UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

Una primera aproximación al problema de Davenport para grupos de rango 3

Matías Saucedo

Director: Martín Mereb

Julio de 2015

Agradecimientos

A mi mamá y a mi papá, por la educación que me brindaron y por romperse el lomo trabajando para que nunca me falte nada. Todos los sueños que cumplí en estos veintidós años se dieron porque antes estuvieron ustedes ahí poniendo todo de su parte para que yo pueda aprovechar cada oportunidad que se me presentaba.

A mis tías, que son una fuente inagotable de cariño. Y también a Cecilia, por la misma razón.

A Isabel Orduña, mi maestra de cuarto grado, que decidió que yo no tenía que aburrirme en sus clases y fue la primera en mostrarme problemas de Ñandú.

A Viviana Soltz y María Inés Bieri, las profesoras que me acompañaron en mis comienzos en olimpíadas. Ambas saben cuánto las quiero.

A Mariana Sánchez, la de mayor antigüedad entre mis amigos, y la única de Mercedes. Con ella he compartido todo tipo de aventuras, que recordamos con mucha nostalgia cada tanto.

A Mariano Juncal, el amigo que desde los 4 años soñaba con tener alguna vez, y que conocí recién a los 14. Y junto con él, a Iván, Caro, Maite y Lupi, a quienes conocí en el entrenamiento de Cono de 2007 y cambiaron mi vida para siempre.

A los exolímpicos de aquel entonces, de quienes aprendí muchísimo. Ojalá yo pueda haber sido para las generaciones posteriores aunque sea un poco de todo lo que ustedes fueron para mí. Gracias a Gabriel Carvajal, Carlos di Fiore, Maxi Camporino, Marcos Cossarini, Ramiro Lafuente, Leopoldo Taravilse, Magalí Giaroli, Gabriel Estrany, Lucas Andisco, Julián Eisenschlos y Roberto Morales. Y muchas gracias a Pablo Blanc, que me regaló nada más y nada menos que mi copia del *Retorno a la Geometría*.

A Daniel Kohen, mi compañero de equipo, mi amigo, mi docente. Nunca voy a olvidar el día en que fuimos juntos, con miedo, a decirles a Patricia y Flora que queríamos estudiar matemática, como si pensáramos que nos iban a decir que mejor nos dediquemos a otra cosa. Junto con él, quiero agradecer a todos los demás amigos que hice durante mis años de participante y que aún conservo. En especial a Nico Ponieman, Franco, Taurus, Cogo, Rocío, Margy, Germán, Miguel, Julieta, Chebi y Daniela.

Por supuesto, a la OMA, que me dio (¡y me sigue dando!) muchos de los mejores

recuerdos de mi vida. Si no fuera por ella no habría conocido a todas estas maravillosas personas que nombré en los párrafos anteriores. Quiero agradecer a TODOS los que hacen posible que la olimpíada funcione, cada uno desde su lugar. Dentro de los profesores del área de matemática del CBC que colaboran con la OMA, quiero agradecer especialmente a Ana –a quien le debemos los desayunos en Temuco– y a Bibi, Cintia y Elicita, con quienes compartí muchas olimpíadas rioplatenses.
(No desesperen y continúen leyendo.)

A Natalia Accomazzo, mi compañera desde el primer hasta el último día de carrera. Y mucho más importante que eso, una gran amiga.

A Diego Montero, a quien también conocí en mis primeros días en la facultad. Gracias por tu amistad, por tus consejos y por hacerme reír.

A Sofi, una de las amistades más valiosas que me regaló la facultad. Por estar siempre. Y por los mates.

A Marce y Facu, por todo lo que aprendí en el taller de Topología.

A los que me acompañaron en los primeros viajes académicos y aún no nombré: Aye, Data, Xime, Tochi y Vero.

A Carlo, Santi, Santi, Manu y Mateo por compartir conmigo el verano más interesante de mi vida en Rio de Janeiro. Y a los profesores Jonathan Barmak y Guillermo Cortiñas, que me recomendaron para que pueda tener esa experiencia.

A nuestra querida Botella de Klein, que en realidad ya ocupaba un lugar importante en mi vida en la era pre WhatsApp, en forma de juntadas maratónicas de estudio los fines de semana previos a un parcial. Por alegrarme los días y estar siempre dispuestos a dar una mano. No quiero que ninguno de ustedes quede sin nombrar, así que: gracias Jaz, Maxi, Rafa, Bruno, Kari, Pablo, Euge y Diana.

A todos los docentes de altísimo nivel que tuve durante la licenciatura. Muy especialmente a Marcelo Valdettaro y Mariela Sued, que son mis modelos a seguir en lo que a docencia se refiere.

A la Academia Nacional de Ciencias Exactas, Físicas y Naturales y a la familia Barroso Mastronardi, por otorgarme la beca *In libris carpe rosam*.

Ya mencioné a los amigos que hice durante mi etapa como olímpico. Afortunadamente, hay muchos otros que pasaron a ocupar un lugar especial en mi corazón una vez que ya vivía en Buenos Aires.

A Melanie Sclar y Sebastián Prillo, los hermanitos que nunca tuve. Son quienes mejor me conocen, y aún así me siguen queriendo.

A Nacho Darago, Ariel Zylber, Ale Candioti, Bruno Staffa, Rodrigo Miguel, Carolina Lang, Mariano Chehebar, Ignacio Bombau, y tantos otros que no estoy nombrando. Por las palabras de aliento cuando decidí que me tenía que recibir, y durante todo el proceso de escritura de la tesis.

A todos los que han sido mis alumnos, tanto de olimpíadas como en la facultad. Frases como «ahora con cómo lo explicaste lo entendí mucho mejor» o «me salió con lo que contaste el año pasado» hacen que uno se levante todos los días con muchas ganas de hacer su trabajo.

A mis compañeros JTPs que me dieron la posibilidad de desarrollarme como docente.

Todas las personas que nombré hasta ahora han tenido una gran influencia en mi vida, sin ellas no sería quien soy y no habría llegado a donde estoy. Sin embargo, hay algunas personas que estuvieron directamente relacionadas con el desarrollo de esta tesis y es el momento de agradecerles por ello.

A Charly, que se merece que lo nombre de nuevo. Porque, como si no hubiera sido suficiente ya con sacarme los miedos que tenía sobre estudiar matemática, seis años después fue la persona que me proporcionó una solución en el momento en el que parecía que iba a ser imposible hacer una tesis sobre un tema que realmente me interesara. No alcanzan las palabras para expresar mi gratitud; voy a conformarme con sólo decir gracias.

A Martín, por animarse a dirigir una tesis en un tema distinto a su área de trabajo. Por el tiempo y los consejos, y por darme la posibilidad de trabajar libre, poniéndome mis propios objetivos. No habría podido pedir un mejor director.

A Beto, a quien podría haber nombrado antes pero está acá porque fue justamente a través de sus papers que me encontré por primera vez con el tema de la tesis. Porque es de las pocas personas que realmente tienen la habilidad de transportarte a un mundo maravilloso mientras te enseñan matemática. Gracias por tanta magia.

Al jurado, por tomarse el trabajo de leer la tesis y por sus valiosos comentarios y sugerencias.

Y a Julián Martínez y Willem van Zuijlen, que nos ayudaron a conseguir unos papers holandeses que parecían no estar en ningún lado.

Cuando era chico, mi mamá me leía cuentos con *hadas madrinas*, esos seres mágicos que aparecen un día sin que te lo esperes y que tienen el poder de transformar tu vida por completo, llevándote a niveles de felicidad que ni siquiera sabías que existían. Las últimas dos personas a las que quiero agradecer encajan perfectamente con esta descripción.

Lo más importante que aprendí después de mi primer entrenamiento fue que no hacía falta tratar de ser una persona distinta para poder tener más amigos. Me sentí, por primera vez, realmente parte de un grupo. Este descubrimiento, crucial para cualquier adolescente, ayudó a terminar de formar la personalidad que hoy me caracteriza. En pocas palabras, a partir de entonces fui más feliz.

Todo esto se lo debo en última instancia a dos personas, que si no fuera por

el increíble trabajo que vienen haciendo desde hace décadas, casi ninguna de las personas que nombro en estos agradecimientos habría llegado a mi vida. Porque mi mayor sueño es poder sentir algún día que lo que yo hice impactó en la vida de otro de la misma manera que ellas impactaron en la mía, y en la de tantos otros antes que yo. Porque me hicieron vivir experiencias únicas, y me dieron la posibilidad de seguir involucrado con lo que más feliz me hizo y me hace en este mundo. Porque la gratitud que siento hacia ellas es infinita, y porque las quiero como si fueran parte de mi familia. Por todo esto, y por tantas cosas más.

A Patricia Fauring y Flora Gutiérrez: esta tesis está dedicada a ustedes.

A mis hadas madrinas

Índice general

Introducción

La teoría de suma cero es un área de la combinatoria que comenzó a ser investigada hace poco más de 50 años. Se considera que el punto de partida de estas investigaciones está en el resultado de Erdős, Ginzburg y Ziv [EGZ61] que establece que el menor entero positivo ℓ con la propiedad de que toda sucesión de longitud ℓ en el grupo cíclico $\mathbb{Z}_n$ contiene una subsucesión de longitud exactamente n cuyos elementos suman 0 es $2n-1$.

Este resultado admite muchas posibles reinterpretaciones y generalizaciones. Un típico problema de suma cero *directo* busca encontrar condiciones que garanticen que una sucesión dada en un grupo abeliano finito G contenga una subsucesión de suma 0 que cumpla ciertas propiedades prefijadas. Todo problema directo tiene asociado un problema *inverso*, que estudia la estructura de aquellas sucesiones extremales que no poseen tales subsucesiones de suma 0.

Estas preguntas surgen naturalmente en contextos muy variados, principalmente en las áreas de combinatoria, teoría de números y geometría. Para mayores detalles sobre estas conexiones se puede consultar [GG06].

El menos restrictivo de estos problemas de suma cero fue planteado por Harold Davenport en 1966, y corresponde a hallar el menor ℓ tal que toda sucesión en G de longitud ℓ contiene alguna subsucesión de suma 0, sin imponer condiciones sobre la longitud de la subsucesión o la multiplicidad de sus elementos. En la literatura posterior, dicho entero ℓ recibe el nombre de *constante de Davenport* del grupo G, y se lo denota $D(G)$.

Calcular $D(G)$ en términos de los factores invariantes de G es un problema que permanece abierto hasta el día de hoy, habiendo sido resuelto sólo en casos muy particulares, entre los que se destacan los p-grupos y los grupos de rango menor o igual que 2. Por otra parte, existen infinitos ejemplos de grupos para los cuales la mejor cota inferior que se conoce para $D(G)$ no es óptima. Sin embargo, todos ellos tienen rango mayor o igual que 4. Es por eso que el caso de rango 3 resulta particularmente atractivo, pues se conjetura que la respuesta obedece a la misma fórmula en todos los casos.

En el influyente artículo [vEB69], van Emde Boas plantea la posibilidad de usar métodos inductivos para obtener progresos en este problema a partir de la resolución

de cierto problema inverso en rango 2, particularmente sobre grupos de la forma $\mathbb{Z}_p \oplus \mathbb{Z}_p$ con p primo. En caso de que el primo p se comporte de acuerdo a lo esperado por van Emde Boas, se dice que p tiene la *Propiedad C*. Inmediatamente surge la conjetura de que todos los primos tienen esta propiedad.

A fines de la década del 90 y principios de este siglo, autores como Gao y Geroldinger [GG99, Gao00] retoman el trabajo iniciado por van Emde Boas, probando varios resultados condicionales que dependen del hecho de que los divisores primos de las constantes relevantes tengan la Propiedad C. Estos resultados adquieren mayor entidad en 2010, cuando Reiher prueba en su tesis de doctorado [Rei10] un teorema que implica que todo número primo tiene la Propiedad C.

Este trabajo fue realizado con el objetivo de estudiar el estado actual del problema de Davenport para grupos de rango 3. Sin embargo, como el lector pronto descubrirá, hacer esto requiere familiarizarse con otros problemas de suma cero relacionados, tanto directos como inversos.

La tesis está organizada de la siguiente manera.

En el **Capítulo 1** mencionamos los primeros resultados que se obtuvieron desde la formulación original del problema. En particular, incluimos demostraciones de los teoremas que calculan el valor de $D(G)$ para p-grupos y grupos de rango 2, ambos debidos a Olson.

En el **Capítulo 2** introducimos una poderosa herramienta conocida con el nombre de *Combinatorial Nullstellensatz*, que se puede ver como una generalización al caso multivariado del hecho de que un polinomio de grado n en una variable tiene a lo sumo n raíces. Este teorema, de 1999, inaugura un nuevo arsenal de métodos algebraicos para atacar problemas combinatorios, al traducir la información relevante del problema a una condición sobre el conjunto de ceros de un cierto polinomio. En particular, este teorema resulta ser uno de los pilares de la demostración del teorema de Reiher.

En el **Capítulo 3** discutimos la noción de problemas inversos en este contexto. Mostramos el trabajo hecho por van Emde Boas, damos la definición de las propiedades B y C para números primos, y explicamos cómo se pueden obtener avances en nuestro problema de interés usando estas nociones. Finalmente probamos que la Propiedad B es más fuerte que la Propiedad C.

Por último, en el **Capítulo 4** reproducimos y explicamos la demostración de Reiher de que todo número primo tiene la Propiedad B, comentando las herramientas elementales de geometría algebraica introducidas para tal fin, y mostramos cómo esto se puede combinar con los resultados del capítulo anterior para calcular $D(G)$ en el caso particular en que G es un grupo de rango 3 cuyo primer factor invariante es igual a 2.

Capítulo 1

Resultados clásicos sobre $D(G)$

Todos los grupos que aparecen en esta tesis son abelianos, finitos, y usan notación aditiva (denotamos + a la operación del grupo y 0 a su elemento neutro). En adelante, siempre que hablemos de «grupo» a secas, estaremos asumiendo tácitamente que se cumplen todas estas hipótesis adicionales.

1.1. Primeras definiciones y ejemplos

Definición 1.1.1. Sea G un grupo. La *constante de Davenport* de G, que denotamos $D(G)$, se define como el menor entero positivo ℓ con la siguiente propiedad: toda sucesión de longitud ℓ de elementos de G contiene una subsucesión (no vacía) cuyos elementos suman 0.
(Notar que todo número mayor que $D(G)$ también tiene esta propiedad.)

Aquí, la palabra «sucesión» se corresponde con la noción de *multiconjunto*, es decir, una colección no ordenada de elementos de G entre los cuales puede haber repetidos. Por el momento, denotaremos una sucesión genérica como $(g_1, g_2, \ldots, g_\ell)$, a pesar de que esto puede dar la falsa idea de que el orden de los elementos es relevante. Mejoraremos la notación más adelante.

El problema de calcular $D(G)$ fue propuesto por Harold Davenport en 1966, motivado por la siguiente conexión con la teoría de números: si K es un cuerpo de números y G es su grupo de clases, entonces $D(G)$ es el máximo número de ideales primos (contados con multiplicidad) que pueden aparecer en la descomposición de un irreducible.

Para ir fijando ideas, veamos cómo calcular $D(G)$ en el caso más simple posible, que es cuando G es un grupo cíclico.

Proposición 1.1.2. $D(\mathbb{Z}_n) = n$.

Demostración. Es claro que la sucesión formada por el elemento 1 repetido $n-1$ veces no tiene subsucesiones de suma 0. Por lo tanto, $D(G) \geq n$.

Para la otra desigualdad, sea $S = (g_1, g_2, \ldots, g_n)$ una sucesión de longitud n. Probaremos que S tiene alguna subsucesión de suma 0. Consideramos los elementos

$$\begin{aligned} s_1 &= g_1, \\ s_2 &= g_1 + g_2, \\ s_3 &= g_1 + g_2 + g_3, \\ &\vdots \\ s_n &= g_1 + g_2 + g_3 + \ldots + g_n. \end{aligned}$$

Si algún s_k es igual a 0, ya tenemos lo que buscábamos. Si no, como hay n números s_k y solamente $n-1$ posibles valores para los mismos, por el principio del palomar debe haber dos índices distintos $i < j$ tales que $s_i = s_j$. Pero entonces la subsucesión $(g_{i+1}, \ldots, g_j)$ tiene suma 0, así que también en este caso cumplimos el objetivo. □

Los mismos argumentos de la demostración anterior sirven para obtener cotas para $D(G)$ en el caso general. Recordemos que todo grupo abeliano finito G es isomorfo a un único grupo de la forma $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r}$ donde los n_i son enteros mayores o iguales que 2 que satisfacen $n_1 \mid n_2 \mid \ldots \mid n_r$. Los números n_i se llaman los *factores invariantes* de G, y la cantidad de sumandos r es el *rango* de G.

En el grupo $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r}$ hay una sucesión de longitud $\sum_{j=1}^{r}(n_j - 1)$ que no tiene subsucesiones de suma 0: si llamamos, como es habitual, e_j al elemento que tiene un 1 en la j-ésima coordenada y 0 en las restantes, la sucesión S en la cual cada e_j aparece repetido $n_j - 1$ veces tiene la propiedad deseada. De esto deducimos que

$$D(G) \geq 1 + \sum_{j=1}^{r}(n_j - 1)$$

para todo grupo G. A la cantidad del miembro derecho de la desigualdad la denotamos $M(G)$.[1]

Por otra parte, repitiendo textualmente la demostración de 1.1.2 se obtiene que $|G|$ es una cota superior para $D(G)$. Hemos probado entonces:

[1] En ocasiones nos resultará conveniente admitir la posibilidad de que algunos de los (primeros) factores invariantes de G sean iguales a 1. Con esto se pierde la unicidad de la descomposición $G \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r}$, pues podemos agregar tantas copias de $\mathbb{Z}/1\mathbb{Z} = \{0\}$ a la izquierda como queramos. Sin embargo, el valor de $M(G)$ sigue estando bien definido incluso haciendo esta salvedad.

Proposición 1.1.3. *Para todo grupo G, se tienen las desigualdades*

$$M(G) \leq D(G) \leq |G|.$$

En la sección 1.6 veremos que la cota superior $|G|$ se puede mejorar sustancialmente si G no es cíclico.

El primer avance significativo en el problema de calcular $D(G)$ se debe a John Olson, que en 1968 probó que la cota inferior $M(G)$ es óptima si G es un p-grupo o $\text{rango}(G) = 2$. Estos resultados están publicados en [Ols69a] y [Ols69b] respectivamente.

1.2. p-grupos

La principal herramienta que permite resolver el problema en el caso en el que G es un p-grupo son las buenas propiedades del álgebra de grupo $\mathbb{F}_p[G]$. Recordemos que esta álgebra se puede describir como un $\mathbb{F}_p$-espacio vectorial de dimensión $|G|$, con base $\{u_g\}_{g\in G}$, en la cual la multiplicación se define a partir de las relaciones $u_g \cdot u_h := u_{g+h}$ para todos $g, h \in G$, y extendiendo linealmente. De este modo, u_0 resulta ser el elemento neutro para $\cdot$, y podemos pensar a $\mathbb{F}_p$ dentro de $\mathbb{F}_p[G]$ vía $\lambda \mapsto \lambda \cdot u_0$.

A continuación enlistamos algunas de estas propiedades elementales que precisaremos para probar el primer teorema de Olson. En lo sucesivo, siempre denotaremos $n_1, n_2, \ldots, n_r$ a los factores invariantes de G, y $\{e_1, e_2, \ldots, e_r\}$ será un sistema de generadores de G tal que $\text{ord}(e_j) = n_j$ para todo j. (La existencia de tal sistema de generadores es obvia a partir del isomorfismo $G \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r}$.)

Proposición 1.2.1. *Sea $g \in G$ y sea m un entero mayor o igual que $\text{ord}(g)$. Entonces, en $\mathbb{F}_p[G]$ vale la igualdad $(1 - u_g)^m = 0$.*

Demostración. Basta verlo para $m = \text{ord}(g)$. En este caso m es una potencia de p; como estamos en un anillo de característica p resulta

$$(1 - u_g)^m = 1^m - u_g^m = 1 - u_{mg} = 1 - u_0 = 0. \qquad \square$$

Proposición 1.2.2. *El conjunto*

$$B = \left\{ \prod_{j=1}^{r} \left(1 - u_{e_j}\right)^{m_j} \;\middle|\; 0 \leq m_j < n_j \text{ para todo } j \in [\![1, r]\!] \right\}$$

es una base de $\mathbb{F}_p[G]$ como $\mathbb{F}_p$-espacio vectorial.

Demostración. Notemos que el cardinal de B es $\prod_{j=1}^{r} n_j = |G|$, que coincide con la dimensión del espacio. Por lo tanto, para ver que es base basta probar que es un sistema de generadores.

Sea

$$B' = \left\{ \prod_{j=1}^{r} \left(1 - u_{e_j}\right)^{m_j} \;\middle|\; m_j \in \mathbb{N}_0 \text{ para todo } j \in [\![1, r]\!] \right\}.$$

De 1.2.1 se deduce que los elementos de B' que no están en B son todos iguales a 0, así que bastará probar que B' es un sistema de generadores.

Sea $S' = \langle B' \rangle_{\mathbb{F}_p}$. Como B' es multiplicativamente cerrado, también lo es S'. Ahora, $1 \in B'$ (tomar $m_j = 0$ para todo j) y también $1 - u_{e_j} \in B'$ para todo j. De esto se deduce que $u_{e_j} \in S'$ para todo j. Como los e_j generan G, resulta que todo u_g se puede escribir como producto de elementos de la forma u_{e_j}. Entonces todos los u_g están en S', y por lo tanto B' genera $\mathbb{F}_p[G]$, como queríamos. □

Consideremos $\varepsilon : \mathbb{F}_p[G] \to \mathbb{F}_p$ definido por

$$\varepsilon\left(\sum_{g \in G} \lambda_g u_g\right) = \sum_{g \in G} \lambda_g.$$

Es fácil verificar que ε es un morfismo de $\mathbb{F}_p$-álgebras. Se lo conoce como *morfismo de aumentación.*

A partir de la proposición anterior se obtiene fácilmente el siguiente resultado.

Corolario 1.2.3. *$B \setminus \{1\}$ es una base de* $\ker(\varepsilon)$.

Demostración. Como ε no es el morfismo nulo (por ejemplo porque $\varepsilon(u_g) = 1$ para todo $g \in G$), es sobreyectivo; luego por el teorema de la dimensión su núcleo será un subespacio de dimensión $|G| - 1$.

Es evidente que $1 - u_g \in \ker(\varepsilon)$ para todo $g \in G$. Como ε es multiplicativa, resulta que todos los elementos de B, exceptuando el 1 que corresponde a elegir $m_j = 0$ para todo j, están en $\ker(\varepsilon)$. Obtuvimos así $|G| - 1$ elementos linealmente independientes en $\ker(\varepsilon)$: necesariamente son una base. □

Antes de continuar, introducimos un poco de notación que nos resultará práctica más adelante.

Dada una sucesión $S = (g_1, g_2, \ldots, g_\ell)$ de elementos de G, denotamos

$$\sigma(S) = \sum_{i=1}^{\ell} g_i$$

a la suma de los elementos de S, y

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \;\middle|\; \varnothing \neq I \subset [\![1, \ell]\!] \right\}$$

al *conjunto de subsumas* de S. Con esta notación, nuestro problema consiste en hallar la menor longitud ℓ que permite garantizar que $0 \in \Sigma(S)$.

Dada S como antes, un elemento $g \in G$ y un $k \in \mathbb{N}_0$, definimos

$$N_g^k(S) = \left| \left\{ I \subset [\![1, \ell]\!] \;\middle|\; \sum_{i \in I} g_i = g,\ |I| = k \right\} \right|,$$

es decir, $N_g^k(S)$ cuenta la cantidad de subsucesiones de S de longitud k cuya suma es igual a g. (Consideramos que la subsucesión vacía tiene suma 0.) En caso de que no nos interese la longitud de la subsucesión, o que sólo nos interese si dicha longitud es par o impar, usaremos las notaciones

$$N_g(S) = \sum_{k \in \mathbb{N}_0} N_g^k(S), \qquad N_g^+(S) = \sum_{k \in \mathbb{N}_0} N_g^{2k}(S), \qquad N_g^-(S) = \sum_{k \in \mathbb{N}_0} N_g^{2k+1}(S).$$

La idea clave de la demostración de Olson consiste en asignarle a cada sucesión S un elemento de $\mathbb{F}_p[G]$, al que llamaremos $f(S)$, definido por

$$f(S) = \prod_{g \in S} (1 - u_g) = \sum_{g \in G} \lambda_g(S) u_g.$$

La siguiente proposición muestra cómo $f(S)$ codifica información sobre las subsumas de S.

Proposición 1.2.4. *Para cualquier $g \in G$, el coeficiente correspondiente a u_g en $f(S)$, al que denotamos $\lambda_g(S)$, es igual a $\overline{N_g^+(S) - N_g^-(S)}$. (Aquí $\overline{a}$ denota la clase de congruencia del entero a módulo p.)*
En particular,

$$\lambda_0(S) \neq 1 \implies 0 \in \Sigma(S),$$

y si $g \neq 0$, entonces

$$\lambda_g(S) \neq 0 \implies g \in \Sigma(S).$$

Demostración. Al expandir el producto que define a $f(S)$ nos queda una suma de términos de la forma $(-1)^{|I|} \prod_{i \in I} u_{g_i} = (-1)^{|I|} u_s$, donde $s = \sum_{i \in I} g_i$, e I recorre todos los subconjuntos de $[\![1, \ell]\!]$. Por eso cada subsucesión de suma s aporta 1 al coeficiente correspondiente si la longitud de la subsucesión es par y -1 si la longitud es impar.

Para la segunda parte, notemos que $N_0^+(S) \geq 1$ para toda sucesión S (pues la subsucesión vacía tiene suma 0). En caso de que $0 \notin \Sigma(S)$, tenemos $N_0^+(S) = 1$ y $N_0^-(S) = 0$, de donde $\lambda_0(S) = 1$. Por contrarrecíproco, esto prueba la primera implicación. Análogamente, si para algún $g \neq 0$ se tiene $g \notin \Sigma(S)$, es

$$N_g^+(S) = N_g^-(S) = 0,$$

lo cual implica $\lambda_g(S) = 0$. □

Ya estamos en condiciones de probar el teorema de Olson para p-grupos.

Teorema 1.2.5. *Si G es un p-grupo, entonces $D(G) = M(G)$.*

Demostración. Ya sabemos que $D(G) \geq M(G)$, así que sólo tenemos que probar que toda sucesión de longitud $M(G)$ tiene una subsucesión de suma 0. Probaremos que, de hecho, para toda sucesión S de longitud $M(G)$ se tiene que $f(S) = 0$; luego por 1.2.4 podremos concluir que $0 \in \Sigma(S)$.

Notemos que cada factor $1 - u_g$ que aparece en la definición de $f(S)$ está en el núcleo del morfismo de aumentación. Entonces, por 1.2.3 resulta que cada uno de ellos se puede escribir como una combinación lineal de elementos de la forma $\prod_{j=1}^r \left(1 - u_{e_j}\right)^{m_j}$ donde al menos uno de los m_j es no nulo. Si ahora reemplazamos cada factor $1 - u_g$ por su combinación lineal correspondiente y expandimos el producto, el resultado termina siendo una combinación lineal de elementos de la misma forma, donde ahora $m_1 + m_2 + \ldots + m_r \geq \ell$, pues cada factor aporta al menos 1 a la suma de los exponentes.

Supongamos que $\ell = M(G)$. Como $\ell > \sum_{j=1}^r (n_j - 1)$, en la situación anterior debe existir algún j tal que $m_j \geq n_j$. Ahora 1.2.1 implica que

$$\prod_{j=1}^{r} \left(1 - u_{e_j}\right)^{m_j} = 0.$$

Como esto vale para todos los sumandos que aparecen en la combinación lineal, obtenemos $f(S) = 0$, como queríamos probar. □

1.3. El método inductivo

Tanto la demostración del teorema de Olson para grupos de rango 2 como varios de los resultados posteriores utilizan una línea de pensamiento que en la literatura se conoce como el *método inductivo*. No hay una definición precisa de qué es lo que esto significa, pero podemos explicar brevemente cuál es la idea principal subyacente.

Consideremos una sucesión exacta corta de grupos abelianos

$$0 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} Q \longrightarrow 0.$$

Dada una sucesión S de longitud ℓ en G, podemos considerar en Q la sucesión $\beta(S)$, obtenida aplicando β a cada elemento de S, que tiene la misma longitud. Supongamos que ℓ es lo suficientemente grande como para poder extraer con certeza k subsucesiones disjuntas de $\beta(S)$ que tienen suma 0. Podemos obtener entonces k subsucesiones disjuntas de S, digamos $S_1, S_2, \ldots, S_k$, con la propiedad de que $\sigma(S_j) \in \ker(\beta)$ para todo j. Por la exactitud de la sucesión, existen elementos $h_1, h_2, \ldots, h_k \in H$ tales que $\alpha(h_j) = \sigma(S_j)$ para todo j. Ahora consideramos la sucesión $(h_1, h_2, \ldots, h_k)$ en el grupo H. Si k es suficientemente grande, existirá algún subconjunto $\varnothing \neq I \subset [\![1, k]\!]$ tal que $\sum_{i\in I} h_i = 0$. Luego, la sucesión T que se obtiene uniendo las sucesiones S_i tales que $i \in I$ resulta ser una subsucesión de suma 0 de S.

Este razonamiento nos permite obtener cotas para $D(G)$ a partir de la resolución de problemas similares en los grupos H y Q, que se asume que serán más fáciles de manejar.

Con esta breve discusión ya podemos darnos cuenta de que existen otros invariantes, similares en espíritu a la constante de Davenport, cuyo estudio puede resultar útil para resolver el problema que nos convoca.

Definición 1.3.1. Para cada $k \in \mathbb{N}$, denotamos $D_k(G)$ al menor entero positivo ℓ con la siguiente propiedad: de toda sucesión de longitud ℓ de elementos de G se pueden extraer k subsucesiones disjuntas de suma 0.
(Observar que D_1 es simplemente la constante de Davenport.)

Ahora es claro que lo comentado al principio de esta sección nos da una demostración de la siguiente proposición.

Proposición 1.3.2. *Dada una sucesión exacta corta*

$$0 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} Q \longrightarrow 0,$$

se tiene la desigualdad $D(G) \leq D_{D(H)}(Q)$.

Para que este método tenga éxito necesitamos poder dar buenas cotas para los invariantes D_k.

Es obvio que $D_k(G) \leq kD(G)$. Para grupos cíclicos, esta cota es de hecho óptima, lo cual se puede probar considerando una sucesión formada exclusivamente por elementos iguales a 1. Pero no ocurre lo mismo con grupos de rango mayor.

Para ilustrar este fenómeno, vamos a considerar el ejemplo más sencillo posible. Supongamos que $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, y estamos interesados en calcular $D_2(G)$. Como G es un 2-grupo, ya conocemos el valor de $D(G)$, que en este caso es 3. La cota obvia nos dice entonces que $D_2(G) \leq 6$. Veamos que de hecho es $D_2(G) \leq 5$. En efecto, como G tiene 4 elementos, por el principio del palomar en cualquier sucesión de longitud 5

habrá dos elementos que son iguales. Esos dos elementos forman una subsucesión de suma 0. Como $D(G) = 3$, de los elementos restantes podemos extraer una segunda subsucesión de suma 0, cumpliendo así el objetivo.

