UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

BIPLANOS CON UN GRUPO DE AUTOMORFISMOS PRIMITIVO EN PUNTOS, TRANSITIVO EN BANDERAS Y DE TIPO AFÍN DE DIMENSIÓN UNO[1]

TESIS
QUE PARA OPTAR POR EL GRADO DE:
DOCTOR EN CIENCIAS

PRESENTA:
PATRICIO RICARDO GARCÍA VÁZQUEZ

TUTORA PRINCIPAL

EUGENIA O'REILLY REGUEIRO
INSTITUTO DE MATEMÁTICAS, UNAM

COMITÉ TUTOR

JUAN JOSÉ MONTELLANO BALLESTEROS
INSTITUTO DE MATEMATICAS, UNAM

CÉSAR HERNÁNDEZ CRUZ
DEPARTAMENTO DE COMPUTACIÓN, CINVESTAV

CIUDAD DE MÉXICO, ABRIL, 2019.

1 Este trabajo fue realizado con el apoyo del proyecto PAPIIT- IN105616.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradezco a mi asesora por su dedicación, orientación
y paciencia para la realización de este trabajo
del cual estoy profundamente orgulloso.
A mi comité tutor y a los sinodales cuyas correcciones,
comentarios y sugerencias fueron aportaciones
imprescindibles para la completación de esta tesis.
A mi familia y amigos por su cariño, apoyo y comprensión
que convirtieron este proceso en algo entrañable.

ÍNDICE

1. Introducción

Un diseño combinatorio es un arreglo de los puntos de un conjunto finito en subconjuntos de él al cual le podemos pedir que satisfaga diferentes propiedades que le den simetría o balance. En esta investigación estudiamos a los biplanos, que son un caso muy particular de los diseños combinatorios.
Mucho del avance en esta rama de las matemáticas se dio en los siglos XIX y XX. Uno de los principales desarrolladores fue el estadístico, biólogo y matemático Ronald Fisher, quien en la década de 1930, estableció muchos de los fundamentos de esta teoría buscando optimizar la realización de diseños experimentales. Varias décadas antes, en 1850, el Reverendo Thomas Kirkman da una de las principales motivaciones al estudio de los diseños cuando formula una de las preguntas para premio de la revista "Lady's and Gentleman's Diary" [8], esta pregunta es conocida como el problema de las colegialas de Kirkman y se puede plantear de la siguiente manera: Quince alumnas salen a caminar formadas de tres en tres cada día de la semana. ¿Es posible formar a las alumnas de tal manera que en toda la semana cada dos de ellas no caminen juntas más de una vez?
La respuesta es sí, e incluso se puede demostrar que hay siete soluciones no isomorfas. En el Cuadro 1 se exhibe una de estas soluciones.
El ejemplo anterior es lo que llamamos un diseño de bloques incompleto balanceado o BIBD, por sus siglas en inglés. Un BIBD se puede definir de la siguiente manera: Consideremos tres enteros positivos v, k y λ tales que $v > k > \lambda$. Un (v, k, λ)-BIBD es una estructura de incidencia entre un conjunto finito de v puntos y un conjunto de bloques. Cada bloque tiene k puntos y cada pareja de puntos se encuentra contenida en exactamente λ bloques.

Cuadro 1: Solución al problema de las colegialas de Kirkman.

Lun.	Mar.	Miér.	Jue.	Vier.	Sá.	Do.
{1,2,5}	{1,3,6}	{1,4,7}	{1,8,11}	{1,9,12}	{1,10,13}	{1,14,15}
{3,4,10}	{2,4,9}	{2,3,8}	{2,13,15}	{2,10,14}	{2,6,11}	{2,7,12}
{6,9,15}	{5,13,14}	{5,10,15}	{3,9,14}	{3,7,13}	{3,12,15}	{3,5,11}
{7,11,14}	{7,8,15}	{6,12,14}	{4,5,12}	{4,11,15}	{4,8,14}	{4,6,13}
{8,12,13}	{10,11,12}	{9,11,13}	{6,7,10}	{5,6,8}	{5,7,9}	{8,9,10}

Bajo esta definición, una solución al problema de las colegialas de Kirkman es un $(15, 3, 1)$-BIBD. En general, a un $(v, 3, 1)$-BIBD se le conoce como un un Sistema Triple de Steiner en v puntos, más sobre estos diseños se puede consultar en [3].
Diremos que un BIBD es simétrico cuando tiene tantos puntos como bloques y en dicho caso diremos que es un SBIBD, también por sus siglas en inglés. En ocasiones nos referiremos a ellos simplemente como diseños simétricos.
Entre las clases de diseños simétricos se encuentran los planos proyectivos finitos, los diseños de Hadamard y los biplanos. En este trabajo buscamos la clasificación de biplanos que satisfacen ciertas condiciones impuestas a los grupos de automorfismos que actúan en ellos.
En el Capítulo 1 se abordan los diseños simétricos, mostrando algunas propiedades básicas que satisfacen estos se introducen varios conceptos que son fundamentales para su estudio, como por ejemplo, la matriz de incidencia y el grupo de automorfismos asociados a un SBIBD.
En el Capítulo 2 estudiamos otras estructuras de incidencia llamadas conjuntos de diferencia. Vemos cómo se relacionan con los diseños simétricos y mencionamos algunos resultados importantes que se conocen sobre ellos.
El Capítulo 3 se destina a los grupos de automorfismos de tipo afín, muchos de los resultados fueron obtenidos utilizando sus propiedades. Aquí abordamos tanto a los grupos de transformaciones afines como a los grupos de transformaciones afines semilineales, principalmente cuando se definen en un espacio vectorial de dimensión uno.
El Capítulo 4 es sobre biplanos y comienza con algunos resultados básicos sobre estos diseños. En la primera sección se mencionan avances recientes que se han hecho en la clasificación de los biplanos con un grupo de automorfismos primitivo en puntos, transitivo en banderas y de tipo afín de dimensión uno. En la segunda sección se define lo que es un conjunto completo de gráficas de Hussain, los cuales se encuentran en correspondencia biyectiva con los biplanos, y nos ayudan a visualizarlos de manera gráfica. En la tercera sección de este capítulo están los resultados originales que obtuvimos.
Finalmente, en el Capítulo 5 están las conclusiones de la investigación.
En este trabajo se asume que el lector está familiarizado con la Teoría de Grupos y la Teoría de Anillos, sin embargo, al final del texto se encuentran tres apéndices que pueden ayudar a la comprensión del texto. El primero es sobre grupos de permutaciones, el segundo sobre campos finitos y en el tercero se encuentran los programas que se implementaron en Python para obtener algunos de los resultados.

1. Diseños simétricos

Aunque enfocamos nuestro estudio a los biplanos, muchos de los lemas y teoremas que utilizamos pueden ser enunciados para SBIBDs.

Definición 1. Sean $v, k, \lambda \in \mathbb{Z}^+$ tales que $v > k > \lambda$. Un (v, k, λ)-**SBIBD** es un par ordenado $D = (P, B)$ donde P es un conjunto finito de puntos y B una familia de subconjuntos de P llamados **bloques** que cumplen las siguientes propiedades:

(i) $|P| = |B| = v$,

(ii) $|c| = k$ para todo $c \in B$,

(iii) para todo par $p_1, p_2 \in P$ se cumple que $|\{c \in B : \{p_1, p_2\} \subseteq c\}| = \lambda$.

En el caso en el que $v = k + 1$ y $k = \lambda + 1$ decimos que el diseño es **trivial**.

Ejemplo 1. Es posible definir un (v, k, λ)-SBIBD trivial para cada $v \geq 3$ de la siguiente forma. Consideremos $P = \{1, 2, ..., v\}$ y $B = \{P \setminus \{i\} : i \in P\}$. Notemos que $D = (P, B)$ es un $(v, v-1, v-2)$-SBIBD.

Ejemplo 2. Consideremos un conjunto P con 16 puntos colocados en una cuadrícula de 4×4. Para cada punto $p \in P$ definimos un bloque c_p el cual consta de los puntos distintos a p que se encuentran en el mismo renglón y la misma columna que p en la cuadrícula. Es fácil observar que cada bloque tiene 6 puntos y cada dos puntos p y p' están en exactamente 2 bloques (los bloques asociados a los 2 puntos donde se intersectan c_p y $c_{p'}$). Por lo tanto si $B = \{c_p : p \in P\}$, entonces (P, B) es un $(16, 6, 2)$-SBIBD. Ver Figura 1.

Definición 2. Sea $D = (P, B)$ un SBIBD. Una **bandera** es una pareja $(p, c) \in P \times B$ tal que $p \in c$.

Comenzamos con el siguiente lema, este establece una de las principales relaciones entre los parámetros de un SBIBD.

Lema 1. *Si D es un (v, k, λ)-SBIBD, entonces cada punto es incidente con k bloques y*

$$\lambda(v - 1) = k(k - 1). \tag{1}$$

p_1	p_2	p_3	p_4
p_5	p_6	p_7	p_8
p_9	p_{10}	p_{11}	p_{12}
p_{13}	p_{14}	p_{15}	p_{16}

Figura 1: Cuadrícula del Ejemplo 2 con los bloques c_{p_4} y $c_{p_{13}}$ sombreados.

Demostración. Sea x un punto de D y t el número de bloques que inciden con x, entonces $|P \setminus \{x\}| = v - 1$ y para cada $p \in P \setminus \{x\}$ tenemos que $|\{c \in B : \{x, p\} \subseteq c\}| = \lambda$. Se sigue que hay $\lambda(v-1)$ parejas (p, c) tales que $p \neq x$ y $\{x, p\} \subseteq c$. Por otro lado, x está en t bloques cada uno con $k-1$ puntos distintos a x, entonces $\lambda(v-1) = t(k-1)$. Esto ocurre para cada punto de D, por lo que todo punto es incidente con t bloques. Contando el número de banderas de D de dos formas obtenemos que $vk = tv$, lo que implica que $t = k$. □

Con la siguiente definición podemos construir un nuevo SBIBD a partir de un SBIBD ya conocido, este tendrá el mismo número de puntos, pero el resto de los parámetros serán diferentes.

Definición 3. Sea $D = (P, B)$ un (v, k, λ)-SBIBD. Definimos el **complemento** de D como el diseño $D^c = (P, B^c)$ que tiene el mismo conjunto de puntos que D y el conjunto de bloques está dado por los complementos de los bloques de D en P, es decir, $B^c = \{(P \setminus c) : c \in B\}$.

Lema 2. *Si $D = (P, B)$ es un (v, k, λ)-SBIBD, entonces $D^c = (P, B^c)$ es un $(v, v-k, v-2k+\lambda)$-SBIBD.*

Demostración. Por definición D^c tiene v puntos y sus bloques tienen cardinalidad $v-k$. Además notemos que si $c \neq c'$, entonces $P \setminus c \neq P \setminus c'$ por lo que $|B^c| = v$. Sean $p_1, p_2 \in P$. Como D es un (v, k, λ)-SBIBID, tenemos que p_1 y p_2 están contenidos, cada uno, en exactamente k bloques y que $\{p_1, p_2\}$ está contenido en exactamente λ bloques. Por lo tanto $\{p_1, p_2\}$ no está contenido en $v - 2k + \lambda$ bloques de D. □

Ejemplo 3. Por el Lema 2, el complemento del $(16, 6, 2)$-SBIBD definido en el Ejemplo 2, es un $(16, 10, 6)$-SBIBD.

Definición 4. Sea $D = (P, B)$ un (v, k, λ)-SBIBD. Sean $P = \{p_1, p_2, ..., p_v\}$ y $B = \{c_1, c_2, ..., c_v\}$. Definimos la **matriz de incidencia** de D como la matriz M de $v \times v$ tal que

$$M_{ij} = \begin{cases} 1 \text{ si } p_i \in c_j, \\ 0 \text{ en otro caso.} \end{cases}$$

Teorema 1. *Sea M una matriz de $v \times v$ con entradas en $\mathbb{Z}_2$. Entonces M es la matriz de incidencia de un (v, k, λ)-SBIBD si* y *sólo si M cumple que:*

(i) $MM^t = \lambda J_v + (k - \lambda) Id_v$,

(ii) $1_v M = k 1_v$,

donde J_v denota a la matriz de $v \times v$ que tiene todas sus entradas iguales a 1, Id_v es la matriz identidad de $v \times v$ y *1_v es la matriz de $1 \times v$ con todas sus entradas iguales a 1.*

Demostración. Sea M la matriz de incidencia de un (v, k, λ)-SBIBD, el inciso (ii) se sigue de que cada columna tiene k entradas iguales a 1. Sean R_i y R_j el i-ésimo y el j-ésimo reglón de M respectivamente, entonces el producto punto $R_i \cdot R_j = k$ si $i = j$ y $R_i \cdot R_j = \lambda$ cuando $i \neq j$. Entonces $(MM^t)_{ij} = k$ si $i = j$ y $(MM^t)_{ij} = \lambda$ si $i \neq j$, por lo que M cumple (i)
Supongamos ahora que M cumple (i) y (ii). Definimos $D = (P, B)$ de la siguiente forma. Consideremos $P = \{p_1, p_2, ..., p_v\}$ un conjunto con v puntos y $B = \{c_1, c_2, ..., c_v\}$ una familia de subconjuntos de P donde para cada $i, j \in \{1, 2, ..., v\}$, $p_i \in c_j$ si y sólo si $M_{ij} = 1$. La condición (ii) implica que $|c_j| = k$ para toda $j \in \{1, 2, ..., v\}$. Sean $p_i, p_j \in P$ con $i \neq j$, la condición (i) nos dice que $M_{i\ell} = M_{j\ell} = 1$ exactamente para λ valores de ℓ. Por lo tanto $\{p_i, p_j\} \subseteq c_\ell$ exactamente para λ valores de ℓ. Entonces D es un (v, k, λ)-SBIBD y M es su matriz de incidencia. □

Lema 3. *Sea M la matriz de incidencia de un (v, k, λ)-SBIBD. Entonces M es invertible.*

Demostración. Por el Teorema 1, $MM^t = \lambda J_v + (k - \lambda) Id_v$. Restando el primer renglón de MM^t al resto de los renglones y después sumando a la primera columna cada columna distinta de la primera columna obtenemos que:

$$det(MM^t) = det \begin{pmatrix} k + (n-1)\lambda & \lambda & \cdots & \lambda \\ 0 & k - \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k - \lambda \end{pmatrix} = [k + (n-1)\lambda](k - \lambda)^{n-1}.$$

Esto implica que $det(M) \neq 0$ y por lo tanto M es invertible. □

El siguiente teorema nos da una de las propiedades fundamentales de los diseños simétricos.

Teorema 2. *Sea $D = (P, B)$ un (v, k, λ)-SBIBD, entonces todo par de bloques se intersecta en exactamente λ puntos.*

Demostración. Sean $P = \{p_1, p_2, ..., p_v\}$ y $B = \{c_1, c_2, ..., c_v\}$. Consideremos a M la matriz de incidencia de D. La condición (i) del Teorema 1 nos da que $MM^t = \lambda J_v + (k-\lambda)Id_v$. Si multiplicamos por M por la derecha y por M^{-1} por la izquierda obtenemos que $M^tM = M^{-1}\lambda J_v M + (k-\lambda)I_v$. Notemos que por el Lema 1, cada punto incide en k bloques, y entonces se sigue que $\lambda J_v M = M\lambda J_v = k\lambda J_v$. Por lo tanto $M^tM = \lambda J_v + (k-\lambda)I_v$. Concluimos que el producto punto de cualesquiera dos columnas distintas de M es λ, lo que implica que todo par de bloques se intersecta en λ puntos. □

Por el teorema anterior es posible hacer la siguiente construcción; con la cual, al igual que con el complemento, podemos obtener un nuevo SBIBD a partir de uno dado, con la diferencia de que aquí los parámetros de ambos diseños coinciden.

Definición 5. Sea $D = (P, B)$ un (v, k, λ)-SBIBD. Para cada punto $p \in P$ definamos $c_p = \{c \in B : p \in c\}$. El **dual** de D es el (v, k, λ)-SBIBD dado por $D' = (P', B')$ donde $P' = B$, y $B' = \{c_p : p \in P\}$.

La siguiente definición introduce un nuevo parámetro para cada (v, k, λ)-SBIBD, con él es posible clasificar a los disenõs simétricos en términos de la diferencia entre los parámetros k y λ.

Definición 6. El **orden** de un (v, k, λ)-SBIBD es $n = k - \lambda$.

Definición 7. Sea D un $(4n-1, 2n-1, n-1)$-SBIBD, entonces D es un **diseño de Hadamard** de orden n.

El nombre de los diseños de Hadamard proviene del de las matrices con este mismo nombre y del hecho de que para cada una de estas se puede obtener un diseño de Hadamard.

Definición 8. Una matriz M de $v \times v$ con entradas en $\{1, -1\}$ es una **matriz de Hadamard** si $MM^t = vId_v$.

Lema 4. *Sea M una matriz de Hadamard, entonces:*

(*i*) *M^t también es una matriz de Hadamard.*

(*ii*) *Si M' es la matriz obtenida a partir de M al multiplicar un renglón o columna de M por -1, entonces M' también es una matriz de Hadamard.*

Demostración. (*i*) Como $MM^t = vId_v$ entonces $M^tMM^t = M^t(vId_v) = (vId_v)M^t$, lo que implica que $M^tM = vId_v$.

(*ii*) Sea M' la matriz obtenida a partir de M multiplicando el i-ésimo renglón M_i por -1. Entonces $M'_i \cdot M'_i = (-M_i) \cdot (-M_i) = M_i \cdot M_i = v$ y si $i \neq j$, entonces $M'_i \cdot M'_j = (-M_i) \cdot M_j = -(M_i \cdot M_j) = 0$. Concluimos que M' también es una matriz de Hadamard. Similarmente, utilizando el inciso (*i*), si M' es la matriz obtenida a partir de multiplicar una columna por -1, M' es una matriz de Hadamard.

□

Lema 5. *Sea M una matriz de Hadamard de $v \times v$ con $v > 2$, entonces $v = 4n$ para algún $n \in \mathbb{Z}^+$.*

Demostración. Por el Lema 4 podemos suponer que M es una matriz con todas las entradas del primer renglón M_1 iguales a 1. Como $v > 2$, podemos considerar dos renglones más M_i y M_j. Sean:

$$A_1 = \{\ell : M_{j\ell} = 1 \ y \ M_{i\ell} = 1\} \text{ y } |A_1| = a_1,$$
$$A_2 = \{\ell : M_{j\ell} = 1 \ y \ M_{i\ell} = -1\} \text{ y } |A_2| = a_2,$$
$$A_3 = \{\ell : M_{j\ell} = -1 \ y \ M_{i\ell} = 1\} \text{ y } |A_3| = a_3,$$
$$A_4 = \{\ell : M_{j\ell} = -1 \ y \ M_{i\ell} = -1\} \text{ y } |A_4| = a_4.$$

Notemos que $a_1 + a_2 + a_3 + a_4 = n$. Además $M_1 \cdot M_i = a_1 + a_3 - a_2 - a_4 = 0$, $M_1 \cdot M_j = a_1 + a_2 - a_3 - a_4 = 0$ y $M_i \cdot M_j = a_1 + a_4 - a_2 - a_3 = 0$. Entonces $a_1 + a_3 = a_2 + a_4$, $a_1 + a_2 = a_3 + a_4$ y $a_1 + a_4 = a_2 + a_3$. Concluimos que $a_1 = a_2 = a_3 = a_4 = t$. □

Definición 9. Sea M una matriz de Hadamard de $v \times v$ con $v > 2$. El **orden** de M es $\frac{v}{4}$.

