueba se encuentra en [5].

Conjetura de Dyson: El coeficiente del monomio $\prod_{i=1}^{k} x_i^{(k-1)c_i}$ en el polinomio

$$\prod_{1\leq i<j\leq k} (x_i - x_j)^{c_i+c_j}$$

es

$$(-1)^{c_2+2c_3+\cdots+(k-1)c_k} \frac{(c_1 + c_2 + \cdots + c_k)!}{c_1!c_2!\cdots c_k!}.$$

Teorema 3.2. *Sea p un número primo, supongamos $k < p$, sea $(a_1, a_2, \cdots, a_k)$ una secuencia de elementos, no necesariamente distintos, de un campo finito $\mathbb{Z}_p$ y sea B un subconjunto de cardinalidad k de $\mathbb{Z}_p$, entonces, existe una numeración $b_1, b_2, \cdots, b_k$ de elementos de B tal que las sumas $a_i + b_i$ (en $\mathbb{Z}_p$) son distintas dos a dos.*

Demostración. Consideremos el siguiente polinomio en k variables sobre $\mathbb{Z}_p$:

$$f(x_1, x_2, \cdots, x_k) = \prod_{1\leq i<j\leq k} (x_i - x_j) \prod_{1\leq i<j\leq k} (a_i + x_i - a_j - x_j)$$

Consideremos el coeficiente del monomio $\prod_{i=1}^{k} x_i^{k-1}$ en f. Puesto que el grado total de f es $k(k-1)$, el cual es el mismo que el grado del monomio, es obvio que este es precisamente el coeficiente de este monomio en el polinomio

$$\prod_{1\le i<j\le k}(x_i - x_j)\prod_{1\le i<j\le k}(x_i - x_j) = \prod_{1\le i<j\le k}(x_i - x_j)^2$$

Sin embargo, este coeficiente es $(-1)^{\binom{k}{2}}k!$, que es un caso especial de la Conjetura de Dyson. Como $k < p$ este coeficiente es distinto de cero módulo p, y por tanto, por el teorema 2.2 con $t_1 = t_2 = \cdots = t_k = k-1$, y $S_1 = S_2 = \cdots = S_k = B$, se sigue que existen $b_i \in S_i = B$ tales que

$$f(b_1, b_2, \cdots, b_k) = \prod_{1\le i<j\le k}(b_i - b_j)\prod_{1\le i<j\le k}(a_i + b_i - a_j - b_j) \neq 0$$

Así los elementos $b_i \in B$ son distintos dos a dos, y las sumas $a_i + b_i$ también son distintas dos a dos, lo cual completa la prueba. □

Note que este teorema no es verdadero si reemplazamos $\mathbb{Z}_p$ por el anillo de enteros módulo n,donde n no es primo. En efecto, si $n = ks$, $a_1 = a_2 = \cdots = a_{k-1} = 0$, $a_k = s$ y $B = \{0, s, 2s, \ldots, (k-1)s\}$, es fácil verificar que no hay una numeración de los elementos de B tales que las sumas $a_i + b_i$, $1 \le i \le k$ son distintas dos a dos en $\mathbb{Z}_n$.

Ejemplo 3.2. Tomando $k = 3$, $A = (1, 1, 4)$ y $B = (0, 2, 4)$ en $\mathbb{Z}_5$ obtenemos la ordenación de los b_i:

$$\begin{array}{rccc} & 1 & 1 & 4 \\ + & 4 & 2 & 0 \\ \hline & 0 & 3 & 4 \end{array}$$

Donde las sumas $a_i + b_i$ son distintas dos a dos, lo cual equivale a decir que los elementos $0, 3, 4$ en la submatriz:

+	1	1	4
0	1	1	4
2	3	3	1
4	0	0	3

conforman una transversal latina.

3.3. Dasgupta, Károlyi, Serra y Szegedy

Dasgupta, Károlyi, Serra y Szegedy en [3] demostraron otros resultados de la Conjetura de Snevily, los cuales aparecen en este documento como teoremas 3.3 y 3.4, estos son extensiones de los teoremas 3.1 y 3.2. La prueba de estos teoremas se basa en el hecho de que cada grupo cíclico se puede identificar con un subgrupo del grupo multiplicativo de cierto campo, es decir, podemos trabajar un problema aditivo utilizando su análogo multiplicativo, en este sentido el lema siguiente permite reducir el problema original al estudio del permanente de ciertas matrices de Vandermonde.