Lo que sucedió aquí es que aprovechamos el hecho de que la sucesión era lo suficientemente larga como para poder garantizar no solamente la existencia de una subsucesión de suma 0, sino que además podíamos conseguir una de *longitud acotada* (en este caso la longitud era exactamente igual a 2, pero un menor o igual ya nos habría bastado para el argumento), más corta que lo que obtendríamos si sólo usamos que $\ell \geq D(G)$. Se vuelve evidente entonces que, en general, saber cuándo podemos asegurar la existencia de subsucesiones «cortas» de suma 0 nos permitirá obtener mejores cotas para $D_k(G)$.

Posiblemente lo primero que tendríamos que preguntarnos es cuándo una subsucesión califica para que digamos que es corta. Notemos que en general uno no puede pretender encontrar subsucesiones de suma 0 de longitud menor que $\exp(G)$: basta considerar una sucesión formada por un elemento de orden máximo repetido muchas veces. Por este motivo, diremos que una sucesión de suma 0 es *corta* si su longitud es menor o igual que $\exp(G)$.

Definición 1.3.3. Denotamos $\eta(G)$ al menor entero positivo ℓ con la siguiente propiedad: toda sucesión de longitud ℓ de elementos de G contiene una subsucesión corta de suma 0.

La siguiente proposición nos da una forma de acotar los números $D_k(G)$, que usaremos para probar el segundo teorema de Olson.

Proposición 1.3.4. *Si G satisface $\eta(G) \leq D(G) + \exp(G)$, entonces para todo $k \in \mathbb{N}$ se tiene $D_k(G) \leq D(G) + (k-1)\exp(G)$.*

Demostración. Procedemos por inducción en k. Si $k = 1$, trivialmente vale la igualdad y no hay nada que probar. Supongamos que para cierto $k \geq 1$ se cumple $D_k(G) \leq D(G) + (k-1)\exp(G)$, y consideremos una sucesión S de longitud $\ell = D(G) + k\exp(G)$.

Tenemos que $\ell \geq D(G) + \exp(G) \geq \eta(G)$, por lo tanto, podemos extraer una subsucesión de suma 0 de longitud menor o igual que $\exp(G)$. La cantidad de elementos restantes es por lo menos $D(G) + (k-1)\exp(G)$, que por hipótesis inductiva es mayor o igual que $D_k(G)$. Entonces, con estos elementos que sobran podemos obtener k subsucesiones disjuntas de suma 0.

En definitiva conseguimos extraer $k+1$ subsucesiones disjuntas de suma 0, con lo cual $D_{k+1}(G) \leq D(G) + k\exp(G)$. Esto completa el paso inductivo. □

Observación 1.3.5. Consideremos la sucesión S que tiene $n_j - 1$ copias de cada elemento e_j con $j < r$, y $n_r - 1 + (k-1)n_r = k\exp(G) - 1$ copias del elemento e_r.

Es fácil ver que si T es una subsucesión de suma 0 de S, entonces T no contiene a ninguno de los e_j con $j < r$ (porque no hay suficiente cantidad de ellos como para llegar a sumar 0 en esa coordenada). Entonces todas las subsucesiones de suma 0 que se pueden extraer de S se obtienen usando las copias del elemento e_r. Ahora es claro que no se pueden extraer k subsucesiones disjuntas. Esto prueba que $D_k(G) \geq M(G) + (k-1)\exp(G)$. Luego, para grupos G tales que $D(G) = M(G)$, vale la igualdad en 1.3.4.

1.4. Grupos de rango 2

En esta sección usaremos las ideas del método inductivo para probar que la igualdad $D(G) = M(G)$ se cumple para todo grupo G de rango 2. En la demostración usaremos una sucesión exacta corta en la cual Q es un grupo de la forma $\mathbb{Z}_p \oplus \mathbb{Z}_p$ con p primo. El ingrediente que falta, entonces, es saber acotar $D_k(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ para todo k.

Proposición 1.4.1. *Para todo primo p se tiene que $\eta(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 3p - 2$.*

Demostración. Consideremos la sucesión S de longitud $3p-3$ formada por los elementos $(1,0)$, $(0,1)$ y $(1,1)$, repetidos $p-1$ veces cada uno. Supongamos que S tiene una subsucesión corta de suma 0, entonces existen enteros $0 \leq a, b, c \leq p-1$, con $0 < a+b+c \leq p$, tales que $a+c$ y $b+c$ son múltiplos de p. Se deduce inmediatamente que $a = b$. Ahora, $a+c$ es múltiplo de p pero $a+b+c \leq p$, así que $a+c$ sólo puede ser 0 o p. Si es 0, entonces $a = b = c = 0$, absurdo; si es p, entonces $b = 0$, de donde nuevamente se deduce $a = c = 0$. Esto prueba que $\eta(\mathbb{Z}_p \oplus \mathbb{Z}_p) \geq 3p - 2$.

Veamos ahora que $3p-2$ elementos son suficientes para garantizar la existencia de una subsucesión corta de suma 0.

Sea $S = (g_1, g_2, \ldots, g_{3p-2})$ una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Para cada j, consideramos el elemento $g_j^* = (g_j, 1) \in \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Tenemos así una sucesión de longitud $3p-2$ en $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Pero por el Teorema 1.2.5 sabemos que la constante de Davenport de este grupo es precisamente $3p-2$. Entonces, existe $\varnothing \neq I \subset [\![1, 3p-2]\!]$ tal que $\sum_{i \in I} g_i^* = (0,0,0)$. Mirando la tercera coordenada deducimos que $|I|$ debe ser múltiplo de p, así que sólo puede ser p o $2p$.

Si es p, ya cumplimos el objetivo pues los g_i con $i \in I$ forman una subsucesión de suma 0 de longitud p.

Si es $2p$, como $D(\mathbb{Z}_p \oplus \mathbb{Z}_p) < 2p$, la sucesión $(g_i)_{i \in I}$ tiene una subsucesión **propia** de suma 0. Entonces, o bien ella o su complemento es una subsucesión de S de suma 0 de longitud menor o igual que p, y cumplimos el objetivo. □

Corolario 1.4.2. *Para todo $k \in \mathbb{N}$ se tiene que $D_k(\mathbb{Z}_p \oplus \mathbb{Z}_p) = (k+1)p - 1$.*

Demostración. Llamamos $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Como

$$\eta(G) = 3p - 2 < 3p - 1 = D(G) + p,$$

estamos en las hipótesis de la Proposición 1.3.4. Más aún, como G es un p-grupo, se cumple que $D(G) = M(G)$, y entonces la Observación 1.3.5 nos dice el valor exacto de $D_k(G)$. En definitiva,

$$D_k(G) = D(G) + (k-1)\exp(G) = 2p - 1 + (k-1)p = (k+1)p - 1,$$

como queríamos. □

Juntando todo, obtenemos el teorema anunciado.

Teorema 1.4.3. *Sea $G = H \oplus K$ con H y K abelianos de órdenes h y k respectivamente, tales que $h \mid k$. Entonces $D(G) \leq h + k - 1$.*
(En particular, para $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ obtenemos $D(G) \leq n_1 + n_2 - 1 = M(G)$, así que, como ya teníamos la otra desigualdad, resulta $D(G) = M(G)$ para todo grupo G de rango 2.)

Demostración. La demostración es por inducción en h. Si $h = 1$, entonces lo que debemos probar equivale a que $D(K) \leq k$, que es la primera cota que probamos. Supongamos entonces que $h > 1$ y que ya probamos el teorema para valores menores de h. Sea p un primo que divide a h, entonces también divide a k. Tomamos subgrupos $H_1 \leq H$ y $K_1 \leq K$ de índice p, y consideramos la sucesión exacta corta

$$0 \longrightarrow H_1 \oplus K_1 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow 0.$$

Usando la Proposición 1.3.2 y el Corolario 1.4.2 obtenemos

$$D(G) \leq D_{D(H_1 \oplus K_1)}(\mathbb{Z}_p \oplus \mathbb{Z}_p) \leq [D(H_1 \oplus K_1) + 1]\, p - 1. \tag{1.1}$$

Ahora, por hipótesis inductiva es

$$D(H_1 \oplus K_1) \leq |H_1| + |K_1| - 1 = \frac{h+k}{p} - 1.$$

Reemplazando esto en (1.1) obtenemos

$$D(G) \leq \left[\frac{h+k}{p} - 1 + 1\right] p - 1 = h + k - 1,$$

como queríamos probar. □

Para terminar esta sección, mostramos cómo se puede deducir del teorema anterior un clásico resultado en teoría de suma cero, conocido como el Teorema EGZ (nombrado así por las iniciales de Erdös, Ginzburg y Ziv). La demostración original (que no usa estas herramientas) data de 1961 y se puede consultar en [EGZ61]. Recomendamos también el artículo [AD93], que recopila cinco demostraciones distintas de dicho teorema, incluyendo la que aquí presentamos.

Teorema 1.4.4. *Dados $2n-1$ números enteros, se pueden elegir n de ellos tales que su suma sea un múltiplo de n.*

Demostración. El teorema es equivalente a probar que toda sucesión de longitud $2n-1$ en $\mathbb{Z}_n$ contiene una subsucesión de suma 0 de longitud n.

Dada una sucesión $(g_1, g_2, \ldots, g_{2n-1})$, para cada j consideramos el elemento

$$g_j^* = (g_j, 1) \in \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Por el Teorema 1.4.3 sabemos que

$$D(\mathbb{Z}_n \oplus \mathbb{Z}_n) = M(\mathbb{Z}_n \oplus \mathbb{Z}_n) = 2n-1,$$

de modo que la sucesión $(g_1^*, g_2^*, \ldots, g_{2n-1}^*)$ posee alguna subsucesión de suma 0. Mirando la segunda coordenada deducimos que la longitud de esta subsucesión tiene que ser un múltiplo de n. Como es menor que $2n$, debe ser exactamente n, y el teorema sigue. □

1.5. Contraejemplos de rango mayor que 3

Luego de probar los teoremas vistos en las secciones anteriores, Olson conjeturó que la igualdad $D(G) = M(G)$ valía para todo grupo G. Hoy sabemos que esto no es cierto, pero aún quedan muchas preguntas por responder. No se tiene una descripción satisfactoria de los grupos que sí verifican la igualdad. Tampoco se sabe si existe algún contraejemplo con G de rango 3.

En esta sección veremos que para todo $r \geq 4$ existen infinitos grupos G de rango r tales que $D(G) > M(G)$.

En realidad, basta con resolver el caso $r = 4$, como muestra la siguiente proposición.

Proposición 1.5.1. *Sea $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r}$, con $n_1 \mid n_2 \mid \ldots \mid n_r$, y sea $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_s}$, con $m_1 \mid m_2 \mid \ldots \mid m_s$, tales que existen índices $1 \leq i_1 < i_2 < \ldots < i_r \leq s$ con $m_{i_j} = n_j$ para todo j. (En otras palabras, G_1 contiene a todos los factores invariantes de G entre sus factores invariantes.)*
Si $D(G) > M(G)$, entonces también $D(G_1) > M(G_1)$.

Demostración. Podemos escribir $G_1 = G \oplus G'$, donde G' reúne los factores invariantes de G_1 que no están en G. Notar que entonces

$$M(G_1) = M(G) + M(G') - 1.$$

Por otra parte, el hecho de que existan sucesiones sin subsucesiones de suma 0 en G y G' de longitudes $D(G) - 1 \geq M(G)$ y $D(G') - 1 \geq M(G') - 1$ implica que

$$D(G_1) > M(G) + M(G') - 1 = M(G_1),$$

como queríamos probar. □

En la literatura existen numerosas familias de contraejemplos a la conjetura de Olson (ver por ejemplo [GS92], [GG99, Teorema 3.3]). Mostraremos sólo una de ellas.

Proposición 1.5.2. *Sea $G = \mathbb{Z}_m \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \mathbb{Z}_{2n}$, con m, n impares tales que $m \mid n$. Entonces $D(G) > M(G)$.*

Demostración. Tenemos que

$$M(G) = 1 + (m-1) + (n-1) + (n-1) + (2n-1) = m + 4n - 3.$$

Exhibiremos una sucesión S de longitud $m+4n-3$ que no contiene subsucesiones de suma 0.

Consideramos la sucesión S que consiste de los siguientes 7 elementos, cada uno con la multiplicidad especificada.

$g_1 = (-1, 1, 1, 1)$	$m-1$ veces
$g_2 = (1, -1, 1, 1)$	$n-1$ veces
$g_3 = (1, 1, -1, 1)$	$n-1$ veces
$g_4 = (-1, 1, 1, -1)$	$n-1$ veces
$g_5 = (1, 1, 1, 1)$	$n-1$ veces
$g_6 = (0, 1, 2-m, 2-m)$	1 vez
$g_7 = (0, 2-m, 1, 2-m)$	1 vez

Si S tuviera alguna subsucesión de suma 0, significa que existen enteros no negativos $a_1, a_2, \ldots, a_7$, con $a_1 \leq m-1$; $a_2, a_3, a_4, a_5 \leq n-1$; $a_6, a_7 \leq 1$, no todos nulos, tales que $\sum_{i=1}^{7} a_i g_i = (0, 0, 0, 0)$. Es decir que los a_i satisfacen las siguientes cuatro ecuaciones de congruencia:

$$\begin{cases} -a_1 + a_2 + a_3 - a_4 + a_5 \equiv 0 \pmod{m} \\ a_1 - a_2 + a_3 + a_4 + a_5 + a_6 + (2-m)a_7 \equiv 0 \pmod{n} \\ a_1 + a_2 - a_3 + a_4 + a_5 + (2-m)a_6 + a_7 \equiv 0 \pmod{n} \\ a_1 + a_2 + a_3 - a_4 + a_5 + (2-m)a_6 + (2-m)a_7 \equiv 0 \pmod{2n} \end{cases}$$

Restando la tercera ecuación con la segunda obtenemos

$$2a_2 - 2a_3 + (1-m)a_6 - (1-m)a_7 \equiv 0 \pmod{n}. \tag{1.2}$$

Por otra parte, como m divide a $2n$, en la cuarta ecuación también podemos afirmar que el miembro izquierdo es congruente a 0 módulo m. Cancelando los múltiplos de m que hay en el miembro izquierdo, y restando esto con la primera ecuación, obtenemos que

$$2a_1 + 2a_6 + 2a_7 \equiv 0 \pmod{m},$$

que como m es impar es equivalente a

$$a_1 + a_6 + a_7 \equiv 0 \pmod{m}. \tag{1.3}$$

Ahora consideramos dos casos, según si a_6 y a_7 son iguales o distintos.

Caso 1: $a_6 = a_7$.

En este caso (1.2) se simplifica a que $n \mid 2(a_2 - a_3)$, y como n es impar y a_2, a_3 son menores que n, deducimos que $a_2 = a_3$.

Por otra parte, (1.3) se traduce en que $a_1 \equiv -2a_6 \pmod{m}$. Recordando que a_6 vale 0 o 1, concluimos que $a_1 = (m-2)a_6$.

Usando toda esta información, la segunda ecuación de nuestro sistema original nos dice que $a_4 + a_5 + a_6 \equiv 0 \pmod{n}$. Pero esta suma es menor o igual que $(n-1) + (n-1) + 1 < 2n$, así que sólo puede ser 0 o n.

Si es 0, significa que $a_4 = a_5 = a_6 = 0$. Como estamos suponiendo que $a_6 = a_7$, también es $a_7 = 0$, y como vimos que $a_1 = (m-2)a_6$, es $a_1 = 0$. Entonces ahora la cuarta ecuación dice simplemente que $a_2 + a_3$ es múltiplo de $2n$. Pero estos números no pueden ser ambos nulos, y cada uno de ellos es menor que n. Absurdo.

Si en cambio $a_4 + a_5 + a_6 = n$, en particular es $a_4 + a_5 + a_6 \equiv n \pmod{2n}$. Sumamos esto con la cuarta ecuación de nuestro sistema original y obtenemos $2a_2 + 2a_5 + (1-m)a_6 \equiv n \pmod{2n}$, que es imposible porque el lado izquierdo es par y el lado derecho es impar.

Caso 2: $a_6 \neq a_7$.

Por simetría basta considerar el caso en el que $a_6 = 1$, $a_7 = 0$. La ecuación (1.3) ahora implica que $a_1 \equiv -1 \pmod{m}$, y como $a_1 \in [\![0, m-1]\!]$ necesariamente es $a_1 = m - 1$.

Por otra parte, restando la cuarta ecuación del sistema original con la tercera obtenemos que $2a_3 - 2a_4 \equiv 0 \pmod{n}$, de donde $a_3 = a_4$.

Usando toda esta información, la cuarta ecuación de nuestro sistema original nos dice que $(m-1) + a_2 + a_5 + (2-m) = a_2 + a_5 + 1 \equiv 0 \pmod{2n}$. Esto es imposible pues $a_2, a_5 \leq n-1$ y por lo tanto $0 < a_2 + a_5 + 1 < 2n$. La demostración está completa. □

1.6. Otra cota superior para $D(G)$

Para terminar este capítulo probaremos una cota superior para $D(G)$ que es significativamente mejor que la única que teníamos hasta ahora, i.e., $D(G) \leq |G|$. Para ello necesitaremos algunos resultados propios de la teoría de caracteres.

Definición 1.6.1. Sea G un grupo abeliano finito. Un *caracter* de G es un morfismo de grupos $\chi : G \to \mathbb{C}^\times$. Al conjunto de todos los caracteres de G lo denotamos $\widehat{G}$.

Es cuestión de rutina verificar que el producto de dos caracteres de G (definido punto a punto) es también un caracter de G. Más aún, como $z \mapsto z^{-1}$ es un automorfismo de $\mathbb{C}^\times$, vemos que todo caracter tiene inverso respecto de esta operación. En otras palabras, $\widehat{G}$ tiene una estructura de grupo abeliano.

Las siguientes propiedades sobre caracteres son bien conocidas y su demostración se puede consultar por ejemplo en [Ser77].

Proposición 1.6.2. *La cantidad de caracteres distintos de G coincide con el orden de G. En símbolos, $|\widehat{G}| = |G|$.*

Proposición 1.6.3. *La aplicación $G \to \widehat{\widehat{G}}$ definida por $g \mapsto (\chi \mapsto \chi(g))$ es un isomorfismo de grupos.*

Proposición 1.6.4. *Dados $\chi, \psi \in \widehat{G}$, se tiene*

$$\sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} |G| & \text{si } \chi = \psi, \\ 0 & \text{si } \chi \neq \psi. \end{cases}$$

Similarmente, dados $g, h \in G$ se tiene

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |G| & \text{si } g = h, \\ 0 & \text{si } g \neq h. \end{cases}$$

Proposición 1.6.5. *Todo caracter χ admite una única extensión a un morfismo de $\mathbb{C}$-álgebras $\chi : \mathbb{C}[G] \to \mathbb{C}$, dado por*

$$\chi\left(\sum_{g \in G} \lambda_g u_g\right) = \sum_{g \in G} \lambda_g \chi(g).$$

Dado cualquier $f = \sum_{g \in G} \lambda_g u_g \in \mathbb{C}[G]$, se tiene la siguiente relación: para cada $g \in G$,

$$\lambda_g = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(f)\overline{\chi(g)}.$$

En particular, si $\chi(f) = 0$ para todo $\chi \in \widehat{G}$, entonces $f = 0$.

Hechos estos preliminares, comenzamos a probar los resultados auxiliares que precisaremos para obtener nuestra cota.

El siguiente lema es simplemente una consecuencia del principio del palomar.

Lema 1.6.6. *Sean $g_1, g_2, \ldots, g_k \in G$ y sea $X \subset \widehat{G}$ un conjunto de caracteres de G. Entonces, existen $a_1, a_2, \ldots, a_k \in \mathbb{C}^\times$ tales que el cardinal del conjunto*

$$A_k = \{\chi \in X \mid \chi(g_j) \neq a_j \text{ para todo } j \in [\![1, k]\!]\}$$

es a lo sumo $\left[\prod_{j=1}^{k}\left(1 - \frac{1}{\operatorname{ord}(g_j)}\right)\right] \cdot |X|$.

Demostración. La demostración es por inducción en k. Si $k = 1$, tenemos un solo elemento $g_1 \in G$. Sea $m = \operatorname{ord}(g_1)$. Entonces $\chi(g_1)$ es una raíz m-ésima de la unidad. Como hay exactamente m raíces m-ésimas de la unidad en $\mathbb{C}^\times$, por el principio del palomar existe un $a_1 \in \mathbb{C}^\times$ tal que al menos $\frac{1}{m}$ de los elementos de X valen a_1 sobre g_1. Tomando complemento vemos que $|A_1| \leq \left(1 - \frac{1}{\operatorname{ord}(g_1)}\right) \cdot |X|$, como queríamos.

Ahora, supongamos que tenemos $k+1$ elementos de G y que ya encontramos escalares $a_1, a_2, \ldots, a_k$ tales que $|A_k| \leq \left[\prod_{j=1}^{k}\left(1 - \frac{1}{\operatorname{ord}(g_j)}\right)\right] \cdot |X|$. Aplicando el mismo razonamiento que para el caso base vemos que existe $a_{k+1} \in \mathbb{C}^\times$ tal que

$$|\{\chi \in A_k \mid \chi(g_{k+1}) = a_{k+1}\}| \geq \frac{1}{\operatorname{ord}(g_{k+1})} \cdot |A_k|,$$

y entonces, tomando complemento respecto de A_k resulta

$$|A_{k+1}| \leq \left(1 - \frac{1}{\operatorname{ord}(g_{k+1})}\right)|A_k| \leq \left[\prod_{j=1}^{k+1}\left(1 - \frac{1}{\operatorname{ord}(g_j)}\right)\right] \cdot |X|.$$

Esto completa el paso inductivo. □

El próximo lema, al igual que como ya habíamos hecho para p-grupos, explota la posibilidad de codificar la existencia de una subsucesión de suma 0 a través de un álgebra de grupo.

Lema 1.6.7. *Sea $S = (g_1, g_2, \ldots, g_\ell)$ una sucesión en G. Sea k un entero positivo menor o igual que ℓ y sean $a_1, a_2, \ldots, a_k$ elementos de $\mathbb{C}^\times$.*
Llamamos s al cardinal del conjunto

$$A = \left\{\chi \in \widehat{G} \;\middle|\; \chi(g_j) \neq a_j \text{ para todo } j \in [\![1, k]\!]\right\}.$$

Si $k + s \leq \ell$, entonces existen $a_{k+1}, \ldots, a_{k+s} \in \mathbb{C}^\times$ tales que $\prod_{j=1}^{k+s}(a_j - u_{g_j}) = 0$ en $\mathbb{C}[G]$. En particular, mirando el coeficiente correspondiente a u_0 deducimos que $0 \in \Sigma(S)$.

Demostración. Llamamos $\chi_1, \chi_2, \ldots, \chi_s$ a los elementos de A. Definimos, para cada $i \in [\![1, s]\!]$, $a_{k+i} = \chi_i(g_{k+i})$. Veamos que cumplen lo que queremos.

Sea $f = \prod_{j=1}^{k+s}(a_i - u_{g_i})$. Dado $\chi \in \widehat{G}$, si $\chi \notin A$ entonces por definición χ anula a alguno de los primeros k factores; si en cambio $\chi = \chi_i$ para algún $i \in [\![1, s]\!]$, resulta que χ anula al $(k+i)$-ésimo factor. En definitiva estamos probando que $\chi(f) = 0$ para todo $\chi \in \widehat{G}$, y entonces por 1.6.5 resulta $f = 0$, como queríamos.

La última afirmación del lema es inmediata pues si $0 \notin \Sigma(S)$ entonces el coeficiente correspondiente a u_0 en f sería $\prod_{j=1}^{k+s} a_j \neq 0$. □

Ahora sí, la cota que venimos anticipando.

Teorema 1.6.8. *Sea G un grupo abeliano finito de exponente n. Entonces*

$$D(G) \leq n \cdot \left[1 + \log\left(\frac{|G|}{n}\right)\right],$$

donde log *denota logaritmo natural.*

Demostración. Sea $S = (g_1, g_2, \ldots, g_\ell)$ una sucesión en G de longitud máxima tal que $0 \notin \Sigma(S)$. Probaremos que

$$\frac{\ell}{n} \leq \frac{n-1}{n} + \log\left(\frac{|G|}{n}\right), \tag{1.4}$$

de donde (multiplicando por n y sumando 1) se deduce la afirmación del teorema.

Por el Lema 1.6.6 sabemos que para cualquier $k \in [\![1, \ell]\!]$ que elijamos, podemos encontrar elementos $a_1, a_2, \ldots, a_k \in \mathbb{C}^\times$ tales que

$$s := \left|\left\{\chi \in \widehat{G} \;\middle|\; \chi(g_j) \neq a_j \text{ para todo } j \in [\![1, k]\!]\right\}\right| \leq \left[\prod_{j=1}^{k}\left(1 - \frac{1}{\operatorname{ord}(g_j)}\right)\right] \cdot |G|.$$

(Hemos usado que $|\widehat{G}| = |G|$.)

Si podemos elegir k de manera que se cumpla $k + s \leq \ell$, entonces por el Lema 1.6.7 obtendremos que $0 \in \Sigma(S)$, una contradicción.

Supongamos entonces que no vale (1.4), es decir que

$$\frac{\ell}{n} > \frac{n-1}{n} + \log\left(\frac{|G|}{n}\right) = \frac{n-1}{n} + \log|G| - \log n. \tag{1.5}$$

Mulitplicando por n vemos que $\ell > n - 1$, y como es entero, es $\ell \geq n$. Tomamos entonces $k = \ell - n + 1 \in [\![1, \ell]\!]$. Para este valor de k, tenemos

$$s \leq \left[\prod_{j=1}^{k}\left(1 - \frac{1}{\operatorname{ord}(g_j)}\right)\right] \cdot |G| \leq \exp\left(-\sum_{j=1}^{k}\frac{1}{\operatorname{ord}(g_j)}\right) \cdot |G|,$$

pues vale la desigualdad $1 - t \leq e^{-t}$ para todo $t \in \mathbb{R}$. Ahora usamos que cada término de la sumatoria es mayor o igual que $\frac{1}{n}$ y obtenemos

$$s \leq \exp\left(\log|G| - \frac{k}{n}\right) = \exp\left(\log|G| - \frac{\ell}{n} + \frac{n-1}{n}\right),$$

que por (1.5) es menor que $\exp(\log n) = n$. Como s es entero, es $s \leq n-1$, y entonces

$$k + s = (\ell - n + 1) + s \leq (\ell - n + 1) + (n - 1) = \ell,$$

lo que nos lleva a la contradicción deseada. □

Observación 1.6.9. Si llamamos $t = \frac{|G|}{n}$, vemos que la cota que teníamos antes era nt y la nueva cota es $n(1 + \log t)$. Para $t = 1$ ambas cotas coinciden (y está bien que así sea, porque en ese caso es G cíclico y habíamos visto que $D(G) = |G|$); para $t \gg 1$, la nueva cota es mucho mejor.

Sin embargo, esta cota todavía sigue estando demasiado lejos de nuestra cota inferior $M(G)$. Para ilustrar esto, tomemos $G = \mathbb{Z}_p^d$ con $d \in \mathbb{N}$ fijo y p variando sobre los primos. Como G es un p-grupo, sabemos que

$$D(G) = M(G) = 1 + d(p-1);$$

por otra parte, la cota del Teorema 1.6.8 nos dice

$$D(G) \leq p\left(1 + \log(p^{d-1})\right) = p + (d-1)p\log p.$$

En otras palabras, la nueva cota sólo nos dice que $D(G) \in O(p\log p)$, cuando de hecho sabemos que $D(G) \in \Theta(p)$.

Capítulo 2

Combinatorial Nullstellensatz

En este capítulo presentamos un teorema que será una de las principales herramientas utilizadas para obtener los resultados más importantes del Capítulo 4. Este teorema aparece por primera vez en el paper [Alo99] de Noga Alon, publicado en 1999, y se lo conoce como el *Combinatorial Nullstellensatz* o «Nullstellensatz de Alon».

Desde su aparición, el Combinatorial Nullstellensatz ha sido usado para dar nuevas demostraciones, en general más simples que las preexistentes, de varios resultados clásicos en diversas áreas, como así también para resolver algunos problemas abiertos. En todos los casos, lo que se intenta hacer es traducir el problema que se está estudiando a una condición sobre el conjunto de ceros de un cierto polinomio en varias variables.

A lo largo de este capítulo, la letra $\mathbb{F}$ denotará un cuerpo arbitrario.

2.1. Observaciones generales y demostración

El Combinatorial Nullstellensatz se puede ver como una generalización del siguiente resultado bien conocido sobre polinomios de una variable.

Teorema 2.1.1. *Sea $f \in \mathbb{F}[X]$ un polinomio de grado $d \in \mathbb{N}_0$. Sea $A \subset \mathbb{F}$ tal que $|A| > d$. Entonces f no puede anularse sobre todos los puntos de A, es decir, existe $a \in A$ tal que $f(a) \neq 0$.*

En el caso de una variable, el hecho de que el polinomio tenga grado d ya implica que el coeficiente de X^d en f es no nulo. Para dos o más variables, en cambio, existen varios monomios posibles de grado d y no necesariamente todos ellos aparecen en f. El Combinatorial Nullstellensatz considera alguno de estos monomios, cuyo coeficiente en f sea no nulo, y concluye que f no puede anularse sobre todos los

puntos de un cierto conjunto A, cuya estructura depende de los exponentes que aparecen en el monomio elegido. Más precisamente:

Teorema 2.1.2. *Sea $f \in \mathbb{F}[X_1, \ldots, X_n]$ un polinomio de grado d. Supongamos que $d = \sum_{i=1}^{n} d_i$, con $d_i \in \mathbb{N}_0$ para todo i, y que el coeficiente de $\prod_{i=1}^{n} X_i^{d_i}$ en f es no nulo. Sean $A_1, \ldots, A_n \subset \mathbb{F}$ tales que $|A_i| > d_i$ para todo i, y sea $A = A_1 \times \ldots \times A_n$. Entonces f no puede anularse sobre todos los puntos de A, es decir, existe $a \in A$ tal que $f(a) \neq 0$.*

La demostración que presentamos a continuación es más sencilla que la original de Alon, y se encuentra en el artículo [Mic10] publicado en 2010.

Demostración. Supongamos que el teorema es falso, y consideremos un polinomio f de grado mínimo para el cual la conclusión del teorema es falsa (es decir que sí se anula sobre todos los puntos de A). Notemos que no puede ser $d = 0$: en tal caso f es una constante no nula y A es un subconjunto no vacío de $\mathbb{F}^n$, por lo que el teorema se cumple trivialmente. Entonces $d \geq 1$ y alguno de los d_i debe ser no nulo. Sin pérdida de generalidad supongamos que $d_1 > 0$. Fijemos un elemento $a_1 \in A_1$. Pensamos a f como un polinomio en X_1 con coeficientes en $\mathbb{F}[X_2, \ldots, X_n]$. Como el polinomio $X_1 - a_1$ es mónico, podemos usar el algoritmo de división y obtener polinomios q y r tales que

$$f = q(X_1 - a_1) + r.$$

El grado de r como polinomio en X_1 debe ser estrictamente menor que el grado de $X_1 - a_1$, que es 1. Luego la variable X_1 no aparece en r. Entonces, los monomios de grado máximo de qX_1 no se pueden cancelar con qa_1 ni con r. De esto se deduce que el grado de q es $d - 1$, y que el coeficiente del monomio $X_1^{d_1 - 1} \prod_{i=2}^{n} X_i^{d_i}$ en q es no nulo.