Lema 6. *Existe una matriz de Hadamard de orden n si y sólo si existe un diseño de Hadamard de orden n.*

Demostración. Sea M una matriz de Hadamard de orden n. Por el Lema 4 podemos suponer que M tiene todas las entradas de su primer renglón y primera columna iguales a 1. Sea M_D la matriz obtenida a partir de M quitando el primer renglón, la primera columna y sustituyendo cada entrada igual a -1 por 0. Entonces, por la demostración del Lema 5, tenemos que:

(i) $M_D M_D^t = (n-1)J_{4n-1} + nId_{4n-1}$,

(ii) $(1_{4n-1})M = (2n-1)(1_{4n-1})$;

el Teorema 1 implica que M_D es la matriz de incidencia de un diseño de Hadamard de orden n.
Recíprocamente, sea M_D la matriz de incidencia de un diseño de Hadamard de orden n, entonces la matriz M obtenida al agregar un renglón y una columna con todas sus entradas iguales a 1 e intercambiando las entradas iguales a 0 por -1 es una matriz de Hadamard de orden n. Ver Cuadro 2. □

$$\begin{pmatrix} + & + & + & + & + & + & + & + & + & + & + & + \\ + & + & - & - & - & + & - & - & + & + & + & - \\ + & - & + & - & - & + & - & - & - & + & + & + \\ + & + & - & + & - & - & + & - & - & - & + & + \\ + & + & + & - & + & - & - & + & - & - & - & + \\ + & + & + & + & - & + & - & - & + & - & - & - \\ + & - & + & + & + & - & + & - & - & + & - & - \\ + & - & - & + & + & + & - & + & - & - & + & - \\ + & - & - & - & + & + & + & - & + & - & - & + \\ + & + & - & - & - & + & + & + & - & + & - & - \\ + & - & + & - & - & - & + & + & + & - & - & + \\ + & + & - & + & - & - & - & + & + & + & - & - \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Cuadro 2. Una matriz de Hadamard de orden 3 da lugar a la matriz de incidencia de un diseño de Hadamard de orden 3.

Definición 10. Sea D un $(n^2+n+1, n+1, 1)$-SBIBD, entonces D es un **plano proyectivo** de orden n.

Ejemplo 4. Sea q la potencia de un primo. Entonces $P = (\mathbb{F}_q^3 \setminus \{0\})/\mathbb{F}_q^*$ tiene q^2+q+1 elementos. Para cada dos elementos de P existe un único subespacio 2-dimensional U de $\mathbb{F}_q^3$ que los contiene y $(U \setminus \{0\})/\mathbb{F}_q^*$ tiene $q+1$ elementos de P. Si $B = \{(U \setminus \{0\})/\mathbb{F}_q^* : U \leq \mathbb{F}_q^3,\ dim(U) = 2\}$, entonces $|B| = q^2+q+1$ y (P, B) es un plano proyectivo de orden q.

El siguiente teorema acota el número de puntos de un diseño simétrico en términos de su orden.

Teorema 3. *Sea D un (v,k,λ)-SBIBD no trivial de orden n. Entonces*

$$4n-1 \leq v \leq n^2+n+1.$$

La cota inferior se alcanza cuando D es un diseño de Hadamard o el complemento de un diseño de Hadamard y *la superior cuando D es un plano proyectivo o el complemento de un plano proyectivo.*

Demostración. Sustituyendo $\lambda = k-n$ en la Ecuación (1) del Lema 1 y resolviendo para k obtenemos que

$$k = \frac{v \pm \sqrt{v^2-4n(v-1)}}{2}. \tag{2}$$

Como k es un número entero positivo, sabemos que $v^2-4n(v-1) \geq 0$, lo que implica que $\frac{v^2}{v-1} \geq 4n$. Sabemos también que $4n$ es un entero, por lo que la ecuación anterior implica que $v+1 = \lfloor \frac{v^2}{v-1} \rfloor \geq 4n$. Se sigue que $4n-1 \leq v$. Ahora, despejando v de (1), obtenemos $v = \frac{n^2}{\lambda} + (2-\frac{1}{\lambda})n + \lambda = \frac{n^2-n}{\lambda} + 2n + \lambda$. Dado que v es un entero y D es no trivial, $\lambda \leq n^2-n$, de lo que se sigue que $(\lambda-1)(\frac{n^2-n}{\lambda}-1) \geq 0$. Distribuyendo obtenemos que

$$(n^2+n+1) - (\tfrac{n^2}{\lambda} + (2-\tfrac{1}{\lambda})n + \lambda) \geq 0$$

y por lo tanto $v = \frac{n^2}{\lambda} + (2-\frac{1}{\lambda})n + \lambda \leq n^2+n+1$.
Supongamos que se alcanza la cota inferior, es decir, $v = 4n-1$. Sustituyendo en (2) tenemos que $k = 2n-1$ o $k = 2n$. En el primer caso, sustituyendo en (1), obtenemos $\lambda = n-1$ y entonces D es un diseño de Hadamard de orden n. En el otro caso $\lambda = n$, por lo que D es el complemento de un diseño de Hadamard de orden n.
Supongamos que se alcanza la cota superior. Entonces $v = n^2+n+1$. Sustituyendo en (2) tenemos que $k = n^2$ ó $k = n+1$. En el primer caso, sustituyendo en (1), obtenemos $\lambda = n^2-n$ y entonces D es el complemento de un plano proyectivo de orden n. En el otro caso, $\lambda = 1$, y entonces D es un plano proyectivo de orden n. □

A continuación enunciamos el Teorema de Bruck-Ryser-Chowla, este impone fuertes restricciones a los parámetros v, k y λ de un (v,k,λ)-SBIBD y fueron de gran utilidad para descartar la existencia de biplanos. Su demostración puede ser consultada en [9, 306pp, Teorema 2.1].

Teorema 4 (Teorema de Bruck-Ryser-Chowla)**.** *Sea D un (v, k, λ)-SBIBD de orden $n = k - \lambda$*

- *Si v es par, entonces n es un cuadrado perfecto.*
- *Si v es impar, entonces la ecuación $x^2 = ny^2 + (-1)^{\frac{v-1}{2}}\lambda z^2$ tiene solución no trivial en los enteros.*

Muchos de los diseños simétricos muestran un alto grado de simetría, para mostrar este hecho necesitamos las siguientes definiciones para ilustrar este hecho.

Definición 11. Sean $D_1 = (P_1, B_1)$ y $D_2 = (P_2, B_2)$ dos (v, k, λ)-SBIBDs. Un **isomorfismo de SBIBDs** es una función biyectiva $\alpha : P_1 \longrightarrow P_2$ tal que para todo bloque c de D_1 se cumple que $c \in B_1$ si y sólo si $c^\alpha \in B_2$. Cuando hay un ismorfismo entre D_1 y D_2 decimos que D_1 y D_2 son isomorfos y lo denotamos por $D_1 \cong D_2$.

Definición 12. Sea $D = (P, B)$ un (v, k, λ)-SBIBD. Un **automorfismo** de D es un isomorfismo de D en si mismo. El conjunto de todos ellos con la composición forma un grupo llamado el grupo de automofismos de D, denotado por $Aut(D)$.

Ejemplo 5. En el SBIBD construido en el Ejemplo 2 consideremos la biyección φ que intercambia la primera y cuarta columna de la cuadrícula. Entonces $c_{p_i}^{\varphi} = c_{p_i}$ si p_i no está en ninguna de estas columnas y $c_{p_i}^{\varphi} = c_{p_i^{\varphi}}$ si p_i está en una de las columnas que se intercambiaron. Por lo tanto φ es un automorfismo.

Lema 7. *Supongamos que D_1 y D_2 son dos SBIBDs tales que $D_1 \cong D_2$, entonces $Aut(D_1) \cong Aut(D_2)$.*

Demostración. Sea φ un isomorfismo entre $D_1 = (P_1, B_1)$ y $D_2 = (P_2, B_2)$. Definimos $\Theta : Aut(D_1) \longrightarrow Aut(D_2)$ para cada $\sigma \in Aut(D_1)$ como:

$$\Theta : \sigma \mapsto \varphi^{-1}\sigma\varphi.$$

Claramente $\Theta(\sigma)$ es biyectiva y se tiene que $c \in B_2$ si y sólo si $c^{\varphi^{-1}\sigma\varphi} \in B_2$. Por lo tanto Θ está bien definida. Sean σ, $\sigma' \in Aut(D_1)$ tales que $\varphi^{-1}\sigma\varphi = \varphi^{-1}\sigma'\varphi$, entonces $\sigma = \sigma'$. Concluimos que Θ es inyectiva. También es suprayectiva pues si $\gamma \in Aut(D_2)$, entonces $\varphi\gamma\varphi^{-1} \in Aut(D_1)$ y $\Theta(\varphi\gamma\varphi^{-1}) = \gamma$. Finalmente, $\Theta(\sigma_1\sigma_2) = \varphi^{-1}\sigma_1\sigma_2\varphi = \varphi^{-1}\sigma_1\varphi\varphi^{-1}\sigma_2\varphi = \Theta(\sigma_1)\Theta(\sigma_2)$ para todo $\sigma_1, \sigma_2 \in Aut(D_1)$. □

Lema 8. *Sean $D = (P, B)$ un (v, k, λ)-SBIBD y $\sigma \in Aut(D)$, entonces σ fija el mismo número de puntos que de bloques.*

Demostración. Sean f y F el número de puntos y bloques fijados por σ respectivamente. Sea $A = \{(p, c) : \{p, p^\sigma\} \subseteq c\}$. Por cada punto fijo p hay k bloques que lo contienen y por cada punto p no fijado, hay λ bloques que contienen a $\{p, p^\sigma\}$. Concluimos que A tiene $fk + \lambda(v - f)$ parejas.
Por otro lado, por cada bloque fijo c y punto $p \in c$, se cumple que $\{p, p^\sigma\} \subseteq c$, y para cada bloque c no fijado tenemos que $|c \cap c^{\sigma^{-1}}| = \lambda$. Entonces también hay $Fk + \lambda(v - F)$ parejas en A. Igualando obtenemos que $f = F$. □

Definición 13. Sea D un SBIBD. Decimos que $Aut(D)$ es **transitivo en banderas** si actúa transitivamente en las banderas de D.

Ejemplo 6. Consideremos el diseño trivial D con parámetros $(4, 3, 2)$ construido en el Ejemplo 1, es claro que $Aut(D) = S_4$ es transitivo en banderas pues si (p, c) y (p', c') son dos banderas, entonces $c = P \setminus \{i\} = \{p, l, k\}$ y $c' = P \setminus \{j\} = \{p', t, s\}$ donde $p \neq i$ y $p' \neq j$, entonces σ definida como $p^\sigma = p'$, $l^\sigma = t$ y $k^\sigma = s$ es tal que $c^\sigma = c'$.

Teorema 5. *Si D es un (v, k, λ)-SBIBD con grupo de automorfismos G transitivo en banderas e imprimitivo en puntos, entonces se cumple una de las siguientes condiciones:*

(1) $(v, k, \lambda) = (\lambda^2(\lambda + 2), \lambda(\lambda + 1), \lambda)$

(2) $k \leq \lambda(\lambda - 2)$.

Corolario 1. *Si G es el grupo de automorfismos de un (v, k, λ)-SBIBD D con $\lambda \leq 4$, entonces G es primitivo en puntos, o D tiene parámetros $(16, 6, 2)$, $(45, 12, 3)$, $(15, 8, 4)$ o $(96, 20, 4)$.*

Tanto el Teorema 5 como el Corolario 1 se pueden encontrar en [13], son de gran utilidad ya que reducen las posibilidades de SBIBDs con grupos de automorfismos imprimitivos.

2. Conjuntos de diferencia

El concepto de conjunto de diferencia está muy ligado al de diseño simétrico, con la ventaja de que los primeros se pueden estudiar utilizando la estructura que tienen los grupos abelianos finitos.

Definición 14. Sean v, k, $\lambda \in \mathbb{Z}^+$ y C un subconjunto de un un grupo abeliano (aditivo) finito G. Entonces C es un (v, k, λ)-**conjunto de diferencia** en G si $|G| = v$, $|C| = k$, y el conjunto de todas las diferencias de elementos de C contiene a cada $g \in G \setminus \{0\}$ exactamente λ veces.

Ejemplo 7. Sea $C = \{(0,0), (1,0), (1,1), (3,0), (4,1), (7,0)\}$, veamos que C es un $(16, 6, 2)$-conjunto de diferencia en $\mathbb{Z}_8 \times \mathbb{Z}_2$. Para esto escribiremos el conjunto de todas las diferencias de elementos de C.

(0,0)-(1,0)=(7,0)	(1,1)-(0,0)=(1,1)	(4,1)-(0,0)=(4,1)
(0,0)-(1,1)=(7,1)	(1,1)-(1,0)=(0,1)	(4,1)-(1,0)=(3,1)
(0,0)-(3,0)=(5,0)	(1,1)-(3,0)=(6,1)	(4,1)-(1,1)=(3,0)
(0,0)-(4,1)=(4,1)	(1,1)-(4,1)=(5,0)	(4,1)-(3,0)=(1,1)
(0,0)-(7,0)=(1,0)	(1,1)-(7,0)=(2,1)	(4,1)-(7,0)=(5,1)
(1,0)-(0,0)=(1,0)	(3,0)-(0,0)=(3,0)	(7,0)-(0,0)=(7,0)
(1,0)-(1,1)=(0,1)	(3,0)-(1,0)=(2,0)	(7,0)-(1,0)=(6,0)
(1,0)-(3,0)=(6,0)	(3,0)-(1,1)=(2,1)	(7,0)-(1,1)=(6,1)
(1,0)-(4,1)=(5,1)	(3,0)-(4,1)=(7,1)	(7,0)-(3,0)=(4,0)
(1,0)-(7,0)=(2,0)	(3,0)-(7,0)=(4,0)	(7,0)-(4,1)=(3,1)

Cada elemento de $\mathbb{Z}_8 \times \mathbb{Z}_2 \setminus \{(0,0)\}$ aparece exactamente 2 veces.

La siguiente construcción, llamada la Construcción de Payley, nos da más ejemplos de conjuntos de diferencia.

Ejemplo 8. Sea q una potencia de primo tal que $q \equiv 3 \ (mod\ 4)$. Llamemos $C = (\mathbb{F}_q^*)^2$. Para cada $x \in \mathbb{F}_q \setminus \{0\}$, definimos A_x como el conjunto de parejas (u, u') en $C \times C$ tales que $u - u' = x$. Sea $\lambda = |A_1|$. Notemos que si $x \in C$, entonces $\varphi : A_1 \longrightarrow A_x$ dada por $\varphi : (u, u') \mapsto (xu, xu')$, es una biyección. Si $x \notin C$, el Lema 49 implica que $-x \in C$ y claramente $|A_x| = |A_{-x}|$. Por lo tanto $|A_x| = \lambda$ para toda $x \in \mathbb{F}_q^*$. Entonces $\lambda(q-1) = \left(\frac{q-1}{2}\right)\left(\frac{q-1}{2} - 1\right)$. Despejando obtenemos que $\lambda = \frac{q-3}{4}$ y así C es un $(q, \frac{q-1}{2}, \frac{q-3}{4})$-conjunto de diferencia en $\mathbb{F}_q$.

Ahora veamos cómo se relacionan los conjuntos de diferencia con los diseños simétricos, necesitamos la siguiente definición.

Definición 15. Sea C un subconjunto de un grupo abeliano finito G. Definimos al **desarrollo** de C como el conjunto de todos los trasladados de C por elementos de G y lo denotamos por $Dev(C)$, es decir,

$$Dev(C) := \{C + g : g \in G\}.$$

Teorema 6. *Si C es un (v, k, λ)-conjunto de diferencia en un grupo abeliano G, entonces $D = (G, Dev(C))$ es un (v, k, λ)-SBIBD.*

Demostración. Notemos que $\circ(G) = v$ y $|C + g| = k$ para toda $g \in G$, por lo que basta demostrar que $|Dev(G)| = v$ y que todo par de puntos está en exactamente λ bloques. Sean $g, g' \in G$ tales que $g \neq g'$, entonces existen $u_{i_1}, ..., u_{i_\lambda}$ y $u_{i'_1}...u_{i'_\lambda}$ en C tales que $g - g' = u_{i_j} - u_{i'_j}$ para $1 \leq j \leq \lambda$, lo que implica que $|(C + g) \cap (C + g')| = \lambda < k$. Por lo tanto $|Dev(C)| = v$.
Ahora, sean h y h' elementos diferentes de G. Entonces hay λ diferencias de elementos de C iguales a $h - h'$, es decir,

$$h - h' = u_{i_1} - u_{i'_1} = ... = u_{i_\lambda} - u_{i'_\lambda}$$

para ciertos $u_{i_j}, u_{i'_j}$ en C. Se sigue que $h - u_{i_j} = h' - u_{i'_j} := g_j$ para $1 \leq j \leq \lambda$ y por lo tanto $\{h, h'\} \subseteq C + g_j$ donde $1 \leq j \leq \lambda$. De haber otro bloque $C + g \neq C + g_j$ para $1 \leq j \leq \lambda$ tal que $\{h, h'\} \subseteq C + g$, entonces habría más de λ diferencias de elementos de C iguales a $h - h'$. □

Corolario 2. *Sea C un (v, k, λ)-conjunto de diferencia en un grupo abeliano G. Entonces $\lambda(v - 1) = k(k - 1)$.*

Como consecuencia del Teorema 6 y la construcción dada en el Ejemplo 8, tenemos que si q es una potencia de primo tal que $q \equiv 3 \ (mod\ 4)$, entonces $(\mathbb{F}_q, Dev(C))$ es un $(q, \frac{q-1}{2}, \frac{q-3}{4})$-SBIBD, donde $C = (\mathbb{F}_q^*)^2$. Veamos ahora una especie de recíproco del Teorema 6.

Teorema 7. *Si G es un grupo abeliano de orden v y C un k-subconjunto de G tal que $D = (G, Dev(C))$ es un (v, k, λ)-diseño simétrico, entonces C es un (v, k, λ)-conjunto de diferencia en G.*

Demostración. Sea h un elemento no cero de G. Dado que $D = (G, Dev(C))$ es un (v, k, λ)-SBIBD, la pareja $\{0, h\}$ está contenida en exactamente λ bloques $C + g_1, ..., C + g_\lambda$. Entonces existen $u_{i_1}, ..., u_{i_\lambda}$ y $u_{i'_1}, ..., u_{i'_\lambda}$ en C tales que $h = u_{i_j} + g_j$ y $0 = u_{i'_j} + g_j$ para $1 \leq j \leq \lambda$ y entonces $h = u_{i_j} - u_{i'_j}$ para $1 \leq j \leq \lambda$. De haber una diferencia más tal que $h = u - u'$, entonces $u' \neq u_{i'_j}$ para $1 \leq j \leq \lambda$ y $\{0, h\} \subseteq C - u'$, contradiciendo que $\{0, h\}$ está en exactamente λ bloques. □

En [18] se define un par especial de diferentes formas, nosotros elegimos aquella que se relaciona con el concepto de conjunto de diferencia.

