Universidad de Buenos Aires Argentina

Sobre los posets más chicos con grupo de automorfismos abeliano dado

Alumno: Agustín Nicolás Barreto

Director: Jonathan Ariel Barmak

Septiembre 2021

Agradecimientos

En primer lugar quiero agradecer a mis papás, Gustavo y Cynthia. Ellos siempre me apoyaron en todo lo que necesité desde que tengo uso de razón, tanto en mis frustraciones como en mis éxitos, siempre estuvieron ahí; eso es algo que nunca voy a dejar de agradecer. Agradezco todos los valores que siempre me inculcaron, el enorme esfuerzo que hicieron para que nunca me falte nada y cada muestra de amor que me dan todos los días. Gracias a ellos hoy estoy donde estoy y soy la persona que soy.

A mis abuelas, Norma y Tita, por cuidarme de chico, por el amor incondicional que siempre me expresaron y por nunca dejar de darme todos los gustos; sin dudas fueron una parte fundamental de mi vida y parte de lo que me permitió llegar hasta acá. Y por supuesto, a mis abuelos, Roque y Carlos, y a mi tío Juan.

A mi hermanita Isa, la pequeña de la familia, que siempre aporta alegría a la casa y, con su inocencia, nos hace ver el mundo de una manera completamente diferente. Cada abrazo de ella es un mimo al alma que da un montón de energía para seguir.

A mis amigos del secundario, por tantas salidas juntos, por las horas matándonos de risa mientras jugábamos online, por tantas charlas de literalmente cualquier cosa, por Bariloche, por esas dos vacaciones en Gesell, y por todos los lindos momentos: Ale, Agus, Germi, Gian, Iván, Juanga, Juampi, Laucha, Mateo, Mati, Nico, Pedro, Rober, Roko, Santi y Tincho.

A Patricia Fauring y Flora Gutiérrez, por trabajar incansablemente para hacer posible la Olimpíada Matemática Argentina y que todos los chicos y chicas del país tengan la oportunidad de vivir las hermosas experiencias que yo tuve la fortuna de vivir. La olimpíada me cambió la vida, y está presente al día de hoy en la mayor parte de ella: me dió mi carrera, me dió mi trabajo, me hizo conocer a mi novia, me dió un montón de amigos y me dió (y me sigue dando) infinitas experiencias y recuerdos inolvidables.

A todos los que también participan en la organización de OMA, entre ellos especialmente a Marita, Silvia Mamone y Vero Sunkel.

A mis amigos de OMA, por los hermosos viajes compartidos, por las salidas juntos, por las juntadas, y por todas las experiencias compartidas: Bat, Brian, Brunito, Carla, Charles, Charo, Dido, Deamo, Emi, Franco Bongiovanni, Fiebre, Gianni, Ian, Joa, Joacoini, Juli Ferrés, Lauti, Licha, Lichu, Juli Masliah, Male, Mateo, Marchi, Mati Saucedo, Mazzo, Mono, Nico Ferrés, Nostri, Triple J, Turko, Sandy, Santi Cubino, Yami, y a todo Trivial, que son Caro, Chenna, Chino, Euge, Fer, Gal, Gallu, Iván, Lara, Lu, Meli y Nati. Son muchos más así que, a todos los que me haya olvidado de nombrar, les debo un café y un abrazo.

También de OMA, quiero agradecer a Ale Candioti, Ariel Zylber, Azul Fatalini, Bruno Staffa, Charly Di Fiore, Franco Assenza, Gabi Estrany, Gasti Salgado, Iván Sadofschi, Martín Mereb, Martín Vacas Vignolo, Nacho Bombau, Nico Cogorno, Magalí Giaroli, Melanie Sclar, Pablo Blanc, Santi Laplagne, Seba Cherny y Vero Moyano.

A mis amigos de OMA que también fueron alumnos, por hacerme pasar hermosos momentos mientras me enseñaban a enseñar: Bat, Chino, Giuli, Nacho, Nico, Nehuén, Lichu, Luca, Joa, Jose, Santi, Uli, Vitu y Zoe, entre tantos otros. Mención especial para Chino, mi primer alumno; con él aprendí que me gustaba la docencia y de premio me llevé un enorme amigo.

A mis amigos de la facu, por tantas cursadas, tantas salidas y tantas charlas con café en las mesitas del DM, infaltables para transitar la carrera de la mejor manera: Carla, Deamo, Emi, Facu, Guido, Kat, Lauti, Leo, Lu, Marchi, Maki, y Sol. Mención especial para Guido, porque con él y Lu logramos sobrevivir al final de la carrera y al inicio del doctorado bancándonos entre nosotros. También a Darío Aza, porque siempre que uno necesitaba charlar el aparecía en las mesitas a escucharte.

A Mati Saucedo que, además de ser un gran amigo, fue (y es) para mí un "gurú" — para la facultad, para OMA y para la vida.

A todas las personas que alguna vez se sentaron a charlar conmigo en las mesitas del DM, porque entre todos hacemos que ese espacio de la facultad sea muy especial.
Siempre me resultó increíble que en nuestra carrera todos vayamos con gusto a pasar el día en la facultad aunque no tengamos que cursar, sólo para estudiar tomando un café mientras tus conocidos van apareciendo repentinamente en las mesitas a charlar.

A todos los que alguna vez tuve de alumnos en alguna materia, por hacerme disfrutar cada clase que dí.

A mis amigos de ACA, por tantos sábados juntos, salidas, y todos esos viajes: Agus, Ari, Belu x3, Cande, Cami x2, Cata, Dani, Emi, Fati, Feli, Joaco, Juan Emilio, Juana, Juani, Juli, Mario, Marti, Mati, Nano, Pancho, Peter, Regi, Seba, Sofi x2, Tomi x2, Vicky y Vikingo, entre tantos otros.

A mi profesor de secundario Ricardo Malmoria, con quien todos los jueves nos reuníamos para tener el taller de OMA, tarea que al egresar me delegó. Con mis compañeros esperábamos toda la semana para que llegue el jueves, fueron tardes inolvidables.

A Diana Amado, mi mejor profesora del secundario, también mamá de Chino, por recibirme siempre con tanta calidez en su casa, y por todo el cariño que siempre me expresó hasta el día de hoy.

A Nicolás Cogorno, por ayudarme a entrenar en mi último año de OMA. Mis mejores resultados los logré entrenando con él y estoy enormemente agradecido.

A Jonathan Barmak, por dirigir esta tesis, por su infinita paciencia y por todas esas horas que dedicó desinteresadamente.

A Iván Sadofschi Costa y Marco Farinati, por tomarse el trabajo de ser jurados de esta tesis y por todos los comentarios súper útiles sobre la misma.

A todos los que estuvieron en la hinchada haciendo el aguante el día de la defensa, y a los que no pudieron venir pero se tomaron el tiempo de mandarme un mensajito después.

A mi infaltable novia Lu, que es también amiga de OMA, amiga de ACA y amiga de la facu, por ser mi compañera de vida, por bancarme y apoyarme en absolutamente todo, por expresarme su amor todos los días, por esos abrazos tan lindos, por las infinitas salidas, las tardes de estudio, los viajes, las risas y los llantos. Por estar conmigo en todas: sin vos nada hubiese sido igual.

A la educación pública, que hace posible que miles de personas — entre ellas yo — podamos estudiar lo que nos gusta y, al menos en mi experiencia, con un nivel excelente y una enorme calidad humana.

Índice general

Capítulo 1

Introducción

El origen del tipo de problemas que estudiaremos en este trabajo se remonta a 1936, cuando Dénes König realiza la siguiente pregunta en [Kön86]: ¿Dado un grupo G, existe un grafo cuyo grupo de automorfismos sea isomorfo a G? En caso de que sí, ¿cómo podemos construirlo? En ese artículo se menciona que la misma pregunta podía hacerse para grafos dirigidos.

En 1938 Roberto Frucht logra responder esta pregunta en [Fru39] y, más aún, prueba que dado un grupo G existen infinitos grafos no isomorfos que tienen a G como grupo de automorfismos y que, en particular, podemos elegir uno con $2d|G|$ vértices si G no es cíclico, donde d puede ser el cardinal de cualquier conjunto de generadores.

Más adelante, ya en 1959, Gert Sabidussi en [Sab59] logra mejorar esta cota en la cantidad de vértices, probando que podemos encontrar un grafo con grupo de automorfismos G con $\mathcal{O}(|G|\log(d))$ vértices.

Si bien esta cota era muy buena, tenía el problema de depender del cardinal de un conjunto de generadores. En 1974, László "Laci" Babai logró mejorar aún más esta cota en [Bab74] — quitando el parámetro d — probando que, si $G \neq \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$, podemos obtener un grafo con grupo de automorfismos G con exactamente $2|G|$ vértices.

Durante la década del 70 se hizo famoso el concepto de representación regular gráfica (GRR por sus siglas en inglés). Una GRR de un grupo finito G es un grafo cuyo grupo de automorfismos es isomorfo a G y su acción en el grafo es regular. Una de las preguntas centrales a responder durante esta década fue: ¿qué grupos admiten una GRR?

En un principio, Sabidussi [Sab58], M. H. McAndrew [McA65] y Wilfried Imrich [Imr69, Imr70] lograron responderla para grupos abelianos en 1969. Continuando en esta línea, en 1972 Lewis A. Norwiz y Mark E. Watkins [NW72a, NW72b] logran responderlo para todo grupo con orden coprimo con 6.

El siguiente paso ocurre en 1976, cuando Wilfried Imrich [Imr78] logra resolver el problema para grupos de orden impar. Ese mismo año, D. Hetzel en su tesis [Het76] logra

extender los métodos utilizados por Imrich, Norwiz y Watkins para resolver el problema para grupos resolubles.

Finalmente, en 1978 llega Chris Godsil [God81] quien resuelve el problema para grupos no resolubles y, en particular, completa la solución del problema de GRR general: salvo finitas excepciones y salvo las familias (infinitas) de grupos abelianos y de grupos dicíclicos generalizados, todo grupo finito admite una GRR. En ese mismo artículo, plantea la pregunta de GRR para grupos infinitos.

A partir de este resultado, se empiezan a estudiar preguntas sobre estructuras similares. Por ejemplo, sobre el análogo con grafos dirigidos: las DRR. Una DRR de un grupo G es un grafo dirigido cuyo grupo de automorfismos es isomorfo a G y su acción en el grafo es regular.

En 1978 Babai [Bab78] prueba que todos los grupos infinitos admiten una DRR, y luego, en 1980 junto a Imrich prueba que todo grupo de orden impar distinto de $\mathbb{Z}_3^2$ admite una TRR (una DRR donde el grafo dirigido es un torneo).
Finalmente, ese mismo año logró probar que todos los grupos finitos distintos de Q_8, $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_2^4$ y $\mathbb{Z}_3^2$, admiten una DRR. Previo a esta demostración hubo algunos aportes de Wilfried Imrich [Imr69, Imr70], M. H. McAndrew [McA65] y Robert L. Hemminger [Hem78] para algunos grupos abelianos, aunque Babai no necesitó estos resultados para su demostración.

En [Bab80], Babai deja abierta la pregunta de qué grupos admiten una ORR (representación regular orientada, una DRR cuyo grafo dirigido es orientado). Esta pregunta permaneció abierta hasta hace muy poco tiempo: fue completamente respondida en 2017 por Joy Morris y Pablo Spiga [MS17].

Ya en 1982, William Arlinghaus [Arl85] atacó una pregunta relacionada: dado un grupo abeliano G, ¿cuál es el grafo con menor cantidad de vértices que tiene a G como grupo de automorfismos?

Esta pregunta había sido estudiada ya por Sabidussi en 1959 [Sab59], que primero trató el caso G cíclico y luego afirmó que el Teorema de estructura terminaba de probar el caso abeliano general. Lamentablemente, ya la demostración del caso cíclico no era correcta, por lo que una buena parte de su trabajo quedó sin validez.

R. L. Meriwether fue uno de los que notó estos errores y logró dar con la respuesta correcta con su correspondiente demostración para el caso G cíclico [Mer63]. Sin embargo, al igual que Sabidussi, cometió el error de afirmar que del Teorema de estructura se deducía directamente la solución general del problema, lo cual no era cierto. De hecho, los resultados de Meriwether siguen al día de hoy sin publicarse.

Cuando Arlinghaus cuenta los resultados sobre el caso cíclico en su tesis doctoral, si bien da una demostración completamente distinta, los presenta como los Teoremas de Meriwether (parte I y parte II).

La notación usual para el menor número de vértices que puede tener un grafo con grupo de automorfismos G es $\alpha(G)$.

Teorema 1.0.1 (Teorema de Meriwether, parte I)**:** Vale que:

- $\alpha(\mathbb{Z}_2) = 2$,
- $\alpha(\mathbb{Z}_{2^k}) = 2^k + 6$ si $n \geqslant 2$,
- $\alpha\left(\mathbb{Z}_{p^k}\right) = p^k + 2p$ si $p = 3$ o 5,
- $\alpha\left(\mathbb{Z}_{p^k}\right) = p^k + p$ si $p \geqslant 7$ primo.

Si p primo y $n \in \mathbb{N}$, $\nu_p(n)$ denota la multiplicidad de p como factor primo de n.

Teorema 1.0.2 (Teorema de Meriwether, parte II)**:** Si $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ es compuesto con $p_1 < \dots < p_k$ primos y $S = \sum_{i=1}^{k} \alpha\left(\mathbb{Z}_{p_i^{a_i}}\right)$, entonces:

- Si $\nu_3(n) \geqslant 1$, $\nu_2(n) = 2$ y $\nu_5(n) = 1$, entonces $\alpha(\mathbb{Z}_n) = S - 4$.
- Si $\nu_3(n) \geqslant 1$, $\nu_2(n) \neq 2$ y $\nu_5(n) = 1$, entonces $\alpha(\mathbb{Z}_n) = S - 3$.
- Si $\nu_3(n) \geqslant 1$, $\nu_2(n) = 2$ y $\nu_5(n) \neq 1$, entonces $\alpha(\mathbb{Z}_n) = S - 1$.
- Si $\nu_3(n) = 1$, $\nu_2(n) \geqslant 2$ y $\nu_5(n) \neq 1$, entonces $\alpha(\mathbb{Z}_n) = S - 1$.

A pesar de su relevancia, recién en 1963 se hicieron conocidos estos resultados, cuando Sabidussi hizo una reseña del trabajo de Harary y Palmer [HP66] — en el que tratan el caso cíclico — donde exhibe también los resultados de Meriwether.

Arlinghaus, basado en los resultados de Sabidussi y Meriwether, logró resolver exitosamente el caso G abeliano general, pasando primero por el caso $\mathbb{Z}_{p^k}$ con p primo y $k \in \mathbb{N}$, luego por el caso cíclico general, luego por el caso de $p-$grupos, y finalmente llegando al caso abeliano general, que no en todas las situaciones termina de resolverse directamente con el Teorema de estructura en la forma en la que habían afirmado (erróneamente) Sabidussi y Meriwether. Todos los resultados obtenidos pueden encontrarse en [Arl85].

Cabe destacar que, si bien usaremos la referencia [Arl85] para citar sus trabajos, en realidad esta corresponde a las memorias de su tesis doctoral, cuya referencia es [Arl79].

Paralelamente, algunos resultados sobre las preguntas análogas para posets fueron obtenidos. En 1946, Birkhoff [Bir46] probó que para todo grupo G existe un poset con $|G|(|G|+1)$ puntos y grupo de automorfismos G. Luego, en 1948 Frucht [Fru50] logra mejorar esta cota, probando que hay un poset con $|G|^2$ puntos que cumple lo pedido; y en 1950 él mismo logra mejorar esta cota probando que existe un poset con $|G|(d+2)$ puntos con grupo de automorfismos G, donde d puede ser el cardinal de cualquier conjunto de generadores.

En 1972 Melvin Thorton [Tho72] da otra construcción con $|G|(2d+1)$ puntos; aparentemente no estaba al tanto de la construcción de Frucht. Del mismo modo, en 2009 Jonathan Barmak y Gabriel Minian [BM09] — que tampoco estaban al tanto de dicha construcción — modificaron la construcción de Thorton para lograr una con $|G|(d+2)$ puntos. Esta construcción resultó ser esencialmente la misma que la de Frucht.

En 1980, Babai en su paper sobre las DRR [Bab80] prueba, como consecuencia de su resultado principal en ese trabajo, un teorema que dice que todo grupo G puede representarse como el grupo de automorfismos de un poset con a lo sumo $3|G|$ puntos.

En 2020, Jonathan Barmak [Bar20] dió una construcción de un poset con $4|G|$ puntos y grupo de automorfismos isomorfo a G que, a pesar de ser una cota más débil que la de Babai, tiene varias ventajas importantes: la demostración es más corta, más autocontenida y más general (no necesita separar más que en dos casos, a diferencia de la de Babai que necesita separar en muchos más). Además, empezó a estudiar la pregunta de realización para el caso abeliano. Introdujo la siguiente notación, que usaremos en esta tesis:

Notación 1.0.3: $\beta(G)$ es el menor número de puntos que puede tener un poset con grupo de automorfismos isomorfo a G.

En su trabajo exhibió cotas para $\beta\left(\mathbb{Z}_{p^k}\right)$ con p primo y $k \in \mathbb{N}$ que mejoraban las cotas ya conocidas.

En esta tesis, nuestro principal objetivo es dar una respuesta parcial a la pregunta de realización para G abeliano, aunque antes expondremos parte de lo que se sabe para G grupo finito general. En un comienzo vamos a comentar los resultados relacionados con la cota hallada por Babai en [Bab80] y luego, en la sección principal de este trabajo, obtenemos resultados originales que responden buena parte del caso abeliano, llegando a calcular $\beta(G)$ para todo G cíclico y para todo G que sea p−grupo con $p \geqslant 11$. Con excepción de los primos 2, 3, 5 y 7, nuestro análisis cubre tres de los cuatro tramos de la respuesta completa, si uno se basa en la línea descripta en el trabajo de Meriwether, Sabidussi y Arlinghaus.

En el Capítulo 2, contamos en detalle la demostración del resultado de Babai [Bab80] que dice que $\beta(G) \leqslant 3|G|$. Como parte de nuestro aporte, modificamos varias demostraciones

con el objetivo de evitar el uso de la noción de DRR y así trabajar directamente en el contexto de posets. También completamos los detalles que Babai dejó sin explicar, probamos resultados que Babai cita de otros artículos, e incluso enunciamos y probamos un resultado que no está en el paper original y creemos importante para entender el final de la demostración del teorema principal.

En el Capítulo 3, los resultados son todos originales. El objetivo es probar el resultado análogo al Teorema de Meriwether (parte I), es decir, calcular $\beta\left(\mathbb{Z}_{p^k}\right)$ para todo p primo y $k \in \mathbb{N}$. En primer lugar hallamos valores de β para algunos casos chicos que debemos tratar por separado, ya que la respuesta es distinta en éstos.
Para ilustrar las primeras ideas empezamos calculando $\beta\left(\mathbb{Z}_3\right)$ y luego pasamos a calcular $\beta\left(\mathbb{Z}_5\right)$ y $\beta\left(\mathbb{Z}_7\right)$ con estrategias similares. En estos tres casos los valores hallados fueron $9, 15$ y 21 puntos respectivamente; el triple del tamaño del grupo.
Una vez que analizamos estos casos patológicos, logramos calcular $\beta\left(\mathbb{Z}_{p^k}\right)$ para todo $p^k \geqslant 8$ dando una demostración general, concluyendo que $\beta\left(\mathbb{Z}_{p^k}\right) = 2p^k$ para todo $p^k \geqslant 8$; el doble del tamaño del grupo.

En el Capítulo 4 logramos resolver el caso cíclico general, es decir, calculamos $\beta\left(\mathbb{Z}_n\right)$ para todo $n \in \mathbb{N}$; el resultado análogo al Teorema de Meriwether (parte II).
En este capítulo también son originales todos los resultados. Al principio del mismo damos una cota para $\beta\left(\mathbb{Z}_n\right)$ que, de hecho, es óptima para muchos valores de n y luego probamos varios lemas auxiliares que nos ayudan a lidiar finalmente con los casos "problemáticos", que serán aquellos en los que n es divisible exactamente por $3, 4, 5$ o 7. Concretamente, si b es una función (con las potencias de primos como dominio) que en 2 vale 1, en $3, 4, 5$ y 7 vale 3 y en las demás potencias de primos vale 2, probamos que:

Teorema 4.2.1: Sea $n = p_1^{a_1} \cdots p_r^{a_r}$ donde los p_i son primos distintos.
Entonces, si $12 \nmid n$, o $8 \mid n$ o $9 \mid n$, se cumple que:

$$\beta(\mathbb{Z}_n) = \sum_{i=1}^{r} \beta(\mathbb{Z}_{p_i^{a_i}}) = \sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i}.$$

En cambio, si $4 \parallel n$ y $3 \parallel n$, se cumple que:

$$\beta(\mathbb{Z}_n) = \left(\sum_{i=1}^{r} \beta(\mathbb{Z}_{p_i^{a_i}})\right) - 1 = \left(\sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i}\right) - 1.$$

En el Capítulo 5 tratamos con el caso $p-$grupo, el más laborioso de esta tesis.
En la primera sección contamos varios resultados preliminares sobre permutaciones, algunos originales y muchos otros extraídos de [Arl85]; aunque algunas de sus demostraciones no están completas, así que parte de nuestro aporte fue completarlas.

En la segunda sección tratamos un caso patológico del problema, que es cuando aparecen *intersecciones raras*; noción que definimos en ese capítulo. Los resultados de la misma, si bien usan varias ideas que fueron inspiradas por el trabajo de Arlinghaus, son todos originales. El objetivo es reducir el problema a un caso en el que, o bien no hay intersecciones raras, o bien hay pero cumpliendo varias restricciones que nos ayudarán a resolver el problema.
En la tercera y última sección, cuyos resultados son también originales, tratamos el caso recién mencionado, donde o bien no hay intersecciones raras o bien estas cumplen varias restricciones. Una vez resuelto este caso, y habiendo probado en la sección anterior que cualquier situación puede reducirse al mismo, logramos calcular $\beta(G)$ para todo G que sea $p-$grupo con $p \geqslant 11$; aunque de las demostraciones dadas también se deducen cotas para los casos $p = 5$ y $p = 7$. El teorema final del capítulo es:

Teorema 5.3.15: Para todo $p \geqslant 11$ primo y $a_1, \dots a_n \in \mathbb{N}$,

$$\beta\left(\bigoplus_{i=1}^{n} \mathbb{Z}_{p^{a_i}}\right) = \sum_{i=1}^{n} 2p^{a_i}.$$

Capítulo 2

La cota de Babai

El objetivo de este capítulo es dar una demostración del siguiente resultado de László "Laci" Babai: todo grupo finito G puede representarse como el grupo de automorfismos de un poset $\mathcal{P}$ con a lo sumo $3|G|$ puntos.

La demostración original de Babai [Bab80] está fuertemente ligada a la noción de representación regular digráfica (DRR) mencionada en la introducción. Una DRR de G es un digrafo con grupo de automorfismos isomorfo a G, sobre el cuál la acción de G es regular.

El aporte principal de este capítulo es doble. Si bien nuestra demostración es esencialmente la misma que la original, aquí no haremos uso de la noción de DRR, sino que trabajaremos directamente en el contexto de los posets. En segundo lugar, la demostración aquí expuesta resulta totalmente autocontenida. Demostraremos con detalle pasos que Babai no justifica, probaremos resultados que Babai cita de otros artículos y enunciaremos y probaremos un resultado (Lema 2.0.21) que no está en el paper original y es esencial para entender el final de la demostración del teorema.