Ahora bien, como f se anula en A, en particular se anula en $\{a_1\} \times A_2 \times \ldots \times A_n$. Como $q(X_1 - a_1)$ se anula en este conjunto, sucede lo mismo con r. Pero como r no depende de X_1, resulta que r también se anula en $A' = A_1' \times A_2 \times \ldots \times A_n$, donde hemos denotado $A_1' = A_1 \setminus \{a_1\}$. Ahora se deduce que q se anula en A', y por lo tanto el teorema también es falso para el polinomio q, cuyo grado es estrictamente menor que el grado de f. Contradicción. □

2.2. Algunas aplicaciones

Dedicamos el resto de este capítulo a mostrar algunos ejemplos de resultados que se pueden probar usando el Combinatorial Nullstellensatz, para ilustrar su gran potencial.

El primero de ellos es el teorema de Cauchy-Davenport, un teorema fundamental en teoría de números aditiva. La pregunta que busca responder este teorema es la

siguiente: dados dos subconjuntos $A, B \subset \mathbb{F}_p$, ¿qué tan chico puede ser el conjunto $A + B := \{a + b \mid a \in A,\, b \in B\}$ en términos de los tamaños de A y B?

Teorema 2.2.1. *Si A y B son subconjuntos no vacíos de $\mathbb{F}_p$, entonces*

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

Demostración. Si $|A|+|B| > p$, entonces para todo $x \in \mathbb{F}_p$ es $A \cap (x - B) \neq \varnothing$ (pues el cardinal de $x - B$ es el mismo que el de B), de donde se deduce que $x \in A + B$. Entonces en este caso $A + B = \mathbb{F}_p$ y por lo tanto vale la igualdad en el enunciado del teorema.

Ahora supongamos que $|A| + |B| \leq p$. Debemos probar entonces que

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

Supongamos lo contrario, es decir que $|A + B| \leq |A| + |B| - 2$, y tomemos un conjunto $C \subset \mathbb{F}_p$ de cardinal exactamente $|A| + |B| - 2$ que contenga a $A + B$. Consideramos el polinomio

$$f = \prod_{c \in C} (X + Y - c) \in \mathbb{F}_p[X, Y].$$

Sean $m = |A| - 1$, $n = |B| - 1$. Entonces f tiene grado $m + n$, y el coeficiente del monomio $X^m Y^n$ en f es $\binom{m+n}{m}$, que es no nulo pues $m + n < p$. Sin embargo f se anula en $A \times B$, contradiciendo el Combinatorial Nullstellensatz. El absurdo provino de suponer que no se cumplía que $|A + B| \geq |A| + |B| - 1$. □

El próximo resultado fue propuesto como problema en la Olimpíada Internacional de Matemática de 2007 en Vietnam. Sólo 5 de los 520 participantes, todos ellos alumnos de secundaria, pudieron resolverlo correctamente. El resultado se puede generalizar fácilmente para cualquier dimensión d, pero aquí lo enunciaremos sólo para $d = 3$, tal como sucedió en la prueba de la IMO.

Proposición 2.2.2. *Sea n un entero positivo y sea*

$$S = \{(x, y, z) \in \mathbb{R}^3 \mid x, y, z \in [\![0, n]\!],\, x + y + z > 0\}.$$

Sea $\mathcal{F}$ una familia de planos en $\mathbb{R}^3$ tal que la unión de todos los elementos de $\mathcal{F}$ contiene a S pero no contiene al $(0, 0, 0)$. Entonces $|\mathcal{F}| \geq 3n$.

Demostración. Llamemos $k = |\mathcal{F}|$ y sean $\Pi_1, \Pi_2, \ldots, \Pi_k$ los planos de $\mathcal{F}$. Cada Π_i se puede describir por una cierta ecuación de la forma

$$a_i X + b_i Y + c_i Z - d_i = 0,$$

en la cual $d_i \neq 0$ (pues Π_i no pasa por el origen).

Consideramos el siguiente polinomio en $\mathbb{R}[X, Y, Z]$:

$$f = \left[\prod_{i=1}^{k}(a_i X + b_i Y + c_i Z - d_i)\right] - \alpha \left[\prod_{j=1}^{n}(X-j)(Y-j)(Z-j)\right],$$

donde la constante α se elige de modo tal que $f(0,0,0) = 0$. (Notar que necesariamente es $\alpha \neq 0$, y que tal α existe porque $\prod_{j=1}^{n}(X-j)(Y-j)(Z-j)$ no se anula en el origen.)

Es claro entonces que el polinomio f así construido se anula sobre todo el conjunto $[\![0,n]\!] \times [\![0,n]\!] \times [\![0,n]\!]$. Si fuera $k < 3n$, entonces el grado de f es exactamente $3n$, y el coeficiente del monomio $X^n Y^n Z^n$ es simplemente $-\alpha \neq 0$. Esto contradice el Combinatorial Nullstellensatz. Por lo tanto, necesariamente es $|\mathcal{F}| \geq 3n$, que era lo que queríamos demostrar. □

Como tercer y último ejemplo mostramos un resultado que sí está directamente relacionado con el tema que estudiamos en esta tesis. Más precisamente, veremos una manera alternativa de probar que la igualdad $D(G) = M(G)$ vale para grupos de la forma $G = \mathbb{Z}_p^n$.

Proposición 2.2.3. *Sea S una sucesión en $\mathbb{Z}_p^n$ de longitud*

$$M(\mathbb{Z}_p^n) = 1 + n(p-1).$$

Entonces S contiene una subsucesión de suma 0.

Demostración. Sea $\ell = 1 + n(p-1)$ y sean $P_1, P_2, \ldots, P_\ell$ los elementos de S. Cada P_i es un vector de n coordenadas, $P_i = (a_{i1}, a_{i2}, \ldots, a_{in})$.

Para cada $j \in [\![1,n]\!]$ definimos el polinomio

$$f_j = \sum_{i=1}^{\ell} a_{ij} X_i \in \mathbb{F}_p[X_1, \ldots, X_\ell].$$

Encontrar una subsucesión de suma cero de S es equivalente a encontrar un punto $b \in \{0,1\}^\ell \setminus \{(0,\ldots,0)\}$ en el cual todos los f_j se anulen simultáneamente.

Ahora, consideramos el polinomio

$$f = \underbrace{\prod_{i=1}^{\ell}(1 - X_i)}_{g} - \underbrace{\prod_{j=1}^{n}(1 - f_j^{p-1})}_{h}.$$

Como cada f_j tiene grado 1, el grado de h es $n(p-1) = \ell - 1$. Luego f tiene grado ℓ. Además el coeficiente de $\prod_{i=1}^{\ell} X_i$ en f es $(-1)^\ell \neq 0$.

Por el Combinatorial Nullstellensatz, f no puede anularse sobre todos los puntos de $\{0,1\}^\ell$. Pero f sí se anula en el origen (g y h valen 1 allí). Entonces existe $b \in \{0,1\}^\ell \setminus \{(0,\ldots,0)\}$ tal que $f(b) \neq 0$. Ahora, g se anula en cualquier punto de este conjunto, pues alguna de las coordenadas de b es igual a 1. Entonces h no se anula en b.

Si para algún j fuera $f_j(b) \neq 0$, por el pequeño teorema de Fermat resulta $f_j^{p-1}(b) = 1$, y luego h se anularía en b. Por lo tanto debe ser $f_j(b) = 0$ para todo j, y estamos. □

Capítulo 3

Problemas inversos

En el Capítulo 1 consideramos el problema de calcular algunos invariantes de un grupo G definidos como la mínima longitud que debe tener una sucesión en G para poder garantizar cierta condición.

Sea $*(G)$ alguno de estos invariantes (por ejemplo D, η, etcétera). El *problema inverso* para $*(G)$ consiste en estudiar la estructura de aquellas sucesiones de longitud «casi» $*(G)$ que **no** satisfacen la condición que define al invariante, e idealmente clasificar todos estos contraejemplos salvo isomorfismo.

Antes de comenzar a profundizar sobre esta noción, y tal como habíamos prometido en el primer capítulo, introducimos ahora una nueva manera de interpretar y denotar a las sucesiones en G. Esta notación tiene sus orígenes en la teoría de factorización [And97], área en la cual se aplican varios de los resultados e ideas que discutimos en esta tesis.

3.1. Notación multiplicativa para sucesiones

Dado un grupo G, llamamos $\mathcal{F}(G)$ al monoide abeliano libre con base G. Los elementos de $\mathcal{F}(G)$ tienen la forma $\prod_{j=1}^{\ell} g_j$, con $\ell \in \mathbb{N}_0$ y $g_1, \ldots, g_\ell$ elementos de G. Más aún, todo $w \in \mathcal{F}(G)$ admite una única representación de la forma

$$w = \prod_{g \in G} g^{v_g(w)}$$

con $v_g(w) \in \mathbb{N}_0$ para todo $g \in G$. Resulta claro entonces que cada sucesión S en el grupo G se corresponde naturalmente con un único elemento de $\mathcal{F}(G)$. (Por supuesto, la sucesión vacía se corresponde con el elemento neutro $1 \in \mathcal{F}(G)$.)

Esta correspondencia permite definir ciertas nociones habituales de manera menos engorrosa que al pensar a las sucesiones como multiconjuntos. Por ejemplo:

- Dadas dos sucesiones S y T, decimos que T es una *subsucesión* de S si $T \mid S$ en $\mathcal{F}(G)$.
- La sucesión formada uniendo todos los elementos de S con todos los elementos de T se denotará simplemente ST.
- Dos subsucesiones T_1 y T_2 de una sucesión S se dicen *disjuntas* si $T_1T_2 \mid S$.
- Las funciones $|\ | : \mathcal{F}(G) \to \mathbb{N}_0$ y $\sigma : \mathcal{F}(G) \to G$ que le asignan a cada sucesión su longitud y la suma de sus elementos respectivamente son morfismos de monoides.
- Todo morfismo de grupos $\alpha : G \to G'$ se extiende canónicamente a un morfismo de monoides $\alpha : \mathcal{F}(G) \to \mathcal{F}(G')$. Este morfismo de monoides además satisface $\sigma\alpha = \alpha\sigma$ (es decir, da lo mismo aplicar el morfismo y luego sumar, que sumar primero y aplicarle el morfismo a la suma).

En relación a este último punto es importante notar lo siguiente.

Observación 3.1.1. Sea $\alpha : G \to G'$ un morfismo de grupos, y sea S una sucesión en G. Vale entonces que $\Sigma(\alpha(S)) = \alpha(\Sigma(S))$. En particular, si α es monomorfismo, entonces $0 \in \Sigma(S) \iff 0 \in \Sigma(\alpha(S))$.

3.2. Algunos ejemplos y motivación

Como sucede habitualmente, un buen ejemplo para comprender mejor la noción de problema inverso se puede encontrar en los grupos cíclicos.

Proposición 3.2.1. *Sea S una sucesión en $\mathbb{Z}_n$ de longitud $n-1$ tal que $0 \notin \Sigma(S)$. Entonces, existe $a \in \mathbb{Z}_n^\times$ tal que $S = a^{n-1}$. Recíprocamente, toda sucesión de esta forma cumple que $0 \notin \Sigma(S)$.*

Demostración. Al igual que en la demostración de 1.1.2, llamamos $g_1, \ldots, g_{n-1}$ a los elementos de S y consideramos los elementos $s_k = g_1 + \ldots + g_k$. Si alguno de los s_k es 0, o si hay dos de estos números que son iguales, se deduce que $0 \in \Sigma(S)$, que contradice la hipótesis. De modo que $s_1, s_2, \ldots, s_{n-1}$ deben ser precisamente todos los elementos no nulos de $\mathbb{Z}_n$, en algún orden.

El orden adoptado para los elementos de S es completamente arbitrario. Si por ejemplo intercambiamos g_1 con g_2 y volvemos a mirar la sucesión de sumas parciales, vamos a obtener los mismos valores que antes exceptuando el s_1, que antes valía g_1 y ahora vale g_2. Como tiene que seguir siendo cierto que $s_1, s_2, \ldots, s_{n-1}$ es una permutación de los restos no nulos módulo n, necesariamente $g_1 = g_2$. Esto mismo se puede hacer para cualquier pareja de elementos de G, pues la numeración es

arbitraria. Luego todos los elementos de S son iguales a un cierto $a \in \mathbb{Z}_n$. Pero si $\mathrm{ord}(a) < n$, entonces S contiene subsucesiones de suma 0 (cualquier subsucesión de longitud $\mathrm{ord}(a)$ funciona). Entonces a debe ser una unidad.

Recíprocamente, cualquier sucesión formada por $n-1$ copias de un elemento a de orden n satisface que $0 \notin \Sigma(S)$. Ya habíamos notado en 1.1.2 que esto es cierto para $a = 1$. Como multiplicar por a es un automorfismo de $\mathbb{Z}_n$ si a es unidad, la Observación 3.1.1 implica que la sucesión a^{n-1} también tiene esta propiedad, lo cual completa la demostración. □

Podemos decir que la Proposición 3.2.1 resuelve completamente el problema inverso para $D(\mathbb{Z}_n)$: ya sabíamos que $D(\mathbb{Z}_n) = n$, y ahora caracterizamos completamente las sucesiones de longitud $D(\mathbb{Z}_n) - 1$ sin subsucesiones de suma 0.

En realidad, para el caso de grupos cíclicos existe un resultado que da mucha más información que el anterior, pues caracteriza también sucesiones de longitud menor que $n-1$ que no tienen subsucesiones de suma 0. Este resultado se debe a Svetoslav Savchev y Fang Chen, y fue publicado en 2007. Antes de poder enunciarlo necesitamos introducir la siguiente notación.

Definición 3.2.2. Sea $\pi : \mathbb{Z} \to \mathbb{Z}_n$ la proyección canónica. Dado $a \in \mathbb{Z}_n$, denotamos $a^\star$ al menor entero positivo tal que $\pi(a^\star) = a$.
(Observar que $a^\star \in [\![1, n]\!]$.)

Observación 3.2.3. Sea $S = \prod_{j=1}^{\ell} g_j$ una sucesión en $\mathbb{Z}_n$ tal que $\sum_{j=1}^{\ell} g_j^\star < n$. Entonces $0 \notin \Sigma(S)$.

Teorema 3.2.4. *Sea $S = \prod_{j=1}^{\ell} g_j$ una sucesión de longitud $\ell > \frac{n}{2}$ en $\mathbb{Z}_n$. Entonces, $0 \notin \Sigma(S)$ si y sólo si existe $a \in \mathbb{Z}_n^\times$ tal que $\sum_{j=1}^{\ell} (ag_j)^\star < n$.*

Demostración. Por la observación anterior, si existe un tal $a \in \mathbb{Z}_n^\times$ entonces la sucesión $\prod_{j=1}^{\ell} ag_j$ no tiene subsucesiones de suma 0, y por lo tanto (Observación 3.1.1) lo mismo vale para S.

Para la otra implicación, consultar [SC07]. □

Son muy pocos los grupos G para los cuales se puede decir que el problema inverso para $D(G)$ está resuelto de manera satisfactoria. En general, los problemas inversos pueden llegar a ser bastante más difíciles que el cálculo del invariante correspondiente.

La necesidad de estudiar estos problemas se presenta naturalmente al intentar aplicar métodos inductivos para el cálculo de invariantes, en los casos en los que las cotas obtenidas están muy cerca de las deseadas. Veamos un ejemplo de esta situación.

Supongamos que queremos probar que $D(G) = M(G)$ vale para grupos de rango 3, y decidimos comenzar analizando el caso en el que el primer factor invariante de

G es 2, es decir, $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2m_1} \oplus \mathbb{Z}_{2m_2}$ con $m_1 \mid m_2$. Tenemos la siguiente sucesión exacta corta:

$$0 \longrightarrow G_1 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_2^3 \longrightarrow 0,$$

donde $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$.

Sea S una sucesión en G de longitud $M(G) = 2m_1 + 2m_2$, y consideramos la sucesión $\beta(S)$ de igual longitud en $\mathbb{Z}_2^3$. Nos gustaría poder extraer de $\beta(S)$ la mayor cantidad posible de subsucesiones disjuntas de suma 0.

Proposición 3.2.5. *$\eta(\mathbb{Z}_2^d) = 2^d$ para todo $d \in \mathbb{N}$.*

Demostración. Como el exponente del grupo es 2, las subsucesiones cortas de suma 0 pueden tener longitud 1 (en cuyo caso el elemento en cuestión debe ser el 0) o longitud 2 (en cuyo caso, los dos elementos de la subsucesión deben ser iguales). Entonces, calcular $\eta(\mathbb{Z}_2^d)$ es preguntarse cuál es la mínima longitud que permite garantizar que en nuestra sucesión o bien aparece el 0 o bien hay dos elementos iguales. La sucesión formada por todos los elementos no nulos de $\mathbb{Z}_2^d$ tiene longitud $2^d - 1$ y no cumple la condición deseada, por lo que $\eta(\mathbb{Z}_2^d) \geq 2^d$; por otra parte, es fácil ver usando el principio del palomar que 2^d elementos son suficientes. Esto completa la demostración. □

Observación 3.2.6. La demostración de la proposición anterior también resuelve el problema inverso para $\eta(\mathbb{Z}_2^d)$.

Proposición 3.2.7. $D_k(\mathbb{Z}_2^3) = \begin{cases} 4 & \text{si } k = 1, \\ 2k+3 & \text{si } k \geq 2. \end{cases}$

Demostración. Para $k = 1$ ya conocemos el resultado pues $\mathbb{Z}_2^3$ es un p-grupo. Para el resto, procedemos por inducción en k.

Sea $k = 2$ y supongamos que existe una sucesión S de longitud $7 = 2 \cdot 2 + 3$ de la que no se pueden extraer dos subsucesiones disjuntas de suma 0. Si S contiene alguna subsucesión corta de suma 0, al quitar esta subsucesión nos quedan al menos 5 elementos, y como $D(\mathbb{Z}_2^3) = 4 < 5$, podemos obtener una segunda subsucesión de suma 0, contradiciendo nuestra suposición. Entonces S no tiene subsucesiones cortas de suma 0. De la demostración de 3.2.5 se deduce que S debe consistir de los 7 elementos no nulos de $\mathbb{Z}_2^3$. Pero de esta sucesión se pueden extraer dos subsucesiones disjuntas de suma 0, por ejemplo

$$S_1 = e_1e_2(e_1 + e_2) \text{ y}$$
$$S_2 = e_3(e_1 + e_3)(e_2 + e_3)(e_1 + e_2 + e_3).$$

Cubiertos todos los casos, vemos que 7 elementos son suficientes para garantizar la existencia de 2 subsucesiones disjuntas de suma 0, es decir $D_2(\mathbb{Z}_2^3) \leq 7$.

Supongamos que para cierto $k \geq 2$ vale $D_k(\mathbb{Z}_2^3) \leq 2k+3$ y veamos qué sucede con $k+1$. Sea S una sucesión de longitud $2(k+1)+3 = 2k+5$. Como $k \geq 2$, este número es mayor que 8, así que por 3.2.5 podemos extraer una subsucesión corta de suma 0. Nos quedan al menos $2k+5-2 = 2k+3$ elementos, que por hipótesis inductiva son suficientes para poder extraer k subsucesiones disjuntas de suma 0. Por lo tanto, $D_{k+1}(\mathbb{Z}_2^3) \leq 2(k+1)+3$, lo cual completa el paso inductivo.

Para ver que la desigualdad que probamos hasta ahora es de hecho una igualdad, basta mostrar un ejemplo de una sucesión de longitud $2k+2$ de la cual no se puedan extraer k subsucesiones disjuntas de suma 0.

Sea $S = g_1^{2k-4} g_2 g_3 g_4 g_5 g_6 g_7$, donde los g_i son los elementos no nulos de $\mathbb{Z}_2^3$ en algún orden. Supongamos que se pueden extraer k subsucesiones disjuntas de suma 0 de S. Digamos que a de estas subsucesiones tienen longitud 2 (luego necesariamente consisten de 2 copias del elemento g_1, pues no hay otro elemento que esté repetido) y b de estas subsucesiones tienen longitud mayor o igual que 3. Tenemos entonces las relaciones

$$\begin{aligned} k &= a+b, \\ 2k+2 &\geq 2a+3b, \end{aligned}$$

de donde se deduce $b \leq 2$. Pero como hay sólo $2k-4$ copias del elemento e_1, también tenemos que $a \leq k-2$. Entonces deben valer las igualdades, y en particular las dos subsucesiones de suma 0 de longitud mayor o igual que 3 se deben extraer del conjunto $\{g_2, g_3, g_4, g_5, g_6, g_7\}$. Como este conjunto tiene 6 elementos, las dos subsucesiones en cuestión deberían tener longitud 3 y ser una partición del conjunto. Sin embargo, la suma de estos 6 elementos es $g_1 \neq 0$, por lo que es imposible cumplir el objetivo. Esto completa la demostración. □

Volvamos ahora a nuestra sucesión exacta corta

$$0 \longrightarrow G_1 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_2^3 \longrightarrow 0.$$

La sucesión $\beta(S)$ tiene longitud

$$2m_1 + 2m_2 > 2(m_1+m_2-2)+3,$$

y entonces por lo probado en 3.2.7 podemos garantizar que existen m_1+m_2-2 subsucesiones disjuntas de suma 0.[1]

[1] En realidad, este argumento sólo es correcto si m_1+m_2-2 es positivo. La única manera de que esto no se cumpla es si $m_1 = m_2 = 1$, pero en ese caso sería $G = \mathbb{Z}_2^3$, que es un p-grupo y por lo tanto ya sabemos que $D(G) = M(G)$. Por este motivo no perdemos nada al excluir este caso de nuestro análisis.

Sabiendo esto, con los razonamientos estándar del método inductivo podemos obtener una sucesión de longitud $m_1 + m_2 - 2$ en el grupo $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$. Si esta sucesión tiene alguna subsucesión de suma 0, ganamos (es decir, probamos que $D(G) = M(G)$). El problema es que la constante de Davenport de G_1 es m_1+m_2-1, exactamente uno más que los elementos de los que disponemos. Y como

$$2m_1 + 2m_2 < 2(m_1 + m_2 - 1) + 3,$$

no tenemos manera en principio de asegurarnos extraer la cantidad correcta de subsucesiones de suma 0 de $\beta(S)$. Esto ya sugiere fuertemente que estudiar el problema inverso para $D(G_1)$ podría ayudarnos a avanzar en este problema.

No obstante, el lector atento debería advertir que los resultados y razonamientos vistos en esta sección son suficientes para probar el siguiente teorema.

Teorema 3.2.8. *Sea $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2m_1} \oplus \mathbb{Z}_{2m_2}$ con $m_1 \mid m_2$. Entonces*

$$D(G) \leq M(G) + 1.$$

Demostración. Si $m_1 = m_2 = 1$ ya lo sabemos, pues en ese caso G es un p-grupo y por lo tanto $D(G) = M(G)$. Si no, es $m_1 + m_2 - 1 \geq 2$. Llamamos $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ y aplicamos la Proposición 1.3.2 con la sucesión exacta corta

$$0 \longrightarrow G_1 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_2^3 \longrightarrow 0,$$

obteniendo

$$D(G) \leq D_{m_1+m_2-1}(\mathbb{Z}_2^3) = 2(m_1 + m_2 - 1) + 3 = M(G) + 1,$$

como queríamos. □

3.3. Huecos y el invariante $\nu(G)$

El invariante $\nu(G)$, introducido por van Emde Boas en 1969, está naturalmente vinculado al problema inverso para $D(G)$, y continúa siendo hasta hoy la principal herramienta sobre la que se basan la mayoría de los resultados que prueban la igualdad $D(G) = M(G)$ para ciertas familias de grupos de rango 3. Antes de definirlo, veamos un par de preliminares.

Usaremos la notación $G^\bullet = G \setminus \{0\}$.

Proposición 3.3.1. *Sea G un grupo y sea S una sucesión en G de longitud $D(G)-1$ tal que $0 \notin \Sigma(S)$. Entonces $\Sigma(S) = G^\bullet$.*

Demostración. Sea $g \in G^\bullet$ arbitrario, y sea $S' = gS$. Como $|S'| = D(G)$, debe tener alguna subsucesión de suma 0, y esa subsucesión debe contener al elemento g pues sabíamos que $0 \notin \Sigma(S)$. De esto se deduce que $-g \in \Sigma(S)$. Como esto vale para todo $g \in G^\bullet$, vemos que $G^\bullet \subseteq \Sigma(S)$, y como $0 \notin \Sigma(S)$, vale también la otra inclusión. □

Definición 3.3.2. Dada una sucesión S en G, decimos que un elemento $a \in G$ es un *hueco* de la sucesión S si es no nulo y $a \notin \Sigma(S)$.

Con esta nomenclatura, la Proposición 3.3.1 nos dice que una sucesión de longitud $D(G) - 1$ que no contiene subsucesiones de suma 0 no puede tener huecos. ¿Qué pasa con las sucesiones de longitud $D(G)-2$? Ahora sí pueden haber huecos, pero la pregunta es si estos huecos pueden estar distribuidos de cualquier forma o si deben tener algún tipo de estructura. La definición de $\nu(G)$ muestra qué clase de estructura podríamos esperar encontrar.

Definición 3.3.3. Sea G un grupo. Denotamos $\nu(G)$ al menor entero no negativo ℓ con la siguiente propiedad: para toda sucesión S de longitud ℓ tal que $0 \notin \Sigma(S)$, resulta que todos los huecos de S están contenidos en un coset propio de G. En otras palabras, existen un subgrupo $H \leq G$ y un elemento $a \in G \setminus H$ tal que $G^\bullet \setminus \Sigma(S) \subseteq a + H$.

El invariante $\nu(G)$ está íntimamente ligado a la constante de Davenport, como muestra la siguiente proposición.

Proposición 3.3.4. *Para todo grupo G, se tienen las desigualdades*

$$D(G) - 2 \leq \nu(G) \leq D(G) - 1.$$

Demostración. La segunda desigualdad ya fue probada en 3.3.1, pues si la longitud de S es $D(G) - 1$ y $0 \notin \Sigma(S)$, el conjunto de huecos de S es directamente vacío, y por lo tanto está contenido en cualquier coset propio.

Para probar la primera desigualdad basta ver que toda sucesión de longitud $\nu(G)+2$ contiene una subsucesión de suma 0. Sea $S = g_1 g_2 \cdots g_\nu xy$ una tal sucesión, y sea S' la subsucesión de longitud $\nu(G)$ formada por los g_j.

Supongamos que $0 \notin \Sigma(S)$, entonces, también $0 \notin \Sigma(S')$. Por definición de ν, sabemos que los huecos de S' están contenidos en un coset de la forma $a + H$ con $a \notin H$. Ahora bien, los elementos $-x$, $-y$ y $-(x + y)$ deben ser huecos de S', pues en caso contrario podríamos obtener una subsucesión de suma 0 de S. Se deduce que $x \equiv y \equiv x + y \equiv -a \pmod{H}$. Pero si x e y son congruentes a $-a$ módulo H, sumando obtenemos que $x + y \equiv -2a \pmod{H}$. Luego $-2a \equiv -a \pmod{H}$, es decir $a \in H$, una contradicción.

Por lo tanto, es $D(G) \leq \nu(G) + 2$, que equivale a la primera desigualdad. □

Se conjetura que para todo grupo G vale la igualdad de la izquierda, es decir, que $\nu(G) = D(G) - 2$. Entre las clases de grupos para los cuales esta igualdad ya ha sido probada, se encuentran los grupos cíclicos, los p-grupos, y (mucho más recientemente) los grupos de rango 2.

Proposición 3.3.5. *$\nu(\mathbb{Z}_n) = D(\mathbb{Z}_n) - 2 = n - 2$ para todo $n \geq 2$.*

Demostración. Ya sabemos que vale el mayor o igual gracias a la Proposición 3.3.4. Para la otra desigualdad, sea $S = \prod_{j=1}^{n-2} g_j$ una sucesión en $\mathbb{Z}_n$ de longitud $n-2$, y para cada $k \in [\![1, n-2]\!]$ consideramos el elemento $s_k = g_1 + g_2 + \ldots + g_k$. Ya observamos varias veces que si $0 \notin \Sigma(S)$ entonces los elementos s_k deben ser distintos dos a dos. Se deduce que en este caso $G^\bullet \setminus \Sigma(S)$ tiene a lo sumo un elemento. Por lo tanto, el conjunto de huecos estará contenido en un coset de la forma $a + \{0\}$ con $a \in G^\bullet$. □

Proposición 3.3.6. *Si G es un p-grupo, entonces*

$$\nu(G) = D(G) - 2 = M(G) - 2.$$

Demostración. Sean $n_1, n_2, \ldots, n_r$ los factores invariantes de G y sea $\{e_1, e_2, \ldots, e_r\}$ un sistema de generadores de G tal que $\mathrm{ord}(e_j) = n_j$ para todo j.

Sea S una sucesión en G de longitud $M(G) - 2 = \sum_{j=1}^{r}(n_j - 1) - 1$ tal que $0 \notin \Sigma(S)$. Consideramos, como hicimos en el Capítulo 1, el elemento

$$f(S) = \prod_{g \in S}(1 - u_g) = \sum_{g \in G} \lambda_g(S) u_g \in \mathbb{F}_p[G].$$

Recordemos (Proposición 1.2.4) que el hecho de que $0 \notin \Sigma(S)$ implica que $\lambda_0(S) = 1$, y que si g es un hueco de S entonces $\lambda_g(S) = 0$.

Por lo probado en la sección 1.2 sabemos que $f(S)$ se puede escribir como una combinación lineal con coeficientes en $\mathbb{F}_p$ de elementos de la forma $\prod_{j=1}^{r} \left(1 - u_{e_j}\right)^{m_j}$ con $\sum m_j \geq M(G) - 2$. Pero también sabemos que si para algún j es $m_j \geq n_j$ entonces el elemento en cuestión es 0. Por lo tanto, sólo nos interesan aquellos casos en los que cada m_j es igual a $n_j - 1$, excepto tal vez uno de ellos, que puede valer $n_j - 2$. En definitiva, vemos que $f(S)$ tiene la forma

$$f(S) = b_0 \prod_{j=1}^{r} \left(1 - u_{e_j}\right)^{n_j - 1} + \sum_{k=1}^{r} \left[b_k \left(1 - u_{e_k}\right)^{n_k - 2} \prod_{j \neq k} \left(1 - u_{e_j}\right)^{n_j - 1} \right], \tag{3.1}$$

con $b_0, b_1, \ldots, b_r \in \mathbb{F}_p$.

Ahora, hagamos algunas cuentas. En el anillo de polinomios $\mathbb{F}_p[X]$ vale la identidad

$$(1 - X)^{n_j - 1} = \frac{(1 - X)^{n_j}}{(1 - X)} = \frac{1 - X^{n_j}}{1 - X} = \sum_{s=0}^{n_j - 1} X^s \tag{3.2}$$

(usamos que n_j es una potencia de p). Derivando formalmente (3.2) obtenemos

$$(n_j - 1)(1 - X)^{n_j - 2}(-1) = \sum_{s=0}^{n_j - 2} (s+1)X^s,$$

que como n_j es múltiplo de p se simplifica a

$$(1 - X)^{n_j - 2} = \sum_{s=0}^{n_j - 2} (s+1)X^s. \tag{3.3}$$

Especializando (3.2) y (3.3) en los lugares apropiados, (3.1) se convierte en

$$f(S) = b_0 \sum_{g \in G} u_g + \sum_{k=1}^{r} \left\{ b_k \left[\sum_{\lambda_k = 0}^{n_k - 2} (\lambda_k + 1) u_{\lambda_k e_k} \right] \prod_{j \neq k} \sum_{\lambda_j = 0}^{n_j - 1} u_{\lambda_j e_j} \right\}.$$

Sea g un hueco de S. Escribimos $g = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_r e_r$, donde cada λ_k pertenece al intervalo $[\![0, n_k - 1]\!]$. Entonces

$$\lambda_g(S) = b_0 + \sum_{k=1}^{r} b_k(\lambda_k + 1) = 1 + \sum_{k=1}^{r} b_k \lambda_k.$$

(En el último paso usamos que $\lambda_0(S) = 1$.)