Para una matriz $M = (m_{ij})_{1\leq i,j\leq k}$ el permanente y el determinante de M se definen y se notan respectivamente por:

$$perM = \sum_{\pi\in S_k} m_{1\pi(1)}m_{2\pi(2)}\cdots m_{k\pi(k)}$$

$$Det = \sum_{\pi\in S_k} sig(\pi)m_{1\pi(1)}m_{2\pi(2)}\cdots m_{k\pi(k)}$$

donde S_k es el grupo de todas las permutaciones del conjunto $\{1, 2, \ldots, k\}$.

Denotemos por $V(y_1, \ldots, y_k)$ la matriz de Vandermonde $(y_i^{j-1})_{1\leq i<j\leq k}$.

Lema 3.1. *Sea F un campo arbitrario y supongamos que $PerV(a_1, a_2, \cdots, a_k) \neq 0$ para algunos elementos $a_1, a_2, ..., a_k \in \mathbb{F}$. Entonces, para cualquier subconjunto $B \subset F$ de cardinalidad k existe una numeración $b_1, b_2, \cdots, b_k$ de los elementos de B tal que los productos $a_1b_1, a_2b_2, \cdots, a_kb_k$ son distintos dos a dos.*

Demostración. Considere el siguiente polinomio en $F[x_1, x_2, \cdots, x_k]$

$$f(x_1, \cdots, x_k) = \prod_{1 \le j < i \le k} ((x_i - x_j)(a_i b_i - a_j b_j)).$$

El grado de f claramente no es mayor que $k(k-1)$; además

$$\begin{aligned} f(x_1, \cdots, x_k) &= DetV(x_1, x_2, \cdots, x_k) \cdot DetV(a_1 x_1, a_2 x_2, \cdots, a_k x_k) \\ &= \left(\sum_{\pi \in S_k} (-1)^{I(\pi)} \prod_{i=1}^{k} x_{\pi(i)}^{(i-1)} \right) \left(\sum_{\tau \in S_k} (-1)^{I(\tau)} \prod_{i=1}^{k} a_{\tau(i)} x_{\tau(i)}^{(i-1)} \right) \\ &= \left(\sum_{\pi \in S_k} (-1)^{I(\pi)} \prod_{i=1}^{k} x_{\pi(i)}^{(i-1)} \right) \left(\sum_{\tau \in S_k} (-1)^{I(\tau)} \prod_{i=1}^{k} a_{\tau(k+1-i)} x_{\tau(k+1-i)}^{(k-i)} \right) \\ &= \left(\sum_{\pi \in S_k} (-1)^{I(\pi)} \prod_{i=1}^{k} x_{\pi(i)}^{(i-1)} \right) \left(\sum_{\tau \in S_k} (-1)^{\binom{k}{2} - I(\pi)} \prod_{i=1}^{k} (a_{\pi(i)} x_{\pi(i)})^{(k-i)} \right) \end{aligned}$$

Por tanto, el coefciente $c(a_1, a_2, \cdots, a_k)$ del monomio $\prod_{i=1}^{k} x_i^{k-1}$ en f,

$$\begin{aligned} c(a_1, a_2, \cdots, a_k) &= \sum_{\pi \in S_k} (-1)^{\binom{k}{2}} \prod_{i=1}^{k} a_{\pi(i)}^{k-i} \\ &= (-1)^{\binom{k}{2}} \sum_{\pi \in S_k} \prod_{i=1}^{k} a_{\pi(k+1-i)}^{i-1} \\ &= (-1)^{\binom{k}{2}} \sum_{\tau \in S_k} \prod_{i=1}^{k} a_{\tau(i)}^{i-1} \\ &= (-1)^{\binom{k}{2}} PerV(a_1, a_2, \cdots, a_k) \end{aligned}$$

es diferente de cero (en particular $c(1, 1, \cdots, 1) = (-1)^{\binom{k}{2}} k!$. Por consiguiente, f es de grado $k(k-1)$ y podemos aplicar el teorema 2.2, con $t_i = k-1$ y $S_i = B$ para $i = 1, 2, \cdots, k$ para obtener k elementos distintos $b_1, b_2, \cdots, b_k$ en B tales que los productos $a_1 b_1, a_2 b_2, \cdots, a_k b_k$ son distintas por pares. Esto completa la prueba del lema. □