Para cada par (G, L) con G un grupo finito y $L \subseteq G$ un subconjunto, vamos a definir un poset — que depende de la elección de G y L — que será nuestro candidato a poset con $3|G|$ puntos y grupo de automorfismos isomorfo a G. Tendremos la libertad de elegir L a conveniencia, y nos aprovecharemos de esto ya que, dependiendo del grupo, la forma de elegir L podría ser bastante diferente.

Definición 2.0.1: Sea G un grupo y L un subconjunto de G. Llamaremos $\mathcal{P}(G, L)$ al poset definido por:

- $\mathcal{P}(G, L) = G \times \{0, 1, 2\}$.
- $(x, i) \leqslant (x, j)$ para todo $x \in G$ e $i \leqslant j$.
- $(x, 0) \leqslant (xl, 2)$ para todo $l \in L$.

El siguiente lema refleja parte de la utilidad del poset recién definido.

Lema 2.0.2: $\mathrm{Aut}(\mathcal{P}(G,L))$ contiene un subgrupo isomorfo a G.

Demostración. Notemos que el morfismo $L_g : G\times\{0,1,2\} \to G\times\{0,1,2\}$ de multiplicación a izquierda por g en la primera coordenada es un automorfismo de $\mathcal{P}(G,L)$ para todo $g \in G$. Esto nos dice que $G \simeq \{L_g : g \in G\} \leqslant \mathrm{Aut}(\mathcal{P}(G,L))$ como queríamos. ■

Los enunciados de los siguientes dos resultados están inspirados en [Bab80, Fact 2.4 y Fact 2.5] buscando una utilidad similar, y sus demostraciones son originales de esta tesis.

Proposición 2.0.3: Sea G un grupo finito, L un subconjunto de G, $H = \{h_1,\dots,h_n\}$ un conjunto de generadores de G y $\mathcal{P}(G,L)$ el poset recién definido. Vale que:

$$\forall\ \varphi \in \mathrm{Aut}(\mathcal{P}(G,L)),$$

$$\varphi(e,2) = (e,2) \implies \varphi(h_k,2) = (h_k,2)\ \ \forall\ k = 1,2,\dots,n$$

$$\iff$$

$$\forall\ \varphi \in \mathrm{Aut}(\mathcal{P}(G,L)) \ \text{ y } \ g \in G,$$

$$\varphi(g,2) = (g,2) \implies \varphi(gh_k,2) = (gh_k,2)\ \ \forall\ k = 1,2,\dots,n.$$

Demostración. Asumamos que para todo $\psi \in \mathrm{Aut}(\mathcal{P}(G,L))$ vale que $\psi(e,2) = (e,2)$ implica $\psi(h_k,2) = (h_k,2)$ para todo $k = 1,2,\dots,n$.
Dado $\varphi \in \mathrm{Aut}(\mathcal{P}(G,L))$ y $g \in G$, supongamos que $\varphi(g,2) = (g,2)$ y vamos a probar que se cumple $\varphi(gh_k,2) = (gh_k,2)$ para todo $k = 1,2,\dots,n$.
Recordemos que L_g, el morfismo de multiplicación a izquierda por g en la primer coordenada, pertenece a $\mathrm{Aut}(\mathcal{P}(G,L))$.
Dicho esto, podemos reescribir la igualdad $\varphi(g,2) = (g,2)$ como $\varphi(L_g(e,2)) = L_g(e,2)$, que a su vez es $L_g^{-1}\circ\varphi\circ L_g(e,2) = (e,2)$. Como $L_g^{-1}\circ\varphi\circ L_g \in \mathrm{Aut}(\mathcal{P}(G,L))$, la hipótesis inicial nos dice que $L_g^{-1}\circ\varphi\circ L_g(h_k,2) = (h_k,2)$ para todo $k = 1,2,\dots,n$; pero despejando esto es exactamente $\varphi(gh_k,2) = (gh_k,2)$ para todo $k = 1,2,\dots,n$, como queríamos.
La recíproca se resuelve de manera análoga, considerando el automorfismo $L_{g^{-1}}$ de multiplicación a izquierda por g^{-1} en la primer coordenada. ■

Como H genera G, de esta proposición deducimos el siguiente corolario.

Corolario 2.0.4: Si para todo $\varphi \in \mathrm{Aut}(\mathcal{P}(G, L))$ vale

$$\varphi(e, 2) = (e, 2) \implies \varphi(h_k, 2) = (h_k, 2) \ \ \forall\, k = 1, 2, \ldots, n\,,$$

entonces, si algún $\psi \in \mathrm{Aut}(\mathcal{P}(G, L))$ cumple $\psi(e, 2) = (e, 2)$, es $\psi = \mathrm{Id}$.

Demostración. Como H genera G, de la Proposición 2.0.3 podemos deducir que $\psi(g, 2) = (g, 2)$ para todo $g \in G$. Además, para todo $g \in G$, el único punto de altura 1 que es menor que $(g, 2)$ es $(g, 1)$; por lo que $\psi(g, 1) = (g, 1)$. De la misma forma, como $(g, 0)$ es el único punto de altura 0 que es menor que $(g, 1)$, vale que $\psi(g, 0) = (g, 0)$.
Concluímos que $\psi = \mathrm{Id}$, como queríamos. ∎

Estos últimos dos resultados nos serán de utilidad, ya que nos proveen información acerca de cómo son los automorfismos de $\mathcal{P}(G, L)$. Ahora, necesitamos la siguiente definición.

Definición 2.0.5: Dado un grupo G, decimos que un conjunto de generadores H de G es *irreducible* si ningún subconjunto propio de H genera G.

Notar que para cualquier grupo finito G siempre existe un conjunto irreducible de generadores de G; basta con elegir uno de cardinal mínimo.

Por otro lado, es importante conocer la siguiente definición.

Definición 2.0.6: Dado un poset $\mathcal{P}$, la *altura* de $x \in \mathcal{P}$ se define recursivamente como:

- Si x es minimal, su altura es 0.
- Si x no es minimal, su altura es igual a sumarle 1 al máximo entre las alturas de los elementos de $\mathcal{P}$ que están cubiertos por x.

Además, llamamos *altura* de $\mathcal{P}$ al máximo entre las alturas de los elementos de $\mathcal{P}$.

En el caso de $\mathcal{P}(G, L)$ la altura de sus elementos está dada por la segunda coordenada.

Notar que, como los automorfismos de posets preservan el orden, en particular deben preservar alturas. Esto nos ayuda a probar el siguiente resultado.
Dicho esto, pasamos a probar el resultado principal de este capítulo, que encuentra una manera adecuada de elegir L para una gran familia de grupos finitos; es decir, si G pertenece a tal familia, sabremos hallar un L tal que $\mathrm{Aut}(\mathcal{P}(G, L)) \simeq G$.

Nuestro principal aporte en la demostración de este lema es que fue modificada de forma tal que no sea necesario conocer la definición de DRR y, por lo tanto, sea autocontenida respecto a los contenidos tratados en esta tesis.

Lema 2.0.7: Sea G un grupo finito que no es cíclico. Supongamos que G tiene un conjunto irreducible de generadores $H = \{h_1, \dots, h_d\}$ de modo que H no contiene involuciones y tal que para algún $j \in \{1, \dots, d\}$ se cumplen las siguientes condiciones:

(a) si $j = 1$, entonces $h_1^3 \neq e$.

(b) si $j = d$, entonces $h_1 h_d \neq h_d h_1$.

(c) si $j = d$, entonces $h_1^2 \neq h_d^{-2}$.

(d) $h_j^{-1} h_1 h_j \neq h_1^{-1}$.

(e) $h_{d-1}^{-1} h_d h_{d-1} \neq h_d^{-1}$.

Si definimos $K = \left\{h_i^{-1} h_{i+1} : i = 1, 2, \dots, d-1\right\} \cup \{h_j h_1\}$ y $L = K \cup K^{-1} \cup H$, entonces $H \cap \left(K \cup K^{-1}\right) = \emptyset$ y $\mathrm{Aut}\left(\mathcal{P}(G, L)\right) \simeq G$.

Demostración. Si $H \cap \left(K \cup K^{-1}\right) \neq \emptyset$ existiría $1 \leqslant k \leqslant d$ tal que, o bien existe $1 \leqslant i \leqslant d-1$ con $h_k = \left(h_i^{-1} h_{i+1}\right)^{\pm 1}$ (lo que contradice que H sea irreducible), o bien $h_k = (h_j h_1)^{\pm 1}$ (lo cual contradice que H sea irreducible a menos que $k = j = 1$ y el exponente sea -1, en cuyo caso contradice (a)). Por lo tanto, $H \cap \left(K \cup K^{-1}\right) = \emptyset$.

Una observación importante es que, dado $g \in G$, el único punto de $\mathcal{P}(G, L)$ de altura 1 que es menor que $(g, 2)$ es $(g, 1)$, y el único punto de altura 0 que es menor que $(g, 1)$ es $(g, 0)$. Dicho eso, dados $a, b \in G$ distintos, vamos a decir que $(a, 2)$ es *súper-adyacente* a $(b, 2)$ si y sólo si $(a, 0) \leqslant (b, 2)$ (ver Figura 2.1).

No es difícil notar que $(h_i, 2)$ es súper-adyacente a $(h_{i+1}, 2)$ para todo $i = 1, \dots, d$, ya que $(h_i, 0) \leqslant (h_i h_i^{-1} h_{i+1}, 2) = (h_{i+1}, 2)$. También $(h_{i+1}, 2)$ es súper-adyacente a $(h_i, 2)$.

Sin embargo, dados $p, q \in \{1, \dots, d\}$ con $\{p, q\} \neq \{i, i+1\}$ para todo $i = 1, 2, \dots, d-1$, no puede ocurrir que h_p sea súper-adyacente a h_q. En efecto, para que eso suceda debería darse alguna de las siguientes situaciones:

- $h_q = h_p h_k$ para algún $k \in \{1, 2, \dots, d\}$.
- $h_q = h_p \left(h_k^{-1} h_{k+1}\right)^{\pm 1}$ para algún $k \in \{1, 2, \dots, d-1\}$.
- $h_q = h_p (h_j h_1)^{\pm 1}$

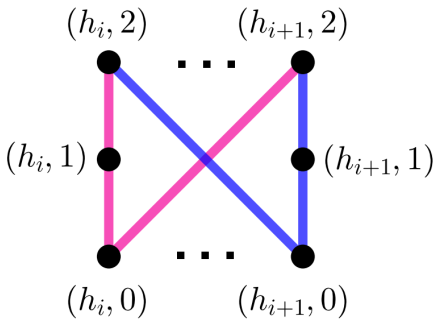

Figura 2.1: h_i súper-adyacente a h_{i+1} (camino rosa) y h_{i+1} súper-adyacente a h_i (camino azul).

La primera situación contradice que H sea irreducible. En la segunda situación, como H es irreducible, debe cumplirse necesariamente que $\{p, q\} = \{k, k+1\}$ — de otro modo podríamos despejar algún generador en función de otros generadores distintos — lo cual estamos suponiendo que no ocurre. En la tercera situación, nuevamente por la irreductibilidad de H, debe cumplirse que $\{p, q\} = \{j, 1\}$. Esta condición se traduce en que, o bien $h_1 = h_j^2 h_1$, o bien $h_j = h_1 h_j h_1$. La primera opción contradice el hecho de que h_j no es una involución, y la segunda contradice (d).
Análogamente podemos probar que h_q no puede ser súper-adyacente a h_p.

De la misma forma se puede ver que $(e, 2)$ es súper-adyacente a $(h_i, 2)$ para todo $i = 1, 2, \ldots, d$. Sin embargo, $(h_i, 2)$ no es súper-adyacente a $(e, 2)$ para ningún $i = 1, 2, \ldots, d$. En efecto, para que eso pase debería ocurrir alguna de las siguiente situaciones:

- $h_i = h_k^{-1}$ para algún $k \in \{1, 2, \ldots, d\}$.
- $h_i = \left(h_k^{-1} h_{k+1}\right)^{\pm 1}$ para algún $k \in \{1, 2, \ldots, d-1\}$.
- $h_i = (h_j h_1)^{\pm 1}$.

Pero todas estas situaciones contradicen el hecho de que H sea irreducible; excepto la tercera situación cuando $j = 1$, pero eso contradice (a).

También podemos notar que $(h_i^{-1}, 2)$ es súper-adyacente a $(e, 2)$ para todo $i = 1, 2, \ldots, d$. Sin embargo, $(e, 2)$ no es súper-adyacente a $(h_i^{-1}, 2)$ para ningún $i = 1, 2, \ldots, d$. En efecto, para que eso pase debería ocurrir alguna de las siguiente situaciones:

- $h_i^{-1} = h_k$ para algún $k \in \{1, 2, \ldots, d\}$.
- $h_i^{-1} = \left(h_k^{-1} h_{k+1}\right)^{\pm 1}$ para algún $k \in \{1, 2, \ldots, d-1\}$.
- $h_i^{-1} = (h_j h_1)^{\pm 1}$.

Pero todas estas situaciones contradicen el hecho de que H sea irreducible; excepto la tercer situación cuando $j = 1$, pero eso contradice (a).

Por otro lado, $(e, 2)$ es súper-adyacente a $(h_j h_1, 2)$, $(h_{i+1}^{-1} h_i, 2)$ y $(h_i^{-1} h_{i+1}, 2)$ para todo $i = 1, 2, \ldots, d-1$, con la diferencia de que estos puntos también son súper-adyacentes a $(e, 2)$.

Por el Lema 2.0.2, sabemos que $G \leqslant \mathrm{Aut}(\mathcal{P}(G, L))$.
Para terminar, basta con ver que $\mathrm{Aut}(\mathcal{P}(G, L)) \leqslant G$. Para probar esto alcanza con probar que el único $\varphi \in \mathrm{Aut}(\mathcal{P}(G, L))$ que cumple $\varphi(e, 2) = (e, 2)$ es $\varphi = \mathrm{Id}$.
En efecto, si eso se cumple y $\psi \in \mathrm{Aut}(\mathcal{P}(G, L))$, como los automorfismos preservan altura, $\psi(e, 2) = (g, 2)$ para algún $g \in G$. Luego, como $L_{g^{-1}} \circ \psi \in \mathrm{Aut}(\mathcal{P}(G, L))$ y $L_{g^{-1}} \circ \psi(e, 2) = (e, 2)$, tenemos $L_{g^{-1}} \circ \psi = \mathrm{Id}$ y entonces $\psi = L_g$ para algún $g \in G$ como queríamos.

Sea $\varphi \in \mathrm{Aut}(\mathcal{P}(G, L))$ un automorfismo tal que $\varphi(e, 2) = (e, 2)$.

Observación 2.0.8: La súper-adyacencia se preserva por automorfismos de $\mathcal{P}(G, L)$.

Como $\{(h_i, 2)\}_{1 \leqslant i \leqslant d}$ son los únicos puntos que satisfacen que no son súper-adyacentes a $(e, 2)$ y a su vez $(e, 2)$ sí es súper-adyacente a todos ellos, debe ocurrir que $\varphi(H \times \{2\}) = H \times \{2\}$. Análogamente, como $\left\{(h_i^{-1}, 2)\right\}_{1 \leqslant i \leqslant d}$ son los únicos puntos que satisfacen que son súper-adyacentes a $(e, 2)$, pero $(e, 2)$ no es súper-adyacente a ninguno de ellos, debe ocurrir que $\varphi\left(H^{-1} \times \{2\}\right) = H^{-1} \times \{2\}$.
Como $(h_1, 2)$ y $(h_d, 2)$ son los únicos puntos en $H \times \{2\}$ que son súper-adyacentes a sólo un punto de $H \times \{2\}$, debe suceder que, o bien $\varphi(h_1, 2) = (h_1, 2)$, o bien que $\varphi(h_1, 2) = (h_d, 2)$.

Si sucede lo primero, como $(h_1, 2)$ sólo es súper-adyacente a $(h_2, 2)$ entre los puntos de $H \times \{2\}$, debe ser $\varphi(h_2, 2) = (h_2, 2)$. Además, usando inductivamente el hecho de que para todo $i = 2, 3, \ldots, d-1$ los únicos puntos de $H \times \{2\}$ tales que $(h_i, 2)$ es súper-adyacente a ellos son $(h_{i-1}, 2)$ y $(h_{i+1}, 2)$, podemos deducir que $\varphi(h_i, 2) = (h_i, 2)$ para todo $i = 1, 2, \ldots, d-1$. Por último, como $(h_d, 2)$ sólo es súper-adyacente a $(h_{d-1}, 2)$ entre los de $H \times \{2\}$, también $\varphi(h_d, 2) = \varphi(h_d, 2)$. El Corolario 2.0.4 nos dice que $\varphi = \mathrm{Id}$ como queríamos.

Supongamos que sucede lo segundo. Notemos que $(h_j^{-1}, 2)$ es súper-adyacente a $(h_1, 2)$ y, recíprocamente, $(h_1, 2)$ es súper-adyacente a $(h_j^{-1}, 2)$. Como $H^{-1} \times \{2\}$ permanece invariante por φ, existe $k \in \{1, \ldots, d\}$ tal que $\varphi\left(h_j^{-1}, 2\right) = \left(h_k^{-1}, 2\right)$. Por la suposición, aplicando φ vemos que $(h_k^{-1}, 2)$ es súper-adyacente a $(h_d, 2)$ y que $(h_d, 2)$ es súper-adyacente a $(h_k^{-1}, 2)$. En particular, debe ocurrir alguna de las siguientes situaciones:

- $h_d = h_k^{-1} \left(h_i^{-1} h_{i+1}\right)^{\pm 1}$.
- $h_d = h_k^{-1} (h_j h_1)^{\pm 1}$.

La primera igualdad, como H es irreducible, implica que $\{k, d\} = \{i, i+1\}$; por lo que $k = i = d-1$. Reemplazando queda $h_d = h_{d-1}^{-1}(h_{d-1}^{-1}h_d)^{\pm 1}$, pero esto no puede ocurrir; en un caso contradice que h_{d-1} no es involución y en el otro contradice (e).
La segunda igualdad implica, por ser H irreducible, que $\{k, d\} = \{j, 1\}$; por lo tanto $k = 1$, $j = d$. Reemplazando queda $h_1 h_d = (h_d h_1)^{\pm 1}$, pero en un caso esto contradice (b) y en el otro caso contradice (c); esta igualdad no puede suceder.

Concluimos que $\varphi = \mathrm{Id}$, como queríamos. ■

Ahora, pasamos a probar algunos resultados que nos proveen de grandes familias de grupos finitos que cumplen las condiciones del Lema 2.0.7.

Definición 2.0.9: Un grupo G es un *grupo diedral generalizado* si contiene un subgrupo abeliano H de índice 2 tal que los elementos de $G \setminus H$ son de orden 2 y, para todo $g \in G \setminus H$ y $h \in H$, se cumple que $ghg^{-1} = h^{-1}$. Decimos que H es un núcleo de G (notar que no está unívocamente determinado).

Lema 2.0.10: Dado un grupo H, existe un único grupo diedral generalizado (salvo isomorfismo) que tiene a H como núcleo.

Demostración. Si G es un grupo diedral generalizado con núcleo H, dado $c \in G \setminus H$ el conjunto $\langle c\rangle H$ con la operación inducida por G es un subgrupo de G. En efecto, dados $ch, ch' \in \langle c\rangle H$ y $h'' \in H$, como $c^2 = e$ tenemos que $chch' = c^{-1}hch' = h^{-1}h' \in \langle c\rangle H$, que $h''ch = cc^{-1}h''ch = ch''^{-1}h \in \langle c\rangle H$ y que $(ch)^{-1} = h^{-1}c^{-1} = cc^{-1}h^{-1}c = ch \in \langle c\rangle H$. Además, $\langle c\rangle \cap H = \{e\}$ ya que $c \in G\setminus H$ y $\langle c\rangle = \{e, c\}$. Por lo tanto, $\langle c\rangle H \simeq H \rtimes \langle c\rangle \simeq H \rtimes_\varphi \langle c\rangle$, el producto semidirecto interno entre $\langle c\rangle$ y H, que es isomorfo al producto semidirecto externo entre ellos, con φ siendo la conjugación. En particular es un subgrupo de G de orden $2|H|$, pero como $|G| = 2|H|$ por tener H índice 2, G debe ser este producto semidirecto, por lo que $G = H \rtimes_\varphi \langle c\rangle \simeq H \rtimes_\varphi \mathbb{Z}_2$. ■

Definición 2.0.11: Un grupo finito G es un 2−grupo abeliano elemental si es $G \simeq \mathbb{Z}_2^k$ para algún $k \in \mathbb{N}$.

La siguiente proposición y su demostración pueden encontrarse [Bab78].

Proposición 2.0.12: Para todo grupo G de orden mayor que 2, vale una y sólo una de las siguientes afirmaciones:

(I) G está generado por sus elementos de orden mayor a 2.

(II) G es un 2−grupo abeliano elemental.

(III) G es un grupo diedral generalizado con un núcleo que está generado por sus elementos de orden mayor a 2.

Demostración. Supongamos que no vale (I) y consideremos H el subgrupo generado por los elementos de G de orden mayor que 2.
Como los elementos de $G \setminus H$ tienen orden 2, para cualquier $g \in G \setminus H$ y $h \in H$ vale que $(gh)^2 = e$; si gh no tuviese orden 2, entonces $gh \in H$ y por lo tanto $g \in H$, que no ocurre. En particular, esto implica que $g^{-1}hg = h^{-1}$. Notemos que esto prueba que H es abeliano; en efecto, si $a, b \in H$ y $g \in G \setminus H$:

$$ab = g(g^{-1}ag)(g^{-1}bg)g^{-1} = ga^{-1}b^{-1}g^{-1} = g(ba)^{-1}g^{-1} = ba.$$

Si además suponemos que no vale (III), tenemos como información extra que $|G : H| > 2$. En particular, esto nos dice que existen $a, b, c \in G \setminus H$ tales que $ab = c$. Por lo tanto, para cualquier $h \in H$,

$$h^{-1} = c^{-1}hc = b^{-1}a^{-1}hab = b^{-1}h^{-1}b = h;$$

así que cualquier elemento de H tiene orden 2. Como H es abeliano y todos sus elementos tienen orden 2, probamos que vale (II) y completamos la demostración. ∎

Definición 2.0.13: Notamos Q_8 al grupo de cuaterniones, que es el grupo con 8 elementos $\{\pm 1, \pm i, \pm j, \pm k\}$ que cumple $-1 = i^2 = j^2 = k^2 = ijk$. También puede ser definido por la conocida presentación

$$Q_8 = \langle x, y : x^4 = e, x^2 = y^2, xyx = y \rangle.$$

La siguiente proposición es dejada como ejercicio en [Bab80].

Proposición 2.0.14: Si $G = \langle a, b : b^{-1}ab = a^{-1}, a^{-1}ba = b^{-1} \rangle$ entonces el orden de a y b es 4 y $G \simeq Q_8$.