En consecuencia, el conjunto de huecos de G está contenido en el conjunto formado por aquellos elementos cuyas coordenadas λ_k satisfacen la ecuación

$$\sum_{k=1}^{r} b_k \lambda_k = -1.$$

Si este conjunto es vacío, entonces S no tiene huecos y no hay nada que probar. Si en cambio el conjunto es no vacío, es evidente que es un coset propio de G. □

A lo largo de este capítulo y el siguiente probaremos varios resultados que nos llevarán a concluir, en última instancia, que todos los grupos de rango 2 también satisfacen $\nu(G) = D(G) - 2$. Antes de dedicarnos a esta tarea, y para no perder la motivación que espero que el lector aún comparta conmigo en este punto, veamos cómo el teorema que queremos probar nos va a permitir transformar la conclusión del Teorema 3.2.8 en algo realmente satisfactorio.

Teorema 3.3.7. *Sea $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2m_1} \oplus \mathbb{Z}_{2m_2}$ con $m_1 \mid m_2$, y supongamos que el grupo $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ satisface $\nu(G_1) = D(G_1) - 2$. Entonces $D(G) = M(G)$.*

Demostración. Sea S una sucesión en G de longitud $M(G) = 2m_1 + 2m_2$. Consideramos la sucesión exacta corta

$$0 \longrightarrow G_1 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_2^3 \longrightarrow 0.$$

Como la longitud de $\beta(S)$ es $2m_1 + 2m_2 = 2(m_1 + m_2 - 4) + 8$ y vimos que $\eta(\mathbb{Z}_2^3) = 8$, tenemos que se pueden extraer $m_1 + m_2 - 3$ subsucesiones cortas de suma 0 disjuntas de $\beta(S)$.[2]

Por hipótesis, el número $m_1 + m_2 - 3$ es precisamente el valor de $\nu(G_1)$. Llamemos entonces $\beta(S_1), \beta(S_2), \ldots, \beta(S_\nu)$ a las subsucesiones del párrafo anterior. Sabemos que existen elementos $h_1, h_2, \ldots, h_\nu$ en G_1 tales que $\alpha(h_j) = \sigma(S_j)$ para todo j.

Sea $T = h_1 h_2 \cdots h_\nu$. Si T contiene alguna subsucesión de suma 0, entonces lo mismo ocurre con S, y la demostración está terminada. Si no, entonces por definición de ν se tiene que los huecos de T están contenidos en un coset de G_1 de la forma $a + H$, con $H \leq G_1$, $a \notin H$.

Consideramos ahora los elementos de $\beta(S)$ que quedan luego de extraer las subsucesiones $\beta(S_j)$. Hay al menos 6 de estos elementos. Si de estos elementos se pueden extraer otras dos subsucesiones disjuntas de suma 0, le podemos agregar dos elementos a T y pasará a tener longitud $D(G_1)$, con lo cual también podremos concluir que $0 \in \Sigma(S)$.

Supongamos entonces que esto no ocurre. En particular notemos que entre esos 6 elementos no puede haber ninguna subsucesión *corta* de suma 0, pues de ser así, al extraer esa subsucesión nos quedan al menos $4 = D(\mathbb{Z}_2^3)$ elementos, con lo cual podremos extraer una segunda subsucesión de suma 0. Entonces, por lo observado en 3.2.5, estos 6 elementos deben ser no nulos y distintos dos a dos. Pero sólo hay 7 elementos no nulos en $\mathbb{Z}_2^3$. Sin pérdida de generalidad (aplicando un automorfismo de $\mathbb{Z}_2^3$ si es necesario) podemos suponer que el elemento que falta es el $(1,1,1)$; es decir, que luego de extraer las $m_1 + m_2 - 3 = D(G_1) - 2$ subsucesiones cortas de suma 0 de $\beta(S)$ todavía disponemos de los siguientes seis elementos:

$$y_1 = (1,0,0), \quad y_2 = (0,1,0), \quad y_3 = (0,0,1),$$

$$y_4 = (1,1,0), \quad y_5 = (1,0,1), \quad y_6 = (0,1,1).$$

Es fácil verificar que este conjunto contiene 7 subsucesiones de suma 0, a saber:

$$T_1 = y_1 y_2 y_4, \quad T_2 = y_1 y_3 y_5, \quad T_3 = y_2 y_3 y_6, \quad T_4 = y_4 y_5 y_6,$$

$$T_5 = y_1 y_2 y_5 y_6, \quad T_6 = y_1 y_3 y_4 y_6, \quad T_7 = y_2 y_3 y_4 y_5.$$

[2] De nuevo, para que esto sea correcto necesitamos asumir que $m_1 + m_2 \geq 4$. Los únicos casos en los que esto no sucede son cuando m_1 vale 1 y m_2 vale 1 o 2. Como en esos casos G es un p-grupo, la conclusión del teorema sigue siendo verdadera.

Sean $x_1, x_2, \ldots, x_6$ los elementos de S tales que $\beta(x_j) = y_j$. Como T_1 tiene suma 0, sabemos que $x_1 + x_2 + x_4$ está en la imagen de α, es decir es de la forma $\alpha(t_1)$ con $t_1 \in G_1$. Si el elemento $-t_1$ no es un hueco de la sucesión T, entonces al agregarle t_1 a T resulta que se puede extraer una subsucesión de suma 0 de T, y por lo tanto $0 \in \Sigma(S)$. Entonces, la única manera de que no se cumpla lo que queremos es que $-t_1, -t_2, \ldots, -t_7$ sean huecos de T (los elementos $t_2, \ldots, t_7$ se definieron de manera análoga a t_1). En particular $t_j \equiv -a \pmod{H}$ para todo j. Pero notemos que $t_1 + t_2 + t_3 + t_4 = t_5 + t_6 + t_7$ (sus imágenes por α son iguales, y α es inyectivo). De esto resulta

$$-4a \equiv -3a \pmod{H},$$

o sea $a \in H$, una contradicción.

Cubiertos todos los casos, vemos que toda sucesión en G de longitud $M(G)$ contiene una subsucesión de suma 0, como queríamos probar. □

3.4. Propiedad C

En 1.4.1 probamos que para todo primo p vale que $\eta(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 3p - 2$. Correspondería ahora preguntarse cómo son todas las sucesiones de longitud $3p-3$ en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que no contienen subsucesiones cortas de suma 0.

Definición 3.4.1. Decimos que un número primo p tiene la *Propiedad C* si toda sucesión S de longitud $3p - 3$ en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que no contiene subsucesiones cortas de suma 0 es de la forma $S = a^{p-1}b^{p-1}c^{p-1}$.

En [vEB69], van Emde Boas define la Propiedad C y dice haber verificado, usando una computadora, que los primos menores o iguales que 7 tienen esta propiedad. La relevancia de que un primo tenga la Propiedad C viene a partir del siguiente teorema.

Teorema 3.4.2. *Sea $G = \mathbb{Z}_{pm_1} \oplus \mathbb{Z}_{pm_2}$ donde p es un primo que tiene la Propiedad C y $m_1 \mid m_2$. Si el grupo $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ satisface $\nu(G_1) = D(G_1) - 2$, entonces también $\nu(G) = D(G) - 2$.*

Observación 3.4.3. Del teorema anterior se deduce que si $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ es un grupo de rango 2 tal que todos los primos que dividen a n_1 tienen la Propiedad C, entonces $\nu(G) = D(G) - 2$. (Comenzamos con un grupo cíclico y vamos agregando primos de a uno.)

Para demostrar el Teorema 3.4.2 necesitamos un lema previo, de carácter profundamente técnico.

Lema 3.4.4. *Sea Q un grupo abeliano finito y sea $G = (\mathbb{Z}_p \oplus \mathbb{Z}_p) \oplus Q$. Sean π_1, π_2 las proyecciones canónicas de G a $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y Q respectivamente. Sea S una sucesión en G de longitud $3p-3$ que satisface las siguientes condiciones:*

- *$\pi_1(S)$ consiste de tres elementos distintos, cada uno de ellos repetido $p-1$ veces.*
- *$\pi_1(S)$ no contiene subsucesiones cortas de suma 0.*
- *Existe $t \in Q^\bullet$ tal que para toda subsucesión T de S con $\sigma(\pi_1(T)) = 0$, se tiene $\sigma(\pi_2(T)) = t$.*

Entonces, existe un coset propio de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, digamos $x + N$, tal que para todo $y \in (\mathbb{Z}_p \oplus \mathbb{Z}_p) \setminus (x + N)$, $y \neq 0$, existen dos subsucesiones de S, digamos T_1 y T_2, tales que $\pi_1(\sigma(T_1)) = \pi_1(\sigma(T_2)) = y$ pero $\pi_2(\sigma(T_1)) \neq \pi_2(\sigma(T_2))$.

Demostración. Consultar [vEB69, Lema 5.3]. □

Ahora sí, damos la demostración del Teorema 3.4.2.

Demostración. Consideramos la sucesión exacta corta

$$0 \longrightarrow G_1 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow 0.$$

Sea S una sucesión en G de longitud $D(G)-2 = pm_1+pm_2-3$ tal que $0 \notin \Sigma(S)$. Debemos demostrar que los huecos de S están contenidos en un coset propio de G.

Consideramos $\beta(S)$, que es una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ de longitud

$$pm_1 + pm_2 - 3 = p(m_1 + m_2 - 3) + 3p - 3.$$

Como $\eta(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 3p-2$, es claro que se pueden extraer m_1+m_2-3 subsucesiones cortas de suma 0 de $\beta(S)$, y se podrá extraer una más si al menos una de estas subsucesiones tiene longitud estrictamente menor que p. Consideramos entonces dos casos.

Caso 1: Se pueden extraer m_1+m_2-2 subsucesiones cortas de suma 0 de $\beta(S)$.

Digamos que estas subsucesiones son $\beta(S_1), \beta(S_2), \ldots, \beta(S_{m_1+m_2-2})$. Como ya hicimos varias veces anteriormente, esto nos permite formar una sucesión

$$T = \prod_{j=1}^{m_1+m_2-2} h_j$$

en el grupo G_1, donde $\alpha(h_j) = \sigma(S_j)$ para todo $j \in [\![1, m_1 + m_2 - 2]\!]$. La sucesión T no puede tener subsucesiones de suma 0, pues esto implicaría $0 \in \Sigma(S)$, una

contradicción. Como la longitud de T es precisamente $D(G_1) - 1$, sabemos por la Proposición 3.3.1 que $\Sigma(T) = G_1^\bullet$.

Ahora, sea S' la sucesión formada por los elementos de S que quedan luego de extraer las subsucesiones S_j. Como $|S_j| \leq p$ para todo j, se tiene

$$|S'| \geq 2p - 3 = \nu(\mathbb{Z}_p \oplus \mathbb{Z}_p).$$

Si la sucesión $\beta(S')$ tuviera una subsucesión de suma 0, podríamos agregarle un elemento a la sucesión T que construimos antes, con lo cual obtendríamos que $0 \in \Sigma(T)$ y entonces también $0 \in \Sigma(S)$, contradicción. Luego $0 \notin \Sigma(\beta(S'))$, y como su longitud es mayor o igual que $\nu(\mathbb{Z}_p \oplus \mathbb{Z}_p)$, deducimos que los huecos de $\beta(S')$ están contenidos en un coset propio de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, es decir un conjunto de la forma $x + N$ con N subgrupo de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y $x \notin N$.

Como podemos obtener subsumas de S combinando subsumas de $\alpha(T)$ y de S', tenemos la siguiente inclusión:

$$\widetilde{\Sigma}(S) \supseteq \widetilde{\Sigma}(\alpha(T)) + \widetilde{\Sigma}(S'),$$

donde $\widetilde{\Sigma}$ denota $\Sigma \cup \{0\}$, es decir, es el conjunto de *todas* las posibles subsumas, incluyendo la que corresponde a la subsucesión vacía. Recordando que $\widetilde{\Sigma}(T) = G_1$, lo anterior es

$$\widetilde{\Sigma}(S) \supseteq \alpha(G_1) + \widetilde{\Sigma}(S'). \tag{3.4}$$

Sabemos que para todo $y \in (\mathbb{Z}_p \oplus \mathbb{Z}_p) \setminus (x + N)$, $y \neq 0$, existe al menos una subsucesión V de S' tal que $\beta(\sigma(V)) = y$. En otras palabras, existe algún z en $\widetilde{\Sigma}(S') \cap \beta^{-1}(y)$. Pero entonces $\widetilde{\Sigma}(S)$ contiene a todo el coset $\alpha(G_1) + z = \beta^{-1}(y)$. Este argumento funciona para $y \neq 0$, pero también es inmediato a partir de (3.4) que $\widetilde{\Sigma}(S) \supseteq \alpha(G_1) = \beta^{-1}(0)$. De todo esto se deduce que los huecos de S están contenidos en $\beta^{-1}(x + N)$, que es un coset propio de G.

Caso 2: Se pueden extraer $m_1 + m_2 - 3$ subsucesiones cortas de suma 0 de $\beta(S)$ y ninguna más.

Por lo observado al principio, esto obliga a que las subsucesiones $\beta(S_j)$ que se pueden extraer tengan todas longitud exactamente p. Si llamamos, como en el caso anterior, S' a la sucesión formada por los elementos de S que quedan luego de extraer las subsucesiones S_j, resulta que $\beta(S')$ es una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ de longitud $3p-3$ que no contiene subsucesiones cortas de suma 0. Como estamos suponiendo que el primo p tiene la Propiedad C, sabemos que $\beta(S')$ consiste de tres elementos distintos, cada uno de ellos repetido $p - 1$ veces.

Como en el caso anterior obtenemos una sucesión $T = \prod_{j=1}^{m_1+m_2-3} h_j$ en G_1 formada por las preimágenes de las sumas de las subsucesiones S_j. Ahora la longitud de T es $D(G_1) - 2$, que por hipótesis es igual a $\nu(G_1)$. Como no puede pasar que

$0 \in \Sigma(T)$ (pues eso implicaría $0 \in \Sigma(S)$), podemos afirmar que el conjunto de huecos de T está contenido en un coset propio de G_1, digamos $t_1 + M$ con M subgrupo de G_1, $t_1 \notin M$.

Sea $Q = G/\alpha(M)$ y consideramos el elemento $t = [-\alpha(t_1)]$ (los corchetes denotan la clase de un elemento de G en el cociente que define a Q). Llamemos $x_1, x_2, \ldots, x_{3p-3}$ a los elementos de S'.

Consideramos ahora, en el grupo $G_0 = (\mathbb{Z}_p \oplus \mathbb{Z}_p) \oplus Q$, la sucesión

$$V = \prod_{j=1}^{3p-3} (\beta(x_j), [x_j]).$$

Vamos a probar que podemos aplicar el Lema 3.4.4 con esta sucesión (y el mismo elemento t que ya definimos). Las primeras dos condiciones que pide el lema ya sabemos que se cumplen. Veamos la tercera.

Consideremos una subsucesión de V tal que la suma de las primeras coordenadas es 0. Equivalentemente, sean $1 \leq i_1 < i_2 < \ldots < i_k \leq 3p-3$ índices tales que $x_{i_1} + x_{i_2} + \ldots + x_{i_k} \in \alpha(G_1)$. Queremos ver que entonces

$$[x_{i_1}] + [x_{i_2}] + \ldots + [x_{i_k}] = t = [-\alpha(t_1)].$$

Sea $h \in G_1$ tal que $\alpha(h) = x_{i_1} + x_{i_2} + \ldots + x_{i_k}$. Entonces podemos agregar el elemento h a la sucesión T y tiene que seguir siendo cierto que no hay subsucesiones de suma 0. Para que esto pase necesitamos que $-h$ sea un hueco de T, y por lo tanto debe ser $-h \in t_1 + M$, o sea $-\alpha(h) \in \alpha(t_1) + \alpha(M)$, y entonces

$$[x_{i_1}] + [x_{i_2}] + \ldots + [x_{i_k}] = [\alpha(h)] = -[\alpha(t_1)] = t,$$

como queríamos.

Ahora el lema nos dice que existe un coset propio $x + N \subset \mathbb{Z}_p \oplus \mathbb{Z}_p$ tal que para todo $0 \neq y \notin (x + N)$ existen dos subsucesiones de V, digamos V_1 y V_2, tales que $\pi_1(\sigma(V_1)) = \pi_1(\sigma(V_2)) = y$ pero $\pi_2(\sigma(V_1)) \neq \pi_2(\sigma(V_2))$, donde π_1 y π_2 son las proyecciones de G_0 a $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y a Q respectivamente.

Probaremos que entonces los huecos de S están contenidos en $\beta^{-1}(x + N)$, lo cual completará la demostración.

Primero veamos que $\widetilde{\Sigma}(S) \supseteq \alpha(G_1)$. En efecto, como

$$3p - 3 \geq 2p - 1 = D(\mathbb{Z}_p \oplus \mathbb{Z}_p),$$

podemos tomar alguna subsucesión de $\beta(S')$ que tenga suma 0, y usarla para extender T a una sucesión de longitud $D(G_1) - 1$, que como no puede tener subsucesiones de suma 0, debe tener todas las posibles subsumas no nulas.

Ahora tomemos algún $z \in G \setminus \alpha(G_1)$, y veamos que si $\beta(z) \notin x + N$ entonces $\Sigma(S) \supseteq \alpha(G_1) + z$. Llamamos $y = \beta(z)$. Notemos que por la elección de z se tiene $0 \neq y \notin x + N$.

Por el Lema 3.4.4, existen dos subsucesiones V_1 y V_2 de la sucesión V tales que $\pi_1(\sigma(V_1)) = \pi_1(\sigma(V_2)) = y$ pero $\pi_2(\sigma(V_1)) \neq \pi_2(\sigma(V_2))$.

Sean W_1 y W_2 las subsucesiones de S' que se corresponden con V_1 y V_2 (es decir, elegimos los mismos subíndices). Si llamamos $\omega = \sigma(W_2) - \sigma(W_1)$, las condiciones anteriores implican que $\omega \in \alpha(G_1) \setminus \alpha(M)$.

Notemos que

$$\begin{aligned}\Sigma(S) &\supseteq \left[\sigma(W_1) + \widetilde{\Sigma}(\alpha(T))\right] \cup \left[\sigma(W_2) + \widetilde{\Sigma}(\alpha(T))\right] \\ &= \sigma(W_1) + \{0, \omega\} + \widetilde{\Sigma}(\alpha(T)).\end{aligned}$$

Ahora bien, como $\widetilde{\Sigma}(\alpha(T))$ contiene a todo $\alpha(G_1)$ salvo el coset $\alpha(t_1) + \alpha(M)$, y $\omega \notin \alpha(M)$, es fácil ver que la suma del segundo y el tercer sumando es $\alpha(G_1)$. Entonces $\Sigma(S)$ contiene al coset $\sigma(W_1) + \alpha(G_1)$. Ahora sólo resta notar que

$$\beta(\sigma(W_1)) = y = \beta(z),$$

y por lo tanto el coset anterior es lo mismo que el coset $z + \alpha(G_1)$. Como z era arbitrario entre los que cumplían $0 \neq \beta(z) \notin x + N$, y ya habíamos visto que $\alpha(G_1) \subseteq \widetilde{\Sigma}(S)$, concluimos que los huecos de $\Sigma(S)$ están contenidos en el coset propio $\beta^{-1}(x + N)$, que era lo que queríamos demostrar. □

3.5. Nubes, seminubes y Propiedad B

En esta sección introducimos una nueva propiedad que puede tener un número primo p, relacionada con el problema inverso para $D(\mathbb{Z}_p \oplus \mathbb{Z}_p)$, a la que llamaremos *Propiedad B*.

Para comenzar vamos a ponerle nombre a algunos objetos con los que trabajaremos todo el tiempo a partir de ahora.

Definición 3.5.1. Una *seminube* es una sucesión $S \in \mathcal{F}(\mathbb{Z}_p \oplus \mathbb{Z}_p)$, de longitud $2p-2$, tal que $0 \notin \Sigma(S)$. En otra palabras, las seminubes son las sucesiones de longitud máxima que no tienen al 0 como subsuma.

Si somos consistentes con el tratamiento que venimos haciendo hasta ahora de los problemas inversos, resolver el problema inverso para $D(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ debería interpretarse como caracterizar completamente todas las seminubes. En breve veremos que esta no es la manera más cómoda de enunciar el problema.

Ejemplo 3.5.2. La sucesión $S = e_1^{p-1}e_2^{p-1}$ es claramente una seminube (de hecho, es la que usamos como ejemplo para ver que $D(G) \geq M(G)$). Más en general, es fácil ver que cualquier sucesión de la forma

$$S = e_1^{p-1}\prod_{j=1}^{p-1}(x_j, 1)$$

es una seminube.

Definición 3.5.3. Dos sucesiones $S, S' \in \mathcal{F}(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ se dicen *equivalentes* si existe $\varphi \in \mathrm{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ tal que $\varphi(S) = S'$.

Una pregunta válida es si toda seminube es equivalente a una que tenga la forma dada en el Ejemplo 3.5.2. Esto no es cierto si $p > 3$. Consideremos una sucesión S de la forma

$$S = e_1^{p-2}\prod_{j=1}^{p}(x_j, 1),$$

donde $\sum_{j=1}^{p} x_j = 1$. De nuevo, es fácil verificar que S es una seminube. Si elegimos los x_j de manera que ningun término de S tenga multiplicidad $p-1$ (por ejemplo tomamos $x_1 = x_2 = \ldots = x_{p-2} = 0$, $x_{p-1} = 2$, $x_p = -1$), resulta evidente que S no es equivalente a una seminube como la del ejemplo, pues un automorfismo preserva las multiplicidades.

Lo que ocurre en realidad es que estos dos ejemplos de seminubes, si bien no son equivalentes, sí corresponden a un mismo caso al analizar el problema con otro enfoque.

Definición 3.5.4. Una *nube* es una sucesión $S \in \mathcal{F}(\mathbb{Z}_p \oplus \mathbb{Z}_p)$, de longitud $2p-1$, que no contiene subsucesiones *propias* de suma 0.

Observación 3.5.5. Como $D(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p-1$, necesariamente toda nube S es una sucesión de suma 0. De hecho, las nubes son las sucesiones *minimales* de suma 0 de longitud máxima.

Todo resultado que se pruebe para seminubes se puede traducir fácilmente a nubes (y viceversa) usando la siguiente observación.

Observación 3.5.6. Si S es una nube, entonces cualquier subsucesión de S que se obtenga descartando uno de los elementos de S es una seminube. Recíprocamente, si T es una seminube y $g = -\sigma(T)$, entonces la sucesión $S = gT$ es una nube.

Notemos que si aplicamos esta construcción con las dos familias de seminubes que describimos antes, en ambos casos obtenemos una nube que contiene un elemento con multiplicidad $p-1$ (en el primer caso, porque ya lo tenía la seminube; en el

segundo caso, porque el elemento que debemos agregar para convertirla en una nube es precisamente el e_1). Entonces, si fuera cierto que toda seminube es equivalente a alguna que pertenezca a una de estas dos familias, podríamos deducir que toda nube contiene un elemento con multiplicidad $p-1$.

Recíprocamente, sea S una nube que contiene un elemento x con multiplicidad $p-1$. Claramente este x es no nulo, así que existe algún automorfismo de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que manda $x \mapsto e_1$. Luego, módulo equivalencia podemos suponer que S es de la forma

$$S = e_1^{p-1} \prod_{j=1}^{p} (x_j, y_j).$$

Si existiera algún $\varnothing \neq J \subsetneq [\![1, p]\!]$ tal que $\sum_{j\in J} y_j = 0$, podríamos formar la subsucesión propia

$$S' = e_1^{\alpha} \prod_{j\in J} (x_j, y_j),$$

donde $\alpha \in [\![0, p-1]\!]$ se elige de modo que $\overline{\alpha} + \sum_{j\in J} x_j = 0$ en $\mathbb{Z}_p$, y resulta $\sigma(S') = (0,0)$, lo cual entra en contradicción con el hecho de que S es una nube.

Por lo tanto, la sucesión $\prod_{j=1}^{p} y_j$ en $\mathbb{Z}_p$ no contiene subsucesiones propias de suma 0. De lo hecho en 3.2.1 se deduce que los y_j deben ser todos iguales a un cierto $a \in \mathbb{Z}_p^{\times}$; más aún, aplicando el automorfismo de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que manda $(x, y) \mapsto (x, a^{-1}y)$ podemos suponer que son todos iguales a 1. Entonces nuestra nube es equivalente a una de la forma

$$S = e_1^{p-1} \prod_{j=1}^{p} (x_j, 1),$$

donde además debe ser $\sum_{j=1}^{p} x_j = 1$ para que S tenga suma 0. Ahora es claro que cualquier seminube que se obtenga quitando un elemento de S pertenece a una de las dos familias antes descriptas (en qué familia está depende de si el elemento que quitamos fue una copia de e_1 o un $(x_j, 1)$).

En definitiva, hemos probado la siguiente proposición.

Proposición 3.5.7. *Las siguientes afirmaciones sobre un número primo p son equivalentes:*

(i) Toda nube contiene un elemento con multiplicidad $p-1$.

(ii) Toda seminube es equivalente a una de la forma $e_1^{p-1} \prod_{j=1}^{p-1} (x_j, 1)$ o bien a una de la forma $e_1^{p-2} \prod_{j=1}^{p} (x_j, 1)$ con $\sum_{j=1}^{p} x_j = 1$.

Esto nos permite definir la Propiedad B en términos de nubes en vez de seminubes.

Definición 3.5.8. Decimos que un número primo p tiene la *Propiedad B* si toda nube contiene un elemento con multiplicidad $p-1$.

3.6. Propiedad $B \Rightarrow$ Propiedad C

Para terminar este capítulo probaremos que la Propiedad B es más fuerte que la Propiedad C que definimos en la sección 3.4. La demostración de este hecho requiere hacer varias observaciones sencillas y probar un lema previo.

Recordemos la siguiente notación, que ya usamos en la sección 1.2: dada una sucesión $S = \prod_{j=1}^{\ell} g_j$ y un $k \in \mathbb{N}_0$, denotamos

$$N_0^k(S) = \left| \left\{ I \subset [\![1, \ell]\!] \;\middle|\; \sum_{i \in I} g_i = 0,\ |I| = k \right\} \right|;$$

es decir, $N_0^k(S)$ cuenta la cantidad de subsucesiones de suma 0 de longitud exactamente k.

Como $\mathbb{Z}_p \oplus \mathbb{Z}_p$ tiene una estructura de espacio vectorial sobre $\mathbb{F}_p$, tiene sentido hablar de independencia lineal de elementos y de subespacios generados. Aprovecharemos mejor esta estructura en el Capítulo 4.

Proposición 3.6.1. *Sea $S = a^{p-1}T$ una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que no contiene subsucesiones cortas de suma 0. Entonces, todo elemento de T es linealmente independiente con a.*

Demostración. Como a es necesariamente no nulo, si lo que dice el enunciado fuera falso significaría que T contiene algún múltiplo de a, digamos $b = ka$ con $1 \leq k \leq p$. En este caso, la sucesión $a^{p-k}b$ resulta ser una subsucesión de S cuya suma es 0 y su longitud es menor o igual que p. Absurdo. □

Proposición 3.6.2. *Sea $S = a^{p-1}T$ una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ tal que $0 \notin \Sigma(S)$. Entonces $\Sigma(T) \cap \langle a \rangle = \varnothing$.*

Demostración. Supongamos que existe T' subsucesión no vacía de T que satisface $\sigma(T') \in \langle a \rangle$. Entonces $\sigma(T') = ka$ para cierto $1 \leq k \leq p$. En esta situación, $a^{p-k}T'$ resulta ser una subsucesión de S de suma 0, lo cual contradice nuestras hipótesis. □

Proposición 3.6.3. *Sea S una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que no contiene subsucesiones cortas de suma 0. Entonces $N_0^{2p}(S) = 0$.*

Demostración. Supongamos que existe T subsucesión de S de longitud $2p$ tal que $\sigma(T) = 0$. Como $D(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p - 1 < 2p$, T contiene alguna subsucesión *propia* de suma 0, digamos T'.

Como T ya tenía suma 0, el complemento de T' en T también tiene suma 0. Pero o bien T' o su complemento tiene longitud menor o igual que p. Esto contradice la hipótesis de que S no contiene subsucesiones cortas de suma 0. □

Proposición 3.6.4. *Sea $S = 0^{p-1}T$ una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ con $|S| < 3p$ tal que $N_0^p(S) = N_0^{2p}(S) = 0$. Entonces $0 \notin \Sigma(T)$.*

Demostración. Observemos que la longitud de T es a lo sumo $2p$. Si T contiene una subsucesión no vacía T' tal que $\sigma(T') = 0$, podemos completar T' con ceros hasta que su longitud sea un múltiplo de p, usando como máximo $p-1$ ceros. La sucesión así obtenida es entonces una subsucesión de S de longitud p o $2p$ cuya suma es 0. Esto contradice la hipótesis del enunciado. □

Ahora usaremos las proposiciones anteriores para demostrar el siguiente lema.

Lema 3.6.5. *Sea p un primo que tiene la Propiedad B. Si*

$$S = a^{p-1}b^{p-1}\prod_{j=1}^{p-1} c_j$$

es una sucesión en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que no contiene subsucesiones cortas de suma 0, entonces $c_1 = c_2 = \ldots = c_{p-1}$.

Demostración. Por la Proposición 3.6.1 sabemos que a y b son linealmente independientes. Aplicando un automorfismo de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ podemos suponer sin perder generalidad que $a = e_1$ y $b = e_2$. Para cada $j \in [\![1, p-1]\!]$, sean (x_j, y_j) las coordenadas del elemento c_j. Se deduce también de 3.6.1 que todos los x_j y todos los y_j son no nulos.

Consideramos la sucesión S' que se obtiene restándole e_2 a todos los elementos de S. Más precisamente tenemos

$$S' = 0^{p-1}(e_1 - e_2)^{p-1}\prod_{j=1}^{p-1}(x_j, y_j - 1).$$

Como S no tiene subsucesiones de suma 0 de longitud p ni $2p$ (lo primero es porque S no tenía subsucesiones cortas de suma 0, y lo segundo es por la Proposición 3.6.3), lo mismo sucede con S'. Ahora 3.6.4 implica que

$$(e_1 - e_2)^{p-1}\prod_{j=1}^{p-1}(x_j, y_j - 1)$$

no tiene subsucesiones de suma 0, y a su vez 3.6.2 implica que la sucesión

$$\prod_{j=1}^{p-1}(x_j, y_j - 1)$$

no tiene ninguna subsucesión cuya suma pertenezca al subespacio generado por $e_1 - e_2$.

Ahora notemos que

$$x_j \cdot e_1 + (y_j - 1) \cdot e_2 = x_j \cdot (e_1 - e_2) + (x_j + y_j - 1) \cdot e_2,$$

y entonces podemos inferir de lo anterior que la sucesión $\prod_{j=1}^{p-1}(x_j + y_j - 1)$ en $\mathbb{Z}_p$ no contiene subsucesiones de suma 0. Pero su longitud es $p-1$, y vimos en 3.2.1 que entonces necesariamente todos sus elementos son iguales. Así, obtenemos que

$$x_1 + y_1 \equiv x_2 + y_2 \equiv \ldots \equiv x_{p-1} + y_{p-1} \pmod{p}. \tag{3.5}$$

Ahora bien, para cada j podemos formar la subsucesión $S_j = a^{p-x_j} b^{p-y_j} c_j$, que claramente tiene suma 0. Como S no contiene subsucesiones cortas de suma 0, resulta

$$|S_j| = 2p - x_j - y_j + 1 > p,$$

de donde $x_j + y_j \leq p$. Esto último junto con (3.5) implica que existe un entero m con $2 \leq m \leq p$ tal que $x_j + y_j = m$ para todo $j \in [\![1, p-1]\!]$.