Definición 16. Sean p un primo y n un divisor de $p-1$. Decimos que (p, n) es un **par especial** si $p = nk + 1$ y el conjunto de las potencias n-ésimas de los elementos del grupo multiplicativo de $\mathbb{F}_p$ es un $(p, k, \frac{k-1}{n})$-conjunto de diferencia.

Ejemplo 9. La Construcción de Payley dada en el Ejemplo 8 nos dice que $(p, 2)$ es un par especial para cada primo $p \equiv 3 \ (mod\ 4)$.

Para obtener algunos resultados utilizamos los siguientes teoremas sobre pares especiales que K. Thas y D. Zagier presentan en [18].

Teorema 8. *Si D es un (p, k, λ)-diseño simétrico con p primo* y *con un grupo de automorfismos regular en banderas, entonces $k = \frac{p-1}{n}$, $\lambda = \frac{k-1}{n}$* y *(p, n) es un par especial.*

Teorema 9. *Sean p un primo* y *$n|(p-1)$. Entonces (p, n) es un par especial en cada uno de los siguientes casos:*

(a) $n = 1$, *p arbitrario.*

(b) $n = 2$, $p \equiv 3 \ (mod\ 4)$.

(c) $n = 4$, $p = 4b^2 + 1$, *con b impar.*

(d) $n = 8$, $p = 64b^2 + 9 = 8d^2 + 1$ *con b* y *d enteros.*

(e) $n = p - 1$, *p arbitrario.*

También en [18] se da la siguiente conjetura la cual se verifica computacionalmente para primos menores que 10^7.

Conjetura 1. *Los únicos pares especiales son los dados en el Teorema 9.*

3. Grupos de tipo afín

El Teorema de O'Nan-Scott clasifica a los grupos primitivos en cinco tipos: Afín, casi simple, diagonal, producto y producto "twisted wreath" [10]. En esta sección haremos una breve descripción de los grupos de tipo afín.

Definición 17. Sea V un espacio vectorial de dimensión n sobre $\mathbb{F}_q$. Definimos a la **geometría afín** de dimensión n como el conjunto de todos los subespacios vectoriales de V junto con todos sus trasladados, la denotamos por $AG_n(q)$.

Definición 18. Sea V un espacio vectorial de dimensión n sobre $\mathbb{F}_q$. Para cada $\beta \in V$ y $\alpha \in GL_n(q)$ definimos la transformación $t_{\alpha,\beta} : V \longrightarrow V$ dada por $t_{\alpha,\beta} : x \mapsto \alpha(x) + \beta$. A estas funciones las llamamos **transformaciones afines** y son automorfismos de V que preservan la geometría afín $AG_n(q)$. El conjunto de todas ellas junto con la composición de funciones forma un grupo, al cual denotaremos por $AGL_n(q)$. Si $G \leq AGL_n(q)$ diremos que G es de tipo **afín**.

Definición 19. Sea V un espacio vectorial de dimensión n sobre $\mathbb{F}_q$. Por cada $\sigma \in Aut(\mathbb{F}_q)$ y $t_{\alpha,\beta} \in AGL_n(q)$ podemos definir una transformación $t_{\alpha,\beta,\sigma} : V \longrightarrow V$ dada por $t_{\alpha,\beta,\sigma} : x \mapsto \alpha(x^\sigma) + \beta$, donde x^σ es el vector en el que a cada componente se le aplicó σ. Estas son las **transformaciones semilineales afines**, y al conjunto de todas ellas se le denotará por $A\Gamma L_n(q)$; este, junto con la composición de funciones, conforma al grupo completo de automorfismos de $AG_n(q)$.

Observemos que si V es un espacio vectorial de dimensión uno sobre $\mathbb{F}_q$, entonces el grupo de transformaciones lineales $GL_1(q)$ es isomorfo al grupo multiplicativo de $\mathbb{F}_q$. La imagen de $x \in \mathbb{F}_q$ bajo dicho isomorfismo está dada por la transformación $\hat{x} : y \mapsto xy$. Por esta observación se sigue que $|AGL_1(q)| = q(q-1)$ y si $q = p^r$ para algún primo p, entonces el Lema 48 nos dice que $|Aut(\mathbb{F}_q)| = r$ y por lo tanto $|A\Gamma L_1(q)| = q(q-1)r$. A lo largo del texto estudiamos principalmente al grupo $A\Gamma L_1(q)$, a continuación están algunas de sus propiedades más importantes.

Lema 9. *El grupo $A\Gamma L_1(q)$ es igual a $\langle T, \hat{\omega}, a\rangle$, donde T es el subgrupo de traslaciones, ω es una raíz primitiva de $\mathbb{F}_q$, $\hat{\omega}$ denota la multiplicación por ω y a es el automorfismo de Frobenius.*

Demostración. Consideremos una transformación semilineal afín $t_{\alpha,\beta,\sigma}$. Por el Lema 48, $Aut(\mathbb{F}_q) = \langle a \rangle$, entonces tenemos que $\alpha = \hat{\omega}^m$ y $\sigma = a^s$. De esta forma $t_{\alpha,\beta,\sigma} = a^s \cdot \hat{\omega}^m \cdot t_{1,\beta,1}$, donde $t_{1,\beta,1} \in T$. □

Lema 10. *Sean p un primo impar* y *q una potencia de p. Entonces el estabilizador puntual de $\{0,1\}$ en $A\Gamma L_1(q)$ está generado por el automorfismo de Frobenius.*

Demostración. Sea a el automorfismo de Frobenius y denotemos por $A_{0,1}$ al estabilizador puntual de $\{0,1\}$ en $A\Gamma L_1(q)$. Claramente $\langle a \rangle \subseteq A_{0,1}$.
Sea $t_{\alpha,\beta,\sigma} \in A_{0,1}$. Entonces existe un entero positivo m tal que $\alpha = \hat{\omega}^m$, donde ω es una raíz primitiva de $\mathbb{F}_q$. Tenemos que $\alpha(0) + \beta = \beta = 0$ y $\alpha(1) + \beta = \omega^m = 1$, por lo que $m = q - 1$ y $\alpha = Id$. Lo anterior implica que $t_{\alpha,\beta,\sigma} = a^k$ para alguna k. □

Lema 11. *Sea q la potencia de un primo. Entonces $AGL_1(q)$ es 2-transitivo en $\mathbb{F}_q$.*

Demostración. Sea $(x_1, x_2) \in \mathbb{F}_q \times \mathbb{F}_q$, con $x_1 \neq x_2$. Basta observar que existe $t_{\alpha,\beta} \in AGL_1(q)$ tal que $t_{\alpha,\beta} : 0 \mapsto x_1$ y $t_{\alpha,\beta} : 1 \mapsto x_2$. Sea α la transformación que multiplica por $(x_2 - x_1)$ y $\beta = x_1$, entonces $t_{\alpha,\beta}$ cumple lo deseado. □

Corolario 3. *Sea q la potencia de un primo. Entonces $A\Gamma L_1(q)$ es 2-transitivo en $\mathbb{F}_q$.*

Como consecuencia de [5, Teorema 2.1] y [6, Lema 4.1], tenemos el siguiente resultado.

Lema 12. *Sean p un primo, q una potencia de p* y *$G = T \cdot G_0 \leq A\Gamma L_1(q)$, entonces $G_0 = \left\langle \hat{\omega}^d, \hat{\omega}^e a^s \right\rangle$ donde ω es una raíz primitiva de $\mathbb{F}_q$, $\hat{\omega}$ denota la multiplicación por ω, a es el automorfismo de Frobenius, d, e* y *s son enteros positivos que satisfacen las siguientes propiedades:*

(*i*) $d > 0$ y $d|(p^r - 1)$,

(*ii*) $s > 0$ y $s|r$,

(*iii*) $0 \leq e < d$ y $\dfrac{e(p^r - 1)}{p^s - 1} \equiv 0 \ (mod\ d)$,

en particular $|G_0| = \dfrac{r(p^r - 1)}{sd}$ y $[G_0 : (G_0 \cap GL_1(p^r))] = \frac{r}{s}$.

En [11, Definición 4.5] se le llama a esta forma de presentar al estabilizador como la **forma estándar** de G_0.

Lema 13. *Sean p un primo, $r \in \mathbb{Z}^+$, y $G = T \cdot G_0 \leq A\Gamma L_1(p^r)$, entonces $H = G_0 \cap GL_1(p^r)$ es normal en G_0 y G_0/H es cíclico y su orden divide a r.*

Demostración. Sea $\varphi : G_0 \longrightarrow Aut(\mathbb{F}_{p^r})$ dada por $\varphi : t_{\alpha,0,\sigma} \mapsto \sigma$. Entonces φ es un homomorfismo y $ker\varphi = H$. Por lo tanto H es normal en G_0 y $G_0/H \cong img\varphi \leq Aut(\mathbb{F}_{p^r})$, lo que implica que G_0/H es cíclico y su orden divide a r.

□

Lema 14. *Sean p un número primo, $r \in \mathbb{Z}^+$, y s un divisor de r. Sea*

$$N = N_{A\Gamma L_1(p^r)}(a^s)$$

donde a denota el automorfismo de Frobenius. Entonces

$$N/\langle a^s \rangle \cong A\Gamma L_1(p^s).$$

Demostración. Sea ω una raíz primitiva de $\mathbb{F}_{p^r}$, por el Lema 45 a^s fija un subcampo F de $\mathbb{F}_{p^r}$ con p^s elementos generado por ω^m, donde m es el cociente de $p^r - 1$ entre $p^s - 1$. Podemos identificar a F con $\mathbb{F}_{p^s}$ y a ω^m con una raíz primitiva ρ de $\mathbb{F}_{p^s}$. Sea $t_{\alpha,\beta,\sigma} \in N$, entonces $t_{\alpha,\beta,\sigma} \cdot a^s = a^s \cdot t_{\alpha,\beta,\sigma}$. Esto implica que $\alpha = \alpha^{p^s}$ y que $\beta = \beta^{p^s}$, por lo tanto $\alpha = \hat{\omega}^{im}$ y $\beta = \omega^{jm}$ para algunos enteros positivos i y j. Definimos $\varphi : N \longrightarrow A\Gamma L_1(p^s)$ como:

$$\varphi : t_{\hat{\omega}^{im},\omega^{jm},a^k} \mapsto t_{\hat{\rho}^i,\rho^j,a^{k'}}$$

donde k' es el residuo de k módulo s. Observamos que φ es un homomorfismo y que $ker\varphi = \langle a^s \rangle$. El resultado se sigue por el Primer Teorema de Isomorfismos de grupos. □

Corolario 4. *Sean p un primo, $r \in \mathbb{Z}^+$, $G \leq A\Gamma L_1(p^r)$ y s un divisor de r. Si $N = N_G(a^s)$, donde a denota al automorfismo de Frobenius, entonces*

$$N/\langle a^s \rangle \cong G' \leq A\Gamma L_1(p^s).$$

Demostración. Se sigue de que $N_G(a^s) \leq N_{A\Gamma L_1(p^r)}(a^s)$ y del lema anterior. □

4. Biplanos

Comenzamos nuestro estudio de los biplanos enfocándonos a aquellos que tienen un grupo de automorfismos transitivo en banderas. En la primera parte de esta sección se demuestra que si además su grupo de automorfismo es imprimitivo, entonces los biplanos sólo pueden tener parámetros $(16, 6, 2)$.

Definición 20. Un **biplano** es un $(v, k, 2)$-SBIBD, para algunos $v, k \in \mathbb{Z}^+$.

Los valores de k para los que se conocen $(v, k, 2)$-biplanos no triviales son 4, 5, 6, 9, 11 y 13. Cuando k es 7, 8, 10 y 12 se puede demostrar, utilizando el Teorema de Bruck-Ryser-Chowla (Teorema 4), que no existen $(v, k, 2)$-biplanos. La siguiente propiedad básica de los biplanos es de gran utilidad ya que establece una relación entre los puntos y las parejas de bloques que inciden con un punto.

Lema 15. *Sean $D = (P, B)$ un biplano* y *$x \in P$. Entonces hay una biyección entre $P \setminus \{x\}$* y *las parejas de bloques incidentes con x.*

Demostración. Definimos φ para cada $y \in P \setminus \{x\}$ como $\varphi(y) = \{c, c'\}$, donde c y c' son los únicos bloques que contienen a $\{x, y\}$. Por el Teorema 2, φ es la biyección buscada. □

A continuación están un par de lemas que se necesitan para poder dar una prueba alternativa e independiente a un corolario del Teorema 5.

Lema 16. *Sea $D = (V, B)$ un $(v, k, 2)$-biplano con un grupo de automorfismos G imprimitivo en puntos* y *transitivo en banderas. Si G induce una partición de P en m bloques de imprimitividad cada uno con c puntos, entonces el número de puntos en que intersecta cada bloque de D a un bloque de imprimitividad es una constante d. Más aún, si s es el número de bloques de imprimitividad que intersecta a cada bloque de D, entonces $v = cm$, $k = ds$ y $c, m, d, s \geq 2$.*

Demostración. La primera parte se sigue de que G es transitivo en banderas. Como la partición de V dada por los bloques de imprimitividad es no trivial, se cumple que $c, m \geq 2$. Supongamos que $s = 1$, entonces $d = k$ y si Δ_1 y Δ_2 son dos bloques de imprimitividad, existen $b_1, b_2 \in B$ tales que $b_1 \subseteq \Delta_1$ y $b_2 \subseteq \Delta_2$, contradiciendo el Teorema 2.

Supongamos ahora que $d = 1$. Sea $x \in P$ y consideremos a Δ_x el bloque de imprimitividad tal que $x \in \Delta_x$, entonces $b \cap \Delta_x = \{x\}$ para todo bloque b tal que $x \in b$. Para cada par $\{b_1, b_2\}$ de bloques incidentes con x, existe un bloque de imprimitividad $\Delta_{b_1,b_2} \neq \Delta_x$ tal que $b_1 \cap \Delta_{b_1,b_2} = b_2 \cap \Delta_{b_1,b_2}$. Si $\{b_1, b_2\}$ y $\{b_3, b_4\}$ son dos parejas distintas de bloques incidentes con x, entonces $\Delta_{b_1,b_2} \neq \Delta_{b_3,b_4}$. Por lo tanto hay al menos $\frac{k(k-1)}{2} + 1 = v$ bloques de imprimitividad, contradiciendo que la partición de V es no trivial. □

Lema 17. *Sea $D = (P, B)$ un $(v, k, 2)$-biplano con un grupo de automorfismos G imprimitivo en puntos* y *transitivo en banderas. Si G induce una partición de P en bloques de imprimitividad cada uno con c puntos y los bloques de D se intersectan con los bloques de imprimitividad en d puntos, entonces:*

$$2(c-1) = k(d-1). \tag{3}$$

Demostración. Sea $x \in P$, entonces $x \in \Delta$ para algún bloque de imprimitividad Δ. Basta contar de dos maneras el número de parejas (y, b) tales que $b \in B$, $\{x, y\} \subseteq b$ y $y \in \Delta$. □

Corolario 5. *Un $(v, k, 2)$-biplano D con un grupo de automorfismos G imprimitivo en puntos* y *transitivo en banderas tiene parámetros* $(16, 6, 2)$.

Demostración. Supongamos que G induce m bloques de imprimitividad cada uno con c puntos y que los bloques de D se intersectan con los bloques de imprimitividad en d puntos. Por el Lema 16, $v = cm$ y $k = ds$, donde s es el número de bloques de imprimitividad que intersectan a cada bloque de D. Por el Lema 1 tenemos que $2(cm - 1) = k(k - 1)$. Despejando k de (3) y sustituyendo en la equación anterior obtenemos que:

$$2(cm-1) = \left(\frac{2(c-1)}{d-1}\right)\left(\frac{2(c-1)}{d-1} - 1\right).$$

Desarrollando y despejando m obtenemos que:

$$m = \frac{2c-4}{(d-1)^2} + \frac{2}{c(d-1)^2} - \frac{1}{d-1} + \frac{1}{c(d-1)} + \frac{1}{c}. \tag{4}$$

Por el algoritmo de la división existen q y r tales que

$$2c - 4 = q(d-1)^2 + r, \tag{5}$$

donde $0 \leq r < (d-1)^2$. Entonces:

$$m = q + \frac{r}{(d-1)^2} + \frac{2}{c(d-1)^2} - \frac{1}{d-1} + \frac{1}{c(d-1)} + \frac{1}{c} = q + \frac{rc + 2 - cd + c + d^2 - d}{c(d-1)^2}$$

$$= q + \frac{r - d + 1}{(d-1)^2} + \frac{d^2 - d + 2}{c(d-1)^2}.$$

Sea $x = \frac{r-d+1}{(d-1)^2} + \frac{d^2-d+2}{c(d-1)^2}$. Consideremos los siguientes casos.

(*i*) Si $d = 2$, sustituímos en (4) y obtenemos que $m = 2c - 5 + \frac{4}{c}$. Dado que m es un entero mayor o igual a 2, concluimos que $c = 4$, $m = 4$, $v = 16$ y $k = 6$.

Por el caso anterior, en adelante podemos suponer que $d \geq 3$.

(*ii*) Supongamos que $r \geq d - 1$, dado que $d < c$ y x alcanza su máximo cuando $r = (d-1)^2 - 1 = d^2 - 2d$, tenemos que:

$$0 < x \leq \frac{(c+1)d^2 - (3c+1)d + c + 2}{c(d-1)^2} < 1,$$

contradiciendo que m es un entero.

(*iii*) Si $r = d-2$, sustituyendo en (5) tenemos que $2c-4 = q(d-1)^2 + d - 2$, lo que implica que $2c - 2 = q(d-1)^2 + d$, pero $2c - 2 = k(d-1)$ y entonces $d - 1$ divide a d, una contradicción.

(*iv*) Si $r = d-3$, entonces $x = -\frac{2}{(d-1)^2} + \frac{d^2-d+2}{c(d-1)^2}$, para que x sea entero debe ocurrir que $c = \frac{d^2-d+2}{2}$, en cuyo caso $x = 0$ y $m = 1$, lo que contradice que $m \geq 2$.

(*v*) Finalmente supongamos que $r < d - 3$. Si $q = 0$, entonces (5) nos dice que $2c - 4 = r \leq d - 4$, y así $c \leq \frac{d}{2}$, lo que contradice que $d < c$. Por lo tanto $q \geq 1$, y entonces (5) nos da que $2c - 4 \geq (d-1)^2 + r$, lo que implica que $c \geq \frac{(d-1)^2}{2} + 2 + \frac{r}{2}$. Observamos que entonces:

$$-1 < x = \frac{r - d + 1}{(d-1)^2} + \frac{d(d-1) + 2}{(d-1)^2 c} \leq \frac{-3}{(d-1)^2} + \frac{d(d-1) + 2}{(d-1)^2 \left(\frac{(d-1)^2}{2} + 2 + \frac{r}{2}\right)} < 0,$$

lo que es otra contradicción.