Demostración. Empecemos probando que $G \simeq Q_8$.
Para eso, primero veamos que a y b cumplen las relaciones de Q_8 tomando $x = a$ e $y = b$. Reemplazando la segunda relación de G en la primera obtenemos $a^{-1}ba^2b = a^{-1}$, que simplificando es $ba^2b = e$. De esta igualdad sale que $a^2 = b^{-2}$. Por otro lado, en la misma igualdad intercalando b, obtenemos $babb^{-1}ab = baba^{-1} = e$, osea que $bab = a$. Intercalando b nuevamente $b^2b^{-1}ab = a$, osea que $b^2a^{-1} = a$ y entonces $b^2 = a^2$. Esta condición junto con $a^2 = b^{-2}$ implica $b^4 = e$ y, por lo tanto, $a^4 = e$.
Por último, la relación $aba = b$ sale de multiplicar $bab = a$ por ba a derecha a ambos lados, y usar que $b^2 = a^2$ y $a^4 = e$. Con esto queda probado que a y b satisfacen las relaciones de Q_8 tomando $x = a$ e $y = b$.

Resta probar que x e y cumplen las relaciones de G tomando $a = x$ y $b = y$.
Como $aba = b$ multiplicando por b^{-1} a izquierda y luego por a^{-1} a derecha a ambos lados, obtenemos $b^{-1}ab = a^{-1}$. Por otro lado, si en la ecuación $aba = b$ multiplicamos ambos lados por a^{-2} a izquierda, obtenemos $a^{-1}ba = a^{-2}b = a^2b = b^3 = b^{-1}$, como queríamos.

Finalmente, podemos afirmar que el morfismo $\phi : G \to Q_8$ que cumple $\phi(a) = x$ y $\phi(b) = y$ es un isomorfismo; y como a y b tienen orden 4, x e y tienen orden 4. ■

Corolario 2.0.15: Sea G un grupo finito y $g, h \in G$. Si $\mathrm{ord}(g) \neq 1, 2$, $\mathrm{ord}(h) \neq 1, 2$ y g y h cumplen las relaciones $g^{-1}hg = h^{-1}$ y $h^{-1}gh = g^{-1}$, entonces $\langle g, h\rangle \simeq Q_8$. En particular, $\mathrm{ord}(g) = 4$ y $\mathrm{ord}(h) = 4$.

Demostración. En efecto, notemos que $\langle g, h\rangle$ es un cociente de Q_8 por cumplir las relaciones de la presentación de la proposición anterior tomando $a = g$ y $b = h$. Es un hecho conocido que todos los cocientes de Q_8 son isomorfos a alguno de los siguientes: el grupo trivial, $\mathbb{Z}_2$, $\mathbb{Z}_2^2$, Q_8. Como $\mathrm{ord}(g) \neq 1, 2$ y el único de esos grupos que tiene elementos con orden distinto de 1 y 2 es Q_8, concluimos que este cociente es exactamente Q_8. ■

La siguiente proposición y su demostración pueden encontrarse en [Bab80], aunque aquí completamos varios detalles que no estaban explicados en el paper.

Proposición 2.0.16: Sea G un grupo finito que no es cíclico, ni diedral generalizado, ni es $\mathbb{Z}_3^2$, ni es Q_8. Entonces G satisface las condiciones del Lema 2.0.7.

Demostración. Sea $F = \{x \in G : x^2 = e\}$. Por el Lema 2.0.12 — teniendo en cuenta que los 2−grupos abelianos elementales son, en particular, diedrales generalizados — como

G no es un grupo diedral generalizado, $G \setminus F$ genera G. Consideramos un subconjunto de cardinal mínimo de $G \setminus F$ con la propiedad de generar G — en particular, será un conjunto irreducible de generadores — y lo llamaremos $H = \{h_1, h_2, \dots, h_d\}$.

Caso 1: si todos los elementos de H tienen orden 3.

Tomando $j = 2$, (a) se satisface trivialmente ya que $d \neq 1$ por no ser cíclico G.
La condición (c) se traduce en $h_1^{-1} \neq h_2$, que se satisface por ser H irreducible.
Supongamos que no vale la condición (d). Despejando y multiplicando por h_j a ambos lados, esto equivale a $(h_1h_j)^2 = h_j^2$. Por un lado, elevando al cubo vemos que $\mathrm{ord}(h_1h_j) \mid 6$; por otro lado, multiplicando por h_1h_j a izquierda ambos lados, podemos ver que $\mathrm{ord}(h_1h_j) \mid 9$.
Esto nos dice que $\mathrm{ord}(h_1h_j) = 1$ o 3. No puede ser 1 porque esto implicaría que $h_1 = h_j^{-1}$, que no ocurre por ser H irreducible; y no puede ser 3 porque esto implicaría que $(h_1h_j)^{-1} = h_1^{-1}$, que despejando es $h_j = e$, lo cual no ocurre. Por lo tanto vale la condición (d).
La condición (e) se verifica de manera análoga, cambiando el rol de h_j por el de h_{d-1} y el de h_1 por h_d. Finalmente, notemos que se satisface también la condición (b) ya que, si no fuese así, sería $j = 2$, conmutarían h_1 y h_d y $G = \langle h_1, h_d \rangle \simeq \mathbb{Z}_3^2$, que no ocurre.

Caso 2: si algún elemento de H — que podemos suponer h_1 — tiene orden distinto de 3.

Tomamos $j = 1$ lo cuál, notando que $d \neq 1$ por no ser cíclico G, hace que se satisfagan trivialmente (a), (b), (c) y (d). Para ver que se satisface (e), vamos a separar en casos según el valor de d.

- Supongamos $d \geqslant 3$.

  Si existen $a, b \in \{h_2, \dots, h_d\}$, $a \neq b$ tales que $b^{-1}ab \neq a^{-1}$, podemos reetiquetar los generadores de modo que $h_{d-1} = b$ y $h_d = a$ y se cumple (e).

  A partir de ahora, supongamos que no existen tales a y b. Si existe $a \in \{h_2, \dots, h_d\}$ tal que $h_1^{-1}ah_1 \neq a^{-1}$ o $a^{-1}h_1a \neq h_1^{-1}$, intercambiamos los roles de h_1 y cualquier $b \in \{h_2, \dots, h_d\}$ con $b \neq a$; esto es posible porque, gracias al Corolario 2.0.15 aplicado a h_i, h_j para cualquier par $i, j \in \{2, \dots, d\}$ — notar que $\mathrm{ord}(h_i) \neq 1, 2$ para todo $2 \leqslant i \leqslant d$ por ser H irreducible y no contener involuciones — vale $\mathrm{ord}(h_i) = 4$ para todo $2 \leqslant i \leqslant d$. Haciendo este cambio, logramos que se satisfaga (e).

  El único caso restante es cuando $b^{-1}ab = a^{-1}$ para todo $a, b \in H$. Por el Corolario 2.0.15, como $\mathrm{ord}(h_{d-1}) \neq 1, 2$ y $\mathrm{ord}(h_d) \neq 1, 2$, sabemos que $\mathrm{ord}(h_{d-1}) = \mathrm{ord}(h_d) = 4$. Definiendo $h'_{d-1} = h_{d-2}h_{d-1}$, como de la identidad $h_{d-2}^{-1}h_{d-1}h_{d-2} = h_{d-1}^{-1}$ podemos despejar $h_{d-2}^{-1}h_{d-1} = (h_{d-2}h_{d-1})^{-1}$, valen

  $$(h_{d-2}h_{d-1})^{-1}h_{d-1}h_{d-2}h_{d-1} = h_{d-1}^{-1}h_{d-2}^{-1}h_{d-1}h_{d-2}h_{d-1} = h_{d-1}^{-1}h_{d-1}^{-1}h_{d-1} = h_{d-1}^{-1}$$

  $$\text{y} \quad h_{d-1}^{-1}h_{d-2}h_{d-1}h_{d-1} = h_{d-2}^{-1}h_{d-1} = (h_{d-2}h_{d-1})^{-1}$$

donde el despeje mencionado se usa en la segunda igualdad del segundo renglón.

Además, $h'_{d-1} \neq e$ por ser H irreducible y no tiene orden 2 porque, si así fuese, usando que $h_{d-1}h_{d-2}h_{d-1} = h_{d-2}$ (que se despeja de $h_{d-2}^{-1}h_{d-1}h_{d-2} = h_{d-1}^{-1}$) tendríamos $e = h_{d-2}h_{d-1}h_{d-2}h_{d-1} = h_{d-2}^2$, que no ocurre. Luego, por el Corolario 2.0.15 aplicado a h_{d-1} y h'_{d-1} se cumple que $\mathrm{ord}(h'_{d-1}) = 4$. Podemos observar que $\{h_1, \ldots, h_{d-2}, h'_{d-1}, h_d\}$ sigue siendo un conjunto de generadores irreducible. Finalmente, como $(h'_{d-1})^{-1}h_d h'_{d-1} = h_d \neq h_d^{-1}$, cambiando h_{d-1} por h'_{d-1} podemos afirmar que vale (e).

- Supongamos $d = 2$.

  Si $h_2^3 \neq e$, entonces o bien ocurre (e), o bien podemos intercambiar los roles de h_1 y h_2 de modo que ahora se cumpla (e); en este último caso seguiría manteniéndose la validez de $(a), (b), (c)$ y (d) por ser $h_2^3 \neq e$. En efecto, si no se cumple (e) e intercambiando los roles de h_1 y h_2 tampoco se cumple (e), entonces — como h_1 y h_2 no tienen orden 1 ni 2 — por el Corolario 2.0.15 es $G \simeq Q_8$, lo cual no es cierto.

  Supongamos que $h_2^3 = e$. Si no vale (e), conmutan h_1^2 y h_2:

  $$h_1^2h_2 = h_1^2h_2h_1^{-2}h_1^2 = h_1^2h_2h_1^2h_1^2 = h_2h_1^2$$

  donde para la última igualdad usamos $h_1h_2h_1 = h_2$ que se despeja de $h_2^{-1}h_1h_2 = h_1^{-1}$.

  Redefinimos h_2 como $h'_2 = h_1^2h_2$, notando que $(h'_2)^2 \neq e$ (de lo contrario, usando que $h_1h_2h_1 = h_2$, es $e = h_1^2h_2h_1^2h_2 = h_2^2$, que no ocurre) y que $\{h_1, h'_2\}$ es un conjunto irreducible de generadores de G. Si $(h'_2)^3 \neq e$ terminamos por lo antes probado, así que supongamos que $(h'_2)^3 = e$. En ese caso, $(h_1^2h_2)^3 = h_1^6 = e$; por lo que $\mathrm{ord}(h_1) \neq 4$. Esto último, como

  $$h_1^{-1}h'_2h_1 = h_1^{-1}h_1^2h_2h_1 = h_1^2h_1^{-1}h_2h_1 = h_1^2h_2^{-1}$$

  y $(h'_2)^{-1} = h_1^{-2}h_2^{-1}$, nos dice que se cumple (e) con estos nuevos generadores.

Habiendo agotado todos los casos, el resultado sigue. ■

Ahora pasamos a probar algunos resultados que nos ayudarán a lidiar con aquellos grupos finitos que no cumplen las condiciones del Lema 2.0.7.
Las proposiciones 2.0.17 y 2.0.23 pueden encontrarse en su versión con grafos dirigidos junto a sus demostraciones en [Bab80]. Nuestro principal aporte en estas demostraciones es modificarlas de modo que no haga falta conocer la definición de DRR, para hacerlas autocontenidas respecto a los contenidos tratados en esta tesis. Además, completamos varios detalles que no estaban explicados en el paper.

Proposición 2.0.17: Sea

$$G = \langle a, b, c : a^3 = b^3 = c^2 = e, ab = ba, c^{-1}ac = a^{-1}, c^{-1}bc = b^{-1} \rangle.$$

Entonces, si definimos $H = \{ca, ca^{-1}, cb\}$, $K = \{a, ab\}$, $\mathrm{Aut}(\mathcal{P}(G, H \cup K)) \simeq G$.

Demostración. Empezamos probando una afirmación importante.

Afirmación 2.0.18: Los elementos de H tienen todos orden 2, los elementos de K tienen todos orden 3 y $a \neq b$.

Demostración. Es sencillo chequear que el orden de los elementos de H es un divisor de 2 y que el de los elementos de K es un divisor de 3; veamos que ninguno tiene orden 1.
Para lo siguiente, necesitamos recordar que $\langle r, s : r^3 = e\ ,\ s^2 = e, s^{-1}rs = r^{-1} \rangle$ es una presentación conocida de D_6, el grupo diedral de 6 elementos.
Consideramos el morfismo de grupos $f : \langle a, b, c \rangle \to D_6$ — que va del grupo libre de tres generadores a D_6 — definido por $f(a) = r$, $f(b) = e$ y $f(c) = s$.
No es difícil chequear que todas las palabras que corresponden a las relaciones de la presentación de G tienen como imagen el neutro, por lo que este morfismo pasa bien al cociente, otorgándonos un morfismo de grupos $\bar{f} : G \to D_6$.
Las imágenes de los elementos a, ab, ca, ca^{-1} y cb por $\bar{f}$ son r, r, sr, sr^{-1} y s respectivamente, que son elementos no triviales de D_6. Por lo tanto, ninguno de estos elementos era trivial en G. Además, $f(a) = r \neq e = f(b)$, por lo que $a \neq b$ en G. ∎

Vamos a necesitar tener presente la noción de súper-adyacencia definida en el Lema 2.0.7.

Observación 2.0.19: Los elementos de $H \times \{2\}$ son súper-adyacentes a $(e, 2)$ y también $(e, 2)$ es súper-adyacente a todos ellos.

En efecto, $(ca, 0) \leqslant \big((ca)^2, 2\big) = (e, 2)$, $(ca^{-1}, 0) \leqslant \big((ca^{-1})^2, 2\big) = (e, 2)$ y $(cb, 0) \leqslant \big((cb)^2, 2\big) = (e, 2)$. Nuevamente, la segunda afirmación es inmediata por la definición de $\mathcal{P}(G, H \cup K)$.

Observación 2.0.20: Ningún elemento de $K \times \{2\}$ es súper-adyacente a $(e, 2)$, pero $(e, 2)$ es súper-adyacente a todos ellos.

La segunda afirmación es inmediata por la definición de $\mathcal{P}(G, H \cup K)$.
Las posibles situaciones para que un elemento de $K \times \{2\}$ sea súper-adyacente a $(e, 2)$ son

$a^2 = e$

$aca = e \implies c = a^{-2} = a$

$aab = e \implies a^{-1} = a^2 = b^{-1}$

$aca^{-1} = e \implies c = e$

$acb = e \implies a = (cb)^{-1}$

$(ab)^2 = e$

$aba = e \implies a^{-1} = a^2 = b^{-1}$

$abca = e \implies ab = (ca)^{-1}$

$abca^{-1} = e \implies ab = \left(ca^{-1}\right)^{-1}$

$abcb = e \implies ab = (cb)^{-1}$

Pero todas ellas nos llevan a una contradicción, algunas porque implican una igualdad de dos elementos de distinto orden, y las otras porque implican una igualdad entre a y b.

Al igual que en la demostración del Lema 2.0.7, para terminar alcanza con ver que el único $\varphi \in \mathrm{Aut}(\mathcal{P}(G, H \cup K))$ que tiene a $(e, 2)$ por punto fijo es $\varphi = \mathrm{Id}$.

Sea $\varphi \in \mathrm{Aut}(\mathcal{P}(G, H \cup K))$ tal que $\varphi(e, 2) = (e, 2)$.
Las dos observaciones anteriores nos dicen que $\varphi(H \times \{2\}) = H \times \{2\}$, ya que son los únicos puntos de $\mathcal{P}(G, H \cup K)$ que cumplen que $(e, 2)$ es súper-adyacente a todos ellos y a su vez todos ellos son súper-adyacentes a $(e, 2)$.
Veamos que $(cb, 2)$ no es súper adyacente a $(ca, 2)$ ni a $(ca^{-1}, 2)$; si alguna de estas dos situaciones ocurre, debe pasar alguna de las siguientes

$cba = ca \implies b = e$

$cbab = ca \implies b^2 = e$

$cbca = ca \implies b = c^{-1}$

$cbca^{-1} = ca \implies (ab)^{-1} = ca$

$(cb)^2 = ca \implies c^{-1} = a$

$cba = ca^{-1} \implies b = a^{-2} = a$

$cbab = ca^{-1} \implies ab = a^2b^2 = e$

$cbca = ca^{-1} \implies b^{-1} = ca^{-2} = ca$

$cbca^{-1} = ca^{-1} \implies cb = e$

$(cb)^2 = ca^{-1} \implies e = ca^{-1}$

Pero todas ellas nos llevan a una contradicción, algunas porque implican una igualdad de dos elementos de distinto orden, y las otras porque implican una igualdad entre a y b. Como $(ca, 2)$ es súper-adyacente a $(ca^{-1}, 2)$ — pues $(ca, 0) \leqslant (caa, 2) = (ca^{-1}, 2)$ — y $(ca^{-1}, 2)$ es súper-adyacente a $(cb, 2)$ — pues $(ca^{-1}, 0) \leqslant (ca^{-1}ab, 2) = (cb, 2)$ —, podemos afirmar que $(cb, 2)$ es el único punto de $H \times \{2\}$ que no es súper-adyacente a otro punto de $H \times \{2\}$, por lo tanto, $\varphi(cb, 2) = (cb, 2)$.
Para terminar, veamos que $(ca, 2)$ no es súper-adyacente a $(cb, 2)$; si esta situación ocurre, debe pasar alguna de las siguientes

$caa = cb \implies e = ab$

$caab = cb \implies a^2 = e$

$(ca)^2 = cb \implies e = cb$

$caca^{-1} = cb \implies a = a^{-2} = cb$

$cacb = cb \implies ca = e$

Pero todas ellas nos llevan a una contradicción, porque implican una igualdad entre elementos de distinto orden.
Como $(ca^{-1}, 2)$ es súper-adyacente a $(cb, 2)$ pero $(ca, 2)$ no — y además $\varphi(H \times \{2\}) = H \times \{2\}$ y $\varphi(cb, 2) = (cb, 2)$ —, concluimos que $\varphi(ca, 2) = (ca, 2)$ y $\varphi(ca^{-1}, 2) = (ca^{-1}, 2)$.

Como H genera G — pues $caca^{-1} = a$, $\left(caca^{-1}\right)^{-1} ca^{-1}cb = a^{-1}ab = b$ y $ca^{-1}caca^{-1} = ca^{-1}a = c$ — el Lema 2.0.4 nos dice que $\varphi = Id$, como queríamos. ■

Ahora probamos el siguiente lema que Babai deja implícito en [Bab80], aunque no lo enuncia ni demuestra. Sin embargo, es clave para entender la demostración del teorema principal.

Lema 2.0.21: G es el grupo diedral generalizado con núcleo $\mathbb{Z}_3^2$.

Demostración. Notar que el subgrupo de G generado por a y b, que llamaremos A, cumple las relaciones de $\mathbb{Z}_3^2$, que está presentado por $\langle a, b : a^3 = b^3 = e\,,\ ab = ba\rangle$, y por lo tanto es isomorfo a un cociente de $\mathbb{Z}_3^2$. De la demostración de la Afirmación 2.0.18 podemos deducir que $b \neq a^2$ y además, repitiendo el mismo argumento con b en vez de a, podemos ver que b es no trivial en G. Como todos los cocientes de $\mathbb{Z}_3^2$ distintos de $\mathbb{Z}_3^2$ tienen orden a lo sumo 3 y ya conocemos cuatro elementos distintos de A ($e, a, a^2, b \in A$), concluimos que A es isomorfo a $\mathbb{Z}_3^2$. Además, este subgrupo tiene índice 2 ya que $G/\langle a, b\rangle \simeq \langle c\rangle \simeq \mathbb{Z}_2$. Como A tiene índice 2, $G = A \cup cA$ donde A y cA son las dos coclases a izquierda.

Como A es abeliano, cualquier elemento de A puede escribirse como $a^n b^m$ para algún par $n, m \in \mathbb{N}$. Veamos por inducción en en el par (n, m) que $c^{-1}a^n b^m c = (a^n b^m)^{-1}$ para todo par $(n, m) \in \mathbb{N} \times \mathbb{N}$. Es claro que vale para $n = m = 1$ ya que $c^{-1}abc = c^{-1}acc^{-1}bc = a^{-1}b^{-1}$. Ahora, supongamos que vale para todo par (n', m') con $n' < n$ o $m' < m$. En ese caso $c^{-1}a^n b^m c = c^{-1}acc^{-1}a^{n-1}b^m c$ que por hipótesis inductiva y la relación correspondiente es igual a $a^{-1}\left(a^{n-1}b^m\right)^{-1} = (a^n b^m)^{-1}$.

Como $c \in G \setminus A$ y cumple $c^2 = e$ y $c^{-1}dc = d^{-1}$ para todo $d \in A$, podemos afirmar que cualquier elemento $x \in G \setminus A \subseteq cA$ se puede escribir como ca' con $a' \in A$ y cumple $(ca')^2 = ca'ca' = c^{-1}a'ca' = a'^{-1}a' = e$ y $(ca')^{-1}dca' = a'^{-1}c^{-1}dca' = a'^{-1}d^{-1}a' = d^{-1}$ para todo $d \in A$ (recordar que A abeliano). Luego G es el grupo diedral generalizado con núcleo $A = \mathbb{Z}_3^2$. ■

La demostración del siguiente hecho puede encontrarse en el próximo capítulo (Afirmación 3.2.2) — ilustra el caso particular cuando $n = 3$, pero es idéntica para cualquier $n \in \mathbb{N}$.

Proposición 2.0.22: Si $G \simeq \mathbb{Z}_n \simeq \langle g\rangle$ para algún $n \in \mathbb{N}$ y $g \in G$, entonces si $L = \{g\}$ tenemos $\mathrm{Aut}(\mathcal{P}(G, L)) \simeq G$.

El resultado anterior va a ser utilizado en la siguiente proposición, cuyo enunciado y demostración puede encontrarse en [Bab80].

Proposición 2.0.23: Sea G un grupo diedral generalizado con núcleo A. Si A es cíclico de orden mayor a 2, o si satisface las condiciones del Lema 2.0.7, entonces existe $L \subseteq G$ tal que $\mathrm{Aut}(\mathcal{P}(G, L)) \simeq G$.

Demostración. Por los lemas 2.0.7 y 2.0.22, sabemos que existe algún subconjunto $L \subseteq A$ tal que $\mathrm{Aut}(\mathcal{P}(A, L)) \simeq A$. Además, en ambos casos podemos asegurar que $L \setminus L^{-1}$ genera A: en el caso cíclico $L \setminus L^{-1} = \{g\}$, y en el otro caso $H \subseteq L \setminus L^{-1}$ pues H no contenía involuciones, $H \cap (K \cup K^{-1}) = \emptyset$ y H genera G. Tomamos $b \in G \setminus A$ y definimos $K = L \cup \{b\}$.
Consideramos ahora el poset $\mathcal{P}(G, K)$.
Dado $x \in G$, vamos a decir que $(x, 2)$ está *en la componente especial de* $\mathcal{P}(G, K)$ si existe una sucesión $a_0, a_1, a_2, \ldots, a_m \in \mathcal{P}(G, K)$ con $a_0 = e$ y $a_m = x$ tal que, para todo $0 \leqslant i \leqslant m-1$, $(a_i, 2)$ es súper-adyacente a $(a_{i+1}, 2)$ pero $(a_{i+1}, 2)$ no es súper-adyacente a $(a_i, 2)$

Observación 2.0.24: Si $a, a' \in G$, entonces $(a, 2)$ es súper-adyacente a $(a', 2)$ y $(a', 2)$ no es súper-adyacente a $(a, 2)$ si y sólo si existe $k \in K \setminus K^{-1}$ tal que $ka = a'$.