Teorema 3.3. *Sea G un grupo cíclico de orden impar. Sea $A = \{a_1, a_2, \ldots, a_k\}$ y B subconjuntos de G, cada uno de cardinalidad k, entonces existe una numeración $b_1, b_2, \cdots, b_k$ de elementos de B tal que las sumas $a_i + b_i$ con $1 \leq i \leq k$, son distintas por pares.*

Demostración. Sea $|G| = m$ y sea $\alpha = \varphi(m)$ donde φ es la función de Euler, entonces $2^\alpha \equiv 1$ (mód m). Consideremos el campo $\mathbb{F} = \mathbb{F}_{2^\alpha}$, su grupo multiplicativo F^* es cíclico de orden $2^\alpha - 1$. Como $m|2^\alpha - 1$, entonces F^* tiene un subgrupo de orden m, así, podemos identificar G con dicho subgrupo, la operación en G es la restricción de la operación en F. Dado que F es de característica 2, tenemos

$$perV(a_1, \ldots, a_k) = DetV(a_1, \ldots, a_k) = \prod_{1 \leq j < i \leq k} (a_i - a_j) \neq 0.$$

Luego del lema 3.1 existe una numeración $\{b_1, \ldots, b_k\}$ de los elementos de B tal que $a_i + b_i$, $1 \leq i \leq k$, son distintas dos a dos. □

Ejemplo 3.3. Consideremos el grupo $G = \langle \mathbb{Z}_9; + \rangle$, el cuál es cíclico generado por 1. Sea $A = \{0, 4, 8\}$ y $B = \{0, 3, 6\}$ subconjuntos de G. Observemos que las sumas $a_i + b_i$ son distintas dos a dos.

$$\begin{array}{rccc} & 0 & 4 & 8 \\ + & 0 & 3 & 6 \\ \hline & 0 & 7 & 5 \end{array}$$

Lo anterior equivale a decir que los elementos $0, 7, 5$ en la submatriz:

+	0	4	8
0	0	4	8
3	3	7	2
6	6	1	5

conforman una transversal latina.

Otro de los resultados parciales de la conjetura dado por Dasgupta y otros se encuentra en el teorema 3.4. El cual requiere para su demostración el siguiente resultado:

Lema 3.2. *(Károlyi [7]) Si $\varepsilon_1, \varepsilon_2 \ldots, \varepsilon_t$ son q-ésimas raíces de la unidad tales que $\sum_{i=1}^{t} \varepsilon_i = 0$ entonces $p \mid t$.*

Demostración. Sea $E(q)$ el conjunto de las q-ésimas raíces de la unidad, como $E(q)$ es cíclico, existe una q-ésima raíz de la unidad ε, para la cual existen enteros positivos α_i tales que $\varepsilon_i = \varepsilon^{\alpha_i}$. Consideremos el polinomio $P(x) = \sum_{i=1}^{t} x^{\alpha_i}$, entonces $p(\varepsilon) = \sum_{i=1}^{t} \varepsilon^{\alpha_i} = \sum_{i=1}^{t} \varepsilon_i = 0$. Se sigue que el q-ésimo polinomio ciclotómico $Q_q(x) = \prod_{\substack{s=1 \\ \gcd(q,s)=1}}^{q} (x - \varepsilon^s)$ el cual es irreducible en $\mathbb{Z}[x]$ es un divisor de $P(x)$ en el anillo $\mathbb{Z}[x]$, así $p = Q_q(1)$ divide a $P(1) = \sum_{i=1}^{t} 1 = t$. □

Teorema 3.4. *Sea p un número primo, α un entero positivo y $G = \mathbb{Z}_{p^\alpha}$ o $G = (\mathbb{Z}_p)^\alpha$, sea $(a_1, \ldots, a_k)$, $k < p$, una sucesión de elementos (no necesariamente distintos) en G. Entonces para cualquier subconjunto $B \subset G$ de cardinalidad k existe una numeración $\{b_1, \ldots, b_k\}$ de los elementos de B tal que las sumas $a_i + b_i$, $1 \leq i \leq k$, son distintas dos a dos.*