Vamos a descartar los casos extremos. Si $m = 2$, entonces necesariamente es $x_j = y_j = 1$ para todo j, y no hay nada más que probar. Sea ahora $m = p$. Si la sucesión en $\mathbb{Z}_p$ formada por los x_j tuviera alguna subsucesión de suma 0, entonces la subsucesión correspondiente de los y_j también tiene suma 0 (pues los y_j son los opuestos de los x_j módulo p). Luego las condiciones que tenemos implican que la sucesión formada por los x_j no tiene subsucesiones de suma 0. Pero ya notamos antes que esto implica que todos los x_j son iguales, y en consecuencia, también los y_j.

Supongamos ahora que $3 \leq m \leq p-1$. Entonces $m-1$ pertenece al intervalo $[\![2, p-2]\!]$, y su inverso módulo p, al que llamaremos t, también se puede tomar en ese intervalo. Lo que haremos a continuación es tomar un subconjunto arbitrario $I \subset [\![1, p-1]\!]$ de cardinal t y mostrar que todos los x_i con $i \in I$ son iguales entre sí, y lo mismo sucede con los y_i. Como $t \geq 2$ e I era arbitrario, de esto se deduce inmediatamente lo que queremos probar.

Fijamos $I \subset [\![1, p-1]\!]$ de cardinal t, y consideramos la subsucesión

$$S_I = e_1^{p-\left(\sum_{i\in I} x_i\right)^\star} e_2^{p-\left(\sum_{i\in I} y_i\right)^\star} \prod_{i\in I} c_i,$$

donde $x^\star$ denota al único entero del intervalo $[\![1, p]\!]$ que satisface $x^\star \equiv x \pmod{p}$.

Es evidente que $\sigma(S_I) = 0$. Por otra parte, la longitud de S_I es

$$|S_I| = 2p + t - \left[\left(\sum_{i\in I} x_i\right)^\star + \left(\sum_{i\in I} y_i\right)^\star\right].$$

La expresión entre corchetes puede ser igual a $\left[\sum_{i\in I}(x_i+y_i)\right]^\star$ o bien a ese mismo número más p. Ahora bien,

$$\left[\sum_{i\in I}(x_i+y_i)\right]^\star = (tm)^\star = t+1,$$

pues por definición de t es $t(m-1)\equiv 1 \pmod p$, es decir $tm \equiv t+1 \pmod p$. Entonces $|S_I|$ es $2p-1$ o $p-1$. El segundo caso queda descartado porque S no contiene subsucesiones cortas de suma 0. Luego $|S_I| = 2p-1$.

Afirmamos que S_I es una nube. En efecto, si este no fuera el caso, existirían subsucesiones no vacías T_1 y T_2 tales que $S_I = T_1T_2$, $\sigma(T_1)=\sigma(T_2)=0$. Pero o bien T_1 o T_2 debe tener longitud menor o igual que p, contradiciendo el hecho de que S no tiene subsucesiones cortas de suma 0. Luego S_I es una nube.

Ahora usamos que p tiene la propiedad B, y concluimos que S_I contiene algún elemento que se repite $p-1$ veces. Como $t\le p-2$, este elemento necesariamente es e_1 o e_2. Supongamos que es e_1 (el otro caso se resuelve de manera análoga). Tenemos

$$S_I = e_1^{p-1}e_2^{p-\left(\sum_{i\in I} y_i\right)^\star}\prod_{i\in I}(x_i,y_i).$$

Razonando como en la demostración de 3.6.2 vemos que el hecho de que S_I sea minimal implica que la sucesión $1^{p-\left(\sum_{i\in I} y_i\right)^\star}\prod_{i\in I} y_i$ es una sucesión minimal de suma 0 en $\mathbb{Z}_p$. Como tiene longitud p, resulta que todos sus elementos son iguales. Es decir que $y_i = 1$ para todo $i\in I$, y en consecuencia también todos los x_i con $i\in I$ son iguales. Esto concluye la demostración. □

A continuación probamos el teorema anunciado al principio de esta sección.

Teorema 3.6.6. *Si p es un primo que tiene la Propiedad B, entonces p también tiene la Propiedad C.*

Demostración. Sea S una sucesión en $\mathbb{Z}_p\oplus\mathbb{Z}_p$ de longitud $3p-3$ que no contiene subsucesiones cortas de suma 0. La sucesión $0\cdot S$ tiene longitud $3p-2 = D(\mathbb{Z}_p^3)$. Considerando la sucesión en $\mathbb{Z}_p^3$ obtenida agregando un 1 en la tercera coordenada de cada elemento, se prueba que $0\cdot S$ contiene una subsucesión de suma 0 de longitud p o $2p$. Si tuviera longitud p, podríamos obtener una subsucesión de suma 0 de S de longitud $p-1$ o p, que no puede ser porque estamos suponiendo que S no tiene subsucesiones cortas de suma 0. Entonces tiene longitud $2p$, y necesariamente tiene que usar el 0, pues en caso contrario entramos en contradicción con la Proposición 3.6.3. De todo esto concluimos que S tiene una subsucesión T de longitud $2p-1$ tal que $\sigma(T)=0$. Razonando como en la demostración del lema anterior concluimos

que T es una nube, y entonces, como p tiene la Propiedad B, hay algún elemento de T que se repite $p-1$ veces.

Hasta aquí tenemos que S es de la forma

$$S = a^{p-1} \prod_{j=1}^{2p-2} c_j.$$

Como S no tiene subsucesiones de suma 0 de longitud p ni $2p$, lo mismo sucede con la sucesión S' obtenida restándole a a todos los elementos de S, es decir

$$S' = 0^{p-1} \prod_{j=1}^{2p-2} (c_j - a).$$

Ahora por la Proposición 3.6.4 sabemos que la sucesión $S'' = \prod_{j=1}^{2p-2}(c_j - a)$ no contiene subsucesiones de suma 0, es decir, es una seminube. Si definimos

$$c = -\sum_{j=1}^{2p-2} (c_j - a),$$

resulta que cS'' es una nube, y por lo tanto, usando nuevamente que p tiene la Propiedad B, sabemos que contiene algún elemento que se repite $p-1$ veces.

Si dicho elemento **no** es c, entonces obtenemos que S contiene dos elementos distintos que se repiten $p-1$ veces cada uno, y para terminar la demostración basta invocar el Lema 3.6.5. Supongamos entonces que el elemento que se repite $p-1$ veces en cS'' es c. En este caso sólo podemos afirmar que entre los elementos c_i hay uno que se repite $p-2$ veces.

Razonando como en la demostración del lema anterior (y usando el Lema 3.6.1) vemos que podemos suponer sin pérdida de generalidad que S es de la forma

$$S = e_1^{p-2} e_2^{p-1} \prod_{j=1}^{p} (x_j, y_j)$$

donde los x_j son no nulos. (Los y_j, por otra parte, pueden tomar cualquier valor del intervalo $[\![1, p]\!]$.)

Lo que probamos antes se traduce ahora en que

$$S'' = (e_1 - e_2)^{p-2} \prod_{j=1}^{p} (x_j, y_j - 1)$$

no tiene subsucesiones de suma 0. El elemento que se repite $p-2$ veces es igual a $-\sigma(S'')$, así que la sucesión

$$(e_1 - e_2)^{p-1} \prod_{j=1}^{p} (x_j, y_j - 1)$$

es una nube.

Ahora, de manera muy similar a lo hecho en la sección anterior, usando que

$$x_j \cdot e_1 + (y_j - 1) \cdot e_2 = x_j \cdot (e_1 - e_2) + (x_j + y_j - 1) \cdot e_2$$

deducimos que la sucesión $\prod_{j=1}^{p}(x_j + y_j - 1)$ en $\mathbb{Z}_p$ es una sucesión minimal de suma 0, y por lo tanto

$$x_1 + y_1 \equiv x_2 + y_2 \equiv \ldots \equiv x_p + y_p \pmod{p}.$$

Sea $j \in [\![1, p]\!]$. De lo anterior se deduce que $x_j + y_j \not\equiv 1 \pmod{p}$. Entonces, si fuera $x_j + y_j > p$, es $x_j + y_j \geq p + 2$, y entonces en particular $x_j \geq 2$. Por lo tanto, podemos considerar la subsucesión $S_j = e_1^{p-x_j} e_2^{p-y_j}(x_j, y_j)$. Claramente S_j tiene suma 0, y su longitud es $|S_j| = 2p + 1 - (x_j + y_j) \leq p$, lo cual no puede ser porque S no contiene subsucesiones cortas de suma 0.

Entonces $x_j + y_j \leq p$ para todo j. Al igual que antes, esto implica que existe un entero m con $2 \leq m \leq p$ tal que $x_j + y_j = m$ para todo $j \in [\![1, p]\!]$.

No puede ser $m = 2$ porque tendríamos $x_j = y_j = 1$ para todo j y entonces $\prod_{j=1}^{p}(x_j, y_j)$ sería una subsucesión corta de suma 0 de S. Tampoco puede ser $m = p$, porque en ese caso para cualquier $\varnothing \neq I \subseteq [\![1, p]\!]$ tal que $\sum_{i \in I} x_i = 0$ (existe porque $D(\mathbb{Z}_p) = p$), también vale $\sum_{i \in I} y_i = 0$, y entonces $\prod_{i \in I}(x_i, y_i)$ sería una subsucesión corta de suma 0 de S.

Por lo tanto es $m \in [\![3, p-1]\!]$. Como antes, existe un único $t \in [\![2, p-2]\!]$ tal que $t(m-1) \equiv 1 \pmod{p}$, y a su vez esto implica que $(tm)^\star = t + 1$.

El resto es igual que en la demostración del Lema 3.6.5. □

Capítulo 4

Todo primo tiene la Propiedad B

En este capítulo reproduciremos y explicaremos la demostración de Christian Reiher de que todo número primo p tiene la Propiedad B. Este resultado es el contenido de su tesis de doctorado [Rei10], presentada en 2010.

Combinando este teorema con los distintos resultados probados en el Capítulo 3, podremos concluir que la igualdad $D(G) = M(G)$ es cierta para grupos de rango 3 cuyo primer factor invariante es igual a 2.

El enfoque adoptado por Reiher consiste en pensar a los elementos de las nubes y seminubes como puntos en el plano afín $\mathbb{F}_p^2$, y aprovechar esta estructura para trabajar con herramientas elementales de geometría algebraica.

4.1. Funciones μ

Sea $S = \prod_{i=1}^{2p-2} P_i$ una seminube. Intentaremos imitar lo hecho en el Capítulo 2 para extraer condiciones que deben cumplir las coordenadas de los puntos de la seminube.

Denotamos (a_i, b_i) a las coordenadas de cada punto P_i. Consideramos los polinomios

$$f_1 = \sum_{i=1}^{2p-2} a_i X_i, \qquad f_2 = \sum_{i=1}^{2p-2} b_i X_i$$

en $\mathbb{F}_p[X_1, X_2, \ldots, X_{2p-2}]$. A continuación definimos

$$f = \left[\prod_{i=1}^{2p-2} (1 - X_i)\right] - (1 - f_1^{p-1})(1 - f_2^{p-1}). \tag{4.1}$$

Al igual que como sucedía en 2.2.3, si existe $b \in \{0,1\}^{2p-2} \setminus \{(0, \ldots, 0)\}$ tal que $f(b) \neq 0$, deducimos que $f_1(b) = f_2(b) = 0$ y por lo tanto S contiene una subsucesión

de suma 0. Por definición de seminube, esto no ocurre, así que f se debe anular sobre todo ese conjunto. Además f se anula en el origen, pues ambos términos valen 1 allí. Entonces podemos decir que f se anula sobre toda la «caja» $\{0,1\}^{2p-2}$.

Lo anterior entra en contradicción con el Combinatorial Nullstellensatz si el grado de f es $2p-2$ y el coeficiente del monomio $\mathcal{M} = \prod_{i=1}^{2p-2} X_i$ en f es no nulo. A diferencia de lo que ocurrió antes, ya no es tan claro cuál es el grado de f, pues ambos términos en (4.1) tienen el mismo grado y podría haber cancelaciones. Sin embargo podemos asegurar que $\deg(f) \leq 2p-2$. En caso de que el coeficiente del monomio $\mathcal{M}$ fuera no nulo, $\deg(f)$ sería exactamente $2p-2$ y caeríamos en la contradicción antes mencionada. Por lo tanto necesariamente el coeficiente de $\mathcal{M}$ en f debe ser 0 para cualquier seminube.

Calculemos este coeficiente. En el primer término de (4.1) es claro que el monomio que nos interesa aparece exactamente una vez, con coeficiente igual a $(-1)^{2p-2} = 1$. En el segundo término, las apariciones de $\mathcal{M}$ vienen de desarrollar $f_1^{p-1} f_2^{p-1}$, así que lo que tenemos que hacer es elegir para cada copia de f_1 un índice $i \in [\![1, 2p-2]\!]$ distinto (y multiplicar los correspondientes a_i) y luego elegir los índices que sobraron en las copias de f_2 (y multiplicar los correspondientes b_j). Cada producto de esta forma lo tendremos repetido $(p-1)!^2$ veces, pues no nos importa el orden en el que elegimos los índices que van con f_1, y lo mismo con f_2. Pero el teorema de Wilson nos dice que en $\mathbb{F}_p$ vale la igualdad $(p-1)! = -1$, y entonces $(p-1)!^2 = 1$, así que no hace falta multiplicar por ese factor.

En definitiva, el coeficiente de $\mathcal{M}$ en f es

$$1 - \sum_{\substack{I \cup J = [\![1,2p-2]\!] \\ |I|=|J|=p-1}} \left(\prod_{i \in I} a_i \prod_{b \in J} b_j \right),$$

y por lo tanto la sumatoria que aparece restada debe valer 1.

En lo sucesivo nos encontraremos muchas veces con sumas de esta forma, así que será conveniente fijar una notación más compacta.

Definición 4.1.1. Sea $S = \prod_{i=1}^{\ell} P_i$ una sucesión en $\mathbb{F}_p^2$, $P_i = (a_i, b_i)$ para cada $i \in [\![1, \ell]\!]$. Si $m \leq \ell$ es un entero no negativo, denotamos

$$\mu_m(S) = \mu_m(P_1, P_2, \ldots, P_\ell) = \sum_{\substack{I \cup J = [\![1,\ell]\!] \\ |I|=m}} \left(\prod_{i \in I} a_i \prod_{b \in J} b_j \right). \tag{4.2}$$

(El símbolo $\cup$ indica unión disjunta.)

Observación 4.1.2. El valor de μ_m depende sólo de cuáles son los puntos de S, y no del orden en el que fueron numerados.

Con esta notación, lo que probamos antes se puede enunciar de la siguiente manera.

Proposición 4.1.3. *Si S es una seminube, entonces $\mu_{p-1}(S) = 1$.*

A continuación probaremos algunas propiedades de las funciones μ_m que usaremos más adelante.

Proposición 4.1.4. *El valor de μ_m se puede calcular de forma recursiva, de la siguiente manera:*

$$\mu_m(P_1, P_2, \ldots, P_\ell) = a_1\mu_{m-1}(P_2, \ldots, P_\ell) + b_1\mu_m(P_2, \ldots, P_\ell).$$

Demostración. Separamos los términos de la sumatoria (4.2) en dos grupos, según si $1 \in I$ o $1 \in J$. En el primer grupo podemos sacar a_1 de factor común, y lo que queda es igual a

$$\sum_{\substack{I' \cup J = [\![2,\ell]\!] \\ |I'| = m-1}} \left(\prod_{i \in I} a_i \prod_{b \in J} b_j \right) = \mu_{m-1}(P_2, \ldots, P_\ell),$$

donde hemos llamado $I' = I \setminus \{1\}$.

Análogamente, en el segundo grupo podemos sacar factor común b_1, y lo que queda es $\mu_m(P_2, \ldots, P_\ell)$, pues ahora el conjunto que perdió un elemento es J, mientras que I sigue teniendo m elementos. Así, obtenemos la igualdad deseada. □

Proposición 4.1.5. *μ_m es multilineal.*

Demostración. Como el valor de μ_m no depende de la numeración de los puntos, basta probar la linealidad en la primera coordenada.

Sea $\lambda \in \mathbb{F}_p$. Usando la Proposición 4.1.4 tenemos que

$$\begin{aligned} \mu_m(\lambda P_1, P_2, \ldots, P_\ell) &= \lambda a_1\mu_{m-1}(P_2, \ldots, P_\ell) + \lambda b_1\mu_m(P_2, \ldots, P_\ell) \\ &= \lambda\mu_m(P_1, P_2, \ldots, P_\ell), \end{aligned}$$

así que μ_m saca escalares.

Ahora sea $P_1' = (a_1', b_1')$ otro punto de $\mathbb{F}_p^2$. Nuevamente usando 4.1.4 obtenemos

$$\mu_m(P_1 + P_1', P_2, \ldots, P_\ell) = (a_1 + a_1')\mu_{m-1}(P_2, \ldots, P_\ell) + (b_1 + b_1')\mu_m(P_2, \ldots, P_\ell).$$

Reagrupando los términos de la derecha se ve que esto es igual a

$$\mu_m(P_1, P_2, \ldots, P_\ell) + \mu_m(P_1', P_2, \ldots, P_\ell).$$

Por lo tanto, μ_m también separa sumas. □

Combinando estas observaciones ya podemos probar un primer resultado interesante sobre la estructura de las nubes en $\mathbb{F}_p^2$.

Corolario 4.1.6. *Si en una nube hay dos puntos que son linealmente dependientes, entonces son iguales.*

Demostración. Sea $S = \prod_{i=1}^{2p-1} P_i$ una nube en la que P_1 y P_2 son linealmente dependientes. Como P_1 es no nulo, existe $\lambda \in \mathbb{F}_p$ tal que $P_2 = \lambda P_1$. Ahora bien, las sucesiones que se obtienen a partir de S quitando el punto P_1 y quitando el punto P_2 son seminubes. Luego podemos aplicar la Proposición 4.1.3 y concluir que

$$\mu_{p-1}(P_1, P_3, \ldots, P_{2p-1}) = \mu_{p-1}(P_2, P_3, \ldots, P_{2p-1}) = 1.$$

Por otra parte, como μ_{p-1} es multilineal, sabemos que

$$\mu_{p-1}(P_2, P_3, \ldots, P_{2p-1}) = \lambda \mu_{p-1}(P_1, P_3, \ldots, P_{2p-1}).$$

Entonces necesariamente es $\lambda = 1$, es decir $P_1 = P_2$, como queríamos demostrar. □

En el caso particular $\ell = 2p-2$, $m = p-1$, con el que nos toparemos con cierta frecuencia en el estudio de nubes y seminubes, se cumple además la siguiente propiedad muy útil.[1]

Proposición 4.1.7. *Sea K un cuerpo de característica p y sea $\varphi \in \mathrm{Aut}(K^2)$. Entonces*

$$\mu_{p-1}(\varphi P_1, \varphi P_2, \ldots, \varphi P_{2p-2}) = (\det \varphi)^{p-1} \cdot \mu_{p-1}(P_1, P_2, \ldots, P_{2p-2}).$$

En particular, si $K = \mathbb{F}_p$, vemos que el valor de μ_{p-1} es estable por cambio de coordenadas.

Demostración. Identificamos a los automorfismos de K^2 con las matrices inversibles de 2×2 con coeficientes en K. Como el determinante es multiplicativo, basta verificar que la proposición se cumple para un conjunto de matrices que generen el grupo $GL(2, K)$. Un tal sistema de generadores viene dado por las matrices $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ con $\lambda \in K^\times$, la matriz $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ y la matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Estas matrices generan $GL(2, K)$ porque se corresponden con las operaciones elementales de multiplicar una fila por un escalar no nulo, intercambiar dos filas, y sumarle una fila a la otra. Es conocido

[1] La razón por la cual enunciamos este resultado para un cuerpo arbitrario K en vez de sólo para $\mathbb{F}_p$ se verá en la demostración de 4.3.6.

que aplicando dichas operaciones se puede llevar cualquier matriz inversible a la identidad. Entonces, multiplicando varias veces estas matrices conseguimos la inversa de cualquier matriz inversible, que es lo mismo que decir que conseguimos cualquier matriz inversible.

Si φ es multiplicar por la matriz $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$, entonces $\varphi P_i = (\lambda a_i, b_i)$. Luego, al aplicar φ, en cada término de la suma

$$\sum_{\substack{I \cup J = [\![1,2p-2]\!] \\ |I|=p-1}} \left(\prod_{i \in I} a_i \prod_{b \in J} b_j \right) \tag{4.3}$$

hay exactamente $p-1$ factores que se multiplican por λ (aquellos que corresponden a índices de I). Entonces

$$\mu_{p-1}(\varphi P_1, \varphi P_2, \ldots, \varphi P_{2p-2}) = \lambda^{p-1} \mu_{p-1}(P_1, P_2, \ldots, P_{2p-2}).$$

Como $\det \varphi = \lambda$, en este caso se cumple la proposición.

Si φ es multiplicar por $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, entonces $\varphi P_i = (b_i, a_i)$. Luego aplicar φ es intercambiar los roles de I y J en la suma (4.3). Pero en el caso que estamos considerando, ambos conjuntos tienen la misma cantidad de elementos. Por lo tanto es claro que el resultado final no se modifica. Esto es consistente con la proposición pues en este caso es $\det \varphi = -1$, y $(-1)^{p-1} = 1$.

Finalmente, supongamos que φ es multiplicar por $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. En este caso se tiene $\varphi P_i = (a_i + b_i, b_i)$. Al desarrollar el producto

$$\prod_{i \in I} (a_i + b_i) \prod_{j \in J} b_j$$

obtenemos

$$\sum_{\substack{K \cup L = [\![1,2p-2]\!] \\ K \subseteq I}} \left(\prod_{k \in K} a_k \prod_{l \in L} b_l \right).$$

Ahora tenemos que sumar esto sobre todas las posibles particiones (I, J) de $[\![1, 2p-2]\!]$ con $|I| = |J| = p-1$. Al hacer esto, cada posible término

$$\prod_{k \in K} a_k \prod_{l \in L} b_l$$

aparece contado tantas veces como subconjuntos I de $p-1$ elementos haya tales que $K \subseteq I$. Equivalentemente, tantas veces como subconjuntos J de $p-1$ elementos

haya tales que $J \cap K = \varnothing$. La cantidad de estos subconjuntos es

$$\binom{2p-2-|K|}{p-1}.$$

De todo esto se obtiene

$$\mu_{p-1}(\varphi P_1, \varphi P_2, \ldots, \varphi P_{2p-2}) = \sum_{m=0}^{p-1} \binom{2p-2-m}{p-1} \mu_m(P_1, P_2, \ldots, P_{2p-2}). \tag{4.4}$$

Ahora bien,

$$\binom{2p-2-m}{p-1} = \frac{(2p-2-m)!}{(p-1)!(p-1-m)!}.$$

Si $m \leq p-2$, el numerador de la fracción es divisible por p, mientras que el denominador no lo es. Como estamos en un cuerpo de característica p, esto significa que todos los términos de la sumatoria (4.4), exceptuando el último, valen 0. En el caso $m = p-1$, el combinatorio que aparece es igual a 1, y entonces queda

$$\mu_{p-1}(\varphi P_1, \varphi P_2, \ldots, \varphi P_{2p-2}) = \mu_{p-1}(P_1, P_2, \ldots, P_{2p-2}),$$

que es lo que queríamos pues en este caso es $\det \varphi = 1$. □

4.2. Ecuaciones estratégicas

Dada una nube $S = (P_1, P_2, \ldots, P_{2p-1})$, para cualquier $i \in [\![1, 2p-1]\!]$ se tiene que la sucesión $(P_1, \ldots, \widehat{P_i}, \ldots, P_{2p-1})$, obtenida quitándole el i-ésimo término a S, es una seminube. A cada una de las seminubes así obtenidas podemos aplicarle la Proposición 4.1.3. De este modo conseguimos varias ecuaciones polinomiales que deben satisfacer las coordenadas de los puntos de cualquier nube.

En esta sección veremos cómo obtener otra familia de ecuaciones polinomiales que debe satisfacer una nube, a las que llamaremos *ecuaciones estratégicas*. Estas ecuaciones, junto con las que ya tenemos, nos ayudarán en nuestro objetivo de caracterizar completamente todas las nubes.

Antes de probar el teorema necesitamos algunos preliminares.

Definición 4.2.1. Si $P = (a_1, b_1)$ y $Q = (a_2, b_2)$ son dos puntos en $\mathbb{F}_p^2$, denotamos

$$[PQ] := \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = a_1 b_2 - b_1 a_2.$$

Observemos que $[PP] = 0$ para todo $P \in \mathbb{F}_p^2$ y que $[PQ] = -[QP]$ para todos $P, Q \in \mathbb{F}_p^2$.

La siguiente propiedad también es de verificación inmediata.

Proposición 4.2.2. *Sea φ un automorfismo de $\mathrm{Aut}(\mathbb{F}_p^2)$. Denotamos $P' = \varphi(P)$, $Q' = \varphi(Q)$. Entonces $[P'Q'] = \det(\varphi)[PQ]$.*

Como último preliminar, veamos cómo calcular un cierto coeficiente de algunos polinomios, que aparecerán varias veces en la demostración del próximo teorema.

Lema 4.2.3. *Sea $S = \prod_{i=1}^{\ell} P_i$ una sucesión en $\mathbb{F}_p^2$, $P_i = (a_i, b_i)$ para cada i. Consideramos los polinomios f_1 y f_2 en $\mathbb{F}_p[X_1, X_2, \ldots, X_\ell]$ dados por*

$$f_1 = \sum_{i=1}^{\ell} a_i X_i, \qquad f_2 = \sum_{i=1}^{\ell} b_i X_i.$$

Entonces, en el polinomio $f = f_1^m f_2^{\ell-m}$, el coeficiente correspondiente al monomio $\prod_{i=1}^{\ell} X_i$ es igual a

$$m!(\ell - m)!\mu_m(P_1, P_2, \ldots, P_\ell).$$

Demostración. Es claro que para obtener el monomio buscado, en cada aparición de f_1 debemos elegir un índice $i \in [\![1, \ell]\!]$ distinto (y multiplicar los correspondientes a_i) y luego elegir los índices que sobraron en las copias de f_2 (y multiplicar los correspondientes b_j). Tendremos entonces una suma donde aparecen los términos que definen a $\mu_m(P_1, P_2, \ldots, P_\ell)$, pero cada uno aparece repetido $m!(\ell - m)!$ veces, pues no nos importa el orden en el que elegimos los índices que van con f_1, y lo mismo con los de f_2. De esto se deduce el lema. □

Ahora sí, podemos probar el teorema correspondiente a esta sección.

Teorema 4.2.4. *Supongamos que $p > 2$ y sea $S = ABCP_1P_2 \cdots P_{2p-5}$ una seminube en $\mathbb{F}_p^2$. Dados tres puntos $U, V, W \in \mathbb{F}_p^2$, denotamos*

$$\mu^\star(U, V, W) := \mu_{p-1}(U, V, W, P_1, P_2, \ldots, P_{2p-5}).$$

Vale entonces la siguiente igualdad:

$$[BC]\mu^\star(A, A, A) + [CA]\mu^\star(B, B, B) + [AB]\mu^\star(C, C, C) + 3([BC] + [CA] + [AB])\mu^\star(A, B, C) = 0. \quad (4.5)$$

Demostración. Si dos de los puntos A, B, C son iguales, entonces el resultado vale trivialmente sin importar la definición de $\mu^\star$. En efecto, si por ejemplo $B = C$, el primer sumando vale 0 pues $[BC] = 0$, el segundo sumando se cancela con el tercero pues $[CA] = -[AB]$, y el cuarto sumando vale 0 pues

$$[BC] + [CA] + [AB] = 0.$$

Supongamos entonces que A, B, C son distintos dos a dos. En virtud del Corolario 4.1.6 podemos afirmar que cada par de ellos son linealmente independientes. Como la conclusión del teorema no cambia al aplicar un automorfismo de $\mathbb{F}_p^2$ (vimos en 4.1.7 que el valor de cada $\mu^\star$ no se modifica, y en 4.2.2 que cada corchete se multiplica por $\det(\varphi) \neq 0$), podemos suponer sin perder generalidad que $A = (1, 0)$ y $B = (0, 1)$.

Sea $C = (x, y)$. Notar que x e y deben ser no nulos para que $\{A, C\}$ y $\{B, C\}$ sean linealmente independientes.

Para no recargar la notación, por el resto de esta demostración escribiremos simplemente μ_m para referirnos a $\mu_m(P_1, P_2, \ldots, P_{2p-5})$.

Aplicando reiteradas veces la Proposición 4.1.4 obtenemos las siguientes expresiones para los $\mu^\star$ en términos de los μ_m:[2]

$$\begin{aligned}
\mu^\star(A, A, A) &= \mu_{p-4}, \\
\mu^\star(B, B, B) &= \mu_{p-1}, \\
\mu^\star(C, C, C) &= x^3\mu_{p-4} + 3x^2y\mu_{p-3} + 3xy^2\mu_{p-2} + y^3\mu_{p-1}, \\
\mu^\star(A, B, C) &= x\mu_{p-3} + y\mu_{p-2}.
\end{aligned}$$

Además $[BC] = -x$, $[CA] = -y$ y $[AB] = 1$. Reemplazando todo esto en (4.5) y reordenando términos vemos que lo que debemos probar es

$$\begin{aligned}
(x^3 - x)\mu_{p-4} + (3x - 3x^2 - 3xy + 3x^2y)\mu_{p-3} \\
+ (3y - 3xy - 3y^2 + 3xy^2)\mu_{p-2} + (y^3 - y)\mu_{p-1} = 0,
\end{aligned}$$

o equivalentemente

$$(x^3 - x)\mu_{p-4} + 3x(x-1)(y-1)\mu_{p-3} + 3y(x-1)(y-1)\mu_{p-2} + (y^3 - y)\mu_{p-1} = 0. \quad (4.6)$$

Para demostrar (4.6) consideramos tres casos, que no son excluyentes pero cubren todas las posibilidades.

Caso 1: $x = 1$ o $y = 1$.

Sin pérdida de generalidad podemos suponer que $x = 1$. En tal caso la ecuación (4.6) se simplifica a $(y^3 - y)\mu_{p-1} = 0$, que como sabemos que $y \neq 0$ equivale a

$$(y^2 - 1)\mu_{p-1} = 0. \quad (4.7)$$

Es claro que esto vale si $y = \pm 1$, así que supongamos que esto no ocurre. (Notar que para que pueda darse esta situación debe ser $p > 3$.)

[2] En estas fórmulas, interpretamos $\mu_m = 0$ en caso de que sea $m < 0$. (Esta situación sólo se da si $p = 3$.)