En efecto, si $(a, 2)$ es súper-adyacente a $(a', 2)$ debe existir $k \in K$ de modo que $ka = a'$; y si ocurriese que $k \in K \cap K^{-1}$, como $a = k^{-1}a'$, tendríamos que $(a', 2)$ sería súper-adyacente a $(a, 2)$, pero eso no ocurre.
Para la recíproca, si existe $k \in K \setminus K^{-1}$ tal que $ka = a'$, entonces $(a, 2)$ es súper-adyacente a $(a', 2)$; pero no puede ocurrir que $(a', 2)$ sea súper-adyacente a $(a, 2)$, porque en ese caso debería existir $k' \in K$ de modo que $k'a' = a$, y combinando las dos ecuaciones obtendríamos que $K \ni k' = k^{-1} \in K^{-1}$, un claro absurdo.

Observación 2.0.25: Como b es una involución, se cumple que $K \setminus K^{-1} = L \setminus L^{-1}$.

Observación 2.0.26: Todos los puntos de $A \times \{2\}$ están en la componente especial de $\mathcal{P}(G, K)$.

En efecto, como $K \setminus K^{-1} = L \setminus L^{-1}$ genera A, podemos escribir cualquier elemento a de A como una palabra en los elementos de $K \setminus K^{-1}$, y por lo tanto existe una sucesión $a_0, a_1, a_2, \ldots, a_m \in A$ con $a_0 = e$ y $a_m = a$ de modo que, para todo $0 \leqslant i \leqslant m-1$, $a_{i+1} = k_i a_i$ con $k_i \in K \setminus K^{-1}$. Por la Observación 2.0.24, esto es exactamente lo pedido.

Observación 2.0.27: Ningún punto de $G \setminus A \times \{2\}$ está en la componente especial de $\mathcal{P}(G, K)$.

Supongamos que existe un punto $(g, 2) \in G \setminus A \times \{2\}$ que está en la componente especial de $\mathcal{P}(G, K)$. En ese caso, existe una sucesión $a_0, a_1, a_2, \ldots, a_m \in G$ con $a_0 = e$ y $a_m = g$ de modo que, para todo $0 \leqslant i \leqslant m-1$, $a_{i+1} = k_i a_i$ con $k_i \in K \setminus K^{-1}$. Pero notemos que $e \in A$ por ser A subgrupo y, si para algún $0 \leqslant i \leqslant m-1$ se cumple $a_i \in A$, entonces

$a_{i+1} = k_i a_i \in A$ por ser $k_i \in K \setminus K^{-1} = L \setminus L^{-1} \subseteq A$. Inductivamente obtenemos que $g = a_m \in A$, lo cuál es absurdo.

Al igual que en el Lema 2.0.7, para probar que $\mathrm{Aut}(\mathcal{P}(G,K)) \simeq G$ alcanza con probar que el único $\varphi \in \mathrm{Aut}(\mathcal{P}(G,K))$ que tiene a $(e,2)$ por punto fijo es $\varphi = \mathrm{Id}$.

Sea $\varphi \in \mathrm{Aut}(\mathcal{P}(G,K))$ tal que $\varphi(e,2) = (e,2)$.
En ese caso, como los puntos de $A \times \{2\}$ son los únicos que están en la componente especial de $\mathcal{P}(G,K)$, tenemos que $\varphi(A \times \{2\}) = A \times \{2\}$. Ahora, notemos que el subposet inducido por los puntos de A es exactamente $\mathcal{P}(A,L)$ y que φ se restringe a un automorfismo de este subposet. Como $\mathrm{Aut}(\mathcal{P}(A,L)) \simeq A$, el único automorfismo de $\mathcal{P}(A,L)$ que deja fijo a $(e,2)$ es la identidad; por lo tanto, $\varphi(a,2) = (a,2)$ para todo $a \in A$.
Por último, notemos que $\varphi(b,2) = (b,2)$, ya que los puntos de $A \times \{2\}$ quedan fijos y b es el único punto de $G \setminus A \times \{2\}$ al que $(e,2)$ es súper-adyacente. Como $G = \langle A, b\rangle$, por el Lema 2.0.4 concluimos que $\varphi = \mathrm{Id}$ como queríamos. ■

Lema 2.0.28: Si $G = \mathbb{Z}_2^k$ para algún $k \in \mathbb{N}$ o $G = \mathbb{Z}_3^2$, existe un poset $\mathcal{P}$ con $|\mathcal{P}| \leqslant 3|G|$ y $\mathrm{Aut}(\mathcal{P}) \simeq G$.

Demostración. El resultado se sigue de recordar que el *join* o *suma ordinal* entre dos posets $\mathcal{P}$ y $\mathcal{P}'$ cumple $\mathrm{Aut}(\mathcal{P} \oplus \mathcal{P}') \simeq \mathrm{Aut}(\mathcal{P}) \times \mathrm{Aut}(\mathcal{P}')$ y conocer la Proposición 2.0.22. ■

La siguiente proposición y su demostración pueden encontrarse en [Bab80].

Proposición 2.0.29: Si $G = Q_8$, existe un poset $\mathcal{P}$ con $|\mathcal{P}| = 3|G|$ y $\mathrm{Aut}(\mathcal{P}) \simeq G$.

Demostración. Para esta demostración, vamos a usar la notación usual para los cuaternios $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

Sea $\mathcal{P} = Q_8 \times \{0,1,2\}$ con el orden parcial $\leqslant$ definido por (para todo $x \in Q_8$):

- $(x,0) \leqslant (x,1) \leqslant (x,2)$.
- $(x,0) \leqslant (xi,1)$.
- $(x,1) \leqslant (xj,2)$.
- $(x,0) \leqslant (-x,2)$.

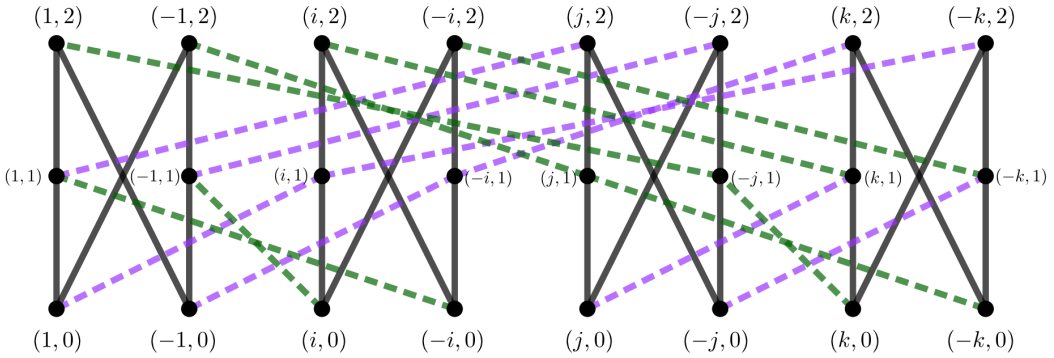

Figura 2.2: Diagrama de Hasse de un poset con grupo de automorfismos Q_8.

Podemos ver su diagrama de Hasse en la Figura 2.2.
No es difícil notar que el morfismo $L_g : Q_8 \to Q_8$ de multiplicación a izquierda por g en la primer coordenada es un automorfismo de $\mathcal{P}$ para todo $g \in Q_8$. Esto nos dice que $Q_8 \leqslant \mathrm{Aut}(\mathcal{P})$.
Para terminar, basta con ver que $\mathrm{Aut}(\mathcal{P}) \leqslant Q_8$. Para probar esto alcanza con probar que el único $\varphi \in \mathrm{Aut}(\mathcal{P})$ que cumple $\varphi(1,0) = (1,0)$ es $\varphi = \mathrm{Id}$.
En efecto, si eso se cumple y $\psi \in \mathrm{Aut}(\mathcal{P})$, como los automorfismos preservan altura, $\psi(1,0) = (g,0)$ para algún $g \in Q_8$. Luego, como $L_{g^{-1}} \circ \psi \in \mathrm{Aut}(\mathcal{P})$ y $L_{g^{-1}} \circ \psi(1,0) = (1,0)$, tenemos $L_{g^{-1}} \circ \psi = \mathrm{Id}$ y entonces $\psi = L_g$ para algún $g \in Q_8$ como queríamos.

Sea $\varphi \in \mathrm{Aut}(\mathcal{P})$ tal que $\varphi(1,0) = (1,0)$.
Los únicos puntos que cubren a $(1,0)$ son $(1,1)$, $(i,1)$ y $(-1,2)$, y como φ es automorfismo y preserva alturas, $\varphi(-1,2) = (-1,2)$. De esto podemos deducir que, si $A = \{(1,1),(i,1)\}$, $\varphi(A) = A$; y como los puntos que están cubiertos por puntos de A son $(1,0)$, $(-i,0)$ e $(i,0)$, si $B = \{(-i,0),(i,0)\}$, $\varphi(B) = B$. Pero $(i,0) \leqslant (-1,1) \leqslant (-1,2)$ y, sin embargo, $(-i,0)$ es incomparable con $(-1,2)$ ya que para que eso ocurra debería pasar alguna de las siguientes:

$$-1 = -i \qquad -1 = -(-i) \qquad -1 = -ij \qquad -1 = -i^2 \qquad -1 = -i^2j$$

pero ninguna de esas igualdades es cierta. Por lo tanto, $\varphi(i,0) = (i,0)$ y $\varphi(-i,0) = (-i,0)$. Ahora, como $(-i,0)$ está cubierto por $(1,1)$ pero no por $(i,1)$ y $\varphi(A) = A$, concluimos que $\varphi(1,1) = (1,1)$ y $\varphi(i,1) = (i,1)$. Además, los únicos puntos que cumplen que existe un punto $(x,1)$ con $x \in Q_8$ que los cubre y además $(x,1)$ cubre a $(i,0)$ son $(1,0)$, $(-1,0)$ e $(i,0)$, así que $\varphi(-1,0) = (-1,0)$.
Por otro lado, notemos que dado $x \in Q_8$ el único punto de $Q_8 \times \{2\}$ que cubre a $(x,0)$ es $(-x,0)$; así que como $(1,0)$, $(-1,0)$, $(i,0)$ y $(-i,0)$ quedan fijos por φ, deben quedar fijos también $(1,2)$, $(-1,2)$, $(i,2)$ y $(-i,2)$.

Los puntos en $Q_8 \times \{2\}$ que cubren a $(1,1)$ son $(1,2)$ y $(j,2)$; como el primero ya es punto fijo, $\varphi(j,2) = (j,2)$. Además, los puntos que cubren a $(i,1)$ son $(i,2)$ y $(k,2)$; como el primero

ya es punto fijo, $\varphi(k,2) = (k,2)$. Por otro lado, notemos que $(i,0) \leqslant (-1,1) \leqslant (-j,2)$ pero, en cambio, $(-k,2)$ es incomparable con $(i,0)$, ya que debería ocurrir alguna de las siguientes:

$$-k = i \qquad -k = -i \qquad -k = ij \qquad -k = i^2 \qquad -k = i^2j$$

pero ninguna de esas igualdades es cierta. Por lo tanto, como ya probamos que todos los puntos de $Q_8 \times \{2\}$ salvo $(-j,2)$ y $(k,2)$ quedan fijos por φ, concluimos que $\varphi(-j,2) = (-j,2)$ y $\varphi(-k,2) = (-k,2)$; o sea que todos los puntos de $Q_8 \times \{2\}$ quedan fijos por φ.

Por la propiedad antes mencionada — que para todo $x \in Q_8$ el único punto en $Q_8 \times \{2\}$ que cubre a $(x,0)$ es $(-x,2)$ — podemos afirmar que φ deja fijos todos los puntos de $Q_8 \times \{0\}$. Finalmente, como para todo $x, y \in Q_8$ se cumple que $(x,0) \leqslant (y,1) \leqslant (x,2)$ si y sólo si $x = y$, tenemos que φ deja fijos todos los puntos de $Q_8 \times \{1\}$ ■

Ahora pasamos a contar la demostración del resultado principal de este capítulo, que podemos encontrar demostrado en [Bab80].

Teorema 2.0.30 (Babai)**:** Si G es un grupo finito, existe un poset $\mathcal{P}$ con $|\mathcal{P}| \leqslant 3|G|$ y $\mathrm{Aut}(\mathcal{P}) \simeq G$.

Demostración. Si G es como en la Proposición 2.0.16, el resultado se sigue del Lema 2.0.7.
Si G es cíclico, el resultado se sigue de la Proposición 2.0.22.
Si $G = Q_8$, el resultado se sigue de la Proposición 2.0.29.
Si G es un 2−grupo abeliano elemental o bien $\mathbb{Z}_3^2$, el resultado se sigue del Lema 2.0.28.
Si G es diedral generalizado con núcleo A, con A cíclico o cumpliendo las condiciones del Lema 2.0.7, el resultado se sigue de la Proposición 2.0.23.
El único caso que queda es cuando G es diedral generalizado y su núcleo A no es cíclico ni cumple las condiciones del Lema 2.0.7. Por la Proposición 2.0.16 las condiciones del Lema 2.0.7 se dan cuando A no es cíclico ni diedral generalizado ni $\mathbb{Z}_3^2$ ni Q_8.
Como $A \neq Q_8$ por ser abeliano, resta analizar cuando A es diedral generalizado y cuando $A = \mathbb{Z}_3^2$.
Si A es diedral generalizado, como es abeliano, todos los elementos de un núcleo tienen orden 2; como los elementos fuera del núcleo también deben tener orden 2, A es un 2−grupo abeliano elemental, pero este caso ya fue resuelto.
Sólo queda ver el caso en que $A = \mathbb{Z}_3^2$, pero este caso fue resuelto en el Lema 2.0.17, como observamos en el Lema 2.0.21. Y el resultado final se sigue. ■

Capítulo 3

El menor poset con grupo de automorfismos $\mathbb{Z}_{p^k}$

En la introducción mencionamos la siguiente definición, en la que se centra todo lo que sigue en este trabajo.

Definición 3.0.1: Dado un grupo G, definimos $\beta(G)$ como el menor cardinal que puede tener un poset $\mathcal{P}$ con $\mathrm{Aut}(\mathcal{P}) \simeq G$.

El objetivo de este capítulo es calcular $\beta\left(\mathbb{Z}_{p^k}\right)$ para todo p primo y todo $k \in \mathbb{N}$.

3.1 Preliminares

A partir de este capítulo, al igual que Arlinghaus en [Arl85] con los grafos, vamos a pensar a $\mathrm{Aut}(\mathcal{P})$ embebido en el grupo $\mathbb{S}_{|\mathcal{P}|}$ de permutaciones de $|\mathcal{P}|$ elementos; ya que los automorfismos son, en particular, permutaciones en el conjunto subyacente de $\mathcal{P}$.

Observación 3.1.1: Toda permutación puede descomponerse como producto de ciclos disjuntos; por lo tanto, usualmente vamos a pensar a los automorfismos de $\mathcal{P}$ como un producto de ciclos disjuntos que permutan puntos del conjunto subyacente de $\mathcal{P}$.

Hecha esta observación, pasa a tener vital importancia la siguiente propiedad, que relaciona el orden de una permutación y el de los ciclos en su descomposición en ciclos disjuntos.

Lema 3.1.2: Dado $k \in \mathbb{N}$ y $g \in \mathbb{S}_k$, y sean $\{\alpha_i\}_{1 \leqslant i \leqslant n}$ ciclos disjuntos que cumplen $g = \alpha_1 \alpha_2 \dots \alpha_n$. Entonces,

$$|g| = \mathrm{mcm}(|\alpha_1|, |\alpha_2|, \dots, |\alpha_n|)$$

Demostración. Como las permutaciones disjuntas conmutan, sabemos que para cualquier $m \in \mathbb{N}$ se cumple

$$g^m = \alpha_1^m \alpha_2^m \dots \alpha_n^m.$$

Como $\{\alpha_i^m\}_{1 \leqslant i \leqslant n}$ sigue siendo un conjunto de permutaciones disjuntas dos a dos, si fuese $g^m = e$, debería ocurrir que $\alpha_i^m = e$ para todo $1 \leqslant i \leqslant n$; por lo que $|\alpha_i| \mid m$ para todo $1 \leqslant i \leqslant n$. Esto nos dice que $|g| \geqslant mcm(|\alpha_1|, \dots, |\alpha_n|)$, pero la desigualdad opuesta es inmediata, y eso concluye la demostración. ■

Recordar que, como los automorfismos de posets preservan el orden, en particular deben preservar alturas. Esto nos ayuda a probar el siguiente resultado.

Lema 3.1.3: Dado un poset $\mathcal{P}$ y $g \in \mathrm{Aut}(\mathcal{P})$, todos los puntos de $\mathcal{P}$ que pertenezcan a una misma órbita de la acción de $\langle g \rangle$ en $\mathcal{P}$ deben formar una anticadena.

Demostración. Si no fuese así, habría dos puntos en la misma órbita de $\langle g \rangle$ que son comparables y, por lo tanto, tendrían alturas distintas; pero esto no puede ocurrir ya que los automorfismos de posets preservan altura. ■

Por último, introducimos la siguiente notación, que no debe confundirse con la definición de órbita.

Notación 3.1.4: Dado un conjunto C y una permutación g de los elementos de C, denotamos $\mathcal{O}_g := \{x \in C : g \cdot x \neq x\}$ al complemento de los puntos fijos de g.

Para ilustrar el principio de las ideas que iremos usando, empezaremos calculando $\beta(\mathbb{Z}_3)$.

3.2 El caso $\mathbb{Z}_3$

Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_3 \simeq \langle g \rangle$. Notemos que, en virtud del Lema 3.1.2, todos los ciclos contenidos en la descomposición en ciclos disjuntos de g tienen longitud múltiplo de 3, y g contiene al menos un ciclo no trivial, dado que $|g| = 3$.

Notación 3.2.1: Denotamos $\mathcal{P}_{<x}$ (respectivamente $\mathcal{P}_{>x}$) al poset inducido por los elementos de $\mathcal{P}$ que son menores (respectivamente mayores) que x.

Supongamos por un momento que g es un ciclo. En ese caso, por el Lema 3.1.3, todos los puntos que no deja fijos g deberán formar una anticadena; luego, si g no deja fijo x,

$\mathcal{P}_{<x} = \mathcal{P}_{<gx}$ y $\mathcal{P}_{>x} = \mathcal{P}_{>gx}$. Esto implica que existe un automorfismo de $\mathcal{P}$ que consiste en intercambiar a x y gx y dejar a todos los demás puntos fijos; un claro absurdo, dado que no coincide con g^i para ningún $i \in \mathbb{N}$ por ser g un ciclo con longitud 3.

Concluimos que g debe contener al menos dos ciclos con longitud múltiplo de 3. Ahora, supongamos por un momento que g contiene exactamente dos 3−ciclos y deja fijos todos los puntos de $\mathcal{P}$ que no pertenecen a esos 3−ciclos; etiquetamos $g = (1\ 2\ 3)(1'\ 2'\ 3')$ de modo que, si 1 está relacionado con alguno de $\{1', 2', 3'\}$, 1 está relacionado con $1'$.

En ese caso, el subposet $\mathcal{Q}$ inducido por los puntos de estos dos 3−ciclos queda determinado por los puntos que cubren al 1 (o que están cubiertos por el 1), ya que todas las demás relaciones se deducen de aplicar sucesivas veces g en $\mathcal{P}$, que debe preservar el orden. Suponemos sin pérdida de la generalidad que 1 no cubre a $1'$ ni $2'$ ni $3'$. Separando en casos, según qué puntos cubren al 1, vemos que $\mathcal{Q}$ debe ser isomorfo a alguno de los posets que se pueden observar en la Figura 3.1.

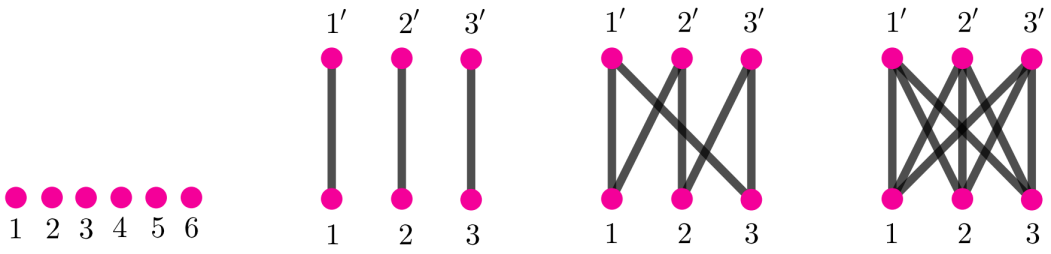

Figura 3.1: Posibles subposets, salvo isomorfismo, inducidos por dos 3−ciclos de $\mathcal{P}$.

Como la acción de $\langle g \rangle$ restringida a cada ciclo es transitiva, vale

$$\mathcal{P}_{<x} - \{1,2,3\} = \mathcal{P}_{<y} - \{1,2,3\} \quad \text{y} \quad \mathcal{P}_{>x} - \{1,2,3\} = \mathcal{P}_{>y} - \{1,2,3\}$$

para todo $x, y \in \{1', 2', 3'\}$ y también

$$\mathcal{P}_{<x} - \{1',2',3'\} = \mathcal{P}_{<y} - \{1',2',3'\} \quad \text{y} \quad \mathcal{P}_{>x} - \{1',2',3'\} = \mathcal{P}_{>y} - \{1',2',3'\}$$

para todo $x, y \in \{1, 2, 3\}$. En particular, cualquier automorfismo de $\mathcal{Q}$ puede extenderse a un automorfismo de $\mathcal{P}$ vía la identidad — es decir, dejando fijos todos los puntos de $\mathcal{P}$ que no estén en $\mathcal{Q}$.

En el primer y cuarto caso, la trasposición $(1\ 2)$ sería un automorfismo de $\mathcal{P}$; absurdo, pues no coincide con g^i para ningún $i \in \mathbb{N}$.

En el segundo caso, la permutación $(1\ 2)(1'\ 2')$ sería un automorfismo de $\mathcal{P}$; absurdo, pues no coincide con g^i para ningún $i \in \mathbb{N}$.

En el tercer caso, la permutación $(1\ 2)(1'\ 3')$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_3$ tiene orden 3, que no es divisible por 2, llegamos a un absurdo.

Habiendo agotado todos los casos, concluimos que, o bien g contiene al menos tres ciclos (con longitud divisible por 3), o bien contiene dos ciclos con longitud divisible por 3 y alguno de ellos es de longitud $3m$ con $m \geqslant 2$. En cualquiera de los dos casos llegamos a que $|\mathcal{P}| \geqslant 9$.

Resta encontrar un ejemplo de un poset $\mathcal{P}_3$ con $|\mathcal{P}_3| = 9$ y $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_3$. Proponemos, respetando la notación del capítulo anterior, $\mathcal{P}_3 = \mathcal{P}(\mathbb{Z}_3, \{1\})$; es decir:

- $\mathcal{P}_3 = \{1,2,3\} \times \{0,1,2\}$.
- $(i,0) \leqslant (i,1)$, $(i,1) \leqslant (i,2)$ e $(i,0) \leqslant (i,2)$ para todo $1 \leqslant i \leqslant n$.
- $(i,0) \leqslant (i+1,2)$ para todo $1 \leqslant i \leqslant n$ (mirando módulo n).