Demostración. Para efectuar la prueba consideremos dos casos:

1. Para $G = (\mathbb{Z}_p)^\alpha$. Sea p un número primo y sea $\mathbb{F}_q$ un campo finito de orden $q = p^\alpha$. Identifiquemos el grupo $(\mathbb{Z}_p)^\alpha$ con el grupo aditivo $\mathbb{F}_q$.
   Consideremos el polinomio

$$\begin{aligned} f(x_1, \cdots, x_k) &= \prod_{1 \leq j < i \leq k} [(x_i - x_j)(a_i + x_i - a_j - x_j)] \\ &= \prod_{1 \leq j < i \leq k} (x_i - x_j)(x_i - x_j) + \text{términos de menor grado.} \end{aligned}$$

   el grado de f es $k(k-1)$ y el coeficiente de $\prod_{i=1}^{k} x_i^{k-1}$ en f es $c = (-1)^{\binom{k}{2}} k!$ (Conjetura de Dyson con $m = 1$). Como la característica del campo $\mathbb{F}_q$ es $p > k$ entonces $c \nmid p$, esto es,

$c \neq 0$ (en $\mathbb{Z}_p$). Aplicando el teorema 2.2 con $t_i = k-1$ y $S_i = B$ para $i = 1, \ldots, k$, existen elementos $b_1, \ldots, b_k \in B$ tales que

$$\prod_{1 \leq j < i \leq k} [(b_i - b_j)(a_i + b_i - a_j - b_j)] \neq 0$$

por lo tanto $b_1, \ldots, b_k$ y las sumas $b_1 + a_1, \ldots, b_k + a_k$ son distintas dos a dos.

2. Para $G = \mathbb{Z}_{p^\alpha}$. Consideremos el campo ciclotómico $F = \mathbb{Q}(\varepsilon)$ donde ε es una q-esima raíz de la unidad y $q = p^\alpha$, entonces el grado de esta extensión es $[\mathbb{Q}(\varepsilon), \mathbb{Q}] = \varphi(q) = \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Dado que

   $E(q) = \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{q-1}\}$ es un subgrupo cíclico de orden q respecto a la multiplicación en $\mathbb{Q}(\varepsilon)$, podemos identificar a G con $E(q)$.

   Como antes si $per = V(a_1, \ldots, a_k) \neq 0$ entonces del lema 3.1 existe una numeración $\{b_1, \ldots, b_k\}$ de los elementos de B tal que las sumas $a_i + b_i$, para $1 \leq i < j \leq k$, son distintas dos a dos. Así que nos resta probar que $perV(a_1, \ldots, a_k) \neq 0$. Para verificar este hecho, dado que el $perV(a_1, \ldots, a_k) = \sum_{\sigma \in S_k} \prod_{i=1}^{k} a_{\sigma_i}^{i-1}$ y como cada término $\prod_{i=1}^{k} a_{\sigma_i}^{i-1}$ de ésta permanente es una q-ésima raíz de la unidad donde el número de sumandos es $k!$. Como $k < p$ entonces $p \nmid k!$, luego del lema 3.2 se sigue que $perV(a_1, \ldots, a_k) \neq 0$, con lo cual se concluye la prueba.

□

Ejemplo 3.4. Consideremos el grupo $G = \mathbb{Z}_{3^2}$, donde $p = 3$, sea $(1, 2)$ una sucesión de elementos en G y sea $B \subset G$, $B = \{0, 1\}$

$$\begin{array}{rcc} & 1 & 2 \\ + & 0 & 1 \\ \hline & 2 & 0 \end{array}$$

Se observa que las sumas $a_i + b_i$ son distintas dos a dos.

3.4. Bodan Arzovsky (Demostración de la Conjetura para G de Orden Impar)

Bodan Arzovsky en el 2009, utilizando técnicas del álgebra lineal, finalmente publica en [2] la demostración para el caso general cuando G es un grupo abeliano de orden impar.