Sean (a_i, b_i) las coordenadas de cada punto P_i. Consideramos los polinomios $f_1 = \sum_{i=1}^{2p-5} a_i X_i$ y $f_2 = \sum_{i=1}^{2p-5} b_i X_i$. Sea

$$f = \left[\prod_{m\in\mathbb{F}_p\setminus\{1\}} (f_1 + m)\right] \cdot \left[\prod_{n\in\mathbb{F}_p\setminus\{0,1,y,y+1\}} (f_2 + n)\right].$$

Supongamos que logramos probar que existe $b \in \{0,1\}^{2p-5}$ tal que $f(b) \neq 0$. Esto significa que la sucesión $P_1P_2\cdots P_{2p-5}$ contiene una subsucesión T tal que la primera coordenada de $\sigma(T)$ es -1 y la segunda coordenada de $\sigma(T)$ es 0, -1, $-y$ o $-(y+1)$. Sin embargo, la sucesión ABC contiene subsucesiones de suma $(1,0)$, $(1,1)$, $(1,y)$ y $(1,y+1)$, que son A, AB, C y BC respectivamente. Entonces, uniendo alguna de estas subsucesiones a T obtendríamos una subsucesión de suma 0 de S, lo cual contradice el hecho de que S sea una seminube.

Si el coeficiente de $\prod_{i=1}^{2p-5} X_i$ en f fuera no nulo, podríamos usar el Combinatorial Nullstellensatz para concluir que f no puede anularse sobre todos los puntos de $\{0,1\}^{2p-5}$ y llegar al absurdo antes mencionado. (Aquí es donde usamos la suposición adicional $y \neq \pm 1$, para que los números $0, 1, y, y+1$ sean distintos dos a dos y por lo tanto $\deg(f) = 2p-5$.)

Es claro que el coeficiente de dicho monomio en f es el mismo que en $f_1^{p-1} f_2^{p-4}$, pues estamos obligados a elegir términos de grado máximo en cada factor. Ahora por el Lema 4.2.3 sabemos que este coeficiente, que tiene que ser igual a 0, es $(p-1)!(p-4)!\mu_{p-1}$. Como ni $(p-1)!$ ni $(p-4)!$ son divisibles por p, concluimos $\mu_{p-1} = 0$, y por lo tanto se cumple (4.7), como queríamos.

Caso 2: $x = -1$ o $y = -1$.

De nuevo, suponemos sin pérdida de generalidad que $x = -1$. En este caso (4.6) se simplifica a

$$6(y-1)\mu_{p-3} - 6y(y-1)\mu_{p-2} + (y^3 - y)\mu_{p-1} = 0,$$

es decir

$$(y-1)\left(6\mu_{p-3} - 6y\mu_{p-2} + (y^2+y)\mu_{p-1}\right) = 0. \tag{4.8}$$

Es claro que esto vale si $y = 1$. Por otra parte, si $y = -1$ es $A + B + C = (0,0)$, lo cual contradice el hecho de que S sea seminube. Entonces, como antes, asumimos $y \neq \pm 1$.

La idea ahora es, como en el caso anterior, armar un polinomio f cuya no anulación nos lleve a algo que implique que S contiene subsucesiones de suma 0; poder deducir entonces que el coeficiente de $\prod_{i=1}^{2p-5} X_i$ en f es nulo, y que eso implique la validez de (4.8).

Consideremos el siguiente polinomio auxiliar:

$$g(s,t) = 2t^2 - 2yst + (y^2+y)s^2 + 2(y+1)t - (y^2+y)s.$$

Este polinomio cumple dos propiedades especiales. En primer lugar, se anula en los siguientes seis puntos:

$$(1,0),(1,-1),(0,0),(0,-y-1),(-1,-y),(-1,-y-1).$$

En segundo lugar, el coeficiente de $\prod_{i=1}^{2p-5} X_i$ en $f_1^{p-3}f_2^{p-4}g(f_1,f_2)$ es

$$2(p-3)!(p-2)!\mu_{p-3} - 2y(p-2)!(p-3)!\mu_{p-2} + (y^2+y)(p-1)!(p-4)!\mu_{p-1}.$$

Sacando factor común $(p-4)!^2 \neq 0$, vemos que este coeficiente es nulo si y sólo si

$$-36\mu_{p-3} + 36y\mu_{p-2} - 6(y^2+y)\mu_{p-1} = 0.$$

Como $p > 3$, podemos dividir por -6, y lo que obtenemos es exactamente el segundo factor de (4.8). (¡Magia!)

Ahora veamos cómo usar estos hechos. El polinomio que consideramos en este caso es

$$f = \left[\prod_{m\in\mathbb{F}_p\setminus\{-1,0,1\}} (f_1+m)\right]\cdot\left[\prod_{n\in\mathbb{F}_p\setminus\{0,1,y,y+1\}} (f_2+n)\right]\cdot g(f_1,f_2).$$

El coeficiente de $\prod_{i=1}^{2p-5} X_i$ en f es el que ya calculamos. Si (4.8) no se cumple, entonces este coeficiente es no nulo. Por el Combinatorial Nullstellensatz, existirá $b \in \{0,1\}^{2p-5}$ tal que $f(b) \neq 0$. De la misma forma que en el caso anterior, vemos que esto se traduce en que existe una subsucesión T de $P_1P_2\cdots P_{2p-5}$ tal que

$$\sigma(T) \in \{1,0,-1\}\times\{0,-1,-y,-y-1\}.$$

Pero de estas 12 parejas debemos descartar 6 donde g se anula. Entonces tenemos 6 posibles valores para $\sigma(T)$. Para cada uno de estos valores, existe una subsucesión de ABC cuya suma es el opuesto de ese valor. Mostramos la información en una tabla.

$\sigma(T)$	Subsucesión con suma $-\sigma(T)$
$(1,-y)$	C
$(1,-y-1)$	BC
$(0,-1)$	B
$(0,-y)$	AC
$(-1,0)$	A
$(-1,-1)$	AB

En cualquiera de los casos llegamos a una contradicción con el hecho de que S es una seminube. Esta contradicción provino de suponer que no se cumplía (4.8), con lo cual también en este caso hemos terminado.

Caso 3: $x \neq \pm 1$ e $y \neq \pm 1$.
Esta vez, el polinomio a considerar es

$$f = \left[\prod_{m \in \mathbb{F}_p \setminus \{0,1,x,x+1\}} (f_1 + m)\right] \cdot \left[\prod_{n \in \mathbb{F}_p \setminus \{0,1,y,y+1\}} (f_2 + n)\right] \cdot g(f_1, f_2),$$

donde

$$\begin{aligned} g(s,t) = {} & (x - x^3)t^3 - x(x-1)(y-1)st^2 - y(x-1)(y-1)s^2t + (y - y^3)s^3 \\ & + (x - x^3)(2y+1)t^2 - (x-1)(y-1)(2xy + x + y)st + (y - y^3)(2x+1)s^2 \\ & + (x - x^3)y(y+1)t + (y - y^3)x(x+1)s. \end{aligned}$$

El coeficiente de $\prod_{i=1}^{2p-5} X_i$ en f es igual a

$$\begin{aligned} & (x - x^3)(p-4)!(p-1)!\mu_{p-4} - x(x-1)(y-1)(p-3)!(p-2)!\mu_{p-3} \\ & \qquad - y(x-1)(y-1)(p-2)!(p-3)!\mu_{p-2} + (y - y^3)(p-1)!(p-4)!\mu_{p-1}. \end{aligned}$$

Sacando factor común $(p-4)!^2 \neq 0$, vemos que este coeficiente se anula si y sólo si

$$-6(x - x^3)\mu_{p-4} + 18x(x-1)(y-1)\mu_{p-3} + 18y(x-1)(y-1)\mu_{p-2} - 6(y - y^3)\mu_{p-1} = 0,$$

y como $p > 3$ podemos dividir por 6, obteniendo que lo anterior equivale a

$$(x^3 - x)\mu_{p-4} + 3x(x-1)(y-1)\mu_{p-3} + 3y(x-1)(y-1)\mu_{p-2} + (y^3 - y)\mu_{p-1} = 0,$$

que es precisamente (4.6).

Entonces, de manera similar a lo hecho en el caso anterior, la falsedad de (4.6) implicaría que $P_1P_2 \cdots P_{2p-5}$ contiene una subsucesión T tal que

$$\sigma(T) \in \{0, -1, -x, -x-1\} \times \{0, -1, -y, -y-1\}.$$

Pero de estas 16 parejas debemos descartar 10, que corresponden a puntos donde g se anula. Más precisamente,

$$\begin{aligned} g(0,0) = g(0,-y) = g(0,-y-1) = g(-1,-y) = g(-1,-y-1) = g(-x,0) \\ = g(-x,-1) = g(-x-1,0) = g(-x-1,-1) = g(-x-1,-y-1) = 0. \end{aligned}$$

De nuevo, nos quedan sólo 6 posibilidades, y en cada una de ellas llegamos a un absurdo, usando la información de la siguiente tabla.

$\sigma(T)$	Subsucesión con suma $-\sigma(T)$
$(0,-1)$	B
$(-1,0)$	A
$(-1,-1)$	AB
$(-x,-y)$	C
$(-x,-y-1)$	BC
$(-x-1,-y)$	AC

La demostración está completa. □

4.3. Sucesiones mágicas

En virtud del Corolario 4.1.6, para probar que un primo p tiene la Propiedad B basta probar que en toda nube hay $p-1$ puntos que están sobre un mismo subespacio de dimensión 1. En esta sección probaremos un lema que nos permite concluir algo similar para sucesiones de longitud $2p-1$ que satisfagan un cierto sistema de ecuaciones polinomiales. Si bien las nubes no cumplen estas condiciones, en varios momentos de la demostración del teorema que da nombre a este capítulo lo que haremos será modificar apropiadamente la nube dada para que cumpla las hipótesis de este lema, y luego ver cómo recuperar desde allí la información que necesitamos.

A lo largo de esta sección, trabajamos sobre un cuerpo arbitrario K de característica p.

Definición 4.3.1. Sea $S = \prod_{i=1}^{2p-1} P_i$ una sucesión de longitud $2p-1$ en K^2. La sucesión S se dice *mágica* si satisface las siguientes dos propiedades:

- $P_i \neq (0,0)$ para todo $i \in [\![1, 2p-1]\!]$,
- $\mu_{p-1}(P_1, \ldots, \widehat{P_i}, \ldots, P_{2p-1}) = 0$ para todo $i \in [\![1, 2p-1]\!]$.

Observación 4.3.2. Ninguna nube es mágica, pues de hecho vimos en 4.1.3 que en tal caso se tiene $\mu_{p-1}(P_1, \ldots, \widehat{P_i}, \ldots, P_{2p-1}) = 1$ para todo i.

Es fácil ver que cualquier sucesión S cuyos términos sean todos distintos del origen y que contenga $p+1$ puntos cuya segunda coordenada es 0, es mágica: no importa cuál sea el punto que quitemos, nos quedan al menos p de dichos puntos, y por lo tanto, en cada uno de los productos que hacemos para calcular μ_{p-1} elegimos la segunda coordenada de alguno de ellos, así que el resultado final es 0. Como además el hecho de que μ_{p-1} se anule o no es invariante por automorfismos, concluimos que cualquier sucesión que contenga $p+1$ puntos sobre un mismo subespacio de dimensión 1 es mágica. El próximo lema muestra que vale la recíproca.

Lema 4.3.3. *Si $S = \prod_{i=1}^{2p-1} P_i$ es una sucesión mágica, entonces S contiene $p+1$ puntos sobre un mismo subespacio de dimensión 1.*

Demostración. Observemos en primer lugar que la propiedad de ser una sucesión mágica se mantiene si multiplicamos alguno de los puntos de la sucesión por un escalar no nulo (pues μ_{p-1} es multilineal). Usando reiteradas veces este hecho, podemos suponer que nuestra sucesión mágica S tiene la propiedad de que para cualesquiera dos índices i, j, los puntos P_i y P_j o bien son iguales o bien son linealmente independientes.

Vamos a demostrar que si tomamos algún P_i que aparece como máximo p veces en la sucesión S, reemplazando este punto por cualquier otro punto distinto del origen volvemos a obtener una sucesión mágica. Teniendo esto, es fácil ver que si existiera una sucesión mágica en la que ningún punto tiene multiplicidad mayor que p, haciendo varios de estos cambios podríamos concluir que la sucesión $e_1^p e_2^{p-1}$ es mágica, lo cual es falso (pues claramente $\mu_{p-1}(e_1^{p-1} e_2^{p-1}) = 1$).

Supongamos que el punto P_1 tiene multiplicidad menor o igual que p. Reacomodando términos podemos suponer que existe un $r \in [\![1, p]\!]$ tal que si $i \leq r$ es $P_i = P_1$, y si $i > r$ entonces P_i es linealmente independiente con P_1.

Llamamos (a_i, b_i) a las coordenadas de cada punto P_i, y sea $Q = (x, y)$ un punto distinto del origen. Queremos probar que la sucesión $QP_2P_3 \cdots P_{2p-1}$ es mágica, es decir que si le quitamos cualquiera de sus puntos obtenemos una sucesión para la cual el valor de μ_{p-1} es 0. Es claro que esto se cumple si el punto que quitamos es Q, pues S era mágica. Ahora veamos qué pasa si quitamos un punto P_i.

Usaremos la siguiente notación: dados ciertos índices

$$1 \leq i_1 < i_2 < \ldots < i_k \leq 2p-1,$$

denotamos

$$\mu_m[i_1, i_2, \ldots, i_k] := \mu_m(P_1, \ldots, \widehat{P_{i_1}}, \ldots, \widehat{P_{i_2}}, \ldots, \widehat{P_{i_k}}, \ldots, P_{2p-1}).$$

Así, por ejemplo, la segunda condición que debe cumplir S para ser mágica es que $\mu_{p-1}[i] = 0$ para todo i.

Usando nuevamente la Proposición 4.1.4, obtenemos que

$$\mu_{p-1}(Q, P_2, \ldots, \widehat{P_i}, \ldots, P_{2p-1}) = x\mu_{p-2}[1, i] + y\mu_{p-1}[1, i].$$

Como queremos ver que esto es 0 independientemente de los valores de x e y, lo que tenemos que probar es que $\mu_{p-2}[1, i] = \mu_{p-1}[1, i] = 0$ para todo $i \in [\![2, 2p-1]\!]$.

Se deduce también de 4.1.4 que valen las siguientes ecuaciones:

$$a_1\mu_{p-2}[1, i] + b_1\mu_{p-1}[1, i] = \mu_{p-1}[i] = 0,$$
$$a_i\mu_{p-2}[1, i] + b_i\mu_{p-1}[1, i] = \mu_{p-1}[1] = 0.$$

Si $i > r$, entonces la matriz $\begin{pmatrix} a_1 & b_1 \\ a_i & b_i \end{pmatrix}$ es inversible, y por lo tanto lo anterior implica $\mu_{p-2}[1,i] = \mu_{p-1}[1,i] = 0$, como queríamos.

Esto concluye la demostración del lema si $r = 1$. Ahora, supongamos que $r > 1$. Nos falta probar que se cumple la igualdad $\mu_{p-2}[1,i] = \mu_{p-1}[1,i] = 0$ para los índices $i \in [\![2, r]\!]$.

Como en una sucesión mágica todos los puntos son distintos del origen, alguna de las dos coordenadas de P_1 debe ser no nula. Supongamos sin pérdida de generalidad que $a_1 \neq 0$.

Afirmamos que

$$\sum_{i=2}^{2p-1} a_i \mu_{p-2}[1,i] = (p-1)\mu_{p-1}[1] = 0. \tag{4.9}$$

Esto es así porque al calcular la sumatoria del primer miembro, cada uno de los sumandos que definen a $\mu_{p-1}[1]$ aparece repetido $p-1$ veces, según cuál sea el índice i que decidimos apartar.

Por otra parte, ya probamos antes que los términos con $i > r$ son iguales a 0, y los restantes son todos iguales (pues los puntos $P_1, P_2, \ldots, P_r$ son iguales). Fijamos un $i \in [\![2, r]\!]$ cualquiera, y entonces (4.9) se simplifica a

$$(r-1)a_i \mu_{p-2}[1,i] = 0,$$

lo cual, como $1 < r \leq p$ y $a_i = a_1 \neq 0$, implica $\mu_{p-2}[1,i] = 0$, como queríamos.

Análogamente se demuestra que

$$\sum_{i=2}^{2p-1} a_i \mu_{p-1}[1,i] = p\mu_p[1] = 0$$

(ahora la razón por la que esto da 0 no es que la sucesión sea mágica sino que estamos trabajando en característica p). Se concluye igual que antes que $\mu_{p-1}[1,i] = 0$ para todo i.

Con esto probamos que la sucesión $QP_2P_3 \cdots P_{2p-1}$ es mágica para cualquier punto Q distinto del origen, y vimos al principio cómo esto implica el enunciado del lema. □

Puede llegar a suceder que no podamos verificar directamente que una sucesión es mágica. Más precisamente, nos toparemos frecuentemente con una situación en la cual sólo sabremos que la igualdad $\mu_{p-1}[i] = 0$ se cumple para «casi» todos los índices i. Afortunadamente, la siguiente generalización del lema anterior nos mostrará que, a veces, con eso ya nos basta.

Usaremos la notación $P \sim Q$ para indicar que dos puntos P y Q de $K^2 \setminus \{(0,0)\}$ son linealmente dependientes, que es lo mismo que decir que ambos generan el mismo subespacio de dimensión 1.

Lema 4.3.4. *Sea $S = \prod_{i=1}^{2p-1} P_i$ una sucesión de longitud $2p-1$ en K^2 que cumple $P_i \neq (0,0)$ para todo i. Supongamos que existe una base $\{Q, R\}$ de K^2 y dos subconjuntos $A, B \subset [\![1, 2p-1]\!]$, con $|A| < p$ y $|B| < p$, tales que se cumplen las siguientes condiciones:*

- *Si $i \in A$, entonces $P_i \sim Q$;*
- *Si $i \in B$, entonces $P_i \sim R$;*
- *Si $i \in [\![1, 2p-1]\!] \setminus (A \cup B)$, entonces $\mu_{p-1}[i] = 0$.*

Entonces S es una sucesión mágica.

Demostración. Claramente, lo que nos queda probar es que la igualdad $\mu_{p-1}[i] = 0$ también vale para los índices i que están en A o en B. Por simetría basta verlo para $i \in A$.

De la misma manera que en la demostración de 4.3.3, podemos suponer sin pérdida de generalidad que todos los P_i con $i \in A$ son iguales a Q y que todos los P_i con $i \in B$ son iguales a R. Más aún, como el resultado no cambia al aplicar un automorfismo de K^2, podemos suponer que $Q = (1,0)$ y $R = (0,1)$.

Con argumentos similares a los que ya usamos se ve que vale la igualdad

$$\sum_{i=1}^{2p-1} a_i \mu_{p-1}[i] = p\mu_p(S) = 0. \tag{4.10}$$

En esta suma, los términos con $i \in B$ se anulan pues en tal caso es $a_i = 0$, y los términos con $i \notin A \cup B$ también se anulan porque en tal caso es $\mu_{p-1}[i] = 0$. Restan únicamente aquellos términos con $i \in A$, que son todos iguales pues los P_i correspondientes lo son. Fijamos un $i \in A$ cualquiera, y (4.10) se simplifica a

$$|A| \cdot \mu_{p-1}[i] = 0.$$

Si fuera $A = \varnothing$ no habría nada que probar; en caso contrario, es $0 < |A| < p$ y por lo tanto la última ecuación implica $\mu_{p-1}[i] = 0$, como queríamos. □

Observación 4.3.5. El lema también se puede usar si los puntos Q y R no son linealmente independientes. En tal caso, basta definir $A' = A \cup B$ y $B' = \varnothing$, cambiar R por cualquier punto que sea linealmente independiente con Q, y usar lo que ya demostramos. La salvedad es que ahora no basta con que $|A|$ y $|B|$ sean menores que p, sino que también precisamos $|A| + |B| < p$.

Finalizamos esta sección con un corolario que requiere trabajar sobre una extensión de K.

Corolario 4.3.6. *Supongamos que* $\mathrm{char}(K) = p > 2$. *Sea* $S = \prod_{i=1}^{2p-3} P_i$ *una sucesión de longitud* $2p-3$ *en* K^2 *tal que* $P_i \neq (0,0)$ *para todo* i. *Si existen* $a, b, c \in K$, *no todos nulos, tales que*

$$a\mu_{p-3}[i] + b\mu_{p-2}[i] + c\mu_{p-1}[i] = 0$$

para todo $i \in [\![1, 2p-3]\!]$, *entonces* S *contiene* $p-1$ *puntos sobre un mismo subespacio de dimensión* 1.

Demostración. Sea E un cuerpo de descomposición del polinomio $aX^2 + bX + c$ sobre K. Existen entonces $u_1, u_2, v_1, v_2 \in E$ tales que en $E[X]$ se cumple la igualdad de polinomios

$$(u_1X + v_1)(u_2X + v_2) = aX^2 + bX + c.$$

(Esto se puede hacer incluso si $a = 0$, tomando $u_1 = 0$ y $v_1 = 1$.)

Definimos $P_{2p-2} = (u_1, v_1)$, $P_{2p-1} = (u_2, v_2)$. Consideramos en E^2 la sucesión $S' = \prod_{i=1}^{2p-1} P_i$. Usando las fórmulas recursivas para μ tenemos que esta sucesión satisface

$$\begin{aligned}\mu_{p-1}^{S'}[i] &= u_1u_2\mu_{p-3}[i] + (u_1v_2 + u_2v_1)\mu_{p-2}[i] + v_1v_2\mu_{p-1}[i] \\ &= a\mu_{p-3}[i] + b\mu_{p-2}[i] + c\mu_{p-1}[i] \\ &= 0\end{aligned}$$

para todo $i \in [\![1, 2p-3]\!]$. (Usamos la notación $\mu_{p-1}^{S'}[i]$ para indicar que estamos usando la sucesión que se obtiene al quitarle el punto P_i a S', en vez de a S como en el enunciado del corolario.)

Ahora sólo hay que notar que podemos aplicar el Lema 4.3.4 y la Observación 4.3.5 con la sucesión S', tomando $Q = P_{2p-2}$, $R = P_{2p-1}$, $A = \{2p-2\}$ y $B = \{2p-1\}$. Esto junto con el Lema 4.3.3 nos dice que S' contiene $p+1$ puntos sobre un mismo subespacio de dimensión 1 de E^2. Como S se obtiene a partir de S' quitando los últimos dos términos, vemos que S contiene $p-1$ puntos sobre un mismo subespacio de dimensión 1 de E^2. Pero como todos los puntos de S tienen sus coordenadas en K, si dos puntos de S son linealmente dependientes sobre E entonces también son linealmente dependientes sobre K.

Esto completa la demostración. □

4.4. Posición general y cuaternas buenas

En esta sección comenzamos a recorrer el camino que conduce a demostrar que todos los primos tienen la Propiedad B.

Los pasos para la demostración serán los siguientes. Primero, en esta sección introduciremos una definición apropiada de lo que significa que 4 puntos estén en

posición general, y veremos una condición suficiente para garantizarla. Al final del capítulo probaremos que si una nube contiene 4 puntos distintos en posición general, entonces contiene un elemento con multiplicidad $p-1$, que es lo que nosotros queremos. Por razones que se verán más adelante, antes de eso analizamos los casos excepcionales, que son cuando la nube directamente no contiene 4 puntos distintos, o cuando contiene 4 puntos distintos que no están en posición general.

Salvo que se especifique lo contrario, a partir de este momento la letra K siempre denotará un cuerpo arbitrario cuya característica sea distinta de 2.

Definición 4.4.1. Sean $P_1, P_2, \ldots, P_n$ puntos en el plano afín K^2. Denotamos

$$\Gamma_d(P_1, P_2, \ldots, P_n) = \left\{ f = \sum_{i+j\leq d} \alpha_{ij} X^i Y^j \in K[X,Y] \;\middle|\; f(P_k) = 0 \ \forall k \in [\![1, n]\!] \right\}.$$

Identificamos Γ_d con un subespacio de $K^{\binom{d+2}{2}}$ asignándole a cada f el vector formado por sus coeficientes.

Para cada $f \in \Gamma_d$ sea $v_d(f) = (\alpha_{d0}, \ldots, \alpha_{0d})$ el vector formado por los coeficientes correspondientes a monomios de grado d. Definimos

$$M_d(P_1, P_2, \ldots, P_n) = \{v_d(f) \mid f \in \Gamma_d(P_1, P_2, \ldots, P_n)\}.$$

Es claro entonces que M_d es un subespacio de K^{d+1} (se obtiene a partir de Γ_d proyectando a las primeras $d+1$ coordenadas).

Observación 4.4.2. Es claro que $\dim M_d \leq \dim \Gamma_d$. En los siguientes ejemplos veremos que la igualdad puede darse o no.

Ejemplo 4.4.3. Sea $K = \mathbb{R}$ y sean $P_1 = (1,0)$, $P_2 = (0,1)$, $P_3 = (-1,0)$, $P_4 = (0,1)$. Calculemos Γ_2 y M_2 para esta cuaterna de puntos.

Estamos buscando polinomios de la forma $aX^2 + bXY + cY^2 + dX + eY + f$ que se anulen sobre esos cuatro puntos. Evaluando en $(1,0)$ y $(-1,0)$ obtenemos

$$\begin{aligned} a + d + f &= 0 \\ a - d + f &= 0, \end{aligned}$$

de donde $d = 0$ y $f = -a$. Análogamente, usando los otros dos puntos se concluye $e = 0$, $f = -c$. Luego $a = c$. Obtuvimos así

$$\Gamma_2 = \langle (1,0,1,0,0,-1); (0,1,0,0,0,0) \rangle,$$

que tiene dimensión 2. Por otra parte,

$$M_2 = \langle (1,0,1); (0,1,0) \rangle.$$

Por lo tanto, en este caso es $\dim M_d = \dim \Gamma_d$.

Ejemplo 4.4.4. Sea $K = \mathbb{R}$ y sean $P_i = (i, 0)$ para $i \in [\![1, n]\!]$, $n \geq 3$. Nuevamente, calculamos Γ_2 y M_2. El polinomio $aX^2 + dX + f$ tiene que anularse para n valores distintos de X. Esto se cumple si y sólo si $a = d = f = 0$. Por lo tanto Γ_2 tiene dimensión 3, pues los valores de b, c, e quedan libres. Por otra parte, M_2 tiene dimensión 2, pues cualquier polinomio que se anule en esos n puntos tiene $a = 0$. Entonces, en este ejemplo, es $\dim M_d < \dim \Gamma_d$.

Definición 4.4.5. Decimos que 4 puntos $A, B, C, D \in K^2$ están en *posición general* si satisfacen las siguientes dos propiedades:

- Los 14 puntos $T_1, T_2, \ldots, T_{14}$ que se pueden obtener sumando 1, 2 o 3 de estos puntos son distintos dos a dos.
- $\dim M_4(T_1, T_2, \ldots, T_{14}) \leq 2$.

Observación 4.4.6. La primera condición implica que para que cuatro puntos puedan estar en posición general, deben ser *distintos*.

Observación 4.4.7. Sea $\phi : K^2 \to K^2$ una transformación afín (es decir, un endomorfismo lineal de K^2 compuesto con una traslación). Sea $\Lambda_d = \Gamma_d(\varnothing)$ el espacio de todos los polinomios de grado menor o igual que d en $K[X, Y]$.

ϕ induce una función $\phi^* : \Lambda_d \to \Lambda_d$ definida como $\phi^*(f) = f \circ \phi$.[3]

Es fácil verificar que ϕ^* es una transformación lineal, que $(\phi\psi)^* = \psi^*\phi^*$, y que $\mathrm{id}^*_{K^2} = \mathrm{id}_{\Lambda_d}$. De todo esto se deduce que si ϕ es inversible, entonces ϕ^* es un isomorfismo.

Si ahora $P_1, P_2, \ldots, P_n$ son puntos en K^2, entonces

$$(\phi^{-1})^*(\Gamma_d(P_1, P_2, \ldots, P_n) \subseteq \Gamma_d(\phi P_1, \phi P_2, \ldots, \phi P_n),$$

y

$$\phi^*(\Gamma_d(\phi P_1, \phi P_2, \ldots, \phi P_n)) \subseteq \Gamma_d(P_1, P_2, \ldots, P_n).$$

Combinando estas dos relaciones, se ve que la dimensión de Γ_d es la misma para los puntos $P_1, P_2, \ldots, P_n$ o para los puntos $\phi P_1, \phi P_2, \ldots, \phi P_n$, y por lo tanto las inclusiones anteriores son igualdades.

Por otra parte, si bien ϕ^* no es homogénea, sí vale que Λ_{d-1}, pensado como subespacio de Λ_d, es ϕ^*-invariante. De esto se deduce que también

$$\dim M_d(P_1, P_2, \ldots, P_n) = \dim M_d(\phi P_1, \phi P_2, \ldots, \phi P_n).$$[4]

[3] Esto es un abuso de notación. Si $\phi(x, y) = (ax + by + c, dx + ey + f)$ para todo $(x, y) \in K^2$, lo que queremos decir es que $(\phi^*(f))(X, Y) = f(aX + bY + c, dX + eY + f)$.

[4] La propiedad que usamos aquí fue la siguiente: si $V = S \oplus T$ es un K-espacio vectorial de dimensión finita y $f : V \to V$ es un isomorfismo tal que T es f-invariante, entonces para cualquier subespacio $M \subseteq V$ vale que $\dim(M \cap T) = \dim(f(M) \cap T)$. Por el teorema de la dimensión se sigue que $\dim \pi_S(M) = \dim \pi_S(f(M))$.

En particular vemos que la noción de posición general es invariante por automorfismos afines.

La segunda condición que pusimos para que 4 puntos estén en posición general puede llegar a ser difícil de verificar. La definición que introduciremos a continuación resultará ser una condición *suficiente* para garantizar posición general.

Recordemos que una *cónica* en K^2 es el conjunto de ceros de un polinomio de grado 2 en $K[X, Y]$.

Definición 4.4.8. Sean $A, B, C, D \in K^2$. Llamamos $T_1, T_2, \ldots, T_{14}$ a los puntos que se pueden obtener sumando 1, 2 o 3 de los puntos A, B, C, D. Dividimos los T_i en 7 parejas de manera que los elementos de cada pareja sumen $A + B + C + D$, esto es:

$$(A, B + C + D); \quad (B, A + C + D); \quad (C, A + B + D); \quad (D, A + B + C);$$

$$(A + B, C + D); \quad (A + C, B + D); \quad (A + D, B + C).$$

Diremos que (A, B, C, D) es una *cuaterna buena* si se cumplen las siguientes tres condiciones:

- Los puntos $T_1, T_2, \ldots, T_{14}$ son distintos dos a dos.
- No se puede elegir 4 de las 7 parejas antes mencionadas de modo que los 8 puntos que las conforman sean colineales.
- No se puede elegir 6 de las 7 parejas antes mencionadas de modo que los 12 puntos que las conforman estén sobre una misma cónica.

Para probar que esta nueva definición implica posición general, necesitamos dos lemas previos.

Lema 4.4.9. *Sean $P_1, P_2, \ldots, P_n$ puntos distintos en K^2, con $n \geq 5$. Supongamos que $\dim M_2(P_1, P_2, \ldots, P_n) \geq 2$. Entonces, entre los P_i hay $n - 1$ puntos que están sobre una misma recta.*

Demostración. Veamos en primer lugar que necesariamente debe haber 3 puntos alineados. Si todos los P_i están alineados no hay nada que probar; si no, podemos encontrar tres puntos de ellos que no son colineales, que es lo mismo que decir que son *afinmente independientes*. Como la Observación 4.4.7 nos permite aplicar un automorfismo afín sin alterar las hipótesis ni la conclusión del teorema, podemos suponer sin pérdida de generalidad que $P_1 = (0, 0)$, $P_2 = (1, 0)$, $P_3 = (0, 1)$.