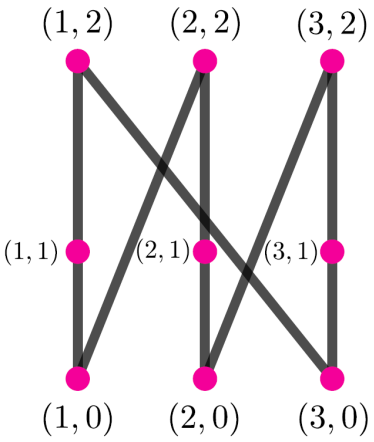

Figura 3.2: Diagrama de Hasse de $\mathcal{P}_3$.

Afirmación 3.2.2: $\mathrm{Aut}(\mathcal{P}_3) \simeq \mathbb{Z}_3$.

Demostración. En primer lugar, notemos que $\mathrm{Aut}(\mathcal{P}_3)$ contiene un subgrupo isomorfo a $\mathbb{Z}_3$, ya que el subgrupo generado por (mirando la primer coordenada módulo n)

$$\begin{aligned} \Phi : \quad \mathcal{P} &\to \mathcal{P} \\ (i,k) &\mapsto (i+1,k) \quad \forall\, k \in \{0,1,2\},\ \forall\, i \in \{1,2,3\} \end{aligned}$$

es isomorfo a $\mathbb{Z}_3$ y es un subgrupo de $\mathrm{Aut}(\mathcal{P}_3)$.
Para terminar, basta con ver que $\mathrm{Aut}(\mathcal{P}_3)$ tiene a lo sumo tres elementos. Para probar esto alcanza con probar que el único $\varphi \in \mathrm{Aut}(\mathcal{P}_3)$ que cumple $\varphi(1,0) = (1,0)$ es $\varphi = \mathrm{Id}$.

En efecto, si eso se cumple y $\psi \in \mathrm{Aut}(\mathcal{P}_3)$, como los automorfismos preservan altura, $\psi(1,0) = (k,0)$ para algún $h \in \mathbb{Z}_3$. Luego, como $L_{h^{-1}} \circ \psi \in \mathrm{Aut}(\mathcal{P}_3)$ y $L_{h^{-1}} \circ \psi(1,0) = (1,0)$, tenemos $L_{h^{-1}} \circ \psi = \mathrm{Id}$ y entonces $\psi = L_h$ para algún $h \in \mathbb{Z}_3$; probando así que hay a lo sumo 3 automorfismos de $\mathcal{P}_3$ y, por lo tanto, $\mathrm{Aut}(\mathcal{P}_3) \simeq \mathbb{Z}_3$ como queríamos.

Si $(1,0)$ queda fijo al aplicar algún $\varphi \in \mathrm{Aut}(\mathcal{P}_3)$, entonces $(1,1)$ queda fijo por ser el único punto de altura 1 que lo cubre; y de la misma forma $(1,2)$ queda fijo por ser el único que cubre a $(1,1)$. Como $(1,2)$ es el único punto distinto de $(1,1)$ que está cubierto por $(2,1)$, también queda fijo. Repitiendo este razonamiento, podemos ver que cada vez que $(i,0)$ queda fijo, también quedan fijos $(i,1), (i,2)$ y $(i+1,0)$; inductivamente, llegamos a que todos los puntos de $\mathcal{P}_3$ quedan fijos. Luego, $\mathrm{Aut}(\mathcal{P}_3) \simeq \mathbb{Z}_3$ como queríamos. ∎

Concluimos que $\beta(\mathbb{Z}_3) = 9$, e inspirados por estas ideas, en las próximas secciones trabajaremos con otros casos chicos, empezando por $\mathbb{Z}_5$ y $\mathbb{Z}_7$ que resultarán similares al de recién.

La definición del poset $\mathcal{P}_3$ también puede generalizarse, tomando $\mathcal{P}_n = \mathcal{P}(\mathbb{Z}_n, \{1\})$ encontramos un poset $\mathcal{P}_n$ con $3n$ puntos y $\mathrm{Aut}(\mathcal{P}_n) \simeq \mathbb{Z}_n$, explícitamente es:

- $\mathcal{P}_n = \{1,2,\dots,n\} \times \{0,1,2\}$.
- $(i,0) \leqslant (i,1)$, $(i,1) \leqslant (i,2)$ e $(i,0) \leqslant (i,2)$ para todo $1 \leqslant i \leqslant n$.
- $(i,0) \leqslant (i+1,2)$ para todo $1 \leqslant i \leqslant n$ (mirando módulo n).

La demostración de que este poset tiene grupo de automorfismos isomorfo a $\mathbb{Z}_n$ es exactamente la misma que para $n = 3$. En particular, esto prueba el resultado de Babai.

Proposición 2.0.22: Si $G \simeq \mathbb{Z}_n \simeq \langle g \rangle$ para algún $n \in \mathbb{N}$ y $g \in G$, entonces si $L = \{g\}$ tenemos $\mathrm{Aut}(\mathcal{P}(G,L)) \simeq G$.

Por otro lado, la idea que usamos para probar que g contenía al menos dos ciclos con longitud múltiplo de 3 también puede generalizarse.

Notación 3.2.3: Dados $n \in \mathbb{Z}$, $k \in \mathbb{N}$ y un primo p decimos que $p^k \parallel n$ si $p^k \mid n$ y $p^{k+1} \nmid n$.

Lema 3.2.4: Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n \simeq \langle g \rangle$ y sea p un primo tal que $p^k \parallel n$ para algún $k \in \mathbb{N}$ y $p^k \neq 2$, entonces g contiene al menos dos ciclos de longitud divisible por p^k.

Demostración. Supongamos, a modo de contradicción, que g contiene exactamente un ciclo α de longitud divisible por p^k. En ese caso, como las longitudes de todos los demás ciclos son divisores de n que no son divisibles por p^k, $\frac{n}{p}$ será múltiplo de todas esas longitudes. Por lo tanto, la acción de $\langle g^{\frac{n}{p}} \rangle$ deja fijos todos los puntos de $\mathcal{P}$, excepto los de α.
Esto último implica que, dado $x \in \mathcal{O}_\alpha$, se cumple que $\mathcal{P}_{<x} = \mathcal{P}_{<g^{\frac{n}{p}}x}$ y que $\mathcal{P}_{>x} = \mathcal{P}_{>g^{\frac{n}{p}}x}$.
Concluimos que existe una trasposición $\tau \in \mathrm{Aut}(\mathcal{P})$ que intercambia dos puntos, x y $g^{\frac{n}{p}}x$ y deja todos los demás puntos de $\mathcal{P}$ fijos. Esto no puede ocurrir, ya que $\tau = g^i$ para algún $i \in \mathbb{N}$ y entonces, como $g^i x = \alpha^i x = gx \neq x$, $|\alpha| \nmid i$, así que g^i contiene al menos p^k (en particular mayor a 2) puntos no fijos, un claro absurdo. ■

Este resultado nos provee el siguiente corolario.

Corolario 3.2.5: Si $\mathcal{P}$ es un poset con grupo de automorfismos $\mathrm{Aut}(\mathcal{P}) = \mathbb{Z}_{p^k}$ para algún p primo y $k \in \mathbb{N}$ con $p^k \neq 2$, entonces $|\mathcal{P}| \geqslant 2p^k$.

Antes de seguir, necesitamos hacer una definición auxiliar que nos ayudará a reducir la cantidad de casos a analizar en las próximas demostraciones.

Definición 3.2.6: Sea $\mathcal{P}$ un poset de altura 1 y llamamos A al conjunto de puntos maximales de $\mathcal{P}$ y B al conjunto de puntos minimales de $\mathcal{P}$.

Definimos como el *poset complementario* de $\mathcal{P}$ al poset $\overline{\mathcal{P}}$ que consiste de los mismos puntos que $\mathcal{P}$ y, además, para todo x en A e y en B cumple

$$x > y \text{ en } \overline{\mathcal{P}} \iff x \text{ es incomparable con } y \text{ en } \mathcal{P}$$

Notemos que, en la definición anterior, las únicas relaciones posibles entre puntos del poset $\mathcal{P}$ ocurren cuando un punto en A es mayor a un punto en B. Por esto, podemos ver la relación $>$ como aristas de un grafo bipartito con partes A y B.

Es importante observar que se cumple

$$\mathrm{Aut}\left(\mathcal{P}\right) = \mathrm{Aut}\left(\overline{\mathcal{P}}\right).$$

Estos grupos son iguales conjuntísticamente, ya que todo automorfismo de $\mathcal{P}$ preserva aristas de $\overline{\mathcal{P}}$ por preservar no-aristas de $\mathcal{P}$. Análogamente, preserva no-aristas de $\overline{\mathcal{P}}$ por preservar aristas de $\mathcal{P}$.

3.3 El caso $\mathbb{Z}_5$

Sea $\mathcal{P}$ un poset $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_5 \simeq \langle g \rangle$. Por el Corolario 3.2.5, sabemos que $|\mathcal{P}| \geqslant 10$ y que tiene al menos dos ciclos de longitud múltiplo de 5.
Ahora, supongamos que g contiene exactamente dos 5−ciclos y deja fijos todos los puntos de $\mathcal{P}$ que no pertenecen a esos 5−ciclos. Etiquetamos $g = (1\,2\,3\,4\,5)(1'\,2'\,3'\,4'\,5')$ de modo que, si 1 está relacionado con alguno de $\{1', 2', 3', 4', 5'\}$, 1 está relacionado con $1'$.

En ese caso, el subposet $\mathcal{Q}$ inducido por los puntos de estos dos 5−ciclos queda determinado por los puntos que cubren al 1 (o que están cubiertos por el 1), ya que todas las demás relaciones se deducen de aplicar sucesivas veces g en $\mathcal{P}$, que debe preservar el orden.

Suponemos sin pérdida de la generalidad que 1 no cubre a $1', 2', 3', 4'$ ni $5'$. Separando en casos, según qué puntos cubren al 1, vemos que $\mathcal{Q}$ debe ser isomorfo a — o isomorfo al complementario de — alguno de los que se pueden observar en la Figura 3.3 (los colores están sólo para una mejor lectura del poset). Con un razonamiento análogo al hecho en el caso $\mathbb{Z}_3$, podemos notar que cualquier automorfismo de $\mathcal{Q}$ puede extenderse a un automorfismo de $\mathcal{P}$ vía la identidad.

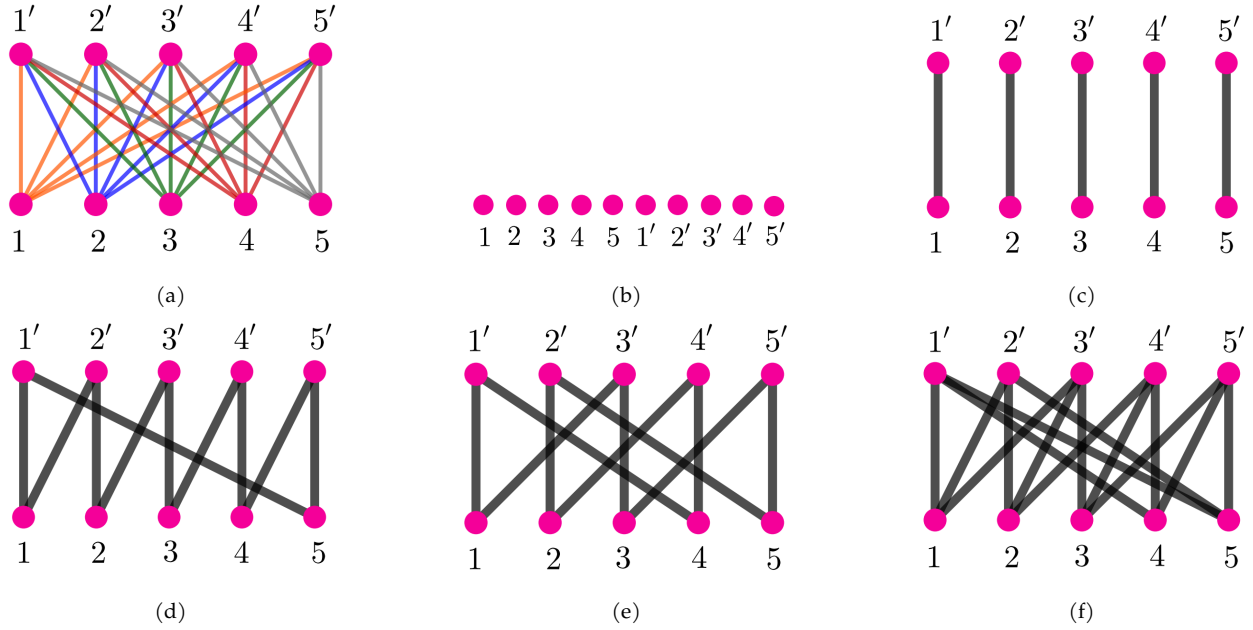

Figura 3.3: Posibles subposets, salvo isomorfismo y complemento, inducidos por dos 5−ciclos de $\mathcal{P}$.

En los casos (a) y (b), la trasposición $(1\,2)$ sería un automorfismo de $\mathcal{P}$; absurdo, pues no coincide con g^i para ningún $i \in \mathbb{N}$.

En el caso (c), la permutación $(1\,2)(1'\,2')$ sería un automorfismo de $\mathcal{P}$; absurdo, pues no coincide con g^i para ningún $i \in \mathbb{N}$.

En el caso (d), la permutación $(2'\ 5')(3'\ 4')(1\ 5)(2\ 4)$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_5$ tiene orden 5, que no es divisible por 2, llegamos a un absurdo. Además, como el poset del caso (e) es isomorfo, este argumento también lo descarta.

En el caso (f), la permutación $(3'\ 5')(1'\ 2')(2\ 4)(1\ 5)$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_5$ tiene orden 5, que no es divisible por 2, llegamos a un absurdo.

Habiendo agotado todos los casos, concluimos que, o bien g contiene al menos tres ciclos (con longitud divisible por 5), o bien contiene dos ciclos con longitud divisible por 5 y alguno de ellos es de longitud $5m$ con $m \geqslant 2$. En cualquiera de los dos casos llegamos a que $|\mathcal{P}| \geqslant 15$ y, por el Teorema 2.0.30, $\beta(\mathbb{Z}_5) = 15$.

3.4 El caso $\mathbb{Z}_7$

Sea $\mathcal{P}$ un poset $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_7 \simeq \langle g \rangle$. Por el Corolario 3.2.5, sabemos que $|\mathcal{P}| \geqslant 14$ y que tiene al menos dos ciclos de longitud múltiplo de 7. Ahora, supongamos por un momento que g contiene exactamente dos $7-$ciclos y deja fijos todos los puntos de $\mathcal{P}$ que no pertenecen a esos $7-$ciclos. Etiquetamos $g = (1\ 2\ 3\ 4\ 5\ 6\ 7)(1'\ 2'\ 3'\ 4'\ 5'\ 6'\ 7')$ de modo que, si 1 está relacionado con alguno de $\{1', 2', 3', 4', 5', 6', 7'\}$, 1 está relacionado con $1'$.

En ese caso, $\mathcal{P}$ deberá contener un subposet $\mathcal{Q}$ isomorfo a — o isomorfo al complementario de — alguno de los que se pueden observar en la Figura 3.4 (los colores están sólo para una mejor lectura de los posets). Con un razonamiento análogo al hecho en el caso $\mathbb{Z}_3$, podemos notar que cualquier automorfismo de $\mathcal{Q}$ puede extenderse a un automorfismo de $\mathcal{P}$ vía la identidad.

En los casos (a) y (b), la trasposición $(1\ 2)$ sería un automorfismo de $\mathcal{P}$; absurdo, pues no coincide con g^i para ningún $i \in \mathbb{N}$.

En el caso (c), la permutación $(1\ 2)(1'\ 2')$ sería un automorfismo de $\mathcal{P}$; absurdo, pues no coincide con g^i para ningún $i \in \mathbb{N}$.

En el caso (d), la permutación $(4'\ 6')(1'\ 2')(3'\ 7')(2\ 7)(6\ 3)(4\ 5)$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_7$ tiene orden 7, que no es divisible por 2, llegamos a un absurdo.

En el caso (e), la permutación $(1'\ 3')(6'\ 5')(4'\ 7')(4\ 5)(2\ 7)(3\ 6)$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_7$ tiene orden 7, que no es divisible por 2, llegamos a un absurdo.
Los posets de los casos (f) y (g) son isomorfos a este, así que este argumento también los descarta.

En el caso (h), la permutación $(1'\ 7')(3'\ 5')(2'\ 6')(1\ 6)(3\ 4)(2\ 5)$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_7$ tiene orden 7, que no es divisible por 2, llegamos a un absurdo.

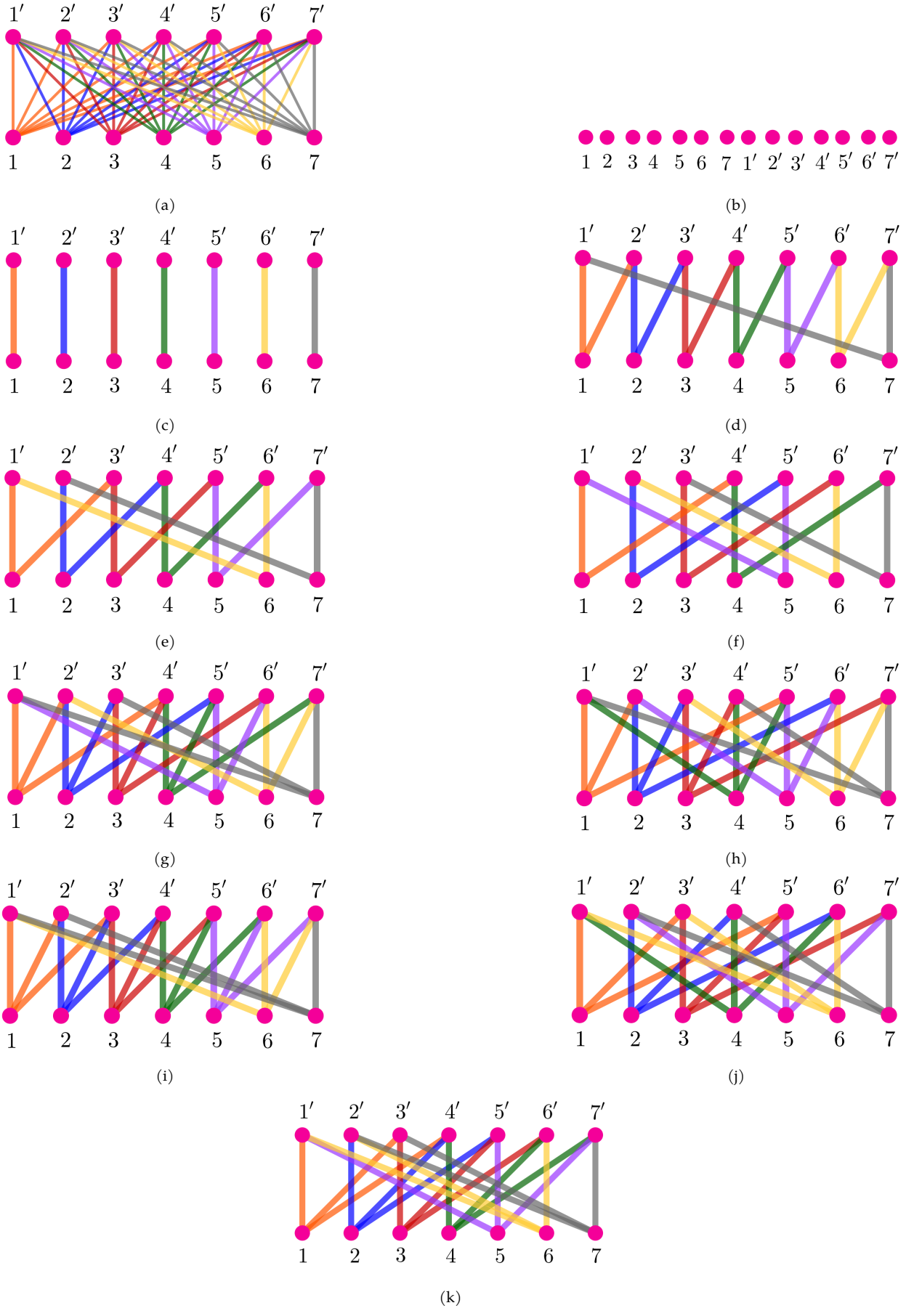

Figura 3.4: Posibles subposets, salvo isomorfismo y complemento, inducidos por dos 7−ciclos de $\mathcal{P}$.

En el caso (i), la permutación $(1'\ 6')(2'\ 5')(3'\ 4')(1\ 4)(5\ 7)(3\ 2)$ es un automorfismo de $\mathcal{P}$ de orden 2. Como $\mathbb{Z}_7$ tiene orden 7, que no es divisible por 2, llegamos a un absurdo.
El poset del caso (j) es isomorfo, así que este argumento también lo descarta.

En el caso (k), la permutación $(6\ 7)(3\ 5)(6'\ 7')(7'\ 9')$ es un automorfismo de $\mathcal{P}$ de orden 2, así que también llegamos a un absurdo.

Habiendo agotado todos los casos, concluimos que, o bien g contiene al menos tres ciclos (con longitud divisible por 7), o bien contiene dos ciclos con longitud divisible por 7 y alguno de ellos es de longitud $7m$ con $m \geqslant 2$. En cualquiera de los dos casos llegamos a que $|\mathcal{P}| \geqslant 21$ y, por el Teorema 2.0.30, $\beta(\mathbb{Z}_7) = 21$.

3.5 El caso $\mathbb{Z}_{p^k}$ con $p^k \geqslant 8$

Vamos a empezar exhibiendo una familia de ejemplos, cuya minimalidad probaremos luego, de posets con grupo de automorfismos $\mathbb{Z}_{p^k}$ para todo $p^k \geqslant 8$ con p primo y $k \in \mathbb{N}$. Definimos $\mathcal{Q}_n$ para cada $n \geqslant 8$ de la siguiente manera:

- El conjunto subyacente de $\mathcal{Q}_n$ es $\{1, \dots, n\} \cup \{1', \dots, n'\}$.
- Si $S = \{0, 2, 3, 4\}$, $i \leqslant (i+s)'$ para todo $s \in S$ e $1 \leqslant i \leqslant n$ (mirando módulo n).

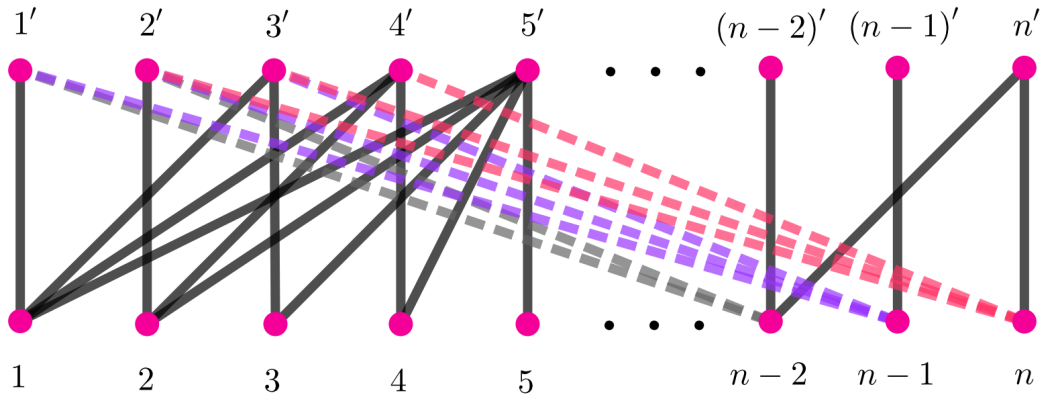

Figura 3.5: Diagrama de Hasse de $\mathcal{Q}_n$

El hecho de que $n \geqslant 8$ se usará principalmente para que valga que, dado $1 \leqslant k \leqslant n$, las etiquetas $k-3, k-2, k-1, k, k+1, k+2, k+3, k+4$ vistas módulo n sean todas distintas; cuando esto no sucede hay más parejas de puntos que se relacionan con un mismo punto, haciendo que no existan ciertos invariantes que son cruciales para la demostración.
Antes de probar que este poset tiene grupo de automorfismos isomorfo a $\mathbb{Z}_n$, necesitamos probar algunos lemas que nos dan información sobre su estructura.