□

El primer ejemplo no trivial de un biplano es el complemento del plano de Fano. El plano de Fano, el cual se puede construir a partir del Ejemplo 4 con $q = 2$, tiene parámetros $(7, 3, 1)$. Por el Lema 2, su complemento tiene parámetros $(7, 7-3, 7-6+1) = (7, 4, 2)$.
En [13], O'Reilly-Regueiro presenta el siguiente teorema que reduce las posibilidades para los biplanos con un grupo de automorfismos primitivo en puntos y transitivo en banderas.

Teorema 10. *Si D es un biplano no trivial con un grupo de automorfismos G primitivo en puntos* y *transitivo en banderas, entonces se satisface una de la siguientes afirmaciones:*

(1) *D tiene parámetros* $(16, 6, 2)$.

(2) *G es de tipo afín y $G \leq A\Gamma L_1(q)$ para una potencia de primo impar q.*

(3) *G es de tipo casi simple.*

El caso (3) es abordado por O'Reilly-Regueiro en [14], [15] y [16]. Ahí se demuestra que los únicos biplanos que admiten un grupo de automorfismos primitivo en puntos, transitivo en banderas y de tipo casi simple son el complemento del plano de Fano con parámetros $(7, 4, 2)$ y el diseño de Hadamard de orden 3 con parámetros $(11, 5, 2)$. En el caso en el que un grupo G sea como en el inciso (2) de la clasificación anterior, decimos que G es de tipo **afín de dimensión uno** y asumimos que actúa en $\mathbb{F}_q$. Un ejemplo de este último caso es el $(37, 9, 2)$-biplano transitivo en banderas construido a partir de que $(\mathbb{F}_{37}^*)^4$ es un $(37, 9, 2)$-conjunto de diferencia en $\mathbb{F}_{37}$.
Los siguientes dos Teoremas también se pueden encontrar en [13], y nos son de gran utilidad para continuar con la clasificación de los biplanos dado que restringen las posibilidades para sus parámetros.

Teorema 11. *Si D es un $(2^b, k, 2)$-biplano no trivial, entonces $b = 4$.*

Teorema 12. *Sea G un grupo de automorfismos afín de un biplano D. Supongamos que $G = TH$, donde T es el grupo de traslaciones de $V(d, p)$ (el cual actúa regularmente en los puntos de D), $H \leq GL(d, p)$,* y *p es impar. Entonces $|G|$ es impar.*

4.1. Biplanos con grupo de automorfismos primitivo en puntos, transitivo en banderas y de tipo afín de dimensión uno.

Consideremos a $D = (V, B)$ un $(v, k, 2)$-biplano. Supongamos que D tiene un grupo de automorfismos G primitivo en puntos, transitivo en banderas, de tipo afín y tal que $(v, k, 2) \neq (16, 6, 2)$. Por los Teoremas 10, 11 y 12 tenemos que $G \leq A\Gamma L_1(q)$ con $v = q = p^r$, $p > 2$ y $\circ(G)$ es impar.
Algunos de los siguientes resultados se encuentran en un artículo sin publicar de C.E. Praeger y E. O'Reilly-Regueiro.

Lema 18. *Sean p un primo impar, $r \in \mathbb{Z}^+$, y $D = (V, B)$ un $(p^r, k, 2)$-biplano. Entonces p no divide a k.*

Demostración. El Lema 1 nos dice que $2(p^r - 1) = k(k - 1)$. Dado que p es impar, p no divide a $2(p^r - 1)$ y por lo tanto tampoco a k. □

Proposición 1. *Sea p un primo impar, $r \in \mathbb{Z}$ y $D = (V, B)$ un $(p^r, k, 2)$-biplano con un grupo de automorfismos G transitivo en banderas y de tipo afín de dimensión uno. Supongamos que p divide a $|G_0|$ y que P es un p-subgrupo de Sylow de G_0. Sean $V' = fix_V(P)$, $B' = fix_B(P)$ y $N = N_G(P)$. Sea $c_0 \in B$. Definamos $v' = |V'|$, $k' = |c_0 \cap V'|$ y $B'' = \{c \cap V' : c \in B'\}$. Bajo las condiciones descritas, se cumplen las siguientes afirmaciones:*

(1) *$r = su$ donde $u = |P| > 1$.*

(2) *$v' = p^s$ y $2(p^s - 1) = k'(k' - 1)$ con $k' > 2$.*

(3) *$D' = (V', B'')$ es un $(v', k', 2)$-biplano con grupo de automorfismos G' (inducido por N) transitivo en banderas tal que $G' = T'G'_0 \leq A\Gamma L_1(p^s)$ donde T' es el grupo de traslaciones y $G'_0 \leq \Gamma L(1, p^s)$, con $(|G'_0|, p) = 1$.*

Demostración. Como G_0 actúa en $V \setminus \{0\}$, el Lema 27 nos dice que existe $x \in V \setminus \{0\}$ tal que $P \leq G_{0,x}$.
El Corolario 3 nos dice que $A\Gamma L_1(q)$ es 2-transitivo en V, por lo que podemos elegir un biplano D isomorfo, de tal forma que $P \leq G_{0,1} \leq \langle a \rangle$, donde a es el automorfismo de Frobenius. Entonces $P = \langle a^s \rangle$ para algún divisor s de r. De lo anterior se sigue (1).
Por el Lema 47 tenemos que $fix_V(P) = fix_V(a^s) = \mathbb{F}_{p^s}$, de aquí que $v' = p^s$. Sea $B_0 = \{c \in B' : 0 \in c\}$, entonces para cada par c_1, $c_2 \in B_0$ se tiene que $c_1 \cap c_2 = \{0, y\}$ para algún $y \in V$. Además P deja fijo a y, por lo que $y \in V'$.

Por otro lado, para cada $y \in V'$, $y \neq 0$ tenemos que existen bloques c_1, c_2 tales que $\{0, y\} \subseteq c_1$, c_2. Estos quedan fijos bajo P pues de lo contrario $|P|$ sería par.
Por lo descrito anteriormente existe una biyección entre $V' \setminus \{0\}$ y las parejas no ordenadas $\{c_1, c_2\} \subseteq B_0$. Si $|B_0| = m$, entonces $p^s - 1 = \frac{m(m-1)}{2}$, de donde se sigue que $m > 2$.
Por el Lema 28, $N \subseteq G_{V'}$ y $N \subseteq G_{B'}$. Por el Lema 30, N es transitivo en V' y en B'. Esto último implica que $|c \cap V'| = k'$ para todo $c \in B'$ y por lo tanto $D' = (V', B'')$ es un $(v', k', 2)$-biplano. Utilizando el Lema 1, obtenemos (2) y $m = k'$.
Sea $H = G_0$ el cual actúa en B_0. Como p no divide a $k' > 2$, por el Lema 27 podemos elegir un bloque $b \in B_0$ tal que $P \leq H_b$. La transitividad en banderas de G implica que H es transitivo en B_0. De nuevo, por el Lema 30 $N' = N_{G_0}(P)$ es transitivo en B_0.
Sean $b \in B_0$ y (x', c') una bandera de D'. Entonces $c' = c \cap V'$ para algún $c \in B'$. Como N es transitivo en V' existe $\sigma \in N$ tal que $x'^{\sigma} = 0$. Sea $c'^{\sigma} = c''$, como N' es transitivo en B_0 existe $\tau \in N'$ tal que $c''^{\tau} = b$. Entonces $(x', c')^{\sigma\tau} = (0, b)$. Lo anterior implica que N es transitivo en las banderas de D'.
Finalmente, por el Corolario 4, N induce un subgrupo $G' \leq A\Gamma L_1(p^s)$. Escribimos a G'_0 en su forma estándar $G'_0 = \langle \hat{\omega}^{d'}, \hat{\omega}^{e'} a^{s'} \rangle$, tenemos que $|G'_0| = \frac{s(p^s-1)}{s'd'}$, como P es un p-subgrupo de Sylow de G_0 tenemos que $(s, p) = 1$, por lo que $(|G'_0|, p) = 1$. □

La proposición anterior nos permite, en la búsqueda de nuevos biplanos, suponer que si p es un primo impar y D es un $(p^r, k, 2)$-biplano con un grupo de automorfismos G transitivo en banderas y de tipo afín de dimensión uno, entonces $(|G_0|, p) = 1$.
El siguiente lema es consecuencia de [17, 106pp, Teorema 5.8 (ii)].

Lema 19. *Sean G un grupo finito y p un primo tal que $p| \circ (G)$. Si P es un p-subgrupo de Sylow normal en G, entonces todos los complementos de P son conjugados.*

Lema 20. *Sean p un primo impar, q una potencia de p y $D = (V, B)$ un $(q, k, 2)$-biplano con un grupo de automorfismos G transitivo en banderas y de tipo afín de dimensión uno tal que $(|G_0|, p) = 1$. Entonces existe un bloque c_0 no incidente con 0, tal que $G_0 = G_{c_0}$.*

Demostración. Podemos identificar a V con $\mathbb{F}_q$. Sea $c \in B$ y $t_{1,\beta,1} \in T$ tal que $t_{1,\beta,1}(c) = c$, entonces $\sum_{u\in c}(u+\beta) = \sum_{u\in c} u$, lo que implica que $k\beta = 0$. Por el Lema 18, p no divide a k y entonces $\beta = 0$. Concluimos que $T \cap G_c = \{Id\}$. Como T es transitivo en V y en B, el Lema 31 dice que $G = T \cdot G_c = T \cdot G_0$, lo que implica que $|G_0| = |G_c|$. Entonces G_c es un complemento de T.
Dado que $(|G_0|, p) = 1$, T es un p-subgrupo de Sylow normal en G. El Lema 19 nos dice que todos los complementos de T son conjugados; en particular existe $t \in T$ tal que $G_0 = t^{-1}G_c t$. Sea $c_0 = c^t$, el Lema 29 nos da que $G_0 = G_{c_0}$. Finalmente, como G es transitivo en banderas, G_0 es transitivo en c_0, lo que implica que $0 \notin c_0$.

□

Lema 21. *Sean p un primo impar, $r \in \mathbb{Z}^+$,* y *$D = (V, B)$ un $(p^r, k, 2)$-biplano con grupo de automorfismos G transitivo en banderas* y *de tipo afín de dimensión uno tal que $(|G_0|, p) = 1$. Entonces $|G_0| = kt$ para algún t que divide a r.*

Demostración. Sea $H = G_0 \cap GL(1, q)$. El Lema 13 implica que H es normal en G_0, G_0/H es cíclico y su orden divide a r. Por el Lema 20, $G_0 = G_{c_0}$ para algún $c_0 \in B$, y podemos tomar $y \in c_0$ tal que $y \neq 0$.
Sea $\pi : G_0 \longrightarrow G_0/H$ el epimorfismo canónico, entonces $\pi(G_{0,y}) \leq G_0/H$, como $G_{0,y} \cap H = \{Id\}$, tenemos que $t := |G_{0,y}|$ divide a $|G_0/H|$ y por lo tanto a r. La transitividad en banderas de G implica que G_0 es transitivo en c_0, y entonces $[G_0 : G_{0,y}] = k$. Concluimos que $|G_0| = kt$. □

Lema 22. *Sean p un primo impar, $r \in \mathbb{Z}^+$,* y *D un $(p^r, k, 2)$-biplano con un grupo de automorfismos G transitivo en banderas* y *de tipo afín de dimensión uno tal que $(|G_0|, p) = 1$. Entonces k es impar.*

Demostración. Es consecuencia del lema anterior y del Teorema 12. □

4.2 Gráficas de Hussain

En esta sección definimos a las gráficas de Hussain, llamadas así por el nombre de su descubridor y las cuales están en correspondencia biyectiva con los biplanos. Estas nos ayudan a visualizar a los biplanos y entender más sobre su estructura.

Definición 21. Una **gráfica** Γ es un par ordenado (V, E) que consta de un conjunto de vértices V y un conjunto E, de 2-subconjuntos de V, llamados aristas. A los conjuntos de vértices y aristas de una gráfica Γ los denotamos por $V(\Gamma)$ y $E(\Gamma)$ respectivamente.

Definición 22. Sea $\Gamma = (V, E)$ una gráfica. Decimos que Γ es 2-**regular** si para todo $v \in V$, existen exactamente 2 aristas $e_1, e_2 \in E$ tales que $v \in e_1$ y $v \in e_2$.

Definición 23. Sean $\Gamma_1 = (V_1, E_2)$ y $\Gamma_2 = (V_2, E_2)$ dos gráficas tales que $|V_1| = |V_2|$. Una biyección $\alpha : V_1 \longrightarrow V_2$ es un **isomorfismo de gráficas** cuando $e \in E_1$ si y sólo si $e^\alpha \in E_2$. Si existe un isomorfismo α entre Γ_1 y Γ_2, decimos que son **isomorfas** y lo denotamos por $\Gamma_1 \overset{\alpha}{\cong} \Gamma_2$.

Definición 24. Sean $D = (P, B)$ un $(v, k, 2)$-biplano y $c_0 \in B$. Para cada $p \in P \setminus c_0$ definimos la **gráfica de Hussain** de p como $\Gamma_p = (V, E)$ donde $V = c_0$ y $\{x, y\} \in E$ si y sólo si el único bloque $c \neq c_0$ que contiene a $\{x, y\}$ cumple que $p \in c$.

Lema 23. *Sean $D = (P, B)$ un biplano, $c_0 \in B$ y $p \in P \setminus c_0$. Entonces la gráfica de Hussain de p es 2-regular.*

Demostración. Para cada $x \in c_0$ existen exactamente dos bloques c, c' que contienen a $\{p, x\}$, por el Teorema 2, $c_0 \cap c = \{x, y\}$ y $c_0 \cap c' = \{x, y'\}$, para algunos $y, y' \in P$. Se sigue que Γ_p es 2-regular. □

Definición 25. Sean $k \geq 3$ un entero positivo, $M = \frac{(k-1)(k-2)}{2}$ y $\{\Gamma_i\}_{i=1}^M$ un conjunto de M gráficas tales que para cada $i \in \{1, 2, ..., M\}$ se tiene que $V(\Gamma_i) = V$, donde V es un conjunto con k vértices, y se satisface que:

(*i*) Γ_i es 2-regular para toda $i \in \{1, 2, ..., M\}$,

(*ii*) Para cualesquiera $i, j \in \{1, 2..., M\}$ se cumple que Γ_i y Γ_j comparten exactamente 2 aristas y estas aristas no comparten vértices,

entonces $\{\Gamma_i\}_{i=1}^M$ es un **conjunto completo de gráficas de Hussain** en k vértices. En la Figura 2 se muestra un ejemplo.

A continuación se demuestra que hay una correspondencia biyectiva entre los biplanos y los conjuntos completos de gráficas de Hussain.

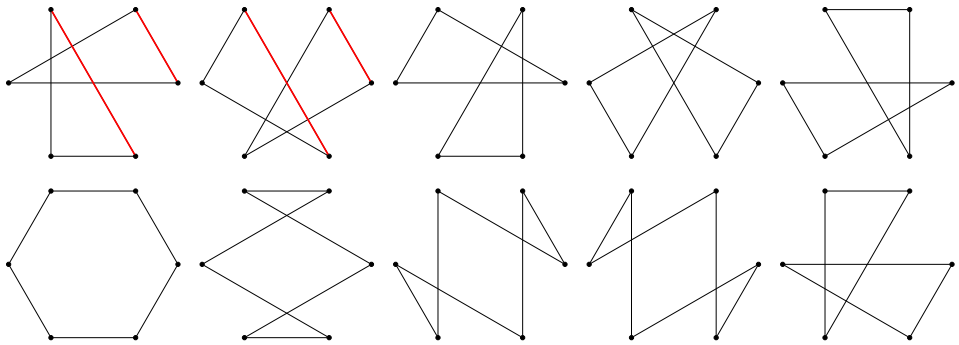

Figura 2: Conjunto completo de gráficas de Hussain en 6 vértices. En rojo se encuentran las aristas que comparten las primeras dos gráficas.

Teorema 13. *Sean $D = (P, B)$ un $(v, k, 2)$-biplano y $c_0 \in B$, entonces $\{\Gamma_p\}_{p \in P \setminus c_0}$ es un conjunto completo de gráficas de Hussain.*

Demostración. Para cada $p \in P \setminus c_0$ podemos construir la gráfica de Hussain Γ_p y por lo tanto tenemos $|P \setminus c_0| = \frac{(k-2)(k-1)}{2}$ de ellas, por el Lema 23 cada una es 2-regular. Consideremos dos puntos p y p' en $P \setminus c_0$, entonces existen exactamente dos bloques c y c' que contienen a $\{p, p'\}$. Sean $c_0 \cap c = \{x_1, y_1\}$ y $c_0 \cap c' = \{x_2, y_2\}$. Entonces Γ_p y $\Gamma_{p'}$ comparten las aristas $\{x_1, y_1\}$ y $\{x_2, y_2\}$. Todo elemento de $\{x_1, y_1\} \cap \{x_2, y_2\}$ es elemento de $c \cap c'$, es distinto a p y distinto a p'. Como $|c \cap c'| = 2$, tenemos que $\{x_1, y_1\} \cap \{x_2, y_2\} = \emptyset$. De compartir otra arista, existiría otro bloque que contiene a $\{p, p'\}$. □

Teorema 14. *Sean v y k enteros tales que $v - k = \frac{(k-1)(k-2)}{2}$ y $\{\Gamma_i\}_{i=1}^{v-k}$ es un conjunto completo de gráficas de Hussain en un conjunto V con k vértices. Sea $P = V \cup \{u_1, u_2, ..., u_{v-k}\}$ y para cada $\{x, y\} \subseteq V$ definimos*

$$c_{\{x,y\}} = \{x, y\} \cup \{u_i : \{x, y\} \in A(\Gamma_i)\}.$$

Si $B = \{V\} \cup \{c_{\{x,y\}} : \{x, y\} \subseteq V\}$, entonces $D = (P, B)$ es un $(v, k, 2)$-biplano.