Evaluando un polinomio genérico $aX^2 + bXY + cY^2 + dX + eY + f$ en estos tres puntos deducimos que $f = 0$, $d = -a$ y $e = -c$. Es decir que un elemento de $\Gamma_2(P_1, P_2, \ldots, P_n)$ tiene la forma

$$a(X^2 - X) + bXY + c(Y^2 - Y).$$

Como por hipótesis es $\dim M_2(P_1, P_2, \ldots, P_n) \geq 2$, podemos encontrar un tal polinomio que sea no nulo y en el que $c = 0$. Así, existen $\alpha, \beta \in K$ tales que

$$\alpha(X^2 - X) + \beta XY = X(\alpha X + \beta Y - \alpha)$$

se anula en todos los P_i. Luego los P_i pertenecen a la unión de dos rectas; como $n \geq 5$, por el principio del palomar hay tres puntos alineados, como queríamos.

Ahora que sabemos que hay tres puntos alineados, nuevamente aplicando un automorfismo afín podemos suponer que los tres puntos están sobre la recta $y = 0$. Evaluando el polinomio genérico en estos tres puntos vemos que $aX^2 + dX + f$ debe anularse para tres valores distintos de X, lo cual implica $a = d = f = 0$. Luego, todo polinomio en $\Gamma_2(P_1, P_2, \ldots, P_n)$ tiene la forma

$$bXY + cY^2 + eY = Y(bX + cY + e).$$

Ahora bien, nosotros sabíamos que $\dim M_2(P_1, P_2, \ldots, P_n) \geq 2$, pero probamos que para cualquier polinomio de Γ_2 es $a = 0$. Entonces necesariamente el vector (b, c) tiene que poder tomar todos los valores posibles. En particular podemos hacer que valga $(1, 0)$ y $(0, 1)$. Obtenemos así dos polinomios de la forma $Y(X + \varepsilon_1)$ e $Y(Y + \varepsilon_2)$ que se anulan sobre todos los P_i.

Si algún P_i no tiene su segunda coordenada igual a 0, deducimos de lo anterior que $P_i = (-\varepsilon_1, -\varepsilon_2)$. Luego puede haber a lo sumo un punto con esta propiedad, y por lo tanto al menos $n-1$ de los puntos P_i son colineales, que era lo que queríamos demostrar. □

Las definiciones que hicimos para Γ_d y M_d se pueden generalizar perfectamente para puntos en el espacio tridimensional. La única diferencia es que ahora se consideran polinomios en tres variables X, Y, Z.

Lema 4.4.10. *Sean $P_1, P_2, \ldots, P_7$ puntos distintos en K^3. Supongamos que*

$$\dim M_2(P_1, P_2, \ldots, P_7) \geq 4.$$

Entonces, entre los P_i hay 4 puntos que son colineales o 6 puntos que son coplanares.

Demostración. Supongamos que la conclusión del teorema es falsa, es decir que entre los puntos P_i no hay 4 colineales ni 6 coplanares.

Como en la demostración anterior, aplicando un automorfismo afín podemos suponer sin pérdida de generalidad que $P_1 = (0, 0, 0)$, $P_2 = (1, 0, 0)$, $P_3 = (0, 1, 0)$, $P_4 = (0, 0, 1)$. Evaluando un polinomio genérico

$$aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ + gX + hY + jZ + i$$

en estos cuatro puntos deducimos que $i = 0$, $g = -a$, $h = -b$, $j = -c$. Es decir que todo elemento de $\Gamma_2(P_1, P_2, \ldots, P_7)$ tiene la forma

$$a(X^2 - X) + b(Y^2 - Y) + c(Z^2 - Z) + dXY + eXZ + fYZ. \tag{4.11}$$

Afirmación 1: *Entre los P_i no puede haber 5 puntos coplanares.*

Supongamos lo contrario. Sin pérdida de generalidad podemos suponer que P_1, P_2, P_3, P_5, P_6 son coplanares, es decir que la tercera coordenada de P_5 y P_6 es igual a 0. Proyectamos estos 5 puntos a las primeras dos coordenadas. Como por hipótesis no hay 4 de ellos que sean colineales, deducimos del Lema 4.4.9 que la dimensión del subespacio de los posibles vectores (a, b, d) en (4.11) es a lo sumo 1. Pero por hipótesis, el subespacio de los posibles vectores (a, b, c, d, e, f) tiene dimensión al menos 4. De esto se deduce[5] que los vectores $(0, 0, 0, 1, 0, 0)$, $(0, 0, 0, 0, 1, 0)$ y $(0, 0, 0, 0, 0, 1)$ están en $M_2(P_1, P_2, \ldots, P_7)$, es decir, que los polinomios $Z^2 - Z$, XZ e YZ se anulan sobre todos los P_i.

El punto P_7 no puede tener su tercera coordenada igual a 0, pues en ese caso habría 6 puntos coplanares. Entonces, de lo anterior se deduce que $P_7 = (0, 0, 1)$. Esto no puede ser, porque los puntos P_i eran todos distintos.

Afirmación 2: *Entre los P_i no puede haber 3 puntos colineales.*

Supongamos lo contrario. Sin pérdida de generalidad podemos suponer que P_1, P_2, P_5 son colineales, es decir que $P_5 = (t, 0, 0)$ con $t \neq 0, 1$. Evaluando (4.11) en P_5 sale que $a = 0$. Se sigue que la dimensión de los posibles vectores (b, c, d, e, f) es al menos 4, y por lo tanto en $M_2(P_1, P_2, \ldots, P_7)$ podemos encontrar dos vectores linealmente independientes de la forma $(0, \alpha, 0, \beta, 0, \gamma)$. Ahora

$$\alpha(Y^2 - Y) + \beta XY + \gamma YZ = Y(\beta X + \alpha Y + \gamma Z - \alpha).$$

Los puntos P_6 y P_7 no pueden tener la segunda coordenada igual a 0 porque en tal caso serían coplanares con P_1, P_2, P_4, P_5. Luego, P_6 y P_7 deben estar sobre el plano de ecuación $\beta X + \alpha Y + \gamma Z = \alpha$. Esto vale para los dos vectores linealmente independientes que dijimos que podíamos encontrar, así que P_6 y P_7 deben pertenecer a la recta donde se intersecan los dos planos. Lo mismo ocurre con el punto P_3, que también tiene la segunda coordenada no nula. En definitiva, P_3, P_6 y P_7 son colineales.

Ahora sólo hay que notar que podemos hacer exactamente el mismo argumento intercambiando los roles de Y y Z, es decir encontrando vectores de la forma $(0, 0, \alpha, 0, \beta, \gamma)$. Con esto concluimos que P_4, P_6 y P_7 son colineales. Pero entonces

[5]Estamos usando el siguiente resultado: si $V = S \oplus T$ es un K-espacio vectorial de dimensión finita y $M \subseteq V$ es un subespacio tal que $\dim M \geq \dim \pi_S(M) + \dim T$, entonces $M \supseteq T$. Para probarlo basta notar que por el teorema de la dimensión es $\dim \pi_S(M) = \dim M - \dim(M \cap T)$.

tenemos 4 puntos sobre una misma recta. Contradicción.

Afirmación 3: *No puede pasar que las tres cuaternas*

$$(P_1, P_2, P_3, P_7)$$
$$(P_1, P_2, P_4, P_6)$$
$$(P_1, P_3, P_4, P_5)$$

sean simultáneamente coplanares.

Supongamos lo contrario. Entonces $P_5 = (0, *, *)$, $P_6 = (*, 0, *)$, $P_7 = (*, *, 0)$, con todos los $*$ no nulos (si no fuera así, habría 3 puntos colineales).

Como $\dim M_2(P_1, P_2, \ldots, P_7) \geq 4$, en ese subespacio podemos encontrar un vector no nulo de la forma $(0, 0, 0, d, e, f)$, es decir, un polinomio no nulo de la forma $dXY + eXZ + fYZ$ que se anula sobre todos los P_i. Supongamos que el coeficiente d es no nulo (los otros casos se resuelven análogamente). Entonces los últimos dos términos se anulan en P_7, pero el primer término no. Contradicción.

Veamos cómo llegar a un absurdo con toda esta información. Como no hay 3 puntos colineales, los puntos P_5, P_6 y P_7 determinan un plano. Este plano puede contener a lo sumo uno de los puntos P_2, P_3, P_4, pues no hay 5 puntos coplanares. Supongamos entonces sin pérdida de generalidad que $P_2, P_3 \notin (P_5P_6P_7)$.

En $M_2(P_1, P_2, \ldots, P_7)$ hay algún vector no nulo de la forma $(a, 0, 0, d, e, 0)$. Entonces, hay un polinomio de la forma

$$a(X^2 - X) + dXY + eXZ = X(aX + dY + eZ - a)$$

que se anula sobre todos los P_i. Si los tres puntos P_5, P_6, P_7 tuvieran la primera coordenada no nula, entonces necesariamente están sobre el plano de ecuación $aX + dY + eZ = a$. Lo mismo ocurre con el punto P_2, que también tiene la primera coordenada no nula. Pero esto no puede ser, pues estábamos suponiendo que $P_2 \notin (P_5P_6P_7)$. Entonces, alguno de los tres puntos P_5, P_6, P_7 tiene la primera coordenada igual a 0. Sin pérdida de generalidad supongamos que $P_5 = (0, *, *)$.

De manera similar, eliminando los tres términos que no tienen Y se concluye que alguno de los puntos P_5, P_6, P_7 tiene la segunda coordenada igual a 0, y no puede ser el P_5 pues habría tres puntos colineales. Entonces, sin pérdida de generalidad es $P_6 = (*, 0, *)$.

Si fuera $P_4 \notin (P_5P_6P_7)$, podríamos repetir el argumento anterior y concluir $P_7 = (*, *, 0)$, que ya vimos en la Afirmación 3 que no puede suceder. Entonces $P_4 \in (P_5P_6P_7)$. Tenemos entonces las siguientes cuaternas de puntos coplanares:

$$\begin{array}{ll} (P_1, P_3, P_4, P_5) & \text{sobre el plano } x = 0 \\ (P_1, P_2, P_4, P_6) & \text{sobre el plano } y = 0 \\ (P_4, P_5, P_6, P_7) & \end{array}$$

Si renombramos los puntos $P_1 \leftrightarrow P_4$, $P_2 \leftrightarrow P_5$, $P_3 \leftrightarrow P_6$, vemos que esto entra en contradicción con la Afirmación 3. □

Ahora sí, probamos la relación entre las dos nociones que introdujimos en esta sección.

Proposición 4.4.11. *Si (A, B, C, D) es una cuaterna buena, entonces A, B, C, D están en posición general.*

Demostración. Supongamos que no. Como la primera condición para estar en posición general es parte de la definición de cuaterna buena, lo que tiene que pasar es que $\dim M_4(T_1, T_2, \ldots, T_{14}) \geq 3$.

Sea $E = \frac{1}{2}(A+B+C+D)$.[6] Entonces, los puntos $T_1, T_2, \ldots, T_{14}$ tienen la forma $E \pm P_i$ para ciertos puntos distintos $P_1, P_2, \ldots, P_7 \in K^2$. Sean (x_i, y_i) las coordenadas de cada punto P_i, y consideramos los puntos $Q_i = (x_i^2, x_i y_i, y_i^2) \in K^3$. Observar que los puntos Q_i son distintos.

Como el valor de $\dim M_4$ no cambia al aplicar una traslación, lo que sabemos equivale a que $\dim M_4(\pm P_1, \pm P_2, \ldots, \pm P_7) \geq 3$. Tomemos tres vectores linealmente independientes $(a_j, b_j, c_j, d_j, e_j)$ en este subespacio, con $j = 1, 2, 3$. Podemos conseguir polinomios en $\Gamma_4(\pm P_1, \pm P_2, \ldots, \pm P_7)$ de la forma

$$a_j X^4 + b_j X^3 Y + c_j X^2 Y^2 + d_j X Y^3 + e_j Y^4 + f_j X^2 + g_j XY + h_j Y^2 + i_j,$$

es decir, que no tienen términos de grado impar.[7]

Notemos que entonces el correspondiente polinomio

$$a_j X^2 + c_j Y^2 + e_j Z^2 + b_j XY + d_j YZ + f_j X + g_j Y + h_j Z + i_j$$

se anula sobre los Q_i. Con esto ya conseguimos tres vectores linealmente independientes en $M_2(Q_1, Q_2, \ldots, Q_7)$, pero podemos obtener uno más, pues el polinomio $Y^2 - XZ$ se anula sobre todos los Q_i. Luego $\dim M_2(Q_1, Q_2, \ldots, Q_7) \geq 4$. Por el Lema 4.4.10 sabemos que entre los Q_i hay 4 puntos colineales o 6 coplanares.

Supongamos que hay 4 puntos colineales, sin pérdida de generalidad $Q_1, \ldots, Q_4$. Entonces $M_2(\pm P_1, \ldots, \pm P_4)$ contiene al subespacio de dimensión 2 ortogonal a la recta que pasa por $Q_1, \ldots, Q_4$. Por el Lema 4.4.9, 7 de los puntos $\pm P_1, \ldots, \pm P_4$ son colineales, pero como esta recta contiene dos puntos opuestos, pasa por el origen y resulta que los 8 puntos son colineales. Como la colinealidad se mantiene al hacer una traslación de vector E, esto entra en contradicción con el hecho de que (A, B, C, D) era una cuaterna buena.

[6] Recordar que estábamos suponiendo que la característica de K no es 2.

[7] Esto es así porque si $f \in \Gamma_4(\pm P_1, \pm P_2, \ldots, \pm P_7)$ entonces el polinomio $\widetilde{f}$ que se obtiene cambiando el signo de los términos de grado impar de f también se anula en esos puntos; podemos tomar entonces $\frac{1}{2}\left(f + \widetilde{f}\right)$.

Supongamos ahora que hay 6 puntos coplanares, sin pérdida de generalidad $Q_1, \ldots, Q_6$. Tomamos un vector (α, β, γ) ortogonal al plano que contiene a $Q_1, \ldots, Q_6$ y vemos que existe un polinomio de la forma $\alpha X^2 + \beta XY + \gamma Y^2 + \delta$ que se anula sobre $\pm P_1, \ldots, \pm P_6$, es decir, los 12 puntos están sobre una misma cónica. De nuevo, esto contradice el hecho de que (A, B, C, D) era buena. □

4.5. Nubes con sólo 3 puntos distintos

Si una nube no contiene 4 puntos que estén en posición general, puede suceder que contenga 4 puntos distintos que no están en posición general, o que directamente no contenga 4 puntos distintos. En esta sección analizamos el segundo caso.

Como una nube tiene $2p-1$ elementos y ninguno de ellos tiene multiplicidad mayor o igual que p, por el principio del palomar debe haber *al menos* 3 puntos distintos. Luego, lo que tenemos que probar es que toda nube con exactamente 3 puntos distintos contiene a alguno de ellos con multiplicidad $p-1$.

Esto es trivial para $p = 2$, así que en el resto de esta sección suponemos $p > 2$.

Sea $S = A^\alpha B^\beta C^\gamma$ dicha nube. Podemos suponer que $\gamma \geq 2$: como α y β son menores que p, la única posibilidad de que esto no se cumpla sería si $\alpha = \beta = p-1$, en cuyo caso no hay nada que probar.

Por el Corolario 4.1.6 sabemos que A, B, C son linealmente independientes dos a dos. Aplicando un automorfismo de $\mathbb{F}_p^2$ podemos suponer sin pérdida de generalidad que $A = (1,0)$, $B = (0,1)$, $C = (x,y)$ con x e y no nulos.

Si a, b, c son tres enteros no negativos cuya suma es $2p-2$, denotamos

$$\mu^{(a,b,c)} := \mu_{p-1}(A^a B^b C^c).$$

Lema 4.5.1. *Si $a, b, c \leq p-1$, entonces*

$$\mu^{(a,b,c)} = \frac{(-1)^{a+b} a!b!c!}{x^a y^b}.$$

Demostración. Es fácil ver, usando las fórmulas recursivas para μ de la Proposición 4.1.4, que

$$\mu^{(a,b,c)} = \mu_{p-1-a}(C^c) = \binom{c}{p-1-a} x^{p-1-a} y^{c-(p-1-a)}. \tag{4.12}$$

Notemos que $a+b+c = 2p-2$ equivale a que $c-(p-1-a) = p-1-b$, así que (4.12) se puede reescribir como

$$\mu^{(a,b,c)} = \frac{c!}{(p-1-a)!(p-1-b)!} x^{p-1-a} y^{p-1-b}. \tag{4.13}$$

Ahora usamos el hecho de que estamos haciendo las cuentas en $\mathbb{F}_p$. Por un lado, como x e y son no nulos sabemos que $x^{p-1} = y^{p-1} = 1$, así que

$$x^{p-1-a}y^{p-1-b} = x^{-a}y^{-b}.$$

Por otra parte, notemos que para cualquier $1 \leq t \leq p-1$ se tiene

$$\frac{(p-1)!}{(p-1-t)!} = (p-t)(p-(t-1))\cdots(p-1) = (-1)^t t!,$$

así que si multiplicamos ambos miembros de (4.13) por $(p-1)!^2$, lo que obtenemos es

$$(p-1)!^2\mu^{(a,b,c)} = \frac{(-1)^{a+b}a!b!c!}{x^a y^b}.$$

Como por el teorema de Wilson es $(p-1)!^2 = 1$, tenemos lo que queríamos. □

Proposición 4.5.2. *Si una nube contiene exactamente* 3 *puntos distintos, entonces alguno de ellos tiene multiplicidad* $p-1$.

Demostración. Sea $S = A^\alpha B^\beta C^\gamma$ una tal nube. Como explicamos al principio, podemos suponer sin pérdida de generalidad que $\gamma \geq 2$, $A = (1,0)$, $B = (0,1)$, $C = (x,y)$.

Consideramos la seminube $A^\alpha B^\beta C^{\gamma-1} = ABC(A^{\alpha-1}B^{\beta-1}C^{\gamma-2})$. Para esta seminube, la ecuación estratégica (Teorema 4.2.4) nos dice que

$$-x\mu^{(\alpha+2,\beta-1,\gamma-2)} - y\mu^{(\alpha-1,\beta+2,\gamma-2)} + \mu^{(\alpha-1,\beta-1,\gamma+1)} + 3(-x-y+1)\mu^{(\alpha,\beta,\gamma-1)} = 0. \quad (4.14)$$

Usando el Lema 4.5.1 y operando, vemos que el primer miembro de la ecuación anterior es igual a

$$\frac{(-1)^{\alpha+\beta}(\alpha+2)!(\beta-1)!(\gamma-2)!}{x^{\alpha+1}y^{\beta-1}} + \frac{(-1)^{\alpha+\beta}(\alpha-1)!(\beta+2)!(\gamma-2)!}{x^{\alpha-1}y^{\beta+1}}$$
$$+ \frac{(-1)^{\alpha+\beta}(\alpha-1)!(\beta-1)!(\gamma+1)!}{x^{\alpha-1}y^{\beta-1}} + 3(-x-y+1)\frac{(-1)^{\alpha+\beta}\alpha!\beta!(\gamma-1)!}{x^\alpha y^\beta},$$

así que multiplicando ambos miembros de (4.14) por

$$\frac{x^{\alpha+1}y^{\beta+1}}{(-1)^{\alpha+\beta}(\alpha-1)!(\beta-1)!(\gamma-2)!}$$

(notar que numerador y denominador son no nulos) obtenemos la ecuación equivalente

$$\alpha(\alpha+1)(\alpha+2)y^2 + \beta(\beta+1)(\beta+2)x^2$$
$$+ (\gamma-1)\gamma(\gamma+1)x^2y^2 + 3(-x-y+1)\alpha\beta(\gamma-1)xy = 0. \quad (4.15)$$

Ahora notemos que x e y se pueden poner fácilmente en función de α, β y γ, pues sabemos que $\alpha A + \beta B + \gamma C = (0,0)$. Igualando cada coordenada a 0 obtenemos las ecuaciones $\alpha + \gamma x = \beta + \gamma y = 0$, de donde

$$x = \frac{-\alpha}{\gamma}, \quad y = \frac{-\beta}{\gamma}.$$

En particular se deduce que

$$-x - y + 1 = \frac{\alpha + \beta + \gamma}{\gamma} = \frac{-1}{\gamma}$$

(recordemos que $\alpha + \beta + \gamma = 2p - 1$, que es igual a -1 en $\mathbb{F}_p$). Reemplazando toda esta información en (4.15) obtenemos

$$\frac{\alpha(\alpha+1)(\alpha+2)\beta^2}{\gamma^2} + \frac{\beta(\beta+1)(\beta+2)\alpha^2}{\gamma^2} + \frac{(\gamma-1)(\gamma+1)\alpha^2\beta^2}{\gamma^3} - \frac{3\alpha^2\beta^2(\gamma-1)}{\gamma^3} = 0.$$

Multiplicamos ambos miembros por $\dfrac{\gamma^2}{\alpha^2\beta^2}$ y obtenemos

$$\frac{(\alpha+1)(\alpha+2)}{\alpha} + \frac{(\beta+1)(\beta+2)}{\beta} + \frac{(\gamma-1)(\gamma-2)}{\gamma} = 0$$

o, lo que es lo mismo,

$$(\alpha + \beta + \gamma) + (3 + 3 - 3) + 2\left(\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma}\right) = 0.$$

Como sabíamos que $\alpha + \beta + \gamma = -1$, de lo anterior se deduce que $\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma} = -1$.

Veamos que estas dos condiciones implican que alguno de los números α, β y γ es igual a $p - 1$, que es lo que queremos probar.

Sea f el polinomio mónico de grado 3 en $\mathbb{F}_p[X]$ cuyas raíces son α, β y γ. Entonces

$$\begin{aligned} f &= (X - \alpha)(X - \beta)(X - \gamma) \\ &= X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)X - \alpha\beta\gamma. \end{aligned}$$

La condición $\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma} = -1$ equivale a que $\alpha\beta + \beta\gamma + \gamma\alpha = -\alpha\beta\gamma$. Como además $\alpha + \beta + \gamma = -1$, vemos que f tiene la forma $X^3 + X^2 + tX + t$. Resulta evidente entonces que -1 es raíz de f. Por lo tanto, alguno de los tres números enteros α, β, γ es congruente a -1 módulo p, y como dicho entero se encuentra en el intervalo $[\![1, p-1]\!]$, necesariamente debe ser igual a $p - 1$.

Esto completa la demostración. □

4.6. Casos excepcionales, Parte I

Ahora nos toca trabajar con nubes que contienen 4 puntos distintos que **no** están en posición general. Esta situación sólo puede darse si $p > 2$ (en $\mathbb{F}_2^2$ las nubes tienen sólo 3 puntos). Entonces, el contrarrecíproco de la Proposición 4.4.11 nos dice que estos cuatro puntos no forman una cuaterna buena, es decir que no cumplen con alguna de las tres condiciones de la Definición 4.4.8. En esta sección veremos qué pasa si la condición que no cumplen es la primera, es decir, si entre los 14 puntos $T_1, T_2, \ldots, T_{14}$ hay repeticiones.

Sean A, B, C, D nuestros cuatro puntos. Sabemos que existen dos subconjuntos distintos de $\{A, B, C, D\}$ (de 1, 2 o 3 elementos) que tienen igual suma. Como A, B, C, D pertenecen a una nube, no tienen subsucesiones de suma 0; por lo tanto, no puede pasar que uno de estos subconjuntos esté contenido en el otro. Además podemos suponer que dichos subconjuntos son disjuntos (si no, les quitamos los elementos que tienen en común). Dicho esto, y usando que los puntos son distintos, vemos que las únicas posibilidades son que (renombrando los puntos si hace falta) ocurra alguna de las siguientes:

- $A + B = C$, es decir que los puntos A, B, C junto con el origen son los vértices de un paralelogramo;
- $A + B + C = D$;
- $A + B = C + D$, que es lo mismo que decir que los puntos A, B, C, D son los vértices de un paralelogramo.

Veremos que en cualquiera de estos tres casos se puede concluir que la nube contiene un punto con multiplicidad $p - 1$. Primero, un lema.

Lema 4.6.1. *Sea $S = ABCP_1P_2 \cdots P_{2p-4}$ una nube en la cual los puntos A, B, C son distintos y colineales. Entonces S contiene algún elemento con multiplicidad $p - 1$.*

Demostración. Sabemos por el Corolario 4.1.6 que A y B son linealmente independientes. Aplicando un automorfismo de $\mathbb{F}_p^2$ podemos suponer que $A = (1, 0)$ y $B = (1, 1)$. Necesariamente entonces es $C = (1, c)$ con $c \neq 0, 1$. Si fuera $p = 3$, la única posibilidad es $C = (1, -1)$, pero entonces $A + B + C = (0, 0)$, lo cual no puede ocurrir pues S es una nube y ABC es una subsucesión **propia**. Por lo tanto, podemos asumir $p > 3$.

Consideramos la seminube $S' = ABCP_1P_2 \cdots P_{2p-5}$. Aplicando la ecuación estratégica del Teorema 4.2.4 con esta seminube obtenemos

$$(c - 1)\mu^\star(A, A, A) - c\mu^\star(B, B, B) + \mu^\star(C, C, C) = 0 \tag{4.16}$$

(notar que $[BC]+[CA]+[AB]=0$, así que el último término de (4.6) no aparece).

Abreviamos $\mu_m = \mu_m(P_1, P_2, \ldots, P_{2p-5})$. Aplicando reiteradas veces las fórmulas recursivas para μ de la Proposición 4.1.4 obtenemos las siguientes expresiones para los $\mu^\star$ en términos de los μ_m:

$$\begin{aligned}
\mu^\star(A,A,A) &= \mu_{p-4},\\
\mu^\star(B,B,B) &= \mu_{p-4} + 3\mu_{p-3} + 3\mu_{p-2} + \mu_{p-1},\\
\mu^\star(C,C,C) &= \mu_{p-4} + 3c\mu_{p-3} + 3c^2\mu_{p-2} + c^3\mu_{p-1}.
\end{aligned}$$

Reemplazando todo esto en (4.16) y cancelando términos repetidos nos queda

$$(3c^2 - 3c)\mu_{p-2} + (c^3 - c)\mu_{p-1} = 0.$$

Como c no es 0 ni 1, podemos dividir por $c(c-1)$ y obtenemos

$$3\mu_{p-2} + (c+1)\mu_{p-1} = 0. \tag{4.17}$$

Sea $Q = A + B + C = (3, c+1)$. Ya observamos antes que $Q \neq (0,0)$. Por otra parte, es fácil ver que el primer miembro de (4.17) es igual a

$$\mu_{p-1}(e_2, e_2, Q, P_1, P_2, \ldots, P_{2p-5}).$$

Esto lo hicimos dejando de lado el punto P_{2p-4}, pero en ningún momento usamos cómo estaban numerados los puntos P_i, así que podríamos haber dejado aparte cualquier otro de ellos. Es decir que la sucesión $S'' = e_2 e_2 Q P_1 P_2 \cdots P_{2p-4}$ cumple que si le quitamos cualquiera de sus puntos, salvo quizás los primeros tres, obtenemos una sucesión cuyo μ_{p-1} es igual a 0. Esta es precisamente la condición que necesitamos para usar el Lema 4.3.4. Así, obtenemos que S'' es una sucesión mágica, y por lo tanto (Lema 4.3.3) contiene $p+1$ puntos sobre un mismo subespacio de dimensión 1. Como e_2 y Q son linealmente independientes, a lo sumo dos de estos puntos no están entre los P_i. Luego S contiene $p-1$ puntos sobre un mismo subespacio de dimensión 1, y sabemos que como S es una nube esto implica que dichos puntos son iguales.

La demostración está completa. □

Proposición 4.6.2. *Sea $S = ABCDP_1P_2\cdots P_{2p-5}$ una nube en la cual los puntos A, B, C, D son distintos y satisfacen $A+B=C$. Entonces S contiene algún elemento con multiplicidad $p-1$.*

Demostración. Como antes, podemos suponer sin perder generalidad que $A = (1,0)$ y $B = (0,1)$. Luego $C = A + B = (1,1)$. Sea $D = (x,y)$. Notar que x, y y $x-y$ son no nulos, pues en caso contrario D sería linealmente dependiente con B, A y C respectivamente.

Consideramos las cuatro seminubes que se obtienen quitándole a S los puntos A, B, C, D respectivamente. Por la Proposición 4.1.3 sabemos que en todas estas seminubes el valor de μ_{p-1} es igual a 1. Planteamos estas ecuaciones, usando las fórmulas recursivas para poner todo en función de los $\mu_m = \mu_m(P_1, P_2, \ldots, P_{2p-5})$, y obtenemos el siguiente sistema:

$$\begin{cases} x\mu_{p-3} + (x+y)\mu_{p-2} + y\mu_{p-1} = 1 \\ x\mu_{p-4} + (x+y)\mu_{p-3} + y\mu_{p-2} = 1 \\ x\mu_{p-3} + y\mu_{p-2} = 1 \\ \mu_{p-3} + \mu_{p-2} = 1 \end{cases}$$

Resolviendo este sistema obtenemos

$$\mu_{p-4} = \frac{y^2 - y}{x(x-y)}, \quad \mu_{p-3} = -\frac{y-1}{x-y}, \quad \mu_{p-2} = \frac{x-1}{x-y}, \quad \mu_{p-1} = -\frac{x^2 - x}{y(x-y)}.$$

A continuación, planteamos la ecuación estratégica con la seminube que se obtiene quitando el punto C. Esta ecuación es la misma que (4.6), que ya habíamos calculado en la demostración del Teorema 4.2.4:

$$(x^3 - x)\mu_{p-4} + 3x(x-1)(y-1)\mu_{p-3} + 3y(x-1)(y-1)\mu_{p-2} + (y^3 - y)\mu_{p-1} = 0.$$

Reemplazamos cada μ_m por el valor que ya calculamos y se obtiene

$$\frac{(x^2-1)(y^2-y)}{x-y} - \frac{3x(x-1)(y-1)^2}{x-y} + \frac{3y(x-1)^2(y-1)}{x-y} - \frac{(y^2-1)(x^2-x)}{x-y} = 0.$$

Ignoramos los denominadores y sacamos factor común $(x-1)(y-1)$, obteniendo

$$(x-1)(y-1)\left[(x+1)y - 3x(y-1) + 3y(x-1) - (y+1)x\right] = 0,$$

es decir,

$$(x-1)(y-1)(2x-2y) = 0.$$

Como también $2x - 2y \neq 0$ (aquí estamos usando que $p > 2$), obtenemos que $x = 1$ o $y = 1$. Pero en cualquiera de los dos casos resulta que S contiene tres puntos colineales. Aplicamos el Lema 4.6.1, y estamos. □

Proposición 4.6.3. *Sea $S = ABCDP_1P_2\cdots P_{2p-5}$ una nube en la cual los puntos A, B, C, D son distintos y satisfacen $A + B + C = D$. Entonces S contiene algún elemento con multiplicidad $p - 1$.*

Demostración. El procedimiento será exactamente el mismo que usamos para la proposición anterior.