Lema 3.5.1: Sea $\mathcal{Q}_n$ el poset recién definido e $i, j \in \{1, \ldots, n\}$ distintos.

(a) Existen dos puntos distintos $a', b' \in \{1', \ldots, n'\}$ que son ambos mayores a i y a j si y sólo si $i - j \equiv -2, -1, 1$ o $2 \pmod{n}$.

(b) Existen dos puntos distintos $a, b \in \{1, \ldots, n\}$ que son ambos menores a i' y a j' si y sólo si $i - j \equiv -2, -1, 1$ o $2 \pmod{n}$.

Demostración. Probamos cada parte por separado.

(a) Los puntos que cubren a i son $i', (i+2)', (i+3)'$ e $(i+4)'$, y los puntos que cubren a j son $j', (j+2)', (j+3)'$ y $(j+4)'$. Como $i \neq j$, las únicas cuatro situaciones en las que pueden existir dos puntos $a', b' \in \{1', \ldots, n'\}$ que cubren a i y j a la vez son cuando $i = j+1, i = j-2, i = j-1$ e $i = j+2$; y esto es exactamente el resultado deseado.

Para la recíproca, dado $j \in \{1, \ldots, n\}$, basta notar que j y $j+1$ están cubiertos por $(j+3)'$ y $(j+4)'$, que $j-2$ y j están cubiertos por j' y $(j+2)'$, que $j-1$ y j están cubiertos por $(j+2)'$ y $(j+3)'$ y que $j+2$ y j están cubiertos por $(j+2)'$ y $(j+4)'$.

(b) La demostración de este inciso es simétrica a la del inciso anterior.

■

Definición 3.5.2: Sea $\mathcal{Q}_n$ el poset antes definido.
Vamos a decir que dos puntos $i', j' \in \mathcal{Q}_n$ con $i, j \in \{1, \ldots, n\}$ distintos son *amigos superiores* si cumplen la condición de la parte (a) del Lema 3.5.1.

Análogamente, diremos que dos puntos $i, j \in \mathcal{Q}_n$ con $i, j \in \{1, \ldots, n\}$ distintos son *amigos inferiores* si cumplen la condición de la parte (b) del Lema 3.5.1.

Observación 3.5.3: Si dos puntos $a', b' \in \mathcal{Q}_n$ (respectivamente $a, b \in \mathcal{Q}_n$) son amigos superiores (respectivamente inferiores) y $\varphi \in \mathrm{Aut}(\mathcal{Q}_n)$, entonces $\varphi(a')$ y $\varphi(b')$ son amigos superiores (respectivamente $\varphi(a)$ y $\varphi(b)$ son amigos inferiores).

Lema 3.5.4: Sea $\mathcal{Q}_n$ el poset recién definido y sea $\varphi \in \mathrm{Aut}(\mathcal{Q}_n)$ un automorfismo que cumple $\varphi(k) = k$ para algún $k \in \{1, \ldots, n\}$. Entonces $\varphi(k-1) = k-1$ y $\varphi(k') = k'$.

Demostración. Como $\varphi(k) = k$, sabemos que el conjunto de puntos que cubren a k es invariante por φ, es decir, $\varphi(H) = H$ con $H = \{k', (k+2)', (k+3)', (k+4)'\}$.

Como k' es el único punto de H que es amigo superior de un sólo punto de H, debe suceder que $\varphi(k') = k'$. Además, como $(k+2)'$ es el único punto de H que es amigo superior de tres puntos de H, $\varphi((k+2)') = ((k+2)')$.
Simétricamente, como $\varphi(k') = k'$, podemos ver que $\varphi(k-2) = k-2$.
Por último, notemos que $k-1$ es el único punto que es amigo inferior de k y de $k-2$ a la vez; por lo tanto, como k y $k-2$ son puntos fijos de φ, es $\varphi(k-1) = k-1$; y el resultado sigue. ■

Ahora, queremos probar el resultado central de esta sección.

Proposición 3.5.5: Para todo $n = p^k \geqslant 8$ con p primo, el poset $\mathcal{Q}_n$ definido anteriormente tiene grupo de automorfismo $\mathrm{Aut}(\mathcal{Q}_n) \simeq \mathbb{Z}_n$.

Demostración. En primer lugar notemos que $\mathrm{Aut}(\mathcal{Q}_n)$ tiene un subgrupo isomorfo a $\mathbb{Z}_n$, para esto basta con notar que el subgrupo de $\mathbb{S}_{2n}$ generado por la composición de $n-$ciclos $(1\,2\,\ldots\,n)(1'\,2'\,\ldots\,n')$ es un subgrupo del grupo de automorfismos de $\mathcal{Q}_n$.

Para terminar, basta con ver que $\mathrm{Aut}(\mathcal{Q}_n)$ tiene a lo sumo n elementos. Para probar esto — usando la misma idea que en la demostración de que $\mathrm{Aut}(\mathcal{P}_3) \simeq \mathbb{Z}_3$ — alcanza con probar que el único $\varphi \in \mathrm{Aut}(\mathcal{Q}_n)$ que cumple $\varphi(1) = 1$ es $\varphi = \mathrm{Id}$.

Sea φ un automorfismo con $\varphi(1) = 1$. Por el Lema 3.5.4, si algún $k \in \mathcal{Q}_n$ es punto fijo de φ, tanto k' como $k+1$ son puntos fijos de φ; por lo que inductivamente obtenemos el resultado deseado. ■

Notar que, por el Corolario 3.2.5, el resultado anterior nos dice que $\beta(\mathbb{Z}_{p^k}) = 2p^k$ para todo $p^k \geqslant 8$ con p primo y $k \in \mathbb{N}$.

Como conclusión de este capítulo, notar que logramos probar la mayor parte del siguiente teorema.

Teorema 3.5.6: Dado p primo y $k \in \mathbb{N}$,

$$\beta(\mathbb{Z}_{p^k}) = \begin{cases} 2 & \text{si } p^k = 2 \\ 3p^k & \text{si } p^k = 3,4,5,7 \\ 2p^k & \text{si } p^k \geqslant 8 \end{cases}$$

Observando que un poset con exactamente 2 puntos incomparables tiene grupo de automorfismos $\mathbb{Z}_2$, notamos que sólo nos falta probar que $\beta(\mathbb{Z}_4) = 12$ para completar la demostración del teorema. Eso lo probaremos en el siguiente capítulo, haciendo uso del Lema 4.1.3.

Capítulo 4

El caso cíclico

El objetivo de este capítulo es calcular $\beta(\mathbb{Z}_n)$ para todo $n \in \mathbb{N}$; el resultado análogo al Teorema 1.0.2 (Teorema de Meriwether, parte II).

4.1 Preliminares

Lo primero que haremos es probar el siguiente resultado:

Lema 4.1.1: Dado un poset $\mathcal{P}$ con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n$ y $n = p_1^{a_1} \cdots p_r^{a_r}$ donde los p_i son primos distintos y $p_i^{a_i} \neq 2$ para todo $1 \leqslant i \leqslant r$, se cumple que:

$$|\mathcal{P}| \geqslant \sum_{i=1}^{r} 2p_i^{a_i}.$$

Si, en cambio, $n = 2 \cdot p_2^{a_2} \cdots p_r^{a_r}$ con $p_i \neq 2$ primos distintos, tenemos:

$$|\mathcal{P}| \geqslant 2 + \sum_{i=2}^{r} 2p_i^{a_i}.$$

Para hacer más amena la demostración, necesitamos probar dos resultados preliminares.

Lema 4.1.2: Sean $x_1, x_2, \ldots, x_n \in \mathbb{N}$ tales que $x_i \geqslant 2$ para todo $1 \leqslant i \leqslant n$. Entonces,

$$x_1 x_2 \cdots x_n \geqslant x_1 + x_2 + \ldots + x_n.$$

Demostración. Vamos a probarlo por inducción en n.
Caso base $n = 2$**:** Dados $a, b \in \mathbb{N}$ con $a, b \geqslant 2$, tenemos que $(a-1)(b-1) \geqslant 1$. Desarrollando y despejando obtenemos $ab \geqslant a + b$; tomando $a = x_1$ y $b = x_2$ probamos el resultado deseado.

Paso inductivo: Supongamos que $x_1x_2\cdots x_{n-1} \geqslant x_1 + x_2 + \cdots + x_{n-1}$. Tomando $a = x_1x_2\cdots x_{n-1}$ y $b = x_n$ en el caso base, tenemos que $ab \geqslant a + x_n \geqslant x_1 + x_2 + \cdots + x_{n+1} + x_n$, como queríamos. ■

Desigualdad fundamental: Sean $a_1, \ldots, a_n$ números naturales. Definimos además el conjunto

$$D = \{p^r : p \text{ primo}, p^r \parallel a_j \text{ para algún } 1 \leqslant j \leqslant n \text{ y } r \in \mathbb{N}\}$$

y numeramos sus elementos como $d_1, d_2, \ldots, d_m$ con $m = |D|$. Si para cada $1 \leqslant i \leqslant m$, k_i es la cantidad de índices $1 \leqslant j \leqslant n$ tales que $d_i \parallel a_j$, entonces:

$$a_1 + a_2 + \cdots + a_n \geqslant k_1d_1 + \cdots k_md_m.$$

Demostración. Empezamos tomando un índice fijo $1 \leqslant j \leqslant n$, y factorizamos a_j en primos:

$$a_j = p_1^{r_1} \cdots p_s^{r_s}.$$

Dicho esto, como $p_i^{r_i} \geqslant 2$ para todo $1 \leqslant i \leqslant s$, por el Lema 4.1.2 tenemos:

$$a_j = p_1^{r_1} \cdots p_s^{r_s} \geqslant p_1^{r_1} + \cdots + p_s^{r_s}.$$

Ahora, usamos esta desigualdad para cada a_j con $1 \leqslant j \leqslant n$, y la suma del enunciado nos queda mayor o igual a una suma de términos entre los cuáles hay, para cada $1 \leqslant i \leqslant m$, k_i términos que valen d_i — uno por cada a_j tal que $d_i \parallel a_j$. Se sigue el resultado deseado. ■

Estamos en condiciones de probar el Lema 4.1.1.

Demostración. Sea $g \in \mathrm{Aut}(\mathcal{P})$ con $|g| = n$ tal que $\mathrm{Aut}(\mathcal{P}) \simeq \langle g \rangle$. Sabemos que g contiene — en su descomposición en ciclos disjuntos — al menos un ciclo α_i de longitud divisible por $p_i^{a_i}$, ya que $p_i^{a_i} \mid |g|$ y $|g|$ es el mcm de las longitudes de los ciclos que contiene.

Por el Lema 3.2.4, para cada $1 \leqslant i \leqslant r$, si $p_i^{a_i} \mid n$ y $p^{a_i} \neq 2$ deben existir al menos dos ciclos contenidos en g de longitud divisible por $p_i^{a_i}$.

Veamos que esto prueba la primer parte del lema: sean $l_1, l_2, \cdots, l_s$ las longitudes de los s ciclos contenidos en g. Por la desigualdad fundamental, sabemos que

$$l_1 + l_2 + \cdots + l_s \geqslant k_1d_1 + \cdots k_md_m$$

donde para cada $1 \leqslant i \leqslant m$, k_i y d_i se definen como en el enunciado de la desigualdad. Pero además, usando el Lema 3.2.4, sabemos que $k_i \geqslant 2$ para cada $1 \leqslant i \leqslant m$ tal que $d_i = p_j^{a_j}$ para algún $1 \leqslant j \leqslant n$, probando el resultado deseado.

Para la segunda parte, cuando $n = 2 \cdot p_2^{a_2} \cdots p_r^{a_r}$, razonamos de la misma forma para cada $2 \leqslant i \leqslant r$, y observamos que además debe haber al menos un ciclo de longitud par. Esto nos dice que algún d_i debe ser una potencia de 2, o sea que $k_i \geqslant 1$ para algún $1 \leqslant i \leqslant m$ tal que d_i es par. Por lo tanto $|\mathcal{P}| \geqslant 2 + 2p_2^{a_2} + \cdots + 2p_r^{a_r}$, como queríamos. ■

Para lo que sigue vamos a necesitar algunos lemas.

Lema 4.1.3: Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n \simeq \langle g \rangle$ y $8 \nmid n$, donde g contiene exactamente dos 4−ciclos en su descomposición en ciclos disjuntos.
Si g contiene un $2m$−ciclo con $m \in \mathbb{N}$ impar, entonces existe al menos otro ciclo η contenido en g de longitud $2s$ con $s \in \mathbb{N}$ impar.

Demostración. Llamemos α y β a los 4−ciclos y supongamos a modo de contradicción que existe sólo un $2m$−ciclo con m impar en g, que llamaremos γ. La acción de $g^{\frac{n}{4}}$ en $\mathcal{P}$ deja fijos todos los puntos de $\mathcal{P}$ excepto los de α, β y γ. Además $(g^{\frac{n}{4}})^2$ deja fijos todos los puntos de $\mathcal{P}$ excepto los de α y β. Más aún, si $\alpha = (1\,2\,3\,4)$ y $\beta = (1'\,2'\,3'\,4')$:

$$g^{\frac{n}{4}} = (1\,2\,3\,4)^{\frac{n}{4}}(1'\,2'\,3'\,4')^{\frac{n}{4}}(\gamma)^{\frac{n}{4}}$$

$$(g^{\frac{n}{4}})^2 = g^{\frac{n}{2}} = (1\,2\,3\,4)^{\frac{n}{2}}(1'\,2'\,3'\,4')^{\frac{n}{2}}$$

Sabiendo que $\dfrac{n}{4}$ es coprimo con 4, tenemos que $(1\,2\,3\,4)^{\frac{n}{4}}$ puede ser igual a:

$$(1\,2\,3\,4) \text{ o } (1\,2\,3\,4)^3.$$

Análogamente, $(1'\,2'\,3'\,4')^{\frac{n}{4}}$ puede ser igual a:

$$(1'\,2'\,3'\,4') \text{ o } (1'\,2'\,3'\,4')^3$$

En cualquiera de los casos, dos de las órbitas de la acción de $\left\langle g^{\frac{n}{4}} \right\rangle$ son:

$$\{1,2,3,4\} \text{ y } \{1',2',3',4'\}.$$

Esto último nos dice que

$$\mathcal{P}_{<x} - (\mathcal{O}_\beta \cup \mathcal{O}_\gamma) = \mathcal{P}_{<y} - (\mathcal{O}_\beta \cup \mathcal{O}_\gamma) \text{ y } \mathcal{P}_{>x} - (\mathcal{O}_\beta \cup \mathcal{O}_\gamma) = \mathcal{P}_{>y} - (\mathcal{O}_\beta \cup \mathcal{O}_\gamma)$$

para todo par $x, y \in \{1,2,3,4\}$ y que

$$\mathcal{P}_{<x} - (\mathcal{O}_\alpha \cup \mathcal{O}_\gamma) = \mathcal{P}_{<y} - (\mathcal{O}_\alpha \cup \mathcal{O}_\gamma) \text{ y } \mathcal{P}_{>x} - (\mathcal{O}_\alpha \cup \mathcal{O}_\gamma) = \mathcal{P}_{>y} - (\mathcal{O}_\alpha \cup \mathcal{O}_\gamma)$$

para todo par $x, y \in \{1',2',3',4'\}$.

Observación 4.1.4: Si $\mathcal{Q}'$ es el subposet inducido por los puntos de α, β y γ, cualquier automorfismo de $\mathcal{Q}'$ que deje fijos los puntos de γ y mande puntos de α en puntos de α y puntos de β en puntos de β, se puede extender a un automorfismo de $\mathcal{P}$ vía la identidad.

Además, sabiendo que $\frac{n}{2} \equiv 2 \pmod 4$, tenemos que $(1\,2\,3\,4)^{\frac{n}{2}} = (1\,2\,3\,4)^2$ y, por lo tanto, las órbitas de la acción de $g^{\frac{n}{2}}$ en $\mathcal{P}$ son $\{1,3\},\{2,4\},\{1',3'\}$ y $\{2',4'\}$.

Esto nos dice que para todo par $x, y \in \{1,2,3,4\}$ tales que $\{x,y\} \in \{\{1,3\},\{2,4\}\}$:

$$\mathcal{P}_{<x} - \mathcal{O}_\beta = \mathcal{P}_{<y} - \mathcal{O}_\beta \;\text{ y }\; \mathcal{P}_{>x} - \mathcal{O}_\beta = \mathcal{P}_{>y} - \mathcal{O}_\beta.$$

Análogamente, para todo par $x, y \in \{1',2',3',4'\}$ tales que $\{x,y\} \in \{\{1',3'\},\{2',4'\}\}$:

$$\mathcal{P}_{<x} - \mathcal{O}_\alpha = \mathcal{P}_{<y} - \mathcal{O}_\alpha \;\text{ y }\; \mathcal{P}_{>x} - \mathcal{O}_\alpha = \mathcal{P}_{>y} - \mathcal{O}_\alpha.$$

Debido a esto último, llamaremos a $\{1,3\},\{2,4\},\{1',3'\}$ y $\{2',4'\}$ *parejas intercambiables*.
Sea $\mathcal{Q}$ el subposet inducido por los puntos de α y β. No es difícil notar que el poset $\mathcal{Q}$ queda definido por la relación entre 1 y $\{1',2',3',4'\}$.

Observación 4.1.5: Cualquier automorfismo de $\mathcal{Q}$ que preserve parejas intercambiables se puede extender a un automorfismo de $\mathcal{P}$ vía la identidad.

Si 1 es menor que todos, es decir, menor que $1', 2', 3'$ y $4'$ (o bien es incomparable con todos ellos) reiteradas aplicaciones de la acción de g nos dicen que $2, 3$ y 4 también son menores que $1', 2', 3'$ y $4'$ (o bien son incomparables con todos ellos). Por esto, la trasposición $(1'\,3')$ sería un automorfismo de $\mathcal{Q}$ que preserva parejas intercambiables, y por lo tanto se podría extender a un automorfismo de $\mathcal{P}$ vía la identidad. Sin embargo, este automorfismo no coincide con g^i para ningún $i \in \mathbb{N}$, así que llegaríamos a una contradicción — y concluimos que estos casos no pueden darse.

Los demás posibles casos pueden observarse en la Figura 4.1, y son:

1. Que 1 esté relacionado con exactamente un punto de β — supondremos sin pérdida de la generalidad que $1 \leqslant 1'$.

2. Que 1 esté relacionado con exactamente dos puntos de β que estén a distancia 1 en el ciclo — supondremos sin pérdida de la generalidad que $1 \leqslant 1'$ y $1 \leqslant 2'$.

3. Que 1 esté relacionado con exactamente dos puntos de β que estén a distancia 2 en el ciclo — supondremos sin pérdida de la generalidad que $1 \leqslant 1'$ y $1 \leqslant 3'$.

4. Que 1 esté relacionado con exactamente tres puntos de β — supondremos sin pérdida de la generalidad que $1 \leqslant 1'$, $1 \leqslant 2'$ y $1 \leqslant 3'$.

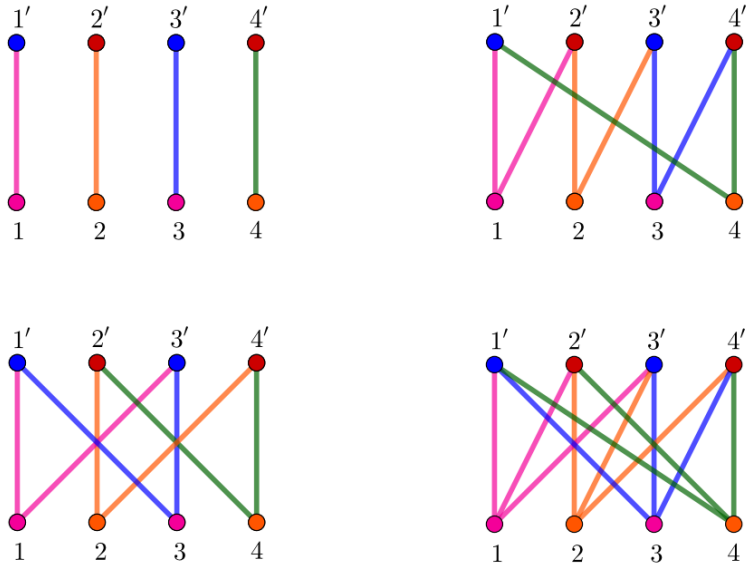

Figura 4.1: Diagrama de Hasse de $\mathcal{Q}$, destacando puntos que tienen mismas relaciones con γ.

Los colores en los puntos destacan las parejas intercambiables.

En los casos de la izquierda, la permutación $(1\ 3)(1'\ 3')$ es un automorfismo de $\mathcal{Q}$ que preserva parejas intercambiables y por lo tanto se extiende a un automorfismo de $\mathcal{P}$, pero no coincide con g^i para ningún $i \in \mathbb{N}$. Entonces estos casos no pueden suceder.

En el caso de abajo a la derecha, la permutación $(1\ 3)(2'\ 4')$ es un automorfismo de $\mathcal{Q}$ que preserva parejas intercambiables y por lo tanto se extiende a un automorfismo de $\mathcal{P}$, pero no coincide con g^i para ningún $i \in \mathbb{N}$. Entonces este caso no puede suceder.

A partir de ahora nos vamos a encargar del caso de arriba a la derecha.
Recordemos que llamamos $\mathcal{Q}'$ al subposet inducido por los puntos de α, β y γ.

Afirmación 4.1.6: No existen $x \in \mathcal{P}$, $r' \in \mathcal{O}_\beta$ y $q \in \mathcal{O}_\alpha$ de modo que $x < r'$ y $x > q$.

Demostración. En lo siguiente, las etiquetas de α serán vistas mód 4. Supongamos que existe un $x \in \mathcal{P}$ tal que $x < r'$ para algún $r' \in \mathcal{O}_\beta$ y $x > q$ para algún $q \in \mathcal{O}_\alpha$. Por propiedad de las parejas intercambiables sería $x > q + 2$. Esto nos dice que $r' > x > q$ y $r' > x > q+2$, lo cuál es absurdo ya que q y $q+2$ tienen la misma paridad, y por definición del poset $\mathcal{Q}$, r' no es mayor que dos puntos de α con etiquetas de la misma paridad. ■

Etiquetemos los puntos de γ como $(1''\ 2''\ \cdots\ (2m)'')$.

Afirmación 4.1.7: Si un punto $z'' \in \mathcal{O}_\gamma$ es mayor (resp. menor o incomparable) a un punto de α o β, entonces cualquier $y'' \in \mathcal{O}_\gamma$, con y de la misma paridad que z, también lo es.