Demostración. Notemos que $|P| = |B| = v$. Consideremos $x, y \in V$, para cada $i \in \{1, ..., v - k\}$ sabemos que Γ_i es 2-regular, entonces podemos encontrar $\{y_i, z_i\} \subseteq V \setminus \{x\}$ tal que $\{x, y_i\}, \{x, z_i\} \in A(\Gamma_i)$. Si $i \neq j$, Γ_i y Γ_j comparten 2 aristas no adyacentes, lo que implica que $\{y_i, z_i\} \neq \{y_j, z_j\}$. El

total de parejas posibles en $V \setminus \{x\}$ es $\frac{(k-1)(k-2)}{2} = v - k$, entonces hay una pareja por cada gráfica de Hussain. El número de parejas en donde aparece y es $k-2$ y por lo tanto $\{x, y\}$ es arista de $k-2$ gráficas de Hussain. Lo anterior implica que $|c_{\{x,y\}}| = k$ para cada par $x, y \in V$.
Sean $p_1, p_2 \in P$. Si $p_1, p_2 \in V$, entonces $\{p_1, p_2\}$ está contenido únicamente en V y en $c_{\{p_1,p_2\}}$. Si $p_1 \in V$ y $p_2 = u_i$ para alguna $i \in \{1, ..., v-k\}$, entonces Γ_i es 2-regular y hay exactamente dos aristas incidentes con p_1, digamos $\{p_1, x\}$ y $\{p_1, y\}$. Entonces $\{p_1, p_2\}$ está contenido en $c_{\{p_1,x\}}$ y en $c_{\{p_1,y\}}$. De estar contenido en otro elemento de B, Γ_i no sería 2-regular. Similarmente ocurre si $p_1 = u_i$ para alguna $i \in \{1, ..., v-k\}$ y $p_2 \in V$. Finalmente, si $p_1 = u_i$ y $p_2 = u_j$ para algunas $i, j \in \{1, ..., v-k\}$, entonces Γ_i y Γ_j comparten dos aristas no adyacentes $\{x_1, y_1\}$ y $\{x_2, y_2\}$. Esto implica que $\{p_1, p_2\}$ está contenido en $c_{\{x_1,y_1\}}$ y en $c_{\{x_2,y_2\}}$. De estar contenido en otro elemento de B, Γ_i y Γ_j compartirían más de dos aristas. Concluimos que $D = (P, B)$ es un (v, k, λ)-biplano. □

Teorema 15. *Sean $D_1 = (P_1, B_1)$ y $D_2 = (P_2, B_2)$ dos $(v, k, 2)$-biplanos. Entonces $D_1 \cong D_2$ si y sólo si existen $c_0 \in B_1$, $c_0' \in B_2$, una biyección $\alpha : c_0 \to c_0'$ y familias de gráficas de Hussain $\{\Gamma_p\}_{p \in P_1 \setminus c_0}$, $\{\Gamma_{p'}\}_{p' \in P_2 \setminus c_0'}$ donde para cada $p \in P_1 \setminus c_0$ existe un único $p' \in P_2 \setminus c_0'$ tal que $\Gamma_p \overset{\alpha}{\cong} \Gamma_p'$.*

Demostración. Sea φ un isomorfismo entre D_1 y D_2. Sean c_0 un bloque en B_1, $c_0' = c_0^{\varphi}$ y $\alpha = \varphi|_{c_0} : c_0 \longrightarrow c_0'$. Sean $p \in P_1 \setminus c_0$ y $p' = p^{\varphi}$. Si $\{x, y\}$ es una arista de Γ_p, entonces existe un único bloque c de D_1 distinto a c_0 que contiene a $\{x, y\}$ y tal que $p \in c$. Notemos que c^{φ} es el único bloque de D_2 distinto a $c_0^{\varphi} = c_0'$ que contiene a $\{x^{\varphi}, y^{\varphi}\}$ y es tal que $p' \in c^{\varphi}$, por lo que $\{x^{\varphi}, y^{\varphi}\}$ es una arista de $\Gamma_{p'}$. Recíprocamente, si $\{x^{\varphi}, y^{\varphi}\}$ es una arista de $\Gamma_{p'}$, entonces existe un único bloque c' de D_2 diferente a c_0' que contiene a $\{x^{\varphi}, y^{\varphi}\}$ y tal que $p' \in c'$. Notemos que $c'^{\varphi^{-1}}$ es el único bloque de D_1 que contiene a $\{x, y\}$ y es tal que $p \in c'^{\varphi^{-1}}$, entonces $\{x, y\}$ es una arista de Γ_p. Concluimos que $\Gamma_p \overset{\alpha}{\cong} \Gamma_{p'}$.
Sea $\varphi : P_1 \longrightarrow P_2$, definida para todo $x \in P_1$ de la siguiente forma: Si $x \in P_1 \setminus c_0$, entonces existe $x' \in P_2 \setminus c_0'$ tal que $\Gamma_x \overset{\alpha}{\cong} \Gamma_{x'}$, en este caso definimos $x^{\varphi} = x'$. Si $x \in c_0$, entonces definimos $x^{\varphi} = x^{\alpha}$. Veamos que φ es un isomorfismo entre D_1 y D_2. Sea $c \in B_1$ distinto de c_0, entonces $c \cap c_0 = \{x, y\}$ para algunos $x, y \in P_1$. Como c tiene k puntos, $\{x, y\}$ es una arista en exactamente $k-2$ gráficas, digamos $\Gamma_{p_1}, \Gamma_{p_2}, ..., \Gamma_{p_{k-2}}$. Por hipótesis,

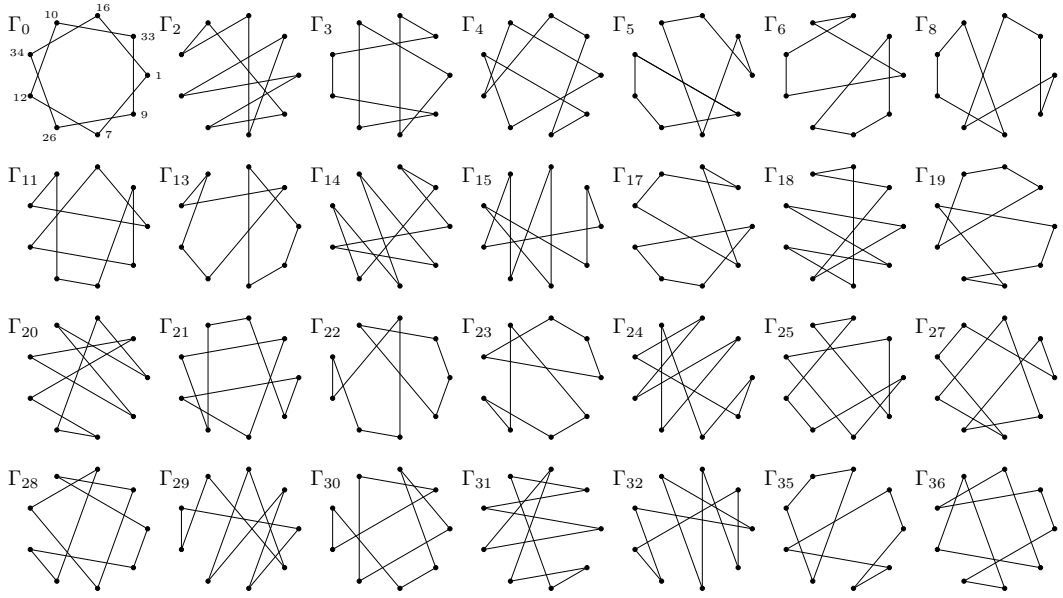

Figura 3: Un conjunto completo de gráficas de Hussain en 9 vértices construido a partir del $(37, 9, 2)$-biplano $D = (\mathbb{F}_{37}, Dev(C))$ en donde $C = (\mathbb{F}_{37}^*)^4$.

para cada Γ_{p_i} existe $p_i' \in P_2 \setminus c_0'$ tal que $\Gamma_{p_i} \overset{\alpha}{\cong} \Gamma_{p_i'}$. Notemos que $\{x^\alpha, y^\alpha\}$ es arista de $\Gamma_{p_i'}$ para cada p_i'. Sea $c' = \{x^\alpha, y^\alpha\} \cup \{p_i' : 1 \leq i \leq k-2\}$, entonces $c' \in B_2$ y $c^\varphi = c'$. Concluimos que φ es un isomorfismo entre D_1 y D_2. $\square$

Ejemplo 10. Consideremos a D el $(37, 9, 2)$-biplano mencionado al principio del capítulo y el cual está construido a partir del $(37, 9, 2)$-conjunto de diferencia $C = (\mathbb{F}_{37}^*)^4$ en $\mathbb{F}_{37}$. La Figura 3 ilustra el conjunto completo de gráficas de Hussain que se corresponde con D.

4.3 Resultados de la investigación

Comenzamos esta sección con la siguiente reducción de nuestra búsqueda de biplanos con un grupo de automorfismos primitivo en puntos, transitivo en

banderas y de tipo afín de dimensión uno a conjuntos de diferencia en los grupos aditivos de campos finitos.

Teorema 16. *Sean p un primo impar* y $r \in \mathbb{Z}^+$. *Existe un $(p^r, k, 2)$-biplano con un grupo de automorfismos G primitivo en puntos, transitivo en banderas, de tipo afín de dimensión uno* y *tal que $(|G_0|, p) = 1$ si* y *sólo si existen enteros positivos d, s, e* y $\alpha \in \mathbb{F}_{p^r}$ *tales que $d|(p^r - 1)$, $s|r$, $0 \leq e < d$, $\frac{e(p^r-1)}{p^s-1} \equiv 0 \ (mod\ d)$* y $C = \{\alpha^\sigma : \sigma \in \langle \hat{\omega}^d, \hat{\omega}^e a^s \rangle\}$ *es un $(p^r, k, 2)$-conjunto de diferencia en $\mathbb{F}_{p^r}$. Donde ω es una raíz primitiva de $\mathbb{F}_{p^r}$, $\hat{\omega}$ denota la multiplicación por ω y a es el automorfismo de Frobenius.*

Demostración. De existir un $(p^r, k, 2)$-biplano $D = (V, B)$ con un grupo de automorfismos G transitivo en banderas, de tipo afín de dimensión uno y tal que $(|G_0|, p) = 1$, podemos identificar V con $\mathbb{F}_{p^r}$ y por el Lema 20, $G_0 = G_C$ para algún bloque C. El Lema 12 implica que $G_C = \langle \hat{\omega}^d, \hat{\omega}^e a^s \rangle$ donde d, s y e son tales que $d|(p^r - 1)$, $s|r$, $0 \leq e < d$ y $\frac{e(p^r-1)}{p^s-1} \equiv 0 \ (mod\ d)$. Como G es transitivo en banderas, $G_0 = G_C$ es transitivo en C, por lo que si $\alpha \in C$ tenemos que $C = \{\alpha^\sigma : \sigma \in G_C\}$. Dado que G contiene a todo el grupo de traslaciones, $C + \beta \in B$ para todo $\beta \in \mathbb{F}_{p^r}$. Por el Lema 18, p no divide a k. Supongamos que $C + \beta = C + \beta'$ para algunos $\beta, \beta' \in \mathbb{F}_{p^r}$ y sea y la suma de los elementos de C, entonces $y + k\beta = y + k\beta'$, por lo que $\beta = \beta'$. Se sigue que $B = Dev(C)$, por el Teorema 7, C es un $(p^r, k, 2)$-conjunto de diferencia en $\mathbb{F}_{p^r}$.
Recíprocamente, dado que $C = \{\alpha^\sigma : \sigma \in \langle \hat{\omega}^d, \hat{\omega}^e a^s \rangle\}$ es un $(p^r, k, 2)$-conjunto de diferencia en $\mathbb{F}_{p^r}$, el Teorema 6 nos dice que $D = (\mathbb{F}_{p^r}, Dev(C))$ es un $(p^r, k, 2)$-biplano. Sean $x \in C$ y (x', C') una bandera de D, entonces podemos escribir $C' = C + \beta$ y $x' = y + \beta$ para algunos $y \in C$ y $\beta \in \mathbb{F}_{p^r}$. No es difícil observar que $\langle \hat{\omega}^d, \hat{\omega}^e a^s \rangle \subseteq Aut(D)$ y que existe $\sigma \in \langle \hat{\omega}^d, \hat{\omega}^e a^s \rangle$ tal que $x^\sigma = y$. Sea t_β la traslación por β, entonces $C^{\sigma \cdot t_\beta} = C'$ y $x^{\sigma \cdot t_\beta} = x'$. Por lo tanto D tiene un grupo de automorfismos G transitivo en banderas y de tipo afín de dimensión uno el cual, por la Proposición 1, podemos asumir que cumple $(|G_0|, p) = 1$. □

El siguiente teorema es un caso particular del teorema anterior; cuando el grupo de automorfismos es subgrupo del grupo de transformaciones afines.

Teorema 17. *Sean p un primo impar* y $r \in \mathbb{Z}^+$. *Entonces existe un $(p^r, k, 2)$-biplano con un grupo de automorfismos G, primitivo en puntos, transitivo en banderas, tal que $G \leq AGL_1(p^r)$* y $(|G_0|, p) = 1$ *si* y *sólo si existe d tal que*

$d|(p^r-1)$ y *el conjunto de las potencias d-ésimas del grupo multiplicativo de* $\mathbb{F}_{p^r}$ *es un* $(p^r,k,2)$*-conjunto de diferencia en* $\mathbb{F}_{p^r}$.

Demostración. Basta observar que por el Teorema 16 tenemos que:

$$C=\{\alpha^\sigma : \sigma \in \langle \hat{\omega}^d, \hat{\omega}^e a^s\rangle\}$$

es un $(p^r,k,2)$-conjunto de diferencia en $\mathbb{F}_{p^r}$, para algún $\alpha \in \mathbb{F}_{p^r}$. Como $G \leq AGL_1(p^r)$, entonces $e=0$, $s=r$ y podemos elegir D, multiplicando por α^{-1}, de tal forma que $C=(\mathbb{F}_{p^r}^*)^d$.
Ahora, si existe $d|(p^r-1)$ y el conjunto C de las potencias d-ésimas del grupo multiplicativo de $\mathbb{F}_{p^r}$ es un $(p^r,k,2)$-conjunto de diferencia en $\mathbb{F}_{p^r}$, podemos aplicar el Teorema 16 con $s=r$, $e=0$ y $\alpha=1$ para concluir que $D=(\mathbb{F}_{p^r}, Dev(C))$ es un $(p^r,k,2)$-biplano con un grupo de automorfismos transitivo en banderas y de tipo afín. □

Haciendo un análisis combinatorio de los conjuntos de diferencia en $\mathbb{F}_{p^r}$ obtenemos el siguiente teorema.

Teorema 18. *Sean p un primo,* $r \in \mathbb{Z}^+$, y C *un* $(p^r,k,2)$*-conjunto de diferencia en* $\mathbb{F}_{p^r}$. *Entonces para cada subespacio U de dimensión n en* $\mathbb{F}_{p^r}$, *considerado como un* $\mathbb{F}_p$*-espacio vectorial, se cumple que* $|C\cap U| \leq 2\left(\frac{p^n-1}{p-1}\right)\sqrt{p}$.

Demostración. Sean U_1,..., $U_{\frac{p^n-1}{p-1}}$, los subespacios de dimensión uno de U. Para cada $i \in \{1,...,\frac{p^n-1}{p-1}\}$ consideramos $\{v_i\}$ una base de U_i. Definimos la biyección $\Gamma_i : U_i \longrightarrow \{0,1,...,p-1\}$ dada por $\Gamma_i : nv_i \mapsto n$. Podemos definir un orden lineal en $C\cap U_i$ dado por $u<v$ si y sólo si $\Gamma_i(u)<\Gamma_i(v)$ para todo $u,v \in C\cap U_i$. Si definimos $|C\cap U_i|=t_i$, podemos etiquetar $C\cap U_i=\{u_{i,j}\}_{1\leq j\leq t_i}$ de tal forma que $u_{i,j}<u_{i,j+1}$ para cada $j\in\{1,...t_i-1\}$. Definimos las distancias $d_{i,j}=\Gamma_i(u_{j+1})-\Gamma_i(u_j)$ para cada $j\in\{1,...t_i-1\}$ y $d_{i,t_i}=p-\Gamma_i(u_{t_i})+\Gamma_i(u_1)$. Si hay j_1,j_2 y j_3 tales que $d_{i,j_1}=d_{i,j_2}=d_{i,j_3}$, entonces $v=\Gamma_i^{-1}(d_{i,j_\ell})=u_{i,j_{\ell+1}}-u_{i,j_\ell}$ con $\ell\in\{1,2,3\}$ y $j_{\ell+1}$ se considera $(mod\ t_i)$. Esto contradice que C sea un $(p^r,k,2)$-conjunto de diferencia en $\mathbb{F}_{p^r}$. Por lo tanto los valores de las distancias se repiten a lo más dos veces y los mínimos valores que pueden tomar son los primeros $\lceil\frac{t_i}{2}\rceil := m$ enteros positivos. Si t_i es par tenemos que $p=\sum_{i=1}^{t_i} d_i \geq m(m+1)=\frac{t_i}{2}(\frac{t_i}{2}+1)$ y si t_i es impar entonces $p=\sum_{i=1}^{t_i} d_i \geq m(m-1)+m=(\frac{t_i+1}{2})^2$. En ambos casos, $t_i<2\sqrt{p}$. Como U es la unión de sus subespacios de dimensión uno, concluimos que $|C\cap U|\leq 2(\frac{p^n-1}{p-1})\sqrt{p}$. □

Lema 24. *Sean p un primo impar, $r \in \{1,2\}$ y $D = (V,B)$ un $(p^r,k,2)$-biplano con un grupo de automorfismos G transitivo en banderas y de tipo afín de dimensión uno, entonces $G \leq AGL_1(p^r)$.*

Demostración. El resultado se sigue trivialmente cuando $r = 1$.
Supongamos que $r = 2$. Por el Teorema 12, $\circ(G)$ es impar. Entonces:

$$[G : (G \cap AGL_1(p^2))] = [G \cdot AGL_1(p^2) : AGL_1(p^2)] < 2$$

por lo que $G \cdot AGL_1(p^2) = AGL_1(p^2)$ y entonces $G \leq AGL_1(p^2)$. □

Si p es un primo impar, el lema anterior nos permite utilizar el Teorema 17 cuando estamos trabajando con biplanos con p ó p^2 puntos y con grupos de automorfismos primitivos en puntos, transitivos en banderas y de tipo afín de dimensión uno.

Teorema 19. *Sean p un primo impar menor a 10^7 y D un $(p,k,2)$-biplano no trivial con grupo de automorfismos $G = Aut(D)$ transitivo en banderas y de tipo afín de dimensión uno. Entonces D es un $(37,9,2)$-biplano.*

Demostración. El Lema 21 implica que G actúa regularmente en las banderas de D. Por el Teorema 8, $k = \frac{(p-1)}{n}$, $2 = \frac{k-1}{n}$ y (p,n) es un par especial. Dado que p es menor que 10^7, el Teorema 9 implica que n debe ser 1, 2, 4, 8 o $p-1$. Sólo cuando $n = 4$, G es de tipo afín, en este caso D tiene parámetros $(37,9,2)$. □

Como $A\Gamma L_1(p) = AGL_1(p)$ para todo primo p y todo grupo que actúa transitivamente en un conjunto con p puntos es primitivo, el siguiente resultado es una consecuencia directa del Teorema 17.

Lema 25. *Sea p un primo impar, entonces existe un $(p,k,2)$-biplano con un grupo de automorfismos transitivo en banderas y de tipo afín de dimensión uno si y sólo si existe un divisor n de $p-1$ tal que $p-1 = nk$, $2 = \frac{k-1}{n}$ y (p,n) es un par especial.*

5. Conclusiones

Conforme ha avanzado la investigación en la búsqueda y clasificación de nuevos biplanos, las posibilidades de encontrarlos parecen reducirse. Por supuesto que los caminos que no exploramos son muchos por lo que, junto con las herramientas utilizadas, se revela un amplio y complicado campo de estudio para continuar con la investigación. Entre las conclusiones más importantes están las siguientes:

(1) Algunas aplicaciones.