Antes de realizar la demostración formal, debemos presentar algunos resultados del álgebra lineal necesarios para la misma:

Lema 3.3. [1] *Si G es un grupo abeliano finito de exponente n y F es un campo finito tales que n divide a $|F^{\times}|$, entonces el sistema de caracteres de G para F forman una base del espacio vectorial de las funciones de G en F.*

Este lema garantiza el hecho de poder expresar cualquier función del grupo abeliano G en el campo finito F como combinación lineal del sistema de todos los caracteres del grupo, hecho que utilizaremos más adelante.

La siguiente afirmación hace parte de las hipótesis que se consideran para los lemas que a continuación se consignan:

Afirmación 1. *Sea G un grupo abeliano finito de orden m y exponente n impares, supongamos que existen dos subconjuntos $\{a_1, a_2, \cdots, a_k\}$ y $\{b_1, b_2, \cdots, b_k\}$ de cardinalidad k de G tales que para alguna permutación $\pi \in S_k$ existe un par de índices distintos $i \neq j$ de tal forma que $a_i + b_{\pi(i)} = a_j + b_{\pi(j)}$. Sea F un campo finito, supongamos que su orden $q = |F|$ es una potencia de 2 tal que $n|q-1$ y $q > m$. Note que, si F es de característica 2 se pueden ignorar los signos de las permutaciones cuando evaluamos el determinante de F.*

Lema 3.4. *Para algún sistema de caracteres $\chi_1, \chi_2, ..., \chi_k : G \to F^{\times}$ tenemos que*

$$\sum_{\pi \in S_k} det||\chi_{\pi(i)}(a_i + b_j)|| = 0.$$

[1] Éste es un resultado estándar del álgebra lineal, su demostración requiere de otras herramientas mucho más fuertes y no es nuestro interés presentar en este trabajo.

Demostración. Expandiendo el determinante obtenemos:

$$\begin{aligned}
\sum_{\pi\in S_k} det||\chi_{\pi(i)}(a_i + b_j)|| &= \sum_{\pi\in S_k}\left(\sum_{\tau\in S_k}\prod_{i=1}^{k}\chi_{\pi(i)}(a_i + b_{\tau(i)})\right);\\
&= \sum_{\pi\in S_k}\left(\sum_{\tau\in S_k}\prod_{i=1}^{k}\chi_i(a_{\pi^{-1}(i)} + b_{\tau(\pi^{-1}(i))})\right);\\
&= \sum_{\pi\in S_k}\left(\sum_{\tau\in S_k}\prod_{i=1}^{k}\chi_i(a_{\pi(i)} + b_{\tau(\pi(i))})\right);\\
&= \sum_{\tau\in S_k}\left(\sum_{\pi\in S_k}\prod_{i=1}^{k}\chi_i(a_{\pi(i)} + b_{\tau(\pi(i))})\right);\\
&= \sum_{\tau\in S_k} det||\chi_i(a_j + b_{\tau(j)})||.
\end{aligned}$$

Como tener la permutación de un caracter evaluado en un elemento específico, es equivalente a fijar un caracter y evaluarlo en la permutación de ese elemento, y el conjunto de permutaciones forman un grupo, entonces esta permutación también va a estar en el grupo de permutaciones; además cada uno de los determinantes de la parte derecha contiene un par de columnas iguales, puesto que $\chi(a_i + b_{\tau(i)}) = \chi(a_j + b_{\tau(j)})$ (por hípótesis $a_i + b_{\tau(i)} = a_j + b_{\tau(j)}$). Luego, cada uno de estos determinantes se anula, así, el determinante de la parte izquierda se anula. Esto concluye la prueba del Lema. □

Otro resultado necesario en la prueba de la Conjetura de Snevily es el siguiente:

Lema 3.5. *Supongamos que χ es alguna función de G en F. entonces*

$$det||\chi(a_i + b_j)|| = 0$$

Demostración. El sistema de todos los caracteres $\chi_1, \chi_2, ..., \chi_m$:$G \to F^{\times}$ forman una base vectorial

de todas las funciones de G en F. Entonces, existen elementos $\lambda_1, \lambda_2, ..., \lambda_m \in F$ tales que

$$\chi = \lambda_1\chi_1 + \lambda_2\chi_2 + \cdots + \lambda_m\chi_m$$

El determinante es una función multilineal, entonces si D es un determinante se cumple que:

$$\begin{aligned} D(\chi(a_1 + b_1), \chi(a_1 + b_2), \cdots, \chi(a_1 + b_k)) &= D\left(\sum_{i=1}^{m} \lambda_i\chi_i(a_1 + b_1), \cdots, \sum_{i=1}^{m} \lambda_i\chi_i(a_1 + b_k)\right); \\ &= \prod_{i=1}^{m} \lambda_i D\left(\chi_1(a_1 + b_1), \cdots, \chi_m(a_1 + b_1)\right) + \cdots \\ &+ \prod_{i=1}^{m} \lambda_i D\left(\chi_1(a_1 + b_k), \cdots, \chi_m(a_1 + b_k)\right) \\ &= \sum_{j=1}^{k} \left(\prod_{i=1}^{m} \lambda_i D(\chi_i(a_1 + b_j))\right). \end{aligned}$$

entonces podemos expandir el determinante como sigue:

$$\begin{aligned} det||\chi(a_i + b_j)|| &= det|| \sum_{s=1}^{m} \lambda_s\chi_s(a_i + b_j)|| \\ &= \sum_{s_1, s_2, ..., s_k = 1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i}\right) det||\chi_{s_i}(a_i + b_j)|| \end{aligned}$$

pero si dos de estos índices $s_1, s_2, ..., s_k$ son iguales, entonces, usando la multiplicidad de χ_{s_i}, concluimos que las dos filas correspondientes de la matriz $||\chi_{s_i}(a_i + b_j)||$ son proporcionales, y por tanto estos determinantes se anulan. Consecuentemente, podemos escribir el determinante como:

$$\sum_{s_1, s_2, \cdots, s_k = 1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i}\right) det||\chi_{s_i}(a_i + b_j)|| = \sum_{s_1 \leq s_2 \leq \cdots s_k \leq m} \left(\prod_{i=1}^{k} \lambda_{s_i}\right)\left(\sum_{\pi \in S_k} det||\chi_{\pi(i)}(a_i + b_j)||\right)$$

Donde cada una de las sumas de los determinantes en la parte derecha se anulan por el lema anterior. □

Lema 3.6. *Sea A una matriz $k \times k$, cada una de cuyas entradas es una variable formal $z_1, z_2, ..., z_m$, y tales que cualesquiera dos entradas en la misma fila o columna son distintas. Entonces a estas variables formales se les pueden asignar valores de F de tal forma que $detA \neq 0$.*

Demostración. La prueba se realiza por inducción sobre k. Para el caso de $k = 1$ es trivial. Si k es mayor que 1, podemos asumir sin pérdida de generalidad que z_1 aparece como una entrada. El determinante de A es un polinomio en z_1, de grado a lo sumo $k < |F|$, con el coeficiente principal como determinante de una submatriz de A. Por la hipótesis de inducción, las variables formales $z_2, z_3, ..., z_m$ pueden asignarseles valores de $\mathbb{F}$ de tal forma que este coeficiente no sea nulo. El polinomio en z_1, obtenido de esta manera, no es el polinomio cero, y es de grado a lo sumo $k < |F|$; por lo tanto, a z_1 puede asignarsele un valor de F de tal forma que el polinomio no se anule. □

Ahora, estamos listo para demostrar la Conjetura 1 de H. Snevily en su versión general:

Teorema 3.5. *Para algún entero positivo k y cualesquiera dos subconjuntos $\{a_1, a_2, ..., a_k\}$ y $\{b_1, b_2, ..., b_k\}$ de $k-$elementos, de un grupo abeliano finito de orden impar, existe una permutación $\pi \in S_k$ tales que todas las sumas $a_i + b_{\pi(i)}$, con $1 \leq i \leq k$, son distintas dos a dos.*