Demostración. En efecto, la acción de $\langle g^{2m+2} \rangle$ en $\mathcal{P}$ deja fijos los puntos de α y β, ya que $2m+2$ es múltiplo de 4. Además, las órbitas de la acción de $\langle g^{2m+2} \rangle$ restringida a γ son:

$$A_1 = \{(2j-1)'' : 1 \leqslant j \leqslant m\} \quad \text{y} \quad A_2 = \{(2j)'' : 1 \leqslant j \leqslant m\}.$$

En otras palabras, en γ, los puntos pertenecen a una de dos posibles órbitas: los puntos de etiqueta impar, o los de etiqueta par. Esto prueba la observación. ■

Vamos a clasificar todos los posibles subposets $\mathcal{Q}'$. Gracias a la Afirmación 4.1.7, sabemos que todos los puntos de γ con etiquetas de la misma paridad tendrán las mismas relaciones con todos los puntos de α y β. Usando este hecho, sin pérdida de la generalidad, en los gráficos sólo mostraremos los subposets $\mathcal{Q}'$ en el caso particular en que $m = 1$, ya que esto nos alcanza para visualizar las relaciones de los puntos de γ con etiqueta impar (que serán las mismas que las de $1''$) y las relaciones de los puntos de γ con etiqueta par (que serán las mismas que las de $2''$).

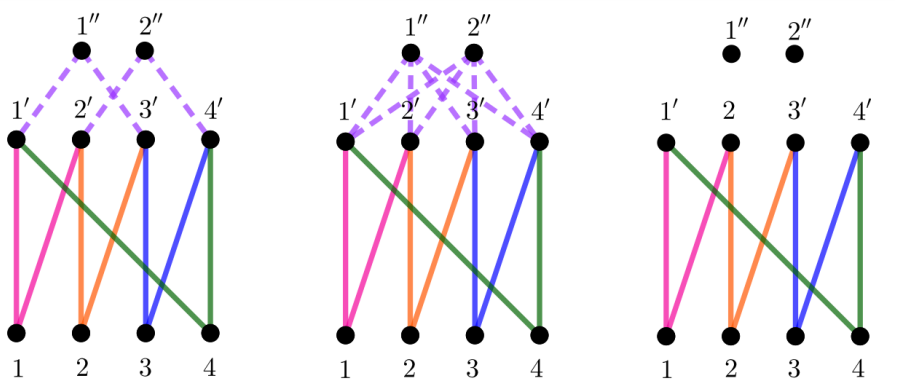

Figura 4.2: Diagrama de Hasse de $\mathcal{Q}'$, subcasos 1, 2 y 5

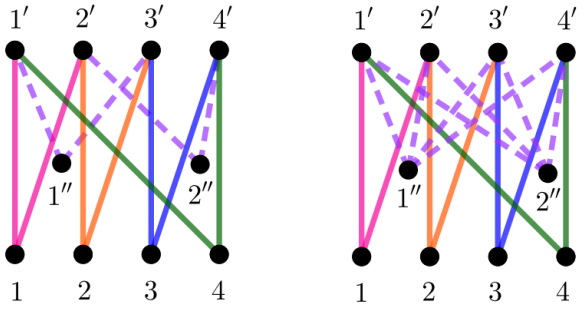

Figura 4.3: Diagrama de Hasse de $\mathcal{Q}'$, subcasos 3 y 4

Subcaso 1: $1'' > 1'$ pero incomparable con $2'$.

Por propiedad de las parejas intercambiables, deberá cumplirse que $1'' > 3'$ y que $1''$ es incomparable con $4'$. Además, como $1' > 1$, $1' > 4$, $3' > 2$ y $3' > 3$, deberá cumplirse

que $1'' > q$ para todo $q \in \mathcal{O}_\alpha$. Por la Afirmación 4.1.7, cualquier x'' con x impar tiene las mismas relaciones que $1''$ con todos los puntos de α y β.

Por otro lado, aplicando una vez g, tenemos que $2'' > 2'$, $2'' > 4'$ y que $2''$ es incomparable con $1'$ y $3'$. Además, como $2' > 1$, $2' > 2$, $4' > 3$ y $4' > 4$, deberá cumplirse que $2'' > q$ para todo $q \in \mathcal{O}_\alpha$. Por la Afirmación 4.1.7, cualquier x'' con x par tiene las mismas relaciones que $2''$ con todos los puntos de α y β.

Podemos ver el diagrama de $\mathcal{Q}'$ cuando $m = 1$ en el primer gráfico de la Figura 4.2.

El caso en el que $1'' > 2'$ pero es incomparable con $1'$ es análogo, ya que proviene de re-etiquetar los puntos de γ, cambiando k'' por $(k+1)''$ para cada $1 \leqslant k \leqslant 2m-1$ y cambiar $(2m)''$ por $1''$.

Subcaso 2: $1'' > 1'$ y $1'' > 2'$.

Por propiedad de las parejas intercambiables, deberá cumplirse que $1'' > 3'$ y $1'' > 4'$. Además, como $1' > 1$, $1' > 4$, $3' > 2$ y $3' > 3$, deberá cumplirse que $1'' > q$ para todo $q \in \mathcal{O}_\alpha$. Por la Afirmación 4.1.7, cualquier x'' con x impar tiene las mismas relaciones que $1''$ con todos los puntos de α y β.

Por otro lado, aplicando una vez g, tenemos que $2'' > 1'$, $2'' > 2'$, $2'' > 3'$ y $2'' > 4'$. Además, como $2' > 1$, $2' > 4$, $2' > 2$ y $2' > 3$, deberá cumplirse que $2'' > q$ para todo $q \in \mathcal{O}_\alpha$. Por la Afirmación 4.1.7, cualquier x'' con x par tiene las mismas relaciones que $2''$ con todos los puntos de α y β.

Podemos ver el diagrama de $\mathcal{Q}'$ cuando $m = 1$ en el segundo gráfico de la Figura 4.2.

Los casos en los que $1''$ es menor a algún punto de α son análogos a los subcasos 1 y 2, ya que podemos obtenerlos tomando el subposet opuesto $(\mathcal{Q}')^{op}$, renombrando los puntos de α — cambiando k por k' para cada $1 \leqslant k \leqslant 4$ —, y renombrando los puntos de β — cambiando k' por k para cada $1 \leqslant k \leqslant 4$.

Subcaso 3: $1'' < 1'$ pero incomparable con $2'$ y con todos los puntos de α.

Por propiedad de las parejas intercambiables, deberá cumplirse que $1'' < 3'$ y que $1''$ es incomparable con $4'$. Por la Afirmación 4.1.7, cualquier x'' con x impar tiene las mismas relaciones que $1''$ con todos los puntos de α y β.

Además, aplicando una vez g, tenemos que $2'' < 2'$, $2'' < 4'$ y que $2''$ es incomparable con $1'$ y $3'$. Por la Afirmación 4.1.7, cualquier x'' con x par tiene las mismas relaciones que $2''$ con todos los puntos de α y β.

Podemos ver el diagrama $\mathcal{Q}'$ cuando $m = 1$ en el primer gráfico de la Figura 4.3.

El subcaso en el que $1'' < 2'$ pero es incomparable con $1'$ y con todos los puntos de α es análogo a este último subcaso, , ya que proviene de re-etiquetar los puntos de γ, cambiando k'' por $(k+1)''$ para cada $1 \leqslant k \leqslant 2m-1$ y cambiar $(2m)''$ por $1''$.

Subcaso 4: $1'' < 1'$ y $1'' < 2'$, pero incomparable con todos los puntos de α.

Por propiedad de las parejas intercambiables, deberá cumplirse que $1'' < 3'$ y $1'' < 4'$. Por la Afirmación 4.1.7, cualquier x'' con x impar tiene las mismas relaciones que $1''$ con todos los puntos de α y β.

Además, aplicando una vez g, tenemos que $2'' < 1'$, $2'' < 2'$, $2'' < 3'$ y $2'' < 4'$. Por la Afirmación 4.1.7, cualquier x'' con x par tiene las mismas relaciones que $2''$ con todos los puntos de α y β.

Podemos ver el diagrama de $\mathcal{Q}'$ cuando $m = 1$ en el segundo gráfico de la Figura 4.3.

Los casos en los que $1''$ es mayor a algún punto de α pero incomparable con todos los puntos de β son análogos, ya que podemos obtenerlos tomando el subposet opuesto $(\mathcal{Q}')^{op}$, renombrando los puntos de α — cambiando k por k' para cada $1 \leqslant k \leqslant 4$ —, y renombrando los puntos de β — cambiando k' por k para cada $1 \leqslant k \leqslant 4$.

Subcaso 5: Si $1''$ es incomparable con todos los puntos de α y β.

Aplicando una vez g, obtenemos que $2''$ también es incomparable con todos los puntos de α y β. De hecho, por la Afirmación 4.1.7, todos los puntos de γ serán incomparables con todos los puntos de α y β.

Podemos ver el diagrama de $\mathcal{Q}'$ cuando $m = 1$ en el tercer gráfico de la Figura 4.2.

Finalmente, la Afirmación 4.1.6 nos dice que no hay más subcasos por analizar.

Veamos que, en todos los subcasos descriptos, $\phi = (4\ 3)(2\ 1)(3'\ 1')$ es efectivamente un automorfismo de $\mathcal{Q}'$. Para empezar, es sencillo ver que ϕ es un automorfismo de $\mathcal{Q}$.
Por otro lado, las relaciones entre puntos de γ y puntos de α se preservan vía ϕ ya que, en todos los subcasos, o bien todos los puntos de γ son mayores que todos los puntos de α o bien todos los puntos de γ son incomparables con todos los puntos de α. Por último, como ϕ preserva parejas intercambiables en β, también se preservan vía ϕ las relaciones entre puntos de γ y puntos de β.

Ahora, como ϕ es un automorfismo de $\mathcal{Q}'$ que deja fijos los puntos de γ, por la Observación 4.1.5 podemos extenderlo a un automorfismo de $\mathcal{P}$ vía la identidad.

Como la extensión de ϕ no coincide con g^i para ningún $i \in \mathbb{N}$, llegamos a un absurdo. El absurdo provino de suponer que había sólo un $2m$−ciclo con m impar, así que debe existir otro $2s$−ciclo con $s \in \mathbb{N}$ impar, como queríamos. ■

Corolario 4.1.8: $\beta(\mathbb{Z}_4) = 12$

Demostración. Sea $\mathcal{P}$ un poset con $\beta(\mathbb{Z}_4)$ puntos y $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_4 \simeq \langle g \rangle$. Por el Lema **??** sabemos que $\beta(\mathbb{Z}_4) \leqslant 12$. Por el Lema 3.2.4 sabemos que g contiene al menos dos 4−ciclos. Si contiene un tercer 4−ciclo, terminamos, así que supongamos que no. Si g contiene un 2−ciclo, el lema anterior nos asegura que contiene otro 2−ciclo y así $\beta(\mathbb{Z}_4) \geqslant 4+4+2+2 = 12$ como queríamos. Resta analizar cuando g contiene exactamente dos 4−ciclos y ningún 2−ciclo; etiquetamos $g = (1\,2\,3\,4)(1'\,2'\,3'\,4')$. Al igual que en el lema anterior, alcanza con analizar los casos en los que 1 está cubierto por $\{1', 2', 3', 4'\}$, por ninguno de ellos y los casos de la Figura 4.1. Como ya vimos, en los primeros dos casos la trasposición $(1'\,3')$ es un automorfismo de $\mathcal{P}$, pero en este caso no coincide con g^i para ningún $i \in \mathbb{N}$. En todos los casos de la Figura 4.1 hay permutaciones de los puntos de $\mathcal{P}$ que son automorfismos pero no coinciden con g^i para ningún $i \in \mathbb{N}$, a saber:

- En los dos casos de la izquierda, tenemos la permutación $(1\,3)(1'\,3')$.
- En el caso de arriba a la derecha, la permutación $(1\,3)(2'\,4')$.
- En el caso de abajo a la derecha, tenemos $(4\,3)(2\,1)(3'\,1')$.

Llegando así a un absurdo y completando la demostración. ■

Este corolario termina de probar el Teorema 3.5.6.

Lema 4.1.9: Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n \simeq \langle g \rangle$ y $n \in \mathbb{N}$. Supongamos que en su descomposición en ciclos disjuntos, g contiene un 3−ciclo y un $3m$−ciclo con $3 \nmid m$. Entonces existe otro ciclo η contenido en g de longitud $3s$ con $s \in \mathbb{N}$.

Demostración. Sea $\mathcal{Q}$ el subposet inducido por los puntos del $3m$−ciclo, que nombraremos $(1'\,2'\,\cdots\,(3m)')$ y el 3−ciclo, que nombraremos $(1\,2\,3)$, y supongamos que todos los demás ciclos contenidos en g tienen longitud no divisible por 3.

La permutación inducida por g en $\mathcal{Q}$ es la composición $(1\,2\,3)(1'\,2'\,\cdots\,(3m)')$. Notar que, gracias a eso, las relaciones entre los puntos del 3−ciclo y los puntos del $3m$−ciclo, quedan determinadas por la relación de 1 con $1', 2'$ y $3'$.

Observemos que, como todos los demás ciclos de g tienen longitud no divisible por 3, la acción de $\langle g^{\frac{n}{3}} \rangle$ sobre $\mathcal{P}$ deja fijos todos los puntos de $\mathcal{P}$ excepto los del 3−ciclo y el $3m$−ciclo. Más aún,

$$g^{\frac{n}{3}} = (1\,2\,3)^{\frac{n}{3}}(1'\,\cdots\,(3m)')^{\frac{n}{3}}.$$

Además, como $\frac{n}{3}$ es coprimo con 3, la acción de $\langle g^{\frac{n}{3}} \rangle$ restringida a $\{1, 2, 3\}$ es transitiva, por lo tanto

$$\mathcal{P}_{<x} - \{1', \ldots, (3m)'\} = \mathcal{P}_{<y} - \{1', \ldots, (3m)'\}$$
$$\text{y} \quad \mathcal{P}_{>x} - \{1', \ldots, (3m)'\} = \mathcal{P}_{>y} - \{1', \ldots, (3m)'\}$$

para todo par $x, y \in \{1,2,3\}$.

Ahora, como n es múltiplo de $3m$ por contener g un $3m-$ciclo, sabemos que $\frac{n}{3}$ es múltiplo de m. Como $\frac{n}{3}$ no es múltiplo de 3 y m tampoco, esto nos dice que, o bien $\frac{n}{3} \equiv m \pmod{3m}$, o bien $\frac{n}{3} \equiv -m \pmod{3m}$. En otras palabras:

$$(1' \cdots (3m)')^{\frac{n}{3}} = (1' \cdots (3m)')^{m} \quad \text{o} \quad (1' \cdots (3m)')^{\frac{n}{3}} = (1' \cdots (3m)')^{-m}.$$

En ambos casos, la acción de $\langle g^{\frac{n}{3}} \rangle$ sobre $\mathcal{P}$ tiene $m+1$ órbitas no unipuntuales, una es $\{1,2,3\}$ y las demás son, para cada $1 \leqslant i \leqslant m$,

$$A_i = \{(mk+i)' : 0 \leqslant k \leqslant 2\}.$$

En consecuencia, para todo par x', y' que pertenezcan a la misma órbita A_i, vale que

$$\mathcal{P}_{<x'} - \{1,2,3\} = \mathcal{P}_{<y'} - \{1,2,3\} \quad \text{y} \quad \mathcal{P}_{>x'} - \{1,2,3\} = \mathcal{P}_{>y'} - \{1,2,3\}.$$

Observación 4.1.10: Cualquier automorfismo ϕ de $\mathcal{Q}$ que cumpla $\phi(\{1,2,3\}) = \{1,2,3\}$ y $\phi(A_i) = A_i$ para todo $1 \leqslant i \leqslant m$ puede extenderse a un automorfismo de $\mathcal{P}$ vía la identidad.

Analicemos en primer lugar el caso en el que 1 está relacionado con sólo uno de los puntos $1', 2'$ y $3'$. Supongamos que $1 \leqslant 1'$ y los demás casos serán análogos. En la Figura 4.4 tenemos un ejemplo de cómo quedaría el poset con $m = 4$, donde los colores de $\{1', \ldots, 12'\}$ señalan a qué órbita pertenece cada punto.

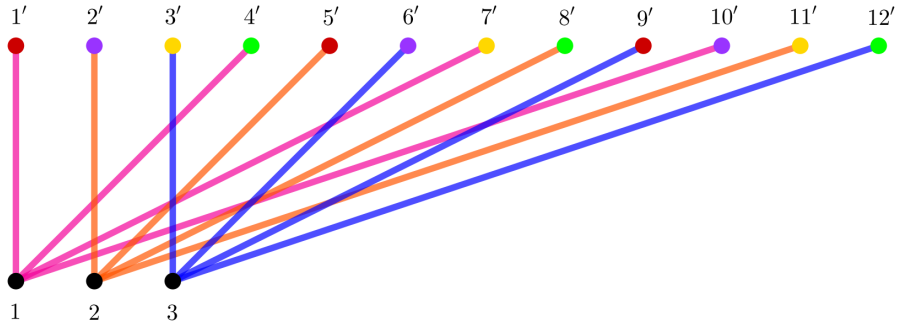

Figura 4.4: Diagrama de Hasse de $\mathcal{Q}$, con $m = 4$ y $1 \leqslant 1'$.

Por un lado, los puntos del $3m-$ciclo que cubren a 1 son $C_1 = \{(3k+1)' : 0 \leqslant k \leqslant m-1\}$.

Por otro, los puntos del $3m-$ciclo que cubren a 2 son $C_2 = \{(3k+2)' : 0 \leqslant k \leqslant m-1\}$.

Consideremos la permutación de puntos de $\mathcal{Q}$ que intercambia los puntos de la pareja $\{1,2\}$ y, para cada $0 \leqslant k \leqslant m-1$, intercambia los puntos de la pareja $\{(3k+1)', (3k+1+qm)'\}$, donde

$$q = \begin{cases} 1 & \text{si } m \equiv 1 \pmod 3 \\ 2 & \text{si } m \equiv 2 \pmod 3 \end{cases}$$

Notemos que $(3k+1)' \in C_1$ y $(3k+1+qm)' \in C_2$ y que esta permutación intercambia todos los puntos de C_1 con los de C_2. Como es usual, las etiquetas son vistas mod $3m$.

Esta permutación de puntos de $\mathcal{Q}$ es, de hecho, un automorfismo de $\mathcal{Q}$ — deja fijo al 3 y a los puntos que lo cubren (los de etiqueta múltiplo de 3), e intercambia 1 con 2 intercambiando también todos los puntos que cubren al 1 (C_1) con todos los puntos que cubren al 2 (C_2).

Además, $3k+1 \equiv 3k+1+qm \pmod{m}$, así que existe $1 \leqslant i \leqslant m$ tal que $(3k+1)' \in A_i$ y $(3k+1+qm)' \in A_i$. En otras palabras, si llamamos ϕ a este automorfismo, se cumple que $\phi(A_1) = A_1$ y $\phi(A_2) = A_2$.

Por la Observación 4.1.10, podemos afirmar que este automorfismo de $\mathcal{Q}$ se extiende a un automorfismo de $\mathcal{P}$ vía la identidad. Esto es absurdo, ya que dicho automorfismo no coincide con g^i para ningún $i \in \mathbb{N}$. Entonces esta situación no es posible.

El caso en el que 1 está relacionado con dos de los puntos $1', 2'$ y $3'$ se trata de un poset complementario a alguno de los anteriores — en los que 1 estaba relacionado sólo con uno de los puntos $1', 2'$ y $3'$ — por lo que tiene exactamente los mismos automorfismos y llegamos nuevamente a una contradicción.

Por último, si 1 está relacionado con $1', 2'$ y $3'$ a la vez (o con ninguno), la permutación de puntos de $\mathcal{Q}$ que intercambia la pareja $\{1, 2\}$ es un automorfismo de $\mathcal{Q}$ que, por la Observación 4.1.10, se extiende a un automorfismo de $\mathcal{P}$ vía la identidad, pero esto no es posible.

Habiendo agotado todos los casos, llegamos a un absurdo. Como el absurdo provino de suponer que todos los demás ciclos tenían longitud no divisible por 3, concluimos que existe algún otro ciclo contenido en g de longitud múltiplo de 3, como queríamos. ■

Lema 4.1.11: Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n \simeq \langle g \rangle$ y $n \in \mathbb{N}$. Supongamos que en su descomposición en ciclos disjuntos, g contiene un $p-$ciclo y un $2p-$ciclo. Entonces, si $p = 5$ o $p = 7$, existe otro ciclo η contenido en g de longitud $p \cdot s$ con $s \in \mathbb{N}$.

Demostración. Sea $\mathcal{Q}$ el subposet inducido por los puntos del $2p-$ciclo, que nombraremos $(1'\ 2'\ \cdots\ (2p)')$ y el $p-$ciclo, que nombraremos $(1\ 2\ \cdots\ p)$ y supongamos que todos los demás ciclos contenidos en g tienen longitud no divisible por p.

La permutación inducida por g en $\mathcal{Q}$ es la composición $(1\ 2\ \cdots\ p)(1'\ 2'\ \cdots\ (2p)')$. Notar que, gracias a eso, las relaciones entre los puntos del $p-$ciclo y los puntos del $2p-$ciclo, quedan determinadas por la relación de 1 con $1', 2', 3', \ldots, p'$.

Observemos que, como todos los demás ciclos de g tienen longitud no divisible por p, la acción de $\langle g^{\frac{n}{p}} \rangle$ sobre $\mathcal{P}$ deja fijos todos los puntos de $\mathcal{P}$ excepto los del $p-$ciclo y el $2p-$ciclo.

Más aún,

$$g^{\frac{n}{p}} = (1 \ \cdots \ p)^{\frac{n}{p}}(1' \ \cdots \ (2p)')^{\frac{n}{p}}.$$

Dicho esto, como $\langle g^{\frac{n}{p}} \rangle$ actúa transitivamente sobre $(1 \ \cdots \ p)$ por ser $\frac{n}{p}$ coprimo con p y deja fijos todos los puntos de $\mathcal{P}$ excepto los del $p-$ciclo y el $2p-$ciclo,

$$\mathcal{P}_{<x} - \{1', \ldots, (2p)'\} = \mathcal{P}_{<y} - \{1', \ldots, (2p)'\}$$
$$\text{y} \ \ \mathcal{P}_{>x} - \{1', \ldots, (2p)'\} = \mathcal{P}_{>y} - \{1', \ldots, (2p)'\}$$

para todo par $x, y \in \{1, 2, \ldots, p\}$.

Algo que nos será de mucha utilidad, es el hecho de que $\frac{n}{p} \cdot k$ toma todos restos distintos en la división por $2p$ para $0 \leqslant k \leqslant p-1$.

En efecto, supongamos que $\frac{n}{p} \cdot k_1 \equiv \frac{n}{p} \cdot k_2 \pmod{2p}$ para algún par $k_1, k_2 \in \mathbb{N}$ con $0 \leqslant k_1 < k_2 \leqslant p-1$. Como $\frac{n}{p}$ es coprimo con p, vale que $k_1 \equiv k_2 \pmod{p}$. Esto último, como $1 \leqslant k_2 - k_1 \leqslant p-1$, es una contradicción.