El siguiente resultado se obtuvo aplicando el Teorema 17 y el Teorema 18, también se utilizaron algoritmos que se implementaron en Python y los cuales están descritos en el Apéndice C.

Teorema 20. *Si p es un primo impar menor a 4×10^5, entonces no existen $(p^2, k, 2)$-biplanos con un grupo de automorfismos primitivo en puntos, transitivo en banderas* y *de tipo afín de dimensión uno.*

Demostración. Supongamos que existe un $(p^2, k, 2)$-biplano con un grupo de automorfismos primitivo en puntos, transitivo en banderas y de tipo afín de dimensión uno. Se puede verificar computacionalmente, utilizando el Programa 2, que cuando $p < 4 \times 10^5$, los valores de p para los que se satisface el Lema 1 son $p = 11$, $p = 23$, $p = 373$ y $p = 12671$. Si p es 11, 373, o 12671 tenemos que k es 16, 528 o 17920 respectivamente, lo que contradice el Corolario 22. Entonces $p = 23$ y $k = 33$. El Lema 24 implica que $G \leq AGL_1(23^2)$, por lo que podemos aplicar el Teorema 17 para obtener que $C = (\mathbb{F}_{23^2}^*)^{16}$ es un $(23^2, 33, 2)$-conjunto de diferencia en $\mathbb{F}_{23^2}$. Notamos que C contiene al subgrupo de orden 11 de $\mathbb{F}_{23}^*$. Pero entonces $|C \cap \mathbb{F}_{23}| \geq 11$, contradiciendo el Teorema 18. $\square$

En [1] se construyen los únicos dos $(79, 13, 2)$-biplanos conocidos, uno dual del otro. También se demuestra que si un $(79, 13, 2)$-biplano tiene un grupo de automorfismos no trivial G y p es un primo que divide a $\circ(G)$, entonces $p \in \{2, 3, 5, 11, 13\}$. Se han hecho muchos avances para descartar la existencia de más $(79, 13, 2)$-biplanos con un grupo de automorfismos no trivial, por ejemplo ver [12].

Podemos aplicar el Lema 25 para determinar si existen biplanos con parámetros $(79, 13, 2)$ y con un grupo de automorfismos transitivo en

banderas. De existir tendríamos que $(79, 6)$ es un par especial, por lo que $C = (\mathbb{F}_{79}^*)^6$ es un $(79, 13, 2)$-conjunto de diferencia en $\mathbb{F}_{79}$. El Teorema 6 nos dice que $D = (\mathbb{F}_{79}, Dev(C))$ es un $(79, 13, 2)$-biplano, sin embargo al computar C obtenemos que:

$$C = \{64, 1, 67, 38, 65, 8, 10, 46, 18, 52, 21, 22, 62\},$$

por lo que $|C \cap C + 2| = 3$, lo que contradice el Teorema 2.

(2) Más sobre el caso de tipo afín de dimensión uno.

El Teorema 16 implica que la búsqueda de biplanos con grupos de automorfismos primitivos en puntos, transitivos en banderas y de tipo afín de dimensión uno se reduce a la búsqueda de conjuntos de diferencia en campos finitos. Los Teoremas 19 y 20 nos confirman que el único biplano que se conoce con estas características, salvo isomorfismo, es el $(37, 9, 2)$-biplano $D = (\mathbb{F}_{37}, Dev(C))$ donde $C = (\mathbb{F}_{37}^*)^4$.

En [2], M. Biliotti y A. Montinaro estudian el caso en el que un (v, k, λ)-diseño simétrico tiene un grupo de automorfismos transitivo en banderas de tipo afín de dimensión uno y cuando $(k, \lambda) = 1$. Notemos que los $(v, k, 2)$-biplanos con grupo de automorfismos transitivo en banderas y de tipo afín cumplen que k es impar, por lo que $(k, 2) = 1$. También en [2] se da la siguiente definición.

Definición 26. Sean p un primo, $r \in \mathbb{Z}^+$ y ω una raíz primitiva de $\mathbb{F}_{p^r}$. Para cada divisor d de $p^r - 1$ definimos la **clase ciclotómica** respecto a d de orden i como $C_i = \langle \omega^d \rangle \omega^i$, donde $0 \leq i < d$.

El siguiente lema, consecuencia de [2, Teorema 2], se sigue directamente del Teorema 16 y nos permite ver a un bloque de un biplano con un grupo de automorfismos primitivo en puntos, transitivo en banderas y de tipo afín de dimensión uno como la unión de clases ciclotómicas.

Lema 26. *Sean p un primo, $r \in \mathbb{Z}^+$, y $D = (\mathbb{F}_{p^r}, B)$ un $(p^r, k, 2)$-biplano con un grupo de automorfismos G primitivo en puntos, transitivo en banderas y de tipo afín de dimensión uno tal que $(|G_0|, p) = 1$. Entonces existe un divisor d de $p^r - 1$ y un bloque C que es la unión de clases ciclotómicas respecto a d.*

(3) Construcción de estructuras de incidencia a partir de biplanos.

Es natural preguntarse si utilizando a los biplanos como "ladrillos de construcción", es posible construir estructuras de incidencia más generales. La siguiente definición da respuesta afirmativa a esta pregunta:

Definición 27. Sean $D_1 = (V_1, B_1)$ un (v, k, λ_1)-BIBD y $D_2 = (V_2, B_2)$ un (v, k, λ_2)-BIBD. Construimos la **suma** $D = (D_1 \oplus D_2)$ tomando un conjunto V tal que $|V| = v$. Sean $\alpha : V_1 \to V$ y $\beta : V_2 \to V$ biyecciones. Consideramos $B_1' = B_1^{\alpha}$ y $B_2' = B_2^{\beta}$. Entonces $D = (V, B_1' \sqcup B_2')$ es un $(v, k, \lambda_1 + \lambda_2)$-BIBD.

Como ejemplo de esta construcción podemos considerar la suma de dos $(11, 5, 2)$-biplanos isomorofos. Para esto sea $D_1 = (\mathbb{F}_{11}, B_1)$ el $(11, 5, 2)$-biplano obtenido al utilizar la construcción de Payley cuando $q = 11$.

Sea $\alpha : \mathbb{F}_{11} \longrightarrow \mathbb{F}_{11}$ dada por $\alpha : x \mapsto 2x$. Sea $D_2 = D_1^{\alpha} = (V_2, B_2)$. Notemos que $V_1 = V_2 = \mathbb{F}_{11}$ y que $B_2 = B_1^{\alpha}$. Para comprobar que $B_1 \cap B_2 = \emptyset$, basta escribir B_1 y B_2 explícitamente:

$$
\begin{array}{ccc}
B_1 & & B_2 \\
\{1,4,5,9,3\} & & \{2,8,10,7,6\} \\
\{2,5,6,10,4\} & & \{4,10,1,9,8\} \\
\{3,6,7,0,5\} & & \{6,1,3,0,10\} \\
\{4,7,8,1,6\} & & \{8,3,5,2,1\} \\
\{5,8,9,2,7\} & & \{10,5,7,4,3\} \\
\{6,9,10,3,8\} & \alpha & \{1,7,9,6,5\} \\
\{7,10,0,4,9\} & \longrightarrow & \{3,9,0,8,7\} \\
\{8,0,1,5,10\} & & \{5,0,2,10,9\} \\
\{9,1,2,6,0\} & & \{7,2,4,1,0\} \\
\{10,2,3,7,1\} & & \{9,4,6,3,2\} \\
\{0,3,4,8,2\} & & \{0,6,8,5,4\}
\end{array}
$$

Como B_1 y B_2 son ajenos, tenemos que $D_1 \oplus D_2$ es un $(11, 5, 4)$-BIBD.

Apéndices

A. Grupos de permutaciones

Definición 28. Un grupo G es un **grupo de permutaciones** si G es visto como un subgrupo de $Sym(X)$ para algún conjunto X.

Definición 29. Sean G un grupo con neutro e y X un conjunto. Una **acción** de G en X es una función $\cdot : G \times X \longrightarrow X$ tal que:

(i) $e \cdot x = x$

(ii) $h \cdot (g \cdot x) = hg \cdot x$ para todo $g, h \in G$.

Decimos que un grupo G actúa en un conjunto X si se tiene definida una acción de G en X.
Si $G \leq Sym(X)$ entonces existe una acción natural de G en X, definida para cada $g \in G$ y $x \in X$ como $g \cdot x = x^g$, donde x^g denota la imagen de x bajo g.
Asumimos que los grupos son finitos y que actúan en conjuntos finitos.

Definición 30. Sean G un grupo y H un subgrupo de G. Definimos el **índice** de H en G como el número de clases laterales de H en G y lo denotamos por $[G : H]$, es decir:

$$[G : H] = |\{Hg : g \in G\}|.$$

Definición 31. Sean G un grupo que actúa en un conjunto X y $x \in X$. Definimos la **órbita** de x como el conjunto $O_x = \{x^g : g \in G\}$.
Si H es un subgrupo de G, entonces H también actúa en X, a las órbitas de esta acción las llamaremos H-**órbitas** de X.

Definición 32. Sea G un grupo y H un subgrupo de G. Decimos que H es **normal** en G si $gHg^{-1} = H$ para todo $g \in G$, donde

$$gHg^{-1} = \{ghg^{-1} : g \in G, h \in H\}.$$

Definición 33. Sea G un grupo que actúa en un conjunto X y sea $Y \subseteq X$. Definimos al **estabilizador** de Y como el subgrupo

$$G_Y = \{g \in G : Y^g = Y\}.$$

Si $Y = \{x\}$ entonces simplemente lo denotamos por G_x.

Definición 34. Sean G un grupo y H un subgrupo de G. Consideremos la acción de H en G por conjugación. Sea K un subgrupo de H. Definimos al **normalizador** de K en H como el estabilizador de K bajo esta acción y lo denotamos por $N_H(K)$.

Teorema 21 (Órbita-estabilizador)**.** *Sea G un grupo que actúa en un conjunto X. Entonces para cada $x \in X$, $|O_x| = [G : G_x]$.*

Demostración. Sea $S = \{G_x h : h \in G\}$. Basta observar que $\theta : S \longrightarrow O_x$ definida como $\theta : G_x h \mapsto x^h$ está bien definida y es una biyección. □

Corolario 6 (Ecuación de clase)**.** *Sea G un grupo que actúa en un conjunto X. Entonces $|X| = \sum[G : G_y]$, donde y toma valores de un conjunto de representantes de las órbitas.*

Definición 35. Sea G un grupo que actúa en un conjunto X y sea $Y \subseteq X$. Definimos el **estabilizador puntual** de Y como el subgrupo

$$G_{(Y)} = \{g \in G : y^g = y, \forall y \in Y\}.$$

Si $Y = \{y_1, y_2\}$ denotamos al estabilizador puntual de Y como G_{y_1,y_2}.

Definición 36. Sea G un grupo y p un primo que divide a $\circ(G)$. Supongamos que $\circ(G) = p^r m$ con $(m, p) = 1$. Decimos que $P \leq G$ es un p**-subgrupo de Sylow** de G si $|P| = p^r$.

Lema 27. *Sean G un grupo que actúa en un conjunto X y p un primo que divide a $|G|$ pero que no divide a $|X|$. Entonces existe un p-subgrupo de Sylow P de G y un punto $x \in X$ tal que $P \leq G_x$.*

Demostración. Supongamos que $|G| = p^r m$ donde $(m, p) = 1$ y sea $u = p^r$. Por el Corolario 6 tenemos que $|X| = \sum[G : G_y]$, donde y corre sobre un conjunto de representantes de las órbitas de G. Como p no divide a $|X|$, existe x tal que p no divide a $[G : G_x]$, y entonces u divide a $|G_x|$. Si P es un p-subgrupo de Sylow de G_x, también lo es de G. □

Definición 37. Sea G un grupo actuando en un conjunto X y sea $H \leq G$. Definimos al **conjunto de puntos fijos** de H sobre X como

$$fix_X(H) = \{x \in X : x^h = x, \forall h \in H\}.$$

Si $H = \{h\}$ denotamos al conjunto de puntos fijos de $\{h\}$ sobre X como $fix_X(h)$.

Lema 28. *Sea G un grupo que actúa en un conjunto X y sea $H \leq G$. Si $Y = fix_X(H)$ y $N = N_G(H)$, entonces $N \subseteq G_Y$.*

Demostración. Sean $g \in N$, $h \in H$ y $y \in Y$. Por definición $y^{gh} = y^{h'g} = y^g$, para algún $h' \in H$. Es decir $y^g \in Y$ para todo $y \in Y$. Entonces $g \in G_Y$. □

Lema 29. *Sean G un grupo que actúa en un conjunto X, $g, h \in G$ y $x, y \in X$. Entonces:*

(*i*) *Si O_x y O_y denotan a las órbitas de x y y respectivamente, entonces $O_x \cap O_y = \emptyset$ o $O_x = O_y$.*

(*ii*) *Si $x^g = y$ entonces $g^{-1}G_x g = G_y$. Más aún, $x^g = x^h$ si y sólo si $G_x g = G_x h$.*

Demostración. Supongamos que $O_x \cap O_y \neq \emptyset$ y sea $z \in O_x \cap O_y$. Entonces existe $g_0 \in G$ tal que $z = y^{g_0}$, además; para todo $x^g \in O_x$, existe $h \in G$ tal que $x^{gh} = z = y^{g_0}$, por lo que $x^g \in O_y$ para todo $g \in G$. De manera análoga $y^g \in O_x$ para cualquier $g \in G$. De lo anterior se sigue (i).
Sea $\bar{g} \in G_x$, entonces $y^{g^{-1}\bar{g}g} = y$ y por ende $g^{-1}G_x g \subseteq G_y$. Si $\hat{g} \in G_y$, entonces $x^{g\hat{g}g^{-1}} = x$ y $\hat{g} = g^{-1}(g\hat{g}g^{-1})g \in g^{-1}G_x g$. Concluimos que $G_y \subseteq g^{-1}G_x g$.
Ahora supongamos que $x^g = x^h$ y sea $\bar{g}g \in G_x g$. Entonces $\bar{g}g = (\bar{g}gh^{-1})h$, pero $\bar{g}gh^{-1} \in G_x$. De aquí que $\bar{g}g \in G_x h$ y por lo tanto $G_x g \subseteq G_x h$. Similarmente $G_x h \subseteq G_x g$ y podemos concluir que $G_x g = G_x h$. Recíprocamente, si $G_x h = G_x g$, entonces $h = \bar{g}g$ para algún $\bar{g} \in G_x$ y por lo tanto $x^g = x^{\bar{g}g} = x^h$. □

A continuación mencionamos algunas de las principales propiedades que pueden tener los grupos de permutaciones.

Definición 38. Un grupo G que actúa en un conjunto X es **transitivo** en X si para todos $x, y \in X$ existe $g \in G$ tal que $x^g = y$.

Definición 39. Un grupo G es **regular** en X si G actúa transitivamente en X y $G_x = \{Id\}$ para todo $x \in X$.

Por el Teorema 21, G es regular en X si y sólo si G actúa transitivamente en X y $|X| = \circ(G)$.

Definición 40. Un grupo G que actúa transitivamente en un conjunto X es 2-**transitivo** en X si para todos $(x_1, x_2), (y_1, y_2) \in X \times X$ tales que $x_1 \neq x_2$ y $y_1 \neq y_2$, existe $g \in G$ tal que $x_1^g = y_1$ y $x_2^g = y_2$.

Lema 30. *Sean G un grupo que actúa transitivamente en un conjunto X, $x \in X$y p un primo que divide a $|G|$. Si P es un p-subgrupo de Sylow de G_x, entonces $N = N_G(P)$ es transitivo en $Y = fix_X(P)$.*

Demostración. Sea $y \in Y$. Como G es transitivo en X, existe $g \in G$ tal que $y^g = x$. Notamos que $g^{-1}Pg \leq G_x$, por lo que $g^{-1}Pg$ también es un p-subgrupo de Sylow de G_x y por lo tanto es conjugado de P en G_x. Sea $h \in G_x$ tal que $P = h^{-1}g^{-1}Pgh$. Entonces $gh \in N$ y $y^{gh} = x$. □

Lema 31. *Sean G un grupo que actúa transitivamente en un conjunto X y H un subgrupo de G. Entonces H es transitivo si y sólo si $G = HG_x$, para todo $x \in X$.*

Demostración. Supongamos que H es transitivo y sean $g \in G$ y $x \in X$. Como H es transitivo, existe $h \in H$ tal que $x^h = x^g$, lo que implica que $x^{hg^{-1}} = x$. Podemos escribir $g^{-1} = h^{-1}(hg^{-1}) \in HG_x$, por lo que $g \in HG_x$.
Supongamos que $G = HG_x$ para todo $x \in X$ y sean $\alpha, \beta \in X$. Entonces $G = HG_{\alpha^h}$ para todo $h \in H$, y dado que G es transitivo, existen $\bar{h} \in H$ y $g \in G_{\alpha^{\bar{h}}}$ tales que $\alpha^{\bar{h}g} = \alpha^{\bar{h}} = \beta$. Así H es transitivo. □

Definición 41. Sean H y K grupos, y supongamos que H actúa en K. Supongamos también que esta acción preserva la estructura de grupo de K, es decir, para cada $x \in H$, la función $u \mapsto x \cdot u$ es un automorfismo de K. Definimos el **producto semidirecto** de H y K como el grupo G dado por:

$$G = K \rtimes H = \{(u, x) : u \in K, x \in H\}$$

Para cada $(u, x), (v, y) \in G$, definimos $(u, x)(v, y) = (u(x^{-1} \cdot v), xy)$.

Usualmente denotaremos $K \rtimes H$ como $K \cdot H$.

Lema 32. *Sea G un grupo, consideremos H y K subgrupos de G tales que $K \lhd G$, $H \cap K = \{1\}$ y $KH = G$. Entonces $G \cong K \cdot H$.*

Demostración. $K \lhd G$ implica que H actúa en K por conjugación. Como $H \cap K = \{1\}$, cada $g \in G$ se expresa de manera única como producto de elementos de H y K. Entonces $\varphi : G \longrightarrow K \cdot H$ dada por $\varphi : g = kh \mapsto (k, h)$, es una biyección.
Sean $g_1, g_2 \in G$, entonces $g_1 = k_1h_1$ y $g_2 = k_2h_2$ para algunos $k_1, k_2 \in K$ y $h_1, h_2 \in H$. Vemos que $\varphi(g_1g_2) = \varphi(k_1h_1k_2h_2) = \varphi(k_1(h_1k_2h_1^{-1})h_1h_2) = (k_1(h_1k_2h_1^{-1}), h_1h_2) = (k_1, h_1)(k_2, h_2)$. □

Definición 42. Sea G un grupo que actúa transitivamente en un conjunto X. Decimos que G es **primitivo** en X si no preserva particiones no triviales de X. De otra forma G es **imprimitivo** en X. Si G es imprimitivo, a cada elemento de la partición no trivial de X preservada por G se le llama **bloque de imprimitividad**.