Supongamos $A = (1, 0)$, $B = (0, 1)$, $C = (x, y)$, $D = (x + 1, y + 1)$. Aplicamos la Proposición 4.1.3 con las seminubes que se obtienen quitando los puntos A, B, C, D, y obtenemos el siguiente sistema:

$$\begin{cases} x(x+1)\mu_{p-3} + (x+y+2xy)\mu_{p-2} + y(y+1)\mu_{p-1} = 1 \\ x(x+1)\mu_{p-4} + (x+y+2xy)\mu_{p-3} + y(y+1)\mu_{p-2} = 1 \\ (x+1)\mu_{p-3} + (y+1)\mu_{p-2} = 1 \\ x\mu_{p-3} + y\mu_{p-2} = 1 \end{cases}$$

La solución de este sistema es[8]

$$\mu_{p-4} = \frac{y(y-2x-1)}{x(x+1)(x-y)}, \quad \mu_{p-3} = \frac{1}{x-y},$$

$$\mu_{p-2} = -\frac{1}{x-y}, \quad \mu_{p-1} = -\frac{x(x-2y-1)}{y(y+1)(x-y)}.$$

Por otra parte, la ecuación estratégica que se obtiene omitiendo el punto D es, nuevamente,

$$(x^3 - x)\mu_{p-4} + 3x(x-1)(y-1)\mu_{p-3} + 3y(x-1)(y-1)\mu_{p-2} + (y^3 - y)\mu_{p-1} = 0.$$

Reemplazamos cada μ_m por su correspondiente valor, y lo que se obtiene se termina simplificando a[9]

$$-2(x-y)(x+y-1) = 0,$$

de donde $x + y = 1$, y por lo tanto A, B, C son colineales. Nuevamente hemos terminado gracias al Lema 4.6.1. □

Proposición 4.6.4. *Sea $S = ABCDP_1P_2 \cdots P_{2p-5}$ una nube en la cual los puntos A, B, C, D son distintos y satisfacen $A + B = C + D$. Entonces S contiene algún elemento con multiplicidad $p - 1$.*

Demostración. Repetir el procedimiento de los casos anteriores. □

[8] Las razones por las que los denominadores son no nulos son las siguientes. Si fuera $x = 0$ o $y = 0$ obtendríamos que C es linealmente dependiente con B o con A respectivamente. Por el mismo motivo, pero considerando el punto D, $x + 1$ e $y + 1$ son distintos de 0. Finalmente, si fuera $x = y$ resulta que C y D son linealmente dependientes.

[9] Omitimos las cuentas por respeto al buen gusto.

4.7. Casos excepcionales, Parte II

En esta sección veremos qué ocurre si nuestra nube contiene una cuaterna de puntos distintos (A, B, C, D) que no cumple alguna de las últimas dos condiciones de la Definición 4.4.8, esto es, que de las parejas

$$(A, B+C+D); \quad (B, A+C+D); \quad (C, A+B+D); \quad (D, A+B+C);$$

$$(A+B, C+D); \quad (A+C, B+D); \quad (A+D, B+C)$$

se puedan elegir 4 tales que los 8 puntos que las conforman sean colineales, o bien se puedan elegir 6 tales que los 12 puntos que las conforman estén sobre una misma cónica.

Supongamos que existe una recta que contiene a los puntos de 4 de las parejas antes mencionadas. Si al menos tres de estas parejas son del primer renglón, entonces entre A, B, C, D hay tres puntos colineales, y hemos terminado por el Lema 4.6.1. Lo mismo sucede si entre estas parejas están las tres del segundo renglón (en este caso se deduce, de hecho, que los 4 puntos son colineales). Entonces deben ser dos y dos. Supongamos sin pérdida de generalidad que nuestra recta pasa por A y B. Si además pasara por $A+B$, resulta que A y B son linealmente dependientes, lo cual es absurdo por el Corolario 4.1.6. El único caso que queda es cuando las cuatro parejas son

$$(A, B+C+D); \quad (B, A+C+D); \quad (A+C, B+D); \quad (A+D, B+C).$$

Pero el hecho de que A, $A+C$, $A+D$ sean colineales implica que C y D son linealmente dependientes. Absurdo.

Para la segunda posibilidad, usaremos el siguiente lema.

Lema 4.7.1. *Sean P, Q, R puntos en K^2. Supongamos que existe una cónica que pasa por los 7 puntos*

$$0,\ P,\ Q,\ R,\ P+Q,\ P+R,\ Q+R.$$

Entonces, entre los puntos P, Q, R hay dos que son linealmente dependientes.

Demostración. Supongamos que P y Q son linealmente independientes (en caso contrario no hay nada que probar). Como la condición del enunciado es invariante por automorfismos de K^2, podemos suponer sin perder generalidad que $P = (1, 0)$, $Q = (0, 1)$. Sea $R = (x, y)$. Debemos demostrar entonces que $x = 0$ o $y = 0$.

Evaluando un polinomio genérico $aX^2+bXY+cY^2+dX+eY+f$ en los puntos 0, P, Q y $P+Q$ obtenemos respectivamente las ecuaciones

$$\begin{aligned} f &= 0,\\ a+d+f &= 0,\\ c+e+f &= 0,\\ a+b+c+d+e+f &= 0. \end{aligned}$$

De esto se deduce que la cónica del enunciado tiene la forma

$$a(X^2-X)+c(Y^2-Y)=0. \tag{4.18}$$

Ahora, especializando (4.18) en los puntos R, $P+R$ y $Q+R$ obtenemos respectivamente las ecuaciones

$$\begin{aligned} a(x^2-x)+c(y^2-y)&=0,\\ a(x^2+x)+c(y^2-y)&=0,\\ a(x^2-x)+c(y^2+y)&=0. \end{aligned}$$

De esto se deduce que $2ax=2cy=0$. Como a y c no pueden ser ambos nulos, y la característica de K no es 2, o bien x o bien y se tiene que anular. Esto completa la demostración. □

Supongamos que existe una cónica que contiene a los puntos de 6 de las parejas antes mencionadas. Hay dos posibilidades: que la pareja que falta sea del primer renglón o que sea del segundo renglón. Si la pareja que falta es del primer renglón, podemos suponer sin pérdida de generalidad que es $(D, A+B+C)$; si la pareja que falta es del segundo renglón, podemos suponer que es $(A+D, B+C)$. En cualquiera de los dos casos resulta que nuestra cónica pasa por los 7 puntos

$$B,\ \ C,\ \ A+B,\ \ B+D,\ \ A+C,\ \ C+D,\ \ A+B+D.$$

Aplicando una traslación de vector $-B$ obtenemos que también existe una cónica que pasa por

$$0,\ \ C-B,\ \ A,\ \ D,\ \ A+C-B,\ \ C+D-B,\ \ A+D.$$

Llamando $P=C-B$, $Q=A$, $R=D$, vemos que estamos en las hipótesis del Lema 4.7.1. Se deduce que entre los puntos $C-B$, A y D hay dos que son linealmente dependientes. No pueden ser A y D, pues pertenecen a una nube y son distintos. Entonces $C-B$ es linealmente dependiente con alguno de los otros dos, sin pérdida de generalidad digamos que es A. Geométricamente, esto significa que los puntos A, B, C junto con el origen son los vértices de un trapecio. Por lo tanto, nuestro trabajo quedará terminado al probar la siguiente proposición.

Proposición 4.7.2. *Sea $S = ABCP_1P_2\cdots P_{2p-4}$ una nube en la cual los puntos A, B, C son distintos y junto con el origen son los vértices de un trapecio. Entonces S contiene algún elemento con multiplicidad $p-1$.*

Demostración. Podemos suponer que $A = (1,0)$, $B = (0,1)$, $C = (c,1)$. No puede ser $c = 0$ porque sería $B = C$. Si fuera $c = \pm 1$, entonces O, A, B, C serían los vértices de un paralelogramo, y el resultado se deduce de lo que ya hicimos. Por lo tanto podemos suponer que $c \notin \{-1, 0, 1\}$. En particular, para que esto pueda suceder asumimos $p > 3$.

Consideramos la seminube $S' = ABCP_1P_2\cdots P_{2p-5}$. Aplicando la ecuación estratégica del Teorema 4.2.4 con esta seminube obtenemos

$$-c\mu^\star(A,A,A) - \mu^\star(B,B,B) + \mu^\star(C,C,C) - 3c\mu^\star(A,B,C) = 0. \tag{4.19}$$

Abreviamos $\mu_m = \mu_m(P_1, P_2, \ldots, P_{2p-5})$. Razonando igual que en el Lema 4.6.1 obtenemos que (4.19) es equivalente a

$$-c\mu_{p-4} - \mu_{p-1} + \left(c^3\mu_{p-4} + 3c^2\mu_{p-3} + 3c\mu_{p-2} + \mu_{p-1}\right) - 3c\left(c\mu_{p-3} + \mu_{p-2}\right) = 0,$$

que luego de cancelar los términos repetidos queda

$$(c^3 - c)\mu_{p-4} = 0.$$

Como $c \notin \{-1, 0, 1\}$ es $c^3 - c \neq 0$. Así, obtuvimos que $\mu_{p-4} = 0$. Pero notemos que $\mu_{p-4} = \mu_{p-1}(A, A, A, P_1, P_2, \ldots, P_{2p-5})$. Como esto mismo lo podemos hacer sacando cualquier otro de los P_i que no sea el P_{2p-4}, resulta que podemos aplicar el Lema 4.3.3 con la sucesión $AAAP_1P_2\cdots P_{2p-4}$ y concluir que esta sucesión contiene $p+1$ puntos sobre un mismo subespacio de dimensión 1. Como esta sucesión difiere de S en sólo dos puntos, resulta que S contiene $p-1$ puntos sobre un mismo subespacio de dimensión 1, y sabemos que esto implica que son iguales.

La demostración está completa. □

El trabajo de las últimas dos secciones se sintetiza en la siguiente proposición.

Proposición 4.7.3. *Sea S una nube que contiene 4 puntos distintos que* **no** *están en posición general. Entonces S contiene algún elemento con multiplicidad $p-1$.*

4.8. El último paso

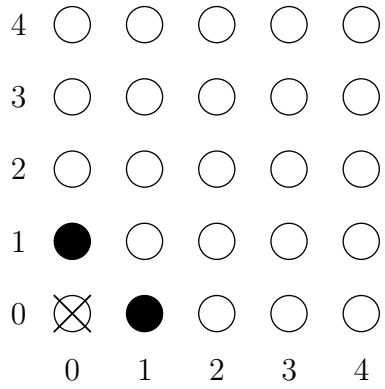
Estamos a punto de completar la demostración de que todos los números primos tienen la Propiedad B. Hay un inconveniente, y es que el teorema principal de esta sección requiere la hipótesis adicional $p > 5$. Por lo tanto, tenemos que encontrar otra manera de lidiar con los casos chicos.

Si p es 2 o 3, no hace falta que probemos nada más: como en $\mathbb{F}_p^2$ no hay 14 puntos distintos, no existen las cuaternas buenas, y por lo tanto los resultados probados hasta el momento ya son suficientes para concluir que p tiene la Propiedad B.

Nos queda analizar $p = 5$. Hacer esto será casi tan divertido como resolver un Sudoku.

Proposición 4.8.1. *Toda nube en $\mathbb{F}_5^2$ contiene un elemento con multiplicidad 4.*

Demostración. Sea S una nube en $\mathbb{F}_5^2$. Sin pérdida de generalidad podemos suponer que en S aparecen los puntos $(1, 0)$ y $(0, 1)$.



En esta figura, los puntos $(1, 0)$ y $(0, 1)$ están sombreados para indicar que están en S. Por otra parte, el punto $(0, 0)$ está tachado para indicar que sabemos que no puede estar en S.

Invitamos al lector a ir tachando puntos del dibujo a medida que comprenda los siguientes argumentos.

Por el Corolario 4.1.6 sabemos que S no puede contener dos puntos distintos que sean linealmente dependientes. Esto nos permite tachar seis puntos, que están sobre las rectas $x = 0$ e $y = 0$.

Si hubiera algún otro punto de S alineado con los dos que ya tenemos, entonces por el Lema 4.6.1 se cumple lo que queremos. La recta que pasa por $(1, 0)$ y $(0, 1)$ es la de ecuación $x + y = 1$, que también contiene a los puntos $(2, 4)$, $(3, 3)$ y $(4, 2)$. Podemos tachar entonces estos tres puntos.

Si hubiera algún otro punto de S sobre las rectas $x = 1$ o $y = 1$, junto con los dos que ya tenemos y el origen serían los vértices de un trapecio, y entonces por la Proposición 4.7.2 se cumple lo que queremos. Tachamos entonces los 7 puntos aún no marcados que están sobre dichas rectas.

Los puntos $(2, 3)$ y $(3, 2)$ también tienen la propiedad de que junto con el $(1, 0)$, el $(0, 1)$ y el origen forman los vértices de un trapecio (las bases de dicho trapecio son paralelas al vector $(1, -1)$). Entonces podemos tachar esos dos puntos.

Por último, el punto $(4,4)$ no puede estar en S porque junto con los dos que ya tenemos suman 0.

Los únicos puntos que quedaron sin tachar son

$$A = (2,2), \qquad B = (3,4), \qquad C = (4,3).$$

Si los puntos A y B están ambos en S, ganamos, porque $A+B = (0,1)$ y estamos en las hipótesis de la Proposición 4.6.2. Análogamente se resuelve el caso en el que A y C están ambos en S. Si B y C están ambos en S, como junto con el $(1,0)$ y el $(0,1)$ son los vértices de un paralelogramo, estamos en las hipótesis de 4.6.4.

Sólo falta considerar el caso en el que a lo sumo uno de los puntos A, B, C está en S, pero esto ya fue analizado en la sección 4.5. □

Sin más preámbulos, he aquí el teorema que habíamos prometido al comienzo de la sección 4.4.

Teorema 4.8.2. *Supongamos que $p > 5$. Sea $S = ABCDP_1 \cdots P_{2p-5}$ una nube en la cual los puntos A, B, C, D están en posición general. Entonces S contiene un elemento con multiplicidad $p-1$.*

Demostración. Supongamos que la conclusión del teorema es falsa, es decir que ningún elemento se repite más de $p-2$ veces. Como $2p-5 > p-2$, entre los P_i hay al menos dos puntos distintos. Estos puntos deben ser linealmente independientes por el Corolario 4.1.6. Ahora la Observación 4.4.7 nos permite suponer sin pérdida de generalidad que estos puntos son e_1 y e_2. Usaremos esta suposición más adelante.

Sean $T_1, T_2, \ldots, T_{14}$ los puntos que se pueden obtener sumando 1, 2 o 3 de los puntos A, B, C, D. En adelante, cuando hablemos de Γ_4 y M_4 nos estaremos refiriendo a $\Gamma_4(T_1, T_2, \ldots, T_{14})$ y $M_4(T_1, T_2, \ldots, T_{14})$ respectivamente.

Para cada $i \in [\![1, 14]\!]$, llamamos (r_i, s_i) a las coordenadas del punto T_i, y consideramos el vector

$$z_i = (r_i^4, r_i^3 s_i, r_i^2 s_i^2, r_i s_i^3, s_i^4, r_i^3, r_i^2 s_i, r_i s_i^2, s_i^3, r_i^2, r_i s_i, s_i^2, r_i, s_i, 1).$$

Sea $f \in \Lambda_4$ un polinomio, pensado como vector de $\mathbb{F}_p^{15}$. Entonces,

$$f \in \Gamma_4 \iff \langle f, z_i \rangle = 0 \ \ \forall i \in [\![1, 14]\!].^{10}$$

Sea W el «complemento ortogonal» de M_4 en $\mathbb{F}_p^5$, es decir,

$$W = \{w \in \mathbb{F}_p^5 \mid \langle w, v \rangle = 0 \ \ \forall v \in M_4\}.$$

[10] Estamos usando la siguiente notación: si $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ son vectores en K^n, entonces $\langle a, b \rangle := \sum_{i=1}^n a_i b_i$.

Notemos que si $(\alpha_{40}, \alpha_{31}, \alpha_{22}, \alpha_{13}, \alpha_{04})$ es cualquier vector de W, entonces el vector

$$z = (\alpha_{40}, \alpha_{31}, \alpha_{22}, \alpha_{13}, \alpha_{04}, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

satisface $\langle f, z\rangle = 0$ para todo $f \in \Gamma_4$. De esto se deduce que z pertenece al subespacio generado por los z_i. En otras palabras, existen escalares $\gamma_1, \gamma_2, \ldots, \gamma_{14} \in \mathbb{F}_p$ tales que

$$\sum_{i=1}^{14} \gamma_i r_i^m s_i^n = \begin{cases} \alpha_{mn} & \text{si } m+n=4, \\ 0 & \text{si } m+n<4. \end{cases}$$

Consideramos el polinomio

$$Q(X,Y) = \sum_{i=1}^{14} \gamma_i \left[(X+r_i)^{p-1} - 1\right]\left[(Y+s_i)^{p-1} - 1\right].$$

Notar que

$$Q(x,y) \neq 0 \Rightarrow (x,y) = (-r_i, -s_i) \text{ para algún } i. \tag{4.20}$$

Sean m, n enteros no negativos con $m+n \leq 4$. Entonces, el coeficiente correspondiente al monomio $X^{p-1-m}Y^{p-1-n}$ en Q es[11]

$$\sum_{i=1}^{14} \gamma_i \binom{p-1}{m}\binom{p-1}{n} r_i^m s_i^n.$$

Como sabemos que la expresión anterior se anula si $m+n<4$, vemos que el grado de Q, que en principio sólo podíamos decir que era a lo sumo $2p-2$, es de hecho a lo sumo $2p-6$. Además sabemos cuáles son los términos de grado $2p-6$. Como $\binom{p-1}{m} = (-1)^m$ en $\mathbb{F}_p$,[12] si $m+n=4$ podemos borrar los combinatorios y los coeficientes que quedan son los que ya conocemos, esto es:

$$\alpha_{40}X^{p-5}Y^{p-1} + \alpha_{31}X^{p-4}Y^{p-2} + \alpha_{22}X^{p-3}Y^{p-3} + \alpha_{13}X^{p-2}Y^{p-4} + \alpha_{04}X^{p-1}Y^{p-5}.$$

Ahora, sean (u_i, v_i) las coordenadas de cada punto P_i con $i \in [\![1, 2p-5]\!]$. Definimos en $\mathbb{F}_p[X_1, X_2, \ldots, X_{2p-6}]$ los polinomios

$$U = \sum_{i=1}^{2p-6} u_i X_i, \qquad V = \sum_{i=1}^{2p-6} v_i X_i$$

[11] Aquí importa que sea $p > 5$, para asegurar que el -1 de cada factor no influye a la hora de calcular el coeficiente.

[12] Esto es claro si pensamos que en el triángulo de Pascal módulo p, la fila siguiente tiene unos en las puntas y ceros en todos los demás lugares.

(pronto se verá por qué excluimos el punto P_{2p-5}). Sea $f = Q(U, V)$. Como U y V tienen grado 1, vale que el grado de f es a lo sumo $2p-6$; además, los términos de grado $2p-6$ de f provienen de desarrollar

$$\alpha_{40}U^{p-5}V^{p-1} + \alpha_{31}U^{p-4}V^{p-2} + \alpha_{22}U^{p-3}V^{p-3} + \alpha_{13}U^{p-2}V^{p-4} + \alpha_{04}U^{p-1}V^{p-5}.$$

Usando el Lema 4.2.3 obtenemos que el coeficiente correspondiente al monomio $\prod_{i=1}^{2p-6} X_i$ en f es

$$\alpha_{40}(p-5)!(p-1)!\mu_{p-5} + \alpha_{31}(p-4)!(p-2)!\mu_{p-4} + \alpha_{22}(p-3)!(p-3)!\mu_{p-3} + \alpha_{13}(p-2)!(p-4)!\mu_{p-2} + \alpha_{04}(p-1)!(p-5)!\mu_{p-1},$$

donde estamos abreviando $\mu_m = \mu_m(P_1, P_2, \ldots, P_{2p-6})$.

Sacando factor común $(p-5)!^2 \neq 0$ y operando vemos que este coeficiente es nulo si y sólo si

$$24\alpha_{40}\mu_{p-5} + 96\alpha_{31}\mu_{p-4} + 144\alpha_{22}\mu_{p-3} + 96\alpha_{13}\mu_{p-2} + 24\alpha_{04}\mu_{p-1} = 0. \tag{4.21}$$

Si el coeficiente fuera no nulo, por el Combinatorial Nullstellensatz obtenemos que existe $b \in \{0,1\}^{2p-6}$ tal que $f(b) \neq 0$. Esto significa que $Q(U(b), V(b)) \neq 0$. Por lo observado en (4.20) sabemos que $(U(b), V(b)) = (-r_i, -s_i)$ para algún i. Entonces $P_1P_2\cdots P_{2p-6}$ contiene una subsucesión cuya suma es $(-r_i, -s_i)$. Pero esto es absurdo, pues al agregarle a esta sucesión los términos de $ABCD$ cuya suma es T_i, obtenemos una subsucesión **propia** de S cuya suma es 0. Por lo tanto el coeficiente se tiene que anular.

Como 24 no es divisible por p, en (4.21) podemos dividir por 24 y así obtenemos que

$$\alpha_{40}\mu_{p-5} + 4\alpha_{31}\mu_{p-4} + 6\alpha_{22}\mu_{p-3} + 4\alpha_{13}\mu_{p-2} + \alpha_{04}\mu_{p-1} = 0.$$

Esto lo hicimos dejando de lado el punto P_{2p-5}, pero en ningún momento usamos cómo estaban numerados los puntos P_i, así que podríamos haber dejado aparte cualquier otro punto. En definitiva lo que hemos probado es que

$$\alpha_{40}\mu_{p-5}[i] + 4\alpha_{31}\mu_{p-4}[i] + 6\alpha_{22}\mu_{p-3}[i] + 4\alpha_{13}\mu_{p-2}[i] + \alpha_{04}\mu_{p-1}[i] = 0$$

para cualquier índice $i \in [\![1, 2p-5]\!]$ y cualquier vector $(\alpha_{40}, \alpha_{31}, \alpha_{22}, \alpha_{13}, \alpha_{04}) \in W$.

Ahora usamos el hecho de que $\dim M_4 \leq 2$. Esto implica que $\dim W \geq 3$, así que en W existe algún vector no nulo de la forma $(0, \alpha, \beta, \gamma, 0)$. Se tiene entonces que

$$4\alpha\mu_{p-4}[i] + 6\beta\mu_{p-3}[i] + 4\gamma\mu_{p-2}[i] = 0.$$

Consideramos la sucesión $S' = e_1e_2P_1P_2\cdots P_{2p-5}$. Notemos que

$$\mu^{S'}_{p-3}[i] = \mu_{p-4}[i],$$
$$\mu^{S'}_{p-2}[i] = \mu_{p-3}[i],$$
$$\mu^{S'}_{p-1}[i] = \mu_{p-2}[i].$$

Entonces, lo que tenemos es

$$4\alpha\mu_{p-3}^{S'}[i] + 6\beta\mu_{p-2}^{S'}[i] + 4\gamma\mu_{p-1}^{S'}[i] = 0.$$

Esto se cumple si le quitamos a S' algún punto P_i, pero también se cumple si quitamos el e_1 o el e_2, pues estábamos suponiendo que estos puntos aparecían entre los P_i. Entonces podemos aplicar el Corolario 4.3.6 y concluir que S' contiene $p-1$ puntos sobre un mismo subespacio de dimensión 1. La única manera de que esto no contradiga nuestra suposición sobre S es que e_1 o e_2 aparezcan con multiplicidad $p-2$ en $P_1P_2\cdots P_{2p-5}$.

Supongamos que el que aparece $p-2$ veces es e_1 (el otro caso es análogo). Ahora repetimos el argumento anterior con un vector $(0,0,\alpha',\beta',\gamma') \in W$ y la sucesión $S'' = e_2^2P_1P_2\cdots P_{2p-5}$. Vemos así que e_2 debe aparecer con multiplicidad $p-3$ en $P_1P_2\cdots P_{2p-5}$. En definitiva, obtuvimos que

$$P_1P_2\cdots P_{2p-5} = e_1^{p-2}e_2^{p-3}.$$

A partir de aquí no es difícil llegar a una contradicción. Cada uno de los puntos A, B, C, D debe pertenecer a alguna de las siguientes rectas:

$$\mathbb{L}_1 : x = 0; \quad \mathbb{L}_2 : x = 1; \quad \mathbb{L}_3 : y = 0; \quad \mathbb{L}_4 : y = 1; \quad \mathbb{L}_5 : y = 2$$

(en caso contrario, combinando este punto con una subsucesión de $P_1P_2\cdots P_{2p-5}$ se obtiene una subsucesión propia de S de suma 0.)

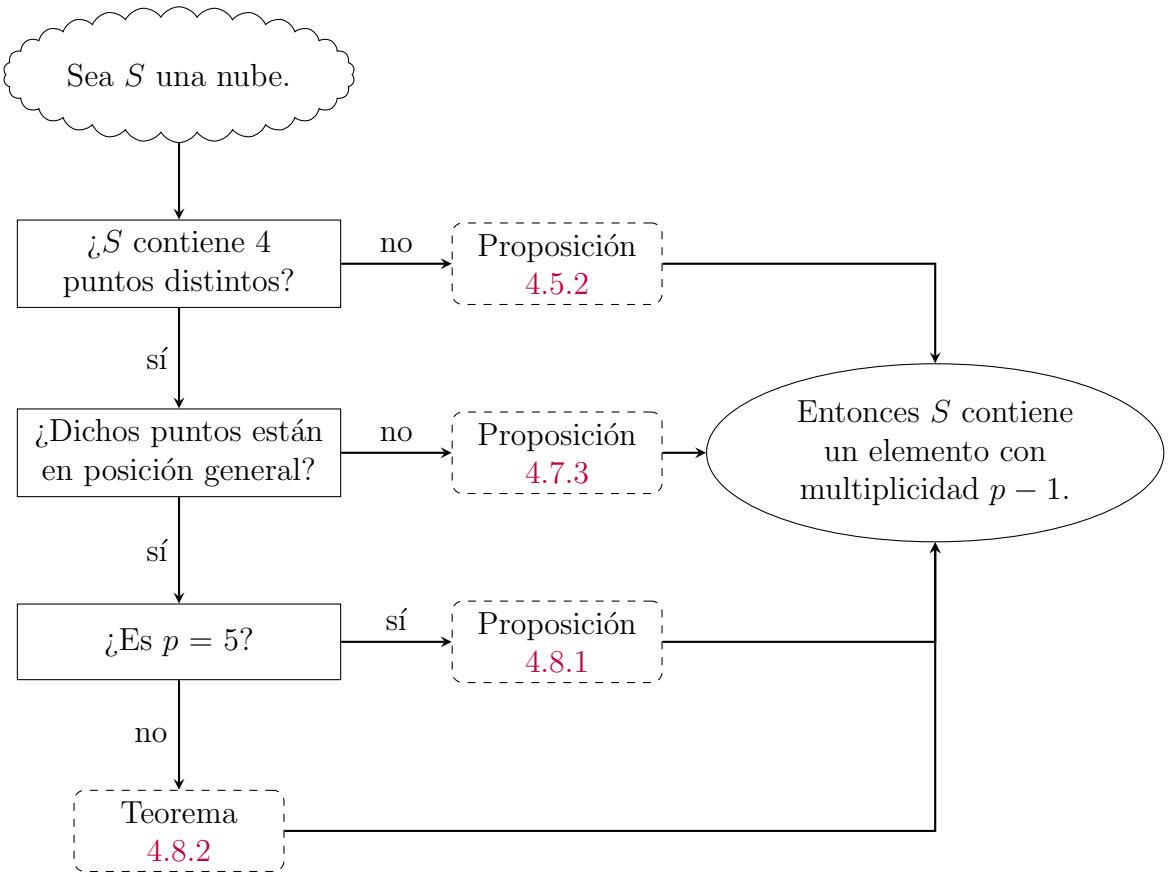
El caso $\mathbb{L}_3$ queda descartado porque como en una nube dos puntos linealmente dependientes son iguales, el punto en cuestión debería ser igual a e_1, y entonces e_1 tendría multiplicidad $p-1$. De manera similar, a lo sumo uno de los puntos A, B, C, D puede pertenecer a $\mathbb{L}_1$, y en tal caso ese punto debe ser igual a e_2. Nos quedan al menos tres puntos, todos ellos distintos de e_1 y e_2, que pertenecen a $\mathbb{L}_2 \cup \mathbb{L}_4 \cup \mathbb{L}_5$. Pero si alguno de estos puntos estuviera en $\mathbb{L}_2 \cup \mathbb{L}_4$, tendríamos en S tres puntos que junto con el origen forman los vértices de un trapecio, lo cual entra en contradicción con la Proposición 4.7.2. Luego, los tres puntos deben estar sobre $\mathbb{L}_5$. Pero esto nos da una contradicción con el Lema 4.6.1.

El absurdo provino de suponer que existía una nube que no contenía elementos de multiplicidad $p-1$. □

Ahora simplemente hay que juntar todo lo que hicimos en las últimas cuatro secciones.

Teorema 4.8.3. *Todo primo tiene la Propiedad B.*

Demostración. Siga las flechas:



□

A modo de cierre, mostramos cómo se puede combinar el teorema anterior con los resultados del Capítulo 3 para resolver un caso particular del problema de Davenport en rango 3.

Teorema 4.8.4. *Sea G un grupo de rango 3 cuyo primer factor invariante es igual a 2, es decir $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2m_1} \oplus \mathbb{Z}_{2m_2}$ con $m_1 \mid m_2$. Entonces $D(G) = M(G)$.*

Demostración. El hecho de que todo primo tenga la Propiedad B implica que también todo primo tiene la Propiedad C. Ahora, de la Observación 3.4.3 se deduce que el grupo $G_1 = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$ satisface $\nu(G_1) = D(G_1) - 2$. Pero entonces, por el Teorema 3.3.7 vale que $D(G) = M(G)$, como queríamos demostrar. □

Bibliografía

[AD93] N. Alon and M. Dubiner. *Zero-sum sets of prescribed size*. In *Combinatorics, Paul Erdős is eighty, Vol. 1*, János Bolyai Math. Soc., Budapest, Bolyai Soc. Math. Stud., 1993.

[Alo99] Noga Alon. *Combinatorial Nullstellensatz*. Combin. Probab. Comput., **8** (1999) (1-2), pp. 7–29.

[And97] Daniel D. Anderson (editor). *Factorization in integral domains*, volume 189 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1997.

[EGZ61] P. Erdős, A. Ginzburg and A. Ziv. *Theorem in the additive number theory*. Bull. Res. Council Israel, **10F** (1961), pp. 41–43.

[Gao00] W. Gao. *On Davenport's constant of finite abelian groups with rank three*. Discrete Math., **222** (2000) (1-3), pp. 111–124.

[GG99] Weidong Gao and Alfred Geroldinger. *On long minimal zero sequences in finite abelian groups*. Period. Math. Hungar., **38** (1999) (3), pp. 179–211.

[GG06] Weidong Gao and Alfred Geroldinger. *Zero-sum problems in finite abelian groups: a survey*. Expo. Math., **24** (2006) (4), pp. 337–369.

[GS92] Alfred Geroldinger and Rudolf Schneider. *On Davenport's constant*. J. Combin. Theory Ser. A, **61** (1992) (1), pp. 147–152.

[Mic10] Mateusz Michalek. *A short proof of combinatorial Nullstellensatz*. Amer. Math. Monthly, **117** (2010) (9), pp. 821–823.

[Ols69a] John E. Olson. *A combinatorial problem on finite Abelian groups. I*. J. Number Theory, **1** (1969), pp. 8–10.

[Ols69b] John E. Olson. *A combinatorial problem on finite Abelian groups. II*. J. Number Theory, **1** (1969), pp. 195–199.

[Rei10] Christian Reiher. *A proof of the theorem according to which every prime number possesses Property B*. Ph.D. thesis, Universität Rostock, 2010.

[SC07] Svetoslav Savchev and Fang Chen. *Long zero-free sequences in finite cyclic groups*. Discrete Math., **307** (2007) (22), pp. 2671–2679.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977.

[vEB69] P. van Emde Boas. *A combinatorial problem on finite abelian groups. II*. Math. Centrum Amsterdam Afd. Zuivere Wisk., (1969) (ZW-007), p. 60.