Demostración. Utilizando todos los lemas anteriormente expuestos, podemos concluir el resultado que nos interesa si asociamos todo elemento $g \in G$ con una variable formal $z(g)$, entonces todas las entradas en una misma columna o una misma fila de la matriz $||z(a_i + b_j)||$ son distintas. Por el Lema 3.6, cada variable $z(g)$ puede asignarsele un valor $\chi(g)$ de tal forma que el determinante de la matriz resultante $|| \chi(a_i + b_j) ||$ sea distinto de cero. Sin embargo, esto contradice el Lema 3.5, y así se completa la prueba del teorema de H. Snevily. □

Capítulo 4

Conclusiones

Trabajar e incursionar en la matemática es entrar en un mundo distinto, lleno de desafíos y grandes emociones. Un tema como el que desarrollamos en este trabajo de una rama tan compleja como la Teoría de Números Aditiva nos abre las puertas para crecer en conocimientos y aumentar nuestro vagaje matemático.

Como podemos apreciar en el desarrollo de nuestro trabajo, los primeros resultados sobre la Conjetura estaban enfocados en resultados netamente de la teoría de números y el álgebra moderna, pero en la demostración propuesta por Arzovsky vemos que involucra resultados importantes del álgebra lineal para su demostración. Esto es un ejemplo claro que las distintas ramas de la matemática no poseen resultados aislados, todos ellos en algún momento convergen para demostrar y generar nuevos resultados que contribuyen con el avance de la matemática. Después de un tiempo y mucho esfuerzo logramos:

1. Elaborar este trabajo monográfico llamado La Conjetura de Snevily recopilando toda la información que hasta el momento existe alrededor de la misma, de lo cual está demostrado para el caso general cuando el grupo abeliano es de orden impar, pero aún queda abierto el problema cuando el orden del grupo es par.
2. Exponer y presentar sistemáticamente y en forma detallada los lemas, teoremas y las pruebas

que se encuentran en [1] y [3] relacionadas con la Conjetura, en el Encuentro Nacional de Álgebra, Teoría de Números y Combinatoria ALTENCOA5-2012 realizado en la ciudad de Bogotá en Diciembre del 2012.

3. Estudiar y comprender todo lo que hay hasta el momento alrededor de la conjetura, tomando como referencia principal los documentos [1], [3] y [2], éste último contiene la prueba para el caso general cuando el grupo es de orden impar.

4. La conjetura 2 planteada por Snevily aún es problema abierto y objeto de estudio para posibles investigaciones posteriores.

Bibliografía

[1] Alon, Noga. Additive Latin Transversal. *Israel J. Math* **117** (2000), 125-130.MR1760589**(2001b:11019)**

[2] Arzovsky, Bodan. A proof of Snevily's Conjeture.*Israel J. Math* **182** (2011), 505-508.DOI:10.1007/s11856-011-0040-6

[3] Dasgupta, Samit; Károlyi, Gyula; Serra, Oriol; Szegedy Balázs. Transversal of Additive Latin Squares. *Israel J. Math* **126** (2001), 17-28.

[4] Fraleigh, John B.1 A first course in abstract algebra. Addison Wesley,2002.

[5] Gunson, J.Proof of a conjeture of Dyson, J. Math. Phys. 3 (1962), 1040-1043.

[6] Herstein, I. N. Álgebra Abstracta. Grupo Editorial Iberoamérica,S.A. de C.V. 1988.

[7] Károlyi, Gyula. A compactness argument in the additive theory and the polynomial method. *Discrete Math* 302 (2005), No. 1-3, 124-144. MR2179640(2006g:20098).

[8] Lidl, R. y Niederreiter, H.Introduction to finite fields and their applications.Cambridge University Press. 1986.

[9] Snevily, Hunter. Unsolved Problems: The Cayley Addition table of Zn,. *Amer. Math. Monthly* **106** (1999), 584-585. MR1543489.

[10] Seminario de Teoría de Números. Caracteres. Disponible en: http://www.uam.es/personal-pdi/ciencias/fchamizo/posgrado/STN-Caracteres.pdf

[11] Pelaez, Rodrigo.Clasificación de Grupos Abelianos. Disponible en:http://www.ub.edu/modeltheory/documentos/cga.pdf

[12] Cárdena, Humberto y Lluis, Emilio.Representaciones de los Grupos Abelianos. Disponible en:http://paginas.matem.unam.mx/publicaciones/phocadownloadpap/Anales-vol8/8-artculo5.pdf