Teorema 22. *Sea G un grupo que actúa transitivamente en un conjunto X. Entonces G es primitivo en X si* y *sólo si G_x es máximo para todo $x \in X$.*

Demostración. Supongamos que G es imprimitivo y que preserva una partición no trivial de X, digamos $\{\Delta_1, \Delta_2, ..., \Delta_\ell\}$. Sea $x \in G$, entonces existe $i \in \{1, ..., \ell\}$ tal que $x \in \Delta_i$ y $G_x \leq G_{\Delta_i}$. Además para $y \in \Delta_i$ tal que $y \neq x$ existe $g_0 \in G$ que cumple $x^{g_0} = y$, entonces $\Delta_i^{g_0} = \Delta_i$, pero $g_0 \notin G_x$, lo que implica que G_x no es maximal.
Supongamos que existe $x \in X$ tal que G_x no es máximo. Entonces hay un subgrupo H tal que $G_x < H < G$. Definimos $\Delta = \{x^h : h \in H\}$. Afirmamos que $\{\Delta^g : g \in G\}$ es una partición no trivial de X preservada por G. La no trivialidad se sigue de que las contenciones en $G_x < H < G$ son propias.
Como G es transitivo $X = \bigcup_{g \in G} \Delta^g$. Sean $g_1, g_2 \in G$ tales que $\Delta^{g_1} \cap \Delta^{g_2} \neq \emptyset$. Entonces existen $h_1, h_2 \in H$ tales que $x^{h_1 g_1} = x^{h_2 g_2}$ por lo que $x^{h_1 g_1 g_2^{-1} h_2^{-1}} = x$, es decir, $h_1 g_1 g_2^{-1} h_2^{-1} \in G_x$ y por lo tanto $g_1 g_2^{-1} := h_0 \in H$.
Utilizando lo anterior tenemos que $w \in \Delta^{g_1}$ si y sólo si $w = x^{h g_1}$ si y sólo si $w = x^{h h_0 g_2}$ y $w \in \Delta^{g_2}$. Entonces $\Delta^{g_1} = \Delta^{g_2}$ y $\{\Delta^g : g \in G\}$ es una partición no trivial de X preservada por G. Por lo tanto si G es primitivo, G_x es maximal para todo $x \in X$. □

B. Campos finitos

Definición 43. Sea K un conjunto con dos operaciones binarias $+$ y $\cdot$, decimos que $(K, +, \cdot)$ es un **campo** si se cumplen las siguientes propiedades:

(*i*) $(K, +)$ y $(K \setminus \{0\}, \cdot)$ son grupos abelianos. Denotaremos por 0 al neutro aditivo y por 1 al neutro multiplicativo.

(*ii*) $a \cdot (b + c) = a \cdot b + a \cdot c$ para todos $a, b, c \in K$.

Expresamos el producto de dos elementos a y b en un campo como la concatenación de ellos, es decir, ab denota a $a \cdot b$. Nos referimos a un campo únicamente escribiendo a su conjunto subyacente.

Definición 44. Sea K un campo. La **característica** de K es el mínimo entero positivo n tal que la suma de cualquier elemento de K consigo mismo n veces es igual a 0. En caso de que dicho entero no exista, diremos que K es de característica cero.

Teorema 23. *Sea K un campo finito. Entonces K tiene característica p, para algún primo p.*

Demostración. Sea $y \in K$, $y \neq 0$. Entonces el siguiente conjunto es finito $\{k \times y : k \in \mathbb{Z}^+\}$, donde $k \times y$ denota la suma de y consigo mismo k veces. Esto implica que la característica de K es un entero positivo n distinto de cero. Sea d un divisor de n, por lo que $n = dm$. La distributividad en K implica que $0 = n \times y = (d \times y)(m \times y)$ y por ende $d = n$ o $m = n$. Se sigue que n es primo. □

Definición 45. Sean K y F campos tales que $F \leq K$. Entonces decimos que K es una **extensión** de F y lo denotamos por K/F.

Lema 33. *Sea K/F una extensión de campos. Entonces $(K, +, \cdot_F)$ es un espacio vectorial sobre F, donde $+$ es la suma en K y $\cdot_F : F \times K \to K$ es el producto en K restringido a F.*

Demostración. Se sigue directamente de las propiedades (i) y (ii) en la Definición 43. □

Definición 46. Sea K/F una extensión de campos, definimos el **grado** de K/F como la cardinalidad de una base de K sobre F, lo denotamos por $[K : F]$. Cuando $[K : F]$ es finito, entonces decimos que K/F es finita.

Teorema 24. *Sean L, K y F campos tales que L/K y K/F son finitas. Entonces L/F es finita* y $[L : F] = [L : K][K : F]$.

Demostración. Sean $n = [L : K]$ y $m = [K : F]$. Consideremos las bases $B_1 = \{w_i\}_{i=1}^n$ y $B_2 = \{v_i\}_{i=1}^m$ de L sobre K y de K sobre F respectivamente. Sea $u \in L$, entonces existe $\{\beta_i\}_{i=1}^n \subset K$ tal que $u = \sum_{i=1}^n \beta_i w_i$. Ahora, para cada $\beta_i \in K$ existe $\{\alpha_{ij}\}_{j=1}^m \subseteq F$ tal que $\beta_i = \sum_{j=1}^m \alpha_{ij} v_j$, sustituyendo $u = \sum_{i,j} \alpha_{ij} w_i v_j$. Entonces $B_3 = \{w_i v_j : 1 \leq i \leq n \ , \ 1 \leq j \leq m\}$ genera a L.

Si suponemos que $0 = \sum_{i,j} \alpha_{ij} w_i v_j = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{ij} v_j \right) w_i$, la independencia lineal de B_1 implica que $0 = \sum_{j=1}^{m} \alpha_{ij} v_j$ para $1 \leq i \leq n$. Por la independencia lineal de B_2 conlcuimos que $\alpha_{ij} = 0$ para $1 \leq i \leq n$ y $1 \leq j \leq m$. Es decir, B_3 también es linealmente independiente. □

Definición 47. Sean K y F tales que K/F. Sea $\alpha \in K$, la **extensión simple** $F(\alpha)$ es el mínimo subcampo de K que contiene a F y a α.

Definición 48. Sean K y F tales que K/F. Sea $\alpha \in K$. Decimos que α es **algebraico** de grado n sobre F si existe $\{a_i\}_{i=0}^{n} \subseteq F$ no todos cero, tales que $0 = \sum_{i=0}^{n} a_i \alpha^i$ y no hay un entero positivo menor a n con esta propiedad.

Definición 49. Sean K un campo y x una indeterminada. El **anillo de polinomios** con coeficientes en K, denotado por $K[x]$, consta de todos los polinomios $\sum_{i=0}^{n} a_i x^i$ donde $n \in \mathbb{N}$ y $a_i \in K$ para $0 \leq i \leq n$.
Sean dos polinomios $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$ donde $m \leq n$. La suma de $f(x)$ y $g(x)$ es el polinomio $f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$ donde $b_i = 0$ cuando $m < i$. El producto de $f(x)$ y $g(x)$ es el polinomio $f(x)g(x) = \sum_{i=0}^{n+m} c_i x^i$ donde $c_i = \sum_{r+s=i} a_r b_s$.

Es importante mencionar que con las operaciones descritas en la definición anterior, $K[x]$ es un anillo euclidiano. Revisar [7, Chap. III, sec. 3].

Definición 50. Sean K un campo y $f(x) \in K[x]$. El **grado** de $f(x)$ es el máximo entero n tal que el n-ésimo coeficiente de $f(x)$ es distinto de 0, lo denotamos por $d(f(x))$.

Dados dos polinomios $f(x)$ y $g(x)$, por la definición de suma y producto de polinomios, tenemos que $d(f(x) + g(x)) \leq máx\{d(f(x)), d(g(x)\}$ y que $d(f(x)g(x)) = d(f(x)) + d(g(x))$.

Definición 51. Sean K/F una extensión de campos y $f(x) \in F[x]$. Decimos que $a \in K$ es una **raíz** de $f(x)$ si $f(a) = 0$.

Definición 52. Sean K un campo y $f(x) \in K[x]$ tal que para todo par de polinomios $g(x)$ y $h(x)$ en $K[x]$ que satisfacen $f(x) = g(x)h(x)$, se cumple que $d(g(x)) = 0$ o $d(h(x)) = 0$. Entonces decimos que $f(x)$ es **irreducible** en K.

Lema 34. *Sean K un campo y $f(x) \in K[x]$. Para todo $b \in K$, existe un polinomio $q(x) \in K[x]$ tal que $f(x) = (x - b)q(x) + f(b)$.*

Demostración. Sean $f(x) \in K[x]$ y $b \in K$. Por el algoritmo de la división, existe $q(x) \in K[x]$ tal que $f(x) = (x-b)q(x) + r(x)$, donde $r(x) = 0$ o $d(r(x)) = 0$. Además $f(b) = r(x)$, entonces $f(x) = (x-b)q(x) + f(b)$. □

Observamos que en la situación del lema anterior, si b es una raíz de $f(x)$, $f(b) = 0$, lo que implica que $(x-b)$ divide a $f(x)$.

Definición 53. Sean K un campo, $f(x) \in K[x]$ y a una raíz de $f(x)$. La **multiplicidad** de a es el máximo natural m tal que $(x-a)^m$ divide a $f(x)$. Decimos que una raíz es **múltiple** si tiene multiplicidad mayor o igual a 2.

Lema 35. *Sean F y $\bar{F}$ dos campos isomorfos. Entonces $F[x]$ y $\bar{F}[x]$ son isomorfos. Más aún, si $p(x)$ es un polinomio irreducible en $F[x]$ y $\bar{p}(x)$ es la imagen de $p(x)$ bajo un isomorfismo, entonces $\bar{p}(x)$ es irreducible en $\bar{F}[x]$ y $F[x]/\langle p(x)\rangle \cong \bar{F}[x]/\langle \bar{p}(x)\rangle$.*

Demostración. Sea $\varphi : F \longrightarrow \bar{F}$ un isomorfismo. Para cada $a \in F$ denotemos por $\bar{a}$ a la imagen de a bajo φ. Entonces

$$\varphi^* : F[x] \longrightarrow \bar{F}[x] \tag{6}$$

definida como $\varphi^* : \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \bar{a}_i x^i$, es un isomorfismo. Para cada $f(x) \in F[x]$ denotemos por $\bar{f}(x)$ a la imagen de $f(x)$ bajo φ^*.
Si $p(x) \in F[x]$ es irreducible y $\bar{p}(x) = \bar{g}(x)\bar{h}(x)$, entonces $p(x) = g(x)h(x)$, lo que implica que $d(g(x)) = 0$ o $d(h(x)) = 0$. Claramente φ^* preserva el grado, por lo que $d(\bar{g}(x)) = 0$ o $d(\bar{h}(x)) = 0$. Es decir, $\bar{p}(x)$ también es irreducible.
Es rutina demostrar que $\varphi^{**} : F[x]/\langle p(x)\rangle \longrightarrow \bar{F}[x]/\langle \bar{p}(x)\rangle$ definida como $\varphi^{**} : \langle p(x)\rangle + f(x) \mapsto \langle \bar{p}(x)\rangle + \bar{f}(x)$ es un isomorfismo. □

Lema 36. *Sean K y L campos tales que L/K y $\alpha \in L$ algebraico de orden n sobre K. Supongamos que $p(x) \in K[x]$ es de grado mínimo tal que $p(\alpha) = 0$, entonces $K[x]/\langle p(x)\rangle \cong K(\alpha)$.*

Demostración. Sea $ev_\alpha : K[x] \longrightarrow K(\alpha)$ dado por $ev_\alpha : f(x) \mapsto f(\alpha)$. Entonces ev_α es un epimorfismo, por lo que $K[x]/ker(ev_\alpha) \cong K(\alpha)$. El resultado se sigue porque $ker(ev_\alpha)$ es el ideal principal generado por $p(x)$. □

Lema 37. *Sean K un campo y $f(x) \in K[x]$ tal que $d(f(x)) = n$. Para cualquier extensión L de K, $f(x)$ tiene a lo más n raíces distintas en L.*

Demostración. Procediendo por inducción sobre el grado de $f(x)$, supongamos que $d(f(x)) = 1$, entonces $f(x) = a_1x + a_0$, donde $a_0, a_1 \in F$. La única raíz de $f(x)$ es $-a_1^{-1}a_0$.
Sean $f(x) \in K[x]$ de grado n y L una extensión de F. Supongamos que $a \in L$ es una raíz de $f(x)$ con multiplicidad m. Entonces existe $q(x)$ tal que $f(x) = (x-a)^m q(x)$, donde $d(q(x)) = n - m$. Por hipótesis inductiva $q(x)$ tiene a lo más $n - m$ raíces distintas en L. Entonces $f(x)$ tiene a lo más $n - m + 1$ raíces distintas en L. □

Teorema 25. *Sean K y F tales que K/F y $\alpha \in K$. Entonces $F(\alpha)/F$ es finita si y sólo si α es algebraico sobre F. Más aún, $[F(\alpha) : F]$ es igual al grado de α sobre F.*

Demostración. Supongamos que $F(\alpha)/F$ es finita y sea $[F(\alpha) : F] = n$. Entonces $\{\alpha^i\}_{i=0}^n$ es linealmente dependiente, lo que implica que α es algebraico de grado n.
Si α es algebraico de grado n sobre F entonces existe $\{a_i\}_{i=0}^n \subseteq F$ tal que $0 = \sum_{i=0}^n a_i\alpha^i$. Sea $p(x) = \sum_{i=0}^n a_i x^i$, observamos que $p(x)$ es irreducible, de lo contrario α sería de grado menor a n. Sea $\varphi : F[x] \longrightarrow F(\alpha)$ dado por $\varphi : f(x) \mapsto f(\alpha)$. Notamos que φ es un epimorfismo, lo que implica que $P = ker(\varphi) = \langle p(x) \rangle$ es un ideal de $F[x]$ y que $F[x]/P \cong F(\alpha)$ y como para todo $P + f(x) \in F[x]/P$ existe $h(x)$ de grado menor a n tal que $P + f(x) = P + h(x)$, tenemos que $F[x]/P$ se puede generar con n elementos sobre $\bar{F} = \{P + c : c \in F\}$. Entonces $[F[x]/P : \bar{F}] = [F(\alpha) : F] = n$. □

Lema 38. *Sean F un campo y $p(x) \in F[x]$ irreducible. Entonces existe una extensión finita de F en donde $p(x)$ tiene una raíz.*

Demostración. Sea $P = \langle p(x) \rangle$ y α una raíz de $p(x)$. El Lema 36 nos dice que $F[x]/P \cong F(\alpha)$ es un campo que contiene a un subcampo $\bar{F}$ isomorfo a F y por el Teorema 25 $[F[x]/P : \bar{F}] = [F(\alpha) : F]$ es finita. Supongamos que $\bar{p}(x) \in \bar{F}[x]$ es la imagen de $p(x)$ bajo φ^* definido como en (6), entonces $\bar{p}(P + x) = P + \bar{p}(x) = P$, por lo que $P + x$ es una raíz de $\bar{p}(x)$. □

Definición 54. Sean K un campo y $f(x) \in K[x]$, decimos que $f(x)$ se **factoriza completamente** en un campo L si existe $\{a_i\}_{i=0}^n \subseteq L$ tales que $f(x) = a_0 \prod_{i=1}^n (x - a_i)$.

Lema 39. *Sean F un campo y $f(x) \in F[x]$ tal que $f(x)$ no se factoriza completamente. Entonces existe una extensión finita de F en donde $f(x)$ se factoriza completamente.*

Demostración. Procederemos por inducción sobre $d(f(x)) - k$, donde k es el número de factores lineales de $f(x)$ en $F[x]$.
Supongamos que $f(x) \in F[x]$ y que $d(f(x)) - k = 2$. Entonces podemos escribir $f(x) = a_0 \left(\prod_{i=1}^{n-2}(x - a_i)\right) p(x)$ donde $p(x)$ es irreducible y mónico de grado 2. Por el Lema 38 existe una extensión K de F en donde $p(x)$ tiene una raíz a_{n-1}. Entonces $p(x) = (x - a_{n-1})(x - a_n)$. Así $f(x) = a_0 \prod_{i=1}^{n}(x - a_i)$ donde $\{a_i\}_{i=1}^{n} \subseteq K$, es decir, $f(x)$ se factoriza completamente en K.
Supongamos que $f(x) \in F[x]$ y que $d(f(x)) - k = m$. Entonces podemos escribir $f(x) = a_0 \left(\prod_{i=1}^{k}(x - a_i)\right) \left(\prod_{i=1}^{r} q_i(x)\right)$ donde $q_i(x)$ es irreducible y mónico de grado al menos 2 para $1 \leq i \leq r$. Por el Lema 38 existe una extensión K de F donde $q_1(x)$ tiene una raíz a_{k+1}. Entonces $d(f(x)) - k \leq m - 1$ donde k es el número de factores lineales de $f(x)$ en $K[x]$, por hipótesis inductiva, existe una extensión finita L de K donde $f(x)$ se factoriza completamente. □

Definición 55. Sean K un campo y $f(x) \in K[x]$. El **campo de descomposición** de $f(x)$ en K es la mínima extensión de K en donde $f(x)$ se factoriza completamente.

Teorema 26. *Sean F y $\bar{F}$ campos tales que $F \overset{\varphi}{\cong} \bar{F}$ y $F[x] \overset{\varphi^*}{\cong} \bar{F}[x]$. Sean $f(x) \in F[x]$ y $\bar{f}(x) \in \bar{F}[x]$ la imagen de $f(x)$ bajo φ^*. Entonces los campos de descomposición de $f(x)$ en F y el de $\bar{f}(x)$ en $\bar{F}$ son isomorfos.*

Demostración. Observamos que si $f(x)$ tiene k factores lineales en $F[x]$, entonces $\bar{f}(x)$ también tiene k factores lineales en $\bar{F}[x]$. Haremos la demostración por inducción sobre $d(f(x)) - k = d(\bar{f}(x)) - k$. Si $d(f(x)) - k = 0$, entonces $f(x)$ y $\bar{f}(x)$ se factorizan completamente en F y en $\bar{F}$, que son isomorfos por hipótesis.
Supongamos que $d(f(x)) - k = 2$, entonces:

$$f(x) = \left(\prod_{i=1}^{n-2}(x - a_i)\right) p(x) \text{ y } \bar{f}(x) = \left(\prod_{i=1}^{n-2}(x - \bar{a}_i)\right) \bar{p}(x),$$

donde $p(x)$ y $\bar{p}(x)$ son mónicos de grado 2. Por el Lema 35 tenemos que:

$$K = F[x]/\langle p(x)\rangle \overset{\varphi^{**}}{\cong} \bar{F}[x]/\langle \bar{p}(x)\rangle = \bar{K},$$

Campos en donde $p(x)$ y $\bar{p}(x)$ se factorizan completamente. Entonces K es el campo de descomposición de $f(x)$ en F y $\bar{K}$ es el campo de descomposición de $\bar{f}(x)$ en $\bar{F}$.

Supongamos que $d(f(x)) - k = m$, entonces podemos escribir:

$$f(x) = \left(\prod_{i=1}^{k}(x - a_i)\right)\left(\prod_{i=1}^{r} q_i(x)\right) \text{ y } \bar{f}(x) = \left(\prod_{i=1}^{k}(x - \bar{a^i})\right)\left(\prod_{i=1}^{r} \bar{q}_i(x)\right),$$

donde $q_i(x)$ y $\bar{q}_i(x)$ son irreducibles y mónicos de grado al menos 2 para $1 \leq i \leq r$. De nuevo, por el Lema 35 tenemos que:

$$K = F[x]/\langle q_1(x)\rangle \overset{\varphi^{**}}{\cong} \bar{F}[x]/\langle \bar{q}_1(x)\rangle = \bar{K},$$

campos donde $f(x)$ y $\bar{f}(x)$ tienen a lo más $m-1$ factores lineales. Por hipótesis inductiva los campos de descomposición L y $\bar{L}$ de $f(x)$ y de $\bar{f}(x)$, respectivamente, son isomorfos. □

Definición 56. Sean K un campo y $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, definimos la **derivada** de $f(x)$ como el polinomio $f'(x) = \sum_{i=0}^{n-1}(i+1)a_{i+1}x^i$.

Lema 40. *Sean K un campo* y $f(x) \in K[x]$ *tal que $f(x) = g(x)h(x)$, entonces $f'(x) = g'(x)h(x) + g(x)h'(x)$.*

Demostración. Sean $g(x) = \sum_{i=0}^{n} a_i x^i$, $h(x) = \sum_{i=0}^{m} b_i x^i$ y $f(x) = \sum_{i=0}^{n+m} c_i x^i$ donde $c_i = \sum_{r+s=i} a_r b_s$.
Entonces $g'(x)h(x) = \sum_{i=0}^{n+m-1} d_i x^i$, donde $d_i = \sum_{r+s=i}(r+1)a_{r+1}b_s$; y $g(x)h'(x) = \sum_{i=0}^{n+m-1} e_i x^i$, donde $e_i = \sum_{r+s=i}(s+1)a_r b_{s+1}$.
Notemos que si $f'(x) = \sum_{i=0}^{n+m-1} c_i' x^i$ entonces $d_i + e_i = c_i'$ y por lo tanto $f'(x) = g'(x)h(x) + g(x)h'(x)$. □

Lema 41. *Sean F un campo* y $f(x) \in F[x]$. *Entonces $(f(x), f'(x)) = 1$ si* y *sólo si $f(x)$ no tiene raíces multiples.*

Demostración. Sea K el campo de descomposición de $f(x)$. Notemos que $(f(x), f'(x)) = 1$ en $F(x)$ si y sólo si $(f(x), f'(x)) = 1$ en $K(x)$.
Supongamos que a es una raíz multiple de $f(x)$. Entonces $(x-a)^2$ divide a $f(x)$, es decir, existe $g(x) \in K[x]$ tal que $f(x) = (x-a)^2 g(x)$. Por el Lema 40, $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x) = (x-a)(2g(x) + (x-a)g'(x))$, lo que implica que $(f(x), f'(x)) \neq 1$.
Recíprocamente, supongamos que $h(x) = (f(x), f'(x)) \neq 1$ y sea a una raíz de $h(x)$, entonces $(x-a)$ divide a $f(x)$ y a $f'(x)$, por lo que existen

$g(x), g'(x) \in K[x]$ tales que $f(x) = (x-a)g(x)$ y $f'(x) = (x-a)g'(x)$. Por el Lema 40, $f'(x) = g(x) + (x-a)g'(x)$, lo que implica que $(x-a)$ divide a $g(x)$. Concluimos que $(x-a)^2$ divide a $f(x)$ y a es una raíz múltiple de $f(x)$. □

Lema 42. *Sea n un entero positivo. Entonces $n = \sum_{d|n} \Phi(d)$, donde Φ denota la función Phi de Euler.*

Demostración. Sea G un grupo cíclico de orden n. Para cada divisor d de n existen $\Phi(d)$ generadores del subgrupo cíclico de G de orden d. Esto implica que para cada divisor d de n, G contiene $\Phi(d)$ elementos de orden d. Entonces $n = \circ(G) = \sum_{d|n} \Phi(d)$. □

Lema 43. *Sea G un grupo abeliano finito de orden n tal que para cada divisor d de n la ecuación $x^d = 1$ tiene a lo más d soluciones. Entonces G es cíclico.*

Demostración. Sea d un divisor de n, como la ecuación $x^d = 1$ tiene a lo más d soluciones, entonces G tiene a lo más $\Phi(d)$ elementos de orden d. Por el lema anterior, G tiene al menos un elemento de orden n y por lo tanto es cíclico. □

Teorema 27. *Sea K un campo finito. Entonces $(K \setminus \{0\}, \cdot)$ es cíclico.*

Demostración. Supongamos que $|K \setminus \{0\}| = n$. Por el Lema 37, para cada divisor d de n, el polinomio $x^d - 1 = 0$ tiene a lo más d raíces distintas en $K \setminus \{0\}$. Por el lema anterior $(K \setminus \{0\}, \cdot)$ es cíclico. □

Definición 57. Sea K un campo finito, una **raíz primitiva** ω de K es un elemento tal que $\langle \omega \rangle = K \setminus \{0\}$.

Lema 44. *Sean k y n enteros tales que $0 \leq k \leq n$ y $\binom{n}{k}$ es el coeficiente binomial, $\frac{n!}{(n-k)!k!}$, donde $0! = 1$ y para $n > 0$, $n! = (n)(n-1)(n-2)...(2)(1)$.*

(a) $\binom{n}{k} = \binom{n}{n-k}$.

(b) $\binom{n}{k} < \binom{n}{k+1}$ *cuando* $k < \frac{n}{2}$.

(c) $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ *cuando* $k < n$.

(d) $\binom{n}{k}$ *es un entero.*

(e) *Si p es un número primo* y $1 \leq k \leq p^n - 1$ *entonces* $\binom{p^n}{k}$ *es divisible entre* p.

Demostración. (a) Se sigue de la definición de $\binom{n}{k}$.

(b) Notemos que $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(k+1)!(n-k-1)!}\frac{k+1}{n-k} = \binom{n}{k+1}\frac{k+1}{n-k}$ y como $k < \frac{n}{2}$ tenemos que $\frac{k+1}{n-k} < 1$.

(c) $\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!} = \frac{(n-1)!(k+n-k)}{(n-k)!k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$.

(d) Supongamos, sin pérdida de generalidad, que $k \leq n - k$. Entonces $\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n(n-1)...(n-k+1)}{k!}$. Observamos que para cada $1 \leq d \leq k$ existen al menos $\lfloor \frac{k}{d} \rfloor$ enteros j tales que $0 \leq j < k$ y $n - j \equiv 0 \pmod{d}$.

Sea q un primo y q^m la máxima potencia de q que divide a k. Para $1 \leq i \leq m$, sea $t_i = \lfloor \frac{k}{q^i} \rfloor$. Entonces hay t_i múltiplos de q^i menores o iguales a k, a saber, q^i, $2q^i$,..., $t_i q^i$.

Por otro lado, si $0 \leq r_i < k$ es máximo tal que $n - r_i \equiv 0 \pmod{q^i}$. Entonces $n - r_i$, $n - r_i + q^i$, ..., $n - r_i + (t_i - 1)q^i$ son también t_i múltiplos de q^i.

Lo anterior implica que la q-parte de $k!$ divide a $n(n-1)...(n-k+1)$. Dado que q fue arbitrario, concluimos d.

(e) Sea $1 \leq k \leq p^n - 1$. Sean p^r la p-parte de $k!$ y p^l la p-parte del producto $(p^n)(p^n - 1)...(p^n - k + 1)$, haciendo un análisis similar al del inciso anterior, tenemos que $r = d_1 + d_2 + ... + d_m$, donde m es la máxima potencia de p que divide a k y $t_i = \lfloor \frac{k}{p^i} \rfloor$. Además $m < n$ y en r sólo se contemplan los factores que tienen potencias de p menores o iguales a m, por lo que $p^r < p^l$ y p divide a $\binom{p^n}{k}$.

□

Teorema 28. *Un campo finito K de característica p tiene orden p^n si* y *sólo si es un campo de descomposición de $f(x) = x^{p^n} - x \in F[x]$, donde F es un campo finito de orden p.*

Demostración. Sea K un campo finito de característica p y de orden p^n. Por el Teorema 27, $a^{p^n - 1} = 1$ para todo $a \in K$, por lo tanto cada elemento de K es raíz de $f(x)$ y entonces K es el campo de descomposición de $f(x)$.

Sea L un campo de descomposición de $f(x)$ y sean a y b raíces de $f(x)$. Por el Lema 44, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, $(ab)^{p^n} = a^{p^n} b^{p^n}$ y $(a^{-1})^{p^n} = (a^{p^n})^{-1}$, lo que implica que L es el conjunto de todas las raíces de $f(x)$. Por el Lema 41, $f(x)$ no tiene raíces con multiplicidad mayor a 2, entonces L tiene orden p^n. □

Teorema 29. *Sean K y $\bar{K}$ dos campos finitos de característica p y de orden p^n. Entonces $K \cong \bar{K}$*

Demostración. Por el Teorema 28, K y $\bar{K}$ son campos de descomposición del polinomio $x^{p^n} - x$ en F y $\bar{F}$ respectivamente. Donde F y $\bar{F}$ son campos de p elementos y por lo tanto $F \cong \bar{F}$. El resultado se sigue del Teorema 26. □

El teorema anterior implica que si p es un primo y $q = p^n$ para $n \geq 1$, entonces existe un único campo, salvo isomorfismo, con orden q, el cual denotamos por $\mathbb{F}_q$.

Lema 45. *Sean p un número primo, $r \in \mathbb{N}$ y s un divisor de r. Entonces $\mathbb{F}_{p^r}$ contiene un subcampo F con p^s elementos dado por $F = \{y \in \mathbb{F}_{p^r} : y^{p^s} = y\}$.*

Demostración. Como s divide a r tenemos que $r = su$ para algún entero positivo u. Sean ω una raíz primitiva de $\mathbb{F}_{p^r}$ y $m = \sum_{i=0}^{u-1} p^{is}$. Supongamos que $y \neq 0$ y que $y = y^{p^s}$. Entonces $y = \omega^n$ donde $1 \leq n < p^r$ y $\omega^n = \omega^{np^s}$. Se sigue que $(p^s - 1)n \equiv 0 \ (mod\ p^r - 1)$, por lo tanto m divide a n. Lo anterior implica que $y = \omega^{mj}$, donde $1 \leq j < p^s$ y entonces $|F| = p^s$. Además $(y_1 + y_2)^{p^s} = y_1^{p^s} + y_2^{p^s} = y_1 + y_2$ y $(y_1 y_2)^{p^s} = y_1^{p^s} y_2^{p^s} = y_1 y_2$ para todo $y_1, y_2 \in F$, concluimos que F es campo. □

Definición 58. Sea K un campo. Una función $\varphi : K \to \bar{K}$ es un **automorfismo de campos** si se cumple que:

(*i*) $\varphi(0) = 0$ y $\varphi(1) = 1$.

(*ii*) $\varphi(x + y) = \varphi(x) + \varphi(y)$ para todos $x, y \in K$.

(*iii*) $\varphi(xy) = \varphi(x)\varphi(y)$ para todos $x, y \in K$.

El conjunto de todos los automorfismos de un campo K forma un grupo al cual denotamos por $Aut(K)$.

Lema 46. *Sean p un primo y q una potencia de p. Entonces la función $a : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, definida como $a : x \mapsto x^p$, es un automorfismo.*

Demostración. Se sigue del inciso (e) del Lema 44. □

Al automorfismo descrito en el lema anterior se le conoce como el **automorfismo de Frobenius**.

Lema 47. *Sea p un primo y r un entero positivo. Si a es el automorfismo de Frobenius de $\mathbb{F}_{p^r}$ y s divide a r, entonces $fix_{\mathbb{F}_{p^r}}(a^s) := F$ es un subcampo de $\mathbb{F}_{p^r}$ con p^s elementos.*

Demostración. Sea ω una raíz primitiva de $\mathbb{F}_{p^r}$, como s divide a r, $r = su$ para algún entero positivo u. Entonces $p^r - 1 = \left(\sum_{i=0}^{u-1} p^{is}\right)(p^s - 1)$. Llamemos $m = \sum_{i=0}^{u-1} p^{is}$. Entonces para cada $1 \leq k < p^s$ tenemos que $(\omega^{km})^{p^s} = \omega^{km}$. Dichos elementos, junto con el 0, conforman un subcampo de $\mathbb{F}_{p^r}$ con p^s elementos. □

Lema 48. *El grupo de automorfismos del campo $K = \mathbb{F}_{p^r}$ es cíclico* y *está generado por el automorfismo de Frobenius.*

Demostración. Sea $\tau \in Aut(K)$ tal que $\tau \neq Id$ y sea ω una raíz primitiva de K. $\omega^\tau = \omega^k$ donde $1 < k < p^r$. Entonces $\alpha^\tau = \alpha^k$ para toda $\alpha \in K$. Si $\circ(\tau) = m$, entonces $\omega^{k^m} = \omega$. Como p^r es la mínima potencia para lo que esto ocurre, tenemos que $k^m \geq p^r$. Supongamos que $k^m > p^r$, como α es una raíz de $f(x) = x^{k^m} - x$ para toda $\alpha \in K$ tenemos que $g(x) = x^{p^r} - x$ divide a $x^{k^m} - x$ y entonces $f(x) = g(x)h(x)$ con $d(h(x)) \geq 1$. Una contradicción. Por lo tanto $k^m = p^r$ y k es una potencia de p. □

Lema 49. *Sea q una potencia de primo impar tal que $q \equiv 3 \pmod 4$. Si $x \in (\mathbb{F}_q^*)^2$ entonces $-x \notin (\mathbb{F}_q^*)^2$.*

Demostración. Sea ω una raíz primitiva de $\mathbb{F}_q$, entonces $x = \omega^{2n}$ para algún entero n. Observamos que como $q - 1 = 4t - 2$, entonces $-1 = \omega^{2t-1}$, se sigue que $-x = \omega^{2(n+t)-1} \notin (\mathbb{F}_q^*)^2$. □

C. Algoritmos implementados en Python

Se implementaron en Python algoritmos para encontrar parámetros $(v, k, 2)$ que satisfacen el Lema 1 cuando $v = p^2$ y p es un primo menor a 4×10^5. También para encontrar las raíces primitivas de un campo y para determinar

la cardinalidad de la intersección de ciertos conjuntos con potencial de ser bloques. A continuación están los programas utilizados así como una breve descripción de su función.

Programa 1. *Para encontrar los números primos menores o iguales a un entero n.*

```
def listaDiv(n):
    divisores=[]
    for i in range(1,int(n/2)+1):
        if n%i==0:
            divisores.append(i)
    return divisores

def primos(n):
    primos=[]
    for i in range(3,n+1,2):
        if len(listaDiv(i))==1:
                primos.append(i)
    return primos
```

Programa 2. *Para encontrar valores de k tales que los parámetros* $(p^2, k, 2)$ *satisfagan el Lema 1 y tales que p sea menor a un entero n.*

```
def lema1ParaPrimoCuadrado(n):
    klista=[]
    for p in primos(n):
        for k in range(p+1,2*p):
            if 2*(p**2-1)==k*(k-1):
                klista.append(k)
    return klista
```

Los siguientes programas se hicieron para encontrar las raíces primitivas del campo $\mathbb{F}_{p^2}$ cuando $p \equiv 3 \ (mod\ 4)$

Programa 3. *Da una lista con los elementos de* $\mathbb{Z}_q \times \mathbb{Z}_q$.

```
def parejas(q):
    listaParejas=[]
```

```
    for h in range(0,q):
        for k in range(0,q):
            listaParejas.append((h,k))
    return listaParejas
```

Programa 4. *Para definir un producto y la potencia en* $\mathbb{Z}_p \times \mathbb{Z}_p$.

```
def producto((a,b),(c,d),p):
    return ((a*d+b*c)%p,(b*d-a*c)%p)

def potencia((a,b),n,p):
    if n==1:
        return (a,b)
    else:
        return producto(potencia((a,b), n-1,p),(a,b),p)
```

Programa 5. *Para encontrar las raíces primitivas de* $\mathbb{F}_{p^2}$ *cuando* $p \equiv 3 \pmod 4$.

```
def listaDePotencias((a,b),p):
    lista1=[]
    for n in range (1,p**2):
        if potencia((a,b),n,p) not in lista1:
            lista1.append(power((a,b),n,p))
        else:
            break
    return lista1

def raicesPrimitivas(p):
    raicesPrimitivas=[]
    for t in parejas(p):
        if len(listaDePotencias(t,p))==p**2-1:
            raicesPrimitivas.append(t)
    return raicesPrimitivas
```

Bibliografía

[1] M. Aschbacher, *On Collineation Groups of Symmetric Block Designs*, J. Combin. Theory **11** (1971) 272-281.

[2] M. Biliotti, A. Montinaro, *On Flag-Transitive Symmetric Designs of Affine Type*. Journal of Combinatorial Designs **25 (2)** (2017) 85-97.

[3] C. J. Colbourn, J. H. Dinitz, *Handbook of Combinatorial Designs.* Chapman and Hall, (2006).

[4] J. D. Dixon, B. Mortimer, *Permutation Groups*, Springer, Nueva York, 1996.

[5] D. A. Foulser, *Solvable flag-transitive affine groups*, Math. Zeitschr. **81** (1964) 191-204.

[6] D. A. Foulser, *The flag-transitive collineation group of the finite Desarguesian affine planes*, Canad. J. Math. **16** (1964) 443-472.

[7] T. W. Hungerford, *Algebra*, Springer-Verlag, (1974).

[8] T. P. Kirkman. *VI Query*, Lady's and Gentleman's Diary, **147** (1850) 48.

[9] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series, Vol. 74, Cambridge University Press, 1983, Cambridge, U. K.

[10] M. W. Liebeck, C. E. Praeger, J. Saxl, *On The O'Nan-Scott Theorem for Finite Primitive Permutation Groups*, J. Austral. Math. Soc. Series A **44** (1988) 389-396.

[11] C. H. Li, T. K. Lim, and C. E. Praeger, *Homogenous factorizations of complete graphs with edge-transitive factors.*

[12] L. Marangunić, *Biplanes* (79,13,2) *with Involutory Automorphism*, Journal of Combinatorial Theory, Series A **61**, 36-49 (1992).

[13] E. O'Reilly Regueiro, *On primitivity and reduction for flag-transitive symmetric designs*, J. Comb. Theory Ser. A **109** (2005) 135-148.

[14] E. O'Reilly Regueiro, *Biplanes with flag-transitive automorphism group of almost simple type, with alternating or sporadic socle*, Europ. J. Combin **26** (2005) 577-584.

[15] E. O'Reilly Regueiro, *Biplanes with flag-transitive automorphism group of almost simple type, with classical socle*, J. Algebr. Comb. **26** (2007) 529-552.

[16] E. O'Reilly Regueiro, *Biplanes with flag-transitive automorphism group of almost simple type, with exeptional socle of Lie*, J. Algebr Comb. **27** (2008) 479-491.

[17] M. Suzuki, *Group Theory II*, Springer-Verlag, 1986.

[18] K. Thas, D. Zagier, *Finite projective planes, Fermat curves, and Gaussian periods*, J. Eur. Math. Soc. **10** (2008) 173-190.

Índice alfabético