Estos p restos distintos son exactamente todos los restos pares en la división por $2p$, porque $\frac{n}{p}$ es par (por contener g un $2p-$ciclo). Luego, la acción de $\langle g^{\frac{n}{p}} \rangle$ sobre $\mathcal{P}$ tiene 3 órbitas no unipuntuales, una es $\{1, 2, \ldots, p\}$ y las otras dos son

$$A_1 = \left\{ (2k-1)' : 1 \leqslant k \leqslant \frac{p+1}{2} \right\} \ \text{y} \ \ A_2 = \left\{ (2k)' : 1 \leqslant k \leqslant \frac{p+1}{2} \right\}.$$

En otras palabras, los puntos de etiqueta par y los puntos de etiqueta impar.
Más aún, para todo par x', y' que pertenezcan a la misma órbita (A_1 o A_2), vale que

$$\mathcal{P}_{<x'} - \{1, \ldots, p\} = \mathcal{P}_{<y'} - \{1, \ldots, p\} \ \text{y} \ \ \mathcal{P}_{>x'} - \{1, \ldots, p\} = \mathcal{P}_{>y'} - \{1, \ldots, p\}.$$

Observación 4.1.12: Cualquier automorfismo ϕ de $\mathcal{Q}$ que cumpla $\phi(\{1 \ \cdots \ p\}) = \{1 \ \cdots \ p\}$, $\phi(A_1) = A_1$ y $\phi(A_2) = A_2$ puede extenderse a un automorfismo de $\mathcal{P}$ vía la identidad.

Vamos a definir ahora un nuevo poset $\mathcal{Q}'$, que consiste en agregarle a $\mathcal{Q}$ un punto $1''$ y agregar las relaciones $1'' \geqslant i'$ para todo $1 \leqslant i \leqslant 2p$ impar.

En la Figura 4.5 podemos observar un ejemplo con $p = 7$ y $1 \leqslant 1'$ — como mencionamos antes, esto último define todas las demás relaciones de $\mathcal{Q}$.

Si 1 no está relacionado con i' para ningún $1 \leqslant i \leqslant 2p$, la permutación de puntos de $\mathcal{Q}$ que intercambia la pareja $\{1, 2\}$ es un automorfismo de $\mathcal{Q}$ que, por la Observación 4.1.12, se extiende a un automorfismo de $\mathcal{P}$ vía la identidad, pero esto no es posible ya que no coincide con g^i para ningún $i \in \mathbb{N}$.

Por lo tanto, a partir de ahora podemos suponer que 1 está relacionado con i' para algún $1 \leqslant i \leqslant 2p$. Sin pérdida de la generalidad supondremos que $1 \leqslant i'$ para algún $1 \leqslant i \leqslant p$.

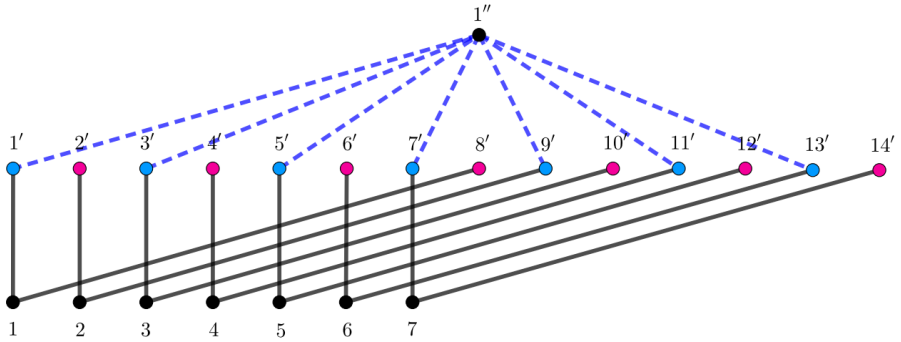

Figura 4.5: Diagrama de Hasse de $\mathcal{Q}'$, con $p = 7$, $1 \leqslant 1'$.

En particular, esto nos permite afirmar que cualquier automorfismo ϕ de $\mathcal{Q}$ cumple $\phi(\{1' \cdots (2p)'\}) = \{1' \cdots (2p)'\}$ y $\phi(\{1 \cdots p\}) = \{1 \cdots p\}$.

Dicho esto, notemos que si encontrásemos un automorfismo ϕ' de $\mathcal{Q}'$, este debe dejar fijo a $1''$ — por tener altura estrictamente mayor que los demás puntos de $\mathcal{Q}'$.
Además, como $1''$ es un punto fijo, deberá suceder que $\phi'(A_1) = A_1$ y $\phi'(A_2) = A_2$, ya que los puntos de A_1 están cubiertos por $1''$ y los de A_2 no.
Por lo tanto, al restringir ϕ' a $\mathcal{Q}$, obtendríamos un automorfismo $\phi'|_{\mathcal{Q}}$ de $\mathcal{Q}$ que cumple $\phi'|_{\mathcal{Q}}(\{1 \cdots p\}) = \{1 \cdots p\}$, $\phi'|_{\mathcal{Q}}(A_1) = A_1$ y $\phi'|_{\mathcal{Q}}(A_2) = A_2$, que por la Observación 4.1.12 se puede extender a un automorfismo de $\mathcal{P}$ vía la identidad.

Por otro lado, a lo sumo p automorfismos ϕ de $\mathcal{Q}$ pueden extenderse vía la identidad a automorfismos de $\mathcal{P}$ y a su vez cumplir $\phi(A_1) = A_1$ y $\phi(A_2) = A_2$.

Esto es porque los únicos automorfismos ψ de $\mathcal{P}$ que cumplen $\psi(A_1) = A_1$ y $\psi(A_2) = A_2$ son los de la forma g^{2k} con $k \in \mathbb{N}$ y estos automorfismos restringidos a $\mathcal{Q}$ inducen exactamente p automorfismos de $\mathcal{Q}$ distintos — si $2k \equiv 2k' \pmod{2p}$ la permutación inducida por g^{2k} en $\mathcal{Q}$ es la misma que la inducida por $g^{2k'}$.

Entonces, si encontramos al menos $p + 1$ automorfismos de $\mathcal{Q}'$, habremos llegado a una contradicción.

Para $p = 5$ y $p = 7$, en `SAGE` iteramos sobre todos los subconjuntos no vacíos $S \subseteq \{1, \ldots, p\}$ y, en cada iteración, preguntamos el cardinal del grupo de automorfismos del poset $\mathcal{Q}'$ descripto anteriormente, en el caso particular en el que $1 \leqslant s'$ para todo $s \in S$.
Tanto en el caso $p = 5$ como en el caso $p = 7$, todas las iteraciones nos devolvieron que el grupo de automorfismos de $\mathcal{Q}'$ tiene cardinal al menos $2p > p+1$ por lo que efectivamente llegamos a un absurdo.

Como el absurdo provino de suponer que no existía otro ciclo con longitud divisible por p, concluimos que sí existe, como queríamos.

En las siguientes páginas, dejamos el código utilizado para los casos $p = 5$ y $p = 7$, para que un lector interesado pueda correrlos por su cuenta. ■

```
import itertools
def findsubsets(s, n):
    return [set(i) for i in itertools.combinations(s, n)]

#del 1 al 10 están "abajo", del 11 al 15 están "arriba", y 16 es 1''
elms = [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16]

for k in range(0,6):
    s = {0, 1, 2, 3, 4}

    #recorro todos los subconjuntos posibles de s, que en la demostración los llamé S
    for x in findsubsets(s, k):
        rels = []
        for i in range(1,11):
            for q in x:
                if (q+i) % 5 != 0:
                    rels.append([i, 10 + (q+i) % 5])
                else:
                    rels.append([i,15])

        #agregamos manualmente las relaciones de 16, o sea 1''
        rels.append([16,10])
        rels.append([16,8])
        rels.append([16,6])
        rels.append([16,4])
        rels.append([16,2])

        #construyo el poset y calculo el grupo de automorfismos de su diagrama de Hasse
        P = Poset((elms, rels), cover_relations = True, facade = False)
        G = P.hasse_diagram().automorphism_group()

        #calculo el cardinal del grupo
        c = G.cardinality()

        #imprimo cardinal y generadores del grupo
        print(c)
        print(G)

        #imprimo el dibujo del diagrama de Hasse, aunque no lo necesito
        P.show()
print('FIN')
```

Caso p = 5

```
import itertools
def findsubsets(s, n):
    return [set(i) for i in itertools.combinations(s, n)]

#del 1 al 14 están "abajo", del 15 al 21 están "arriba", y el 22 es el punto 1''
elms = [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22]

for k in range(0,8):
    s = {0, 1, 2, 3, 4, 5, 6}

    #recorro todos los subconjuntos posibles de s, que en la demostración los llamé S
    for x in findsubsets(s, k):
        rels = []
        for i in range(1,15):
            for q in x:
                if (q+i) % 7 != 0:
                    rels.append([i, 14 + (q+i) % 7])
                else:
                    rels.append([i,21])

        #agregamos manualmente las relaciones de 22, osea 1''.
        rels.append([22,14])
        rels.append([22,12])
        rels.append([22,10])
        rels.append([22,8])
        rels.append([22,6])
        rels.append([22,4])
        rels.append([22,2])

        #construyo el poset y calculo el grupo de automorfismos de su diagrama de Hasse
        P = Poset((elms, rels), cover_relations = True, facade = False)
        G = P.hasse_diagram().automorphism_group()

        #calculo el cardinal del grupo
        c = G.cardinality()

        #imprimo cardinal y generadores del grupo
        print(c)
        print(G)

        #imprimo el dibujo del diagrama de Hasse, aunque no lo necesito
        P.show()

print('FIN')
```

Caso p = 7

Antes de seguir, vamos a definir una función que nos permitirá simplificar los enunciados los siguientes resultados.

Definición 4.1.13: Definimos $b\colon \text{Pot} \to \{1,2,3\}$, donde $\text{Pot} = \{p^k : p \text{ primo y } k \in \mathbb{N}\}$ como:

$$b\left(p^k\right) = \begin{cases} 1 & \text{si } p^k = 2 \\ 3 & \text{si } p^k = 3,4,5,7 \\ 2 & \text{si no} \end{cases}$$

Lema 4.1.14: Sea $n = p_1^{a_1} \cdots p_r^{a_r}$ donde los p_i son primos distintos. Existe un poset $\mathcal{P}$ tal que $\text{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n$ y

$$|\mathcal{P}| = \sum_{i=1}^{r} \beta\left(\mathbb{Z}_{p_i^{a_i}}\right) = \sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i}.$$

Demostración. Sea $\mathcal{P}_i$ un poset con $|\mathcal{P}_i| = \beta(\mathbb{Z}_{p_i^{a_i}})$ puntos y $\text{Aut}(\mathcal{P}_i) \simeq \mathbb{Z}_{p_i^{a_i}}$. Observemos que el *join* o *suma ordinal* entre todos estos posets para cada $1 \leqslant i \leqslant r$, es decir:

$$\mathcal{P} = \mathcal{P}_1 \oplus \cdots \oplus \mathcal{P}_r$$

cumple exactamente lo pedido. ∎

Este último resultado podría sugerirnos que en general

$$\beta\left(\bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{a_i}}\right) = \sum_{i=1}^{n} \beta\left(\mathbb{Z}_{p_i^{a_i}}\right),$$

pero esto no es cierto. En el ejemplo de abajo mostramos que $\beta\left(\mathbb{Z}_{12}\right) = 3\cdot 3 + 4\cdot 3 - 1 = 20$.

El poset de la Figura 4.6 se describe concretamente como:

- El conjunto subyacente es $\{1,2,\ldots,10\} \cup \{1',2',\ldots,10'\}$.
- Si $S = \{0,1,3\}$ entonces, para cada $1 \leqslant i \leqslant 6$, $i \leqslant (i+k)'$ para todo $k \in S$, mirando las etiquetas módulo 6.
- Si $S' = \{0,1\}$ entonces, para cada $7 \leqslant i \leqslant 10$, $i \leqslant (i+k)'$ para todo $k \in S'$, mirando las etiquetas módulo 4.

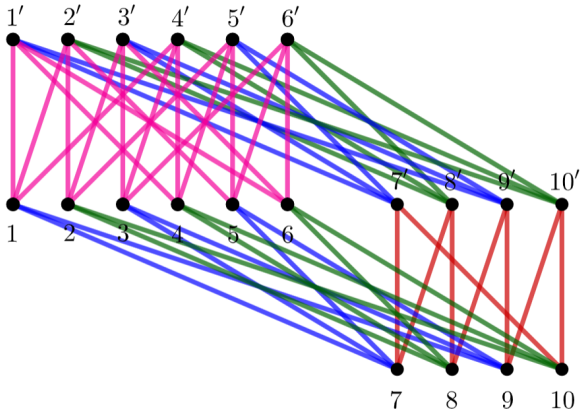

Figura 4.6: Diagrama de Hasse de un poset con 20 puntos y grupo de automorfismos $\mathbb{Z}_{12}$

- $7' \leqslant x'$ y $9' \leqslant x'$ para todo $1 \leqslant x \leqslant 6$ impar.
- $8' \leqslant x'$ y $10' \leqslant x'$ para todo $1 \leqslant x \leqslant 6$ par.
- $7 \leqslant x$ y $9 \leqslant x$ para todo $1 \leqslant x \leqslant 6$ par.
- $8 \leqslant x$ y $10 \leqslant x$ para todo $1 \leqslant x \leqslant 6$ par.

Lema 4.1.15: El poset de la Figura 4.6 tiene grupo de automorfismos $\mathbb{Z}_{12}$.

Demostración. Sean $a = (7\ 8\ 9\ 10)(7'\ 8'\ 9'\ 10')$ y $b = (1\ 2\ 3\ 4\ 5\ 6)(1'\ 2'\ 3'\ 4'\ 5'\ 6')$. Empezamos notando que $\langle ab \rangle$ es un subgrupo del grupo de automorfismos del poset en cuestión. Más aún, como el orden de una permutación es el mcm de las longitudes de los ciclos disjuntos que contiene, este subgrupo cíclico es exactamente $\mathbb{Z}_{12}$.

Para probar la igualdad, alcanza con ver que todo automorfismo de este poset puede escribirse como $(ab)^m$ para algún $m \in \mathbb{N}$. Y para ver eso alcanza con ver que el único automorfismo que tiene a $1'$ y 7 por puntos fijos a la vez es la identidad.

En efecto, supongamos que esto se cumple y ψ es un automorfismo de este poset. Como los automorfismos preservan altura, $\{1', 2', 3', 4', 5', 6'\}$ y $\{7, 8, 9, 10\}$ quedan invariantes por ψ ya que son los puntos maximales y minimales respectivamente. Entonces $\psi(1') = k'$ para algún $1 \leqslant k \leqslant 6$. Como $(ab)^k \cdot 1' = k'$ y ab es un automorfismo, $(ab)^{-k}\psi$ es un automorfismo que cumple $(ab)^{-k}\psi(1') = 1'$. Como 8 y 10 son los únicos puntos de $\{7, 8, 9, 10\}$ que están cubiertos por tres puntos cubiertos por $1'$, el conjunto $\{8, 10\}$ queda invariante por $(ab)^{-k}\psi$, y por lo tanto también $\{7, 9\}$. Luego, debe ser $(ab)^{-k}\psi(7) = q$ con $q = 7$ o 9.
Si $q = 7$, por hipótesis $(ab)^{-k}\psi = Id$ y entonces $\psi = (ab)^k$ como queríamos.
Si $q = 9$, como a y b conmutan por ser ciclos disjuntos, $(ab)^{-k+6}\psi(1') = 1'$ y $(ab)^{-k+6}\psi(7) = 7$, así que por hipótesis $(ab)^{-k+6}\psi = Id$ y entonces $\psi = (ab)^{-k+6}$ como queríamos.

Sea φ un automorfismo del poset en cuestión que cumple $\varphi(1') = 1'$ y $\varphi(7) = 7$.
Como 9 es el único punto de $\{7, 8, 9, 10\}$ — que queda invariante por φ por ser el conjunto de puntos minimales — tal que existen tres puntos de altura 1 que lo cubren a él y a 7 a la vez, es $\varphi(9) = 9$. De los puntos de que están cubiertos por $1'$, el único que cubre a 7 y 9 a la vez es 1, así que $\varphi(1) = 1$. Del mismo modo, de los puntos que están cubiertos por $1'$, el único que cubre a 7 y no a 9 es $7'$, así que $\varphi(7') = 7'$.
Además, $6'$ es el único punto de $\{1', 2', 3', 4', 5', 6'\}$ — que queda invariante por φ pues preserva alturas — que no cubre a 1 y no cubre a $7'$, así que $\varphi(6') = 6'$. Ahora, como los automorfismos preservan altura, el conjunto $\{1, 2, 3, 4, 5, 6\} \cup \{7', 8', 9', 10'\}$ queda invariante al aplicar φ; y como 2 es el único punto de este conjunto que no está cubierto por $1'$ ni $6'$, debe ser $\varphi(2) = 2$. De los puntos que cubren a 2, el único que no cubre a $7'$ es $2'$, así que $\varphi(2') = 2'$. Entre los puntos de $\{1', 2', 3', 4', 5', 6'\}$ que no cubren a $7'$, el único distinto de $2'$ y $6'$ es $4'$, así que $\varphi(4') = 4'$. El único punto que cubren $4'$ y $6'$ que no está cubierto por $2'$ es 3, así que $\varphi(3) = 3$. Los únicos puntos que cubren a 3 son $3'$, $4'$ y $6'$, como los últimos dos quedan fijos por φ debe ser $\varphi(3') = 3'$. Luego, como probamos que todos los puntos maximales salvo $5'$ quedan fijos, debe ser $\varphi(5') = 5'$. Notar que, para todo $1 \leqslant i \leqslant 6$, el punto i está determinado por los tres puntos de $\{1', 2', 3', 4', 5', 6'\}$ que lo cubren, así que $\varphi(i) = i$ para todo $1 \leqslant i \leqslant 6$.
Luego, $\{7', 8', 9', 10'\}$ queda invariante por φ y, como $7'$ es punto fijo y $9'$ es el único punto en este conjunto distinto de $7'$ que está cubierto por $1'$, es $\varphi(9') = 9'$. El único punto cubierto por $7'$ y 2 es 10, así que $\varphi(10) = 10$. El único punto cubierto por $9'$ y 2 es 8, así que $\varphi(8) = 8$. Como, $9'$ es el único punto que cubre a 8 y 9 a la vez, $\varphi(9') = 9'$. Finalmente, como $8'$ es el único punto que cubre a 7 y 8 a la vez, $\varphi(8') = 8'$ y como $10'$ es el único punto que cubre a 9 y 10 a la vez, $\varphi(10') = 10'$. Luego $\varphi = \mathrm{Id}$ como queríamos. ■

Lema 4.1.16: Sea $n = 12 \cdot p_3^{a_3} \cdots p_r^{a_r}$ donde los p_i son primos distintos que no son 2 ni 3. Existe un poset $\mathcal{P}$ tal que $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n$ y (definiendo $p_1^{a_1} = 4$ y $p_2^{a_2} = 3$)

$$|\mathcal{P}| = \left(\sum_{i=1}^{r} \beta\left(\mathbb{Z}_{p_i^{a_i}}\right) \right) - 1 = \left(\sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i} \right) - 1.$$

Demostración. Sea $\mathcal{P}_i$ un poset con $|\mathcal{P}_i| = \beta(\mathbb{Z}_{p_i^{a_i}})$ puntos y $\mathrm{Aut}(\mathcal{P}_i) \simeq \mathbb{Z}_{p_i^{a_i}}$ y sea $\mathcal{P}_0$ un poset con $\beta(\mathbb{Z}_{12}) = 20$ puntos y $\mathrm{Aut}(\mathcal{P}_0) \simeq \mathbb{Z}_{12}$. Observemos que el *join* o *suma ordinal* entre todos estos posets para cada $0 \leqslant i \leqslant r$, es decir:

$$\mathcal{P} = \mathcal{P}_0 \oplus \cdots \oplus \mathcal{P}_r$$

cumple exactamente lo pedido, ya que $\beta(\mathbb{Z}_{12}) = 20 = \beta(\mathbb{Z}_3) + \beta(\mathbb{Z}_4) - 1$. ■

Lema 4.1.17: Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \langle g \rangle$ y $|g| = n$ para algún $n \in \mathbb{N}$, y sea $p_j^{a_j}$ una potencia tal que $p_j^{a_j} \parallel n$. Supongamos que sólo existen dos ciclos α_1 y α_2 en g con longitud divisible por p_j, y que estas longitudes son ambas $p_j^{a_j}$. Si $\mathcal{Q}$ es el subposet de $\mathcal{P}$ inducido por los puntos de estos ciclos, entonces:

$$\mathrm{Aut}(\mathcal{Q}) \simeq \mathbb{Z}_{p_j^{a_j}}.$$

Demostración. Definimos $c_j = \dfrac{n}{p_j^{a_j}}$.

El automorfismo g^{c_j} deja fijos todos los puntos de $\mathcal{P}$, excepto los de α_1 y α_2, así que

$$g^{c_j} = \alpha_1^{c_j}\alpha_2^{c_j}.$$

Como c_j es coprimo con $p_j^{a_j}$, tanto $\alpha_1^{c_j}$ como $\alpha_2^{c_j}$ son $p_j^{a_j}$—ciclos involucrando los mismos puntos que α_1 y α_2 respectivamente.

Esto quiere decir que la acción de $\langle g^{c_j} \rangle$ sobre $\mathcal{P}$ tiene 2 órbitas no unipuntuales, una de $|\alpha_1|$ puntos y otra de $|\alpha_2|$ puntos. Como además deja todos los otros puntos de $\mathcal{P}$ fijos, dados $i, r \in \{1, 2\}$ con $r \neq i$, para todo par de puntos x e y de α_i es:

$$\mathcal{P}_{<x} - \mathcal{O}_{\alpha_r} = \mathcal{P}_{<y} - \mathcal{O}_{\alpha_r} \;\text{ y }\; \mathcal{P}_{>x} - \mathcal{O}_{\alpha_r} = \mathcal{P}_{>y} - \mathcal{O}_{\alpha_r}.$$

Si los puntos de $\mathcal{O}_{\alpha_1} \cup \mathcal{O}_{\alpha_2}$ formaran una anticadena, tendríamos algo más fuerte; para cada $i \in \{1, 2\}$ valdría que

$$\mathcal{P}_{<x} = \mathcal{P}_{<y} \;\text{ y }\; \mathcal{P}_{>x} = \mathcal{P}_{>y}$$

para todo par de puntos x e y de α_i. Esto quiere decir que habríamos encontrado un automorfismo que intercambia dos puntos de, por ejemplo, α_1 y deja todos los demás puntos de $\mathcal{P}$ fijos; pero este no coincide con g^i para ningún $i \in \mathbb{N}$. Por lo tanto, esta situación no puede ocurrir — hay algún x en α_1 e y en α_2 que cumplen $x < y$ ó $x > y$.

Esto nos dice que todo automorfismo de $\mathcal{Q}$ manda puntos de α_1 en puntos de α_1 y puntos de α_2 en puntos de α_2 — ya que los puntos de estos ciclos tienen alturas distintas — y entonces se puede extender vía la identidad a un automorfismo de $\mathcal{P}$.

En otras palabras, cualquier automorfismo de $\mathcal{Q}$ es la restricción de algún automorfismo de $\mathcal{P}$. Los únicos automorfismos de $\mathcal{Q}$ inducidos por automorfismos de $\mathcal{P}$ son los de la forma $\alpha_1^m\alpha_2^m$ con $1 \leqslant m \leqslant p_j^{a_j}$ y, por lo tanto, $\mathrm{Aut}(\mathcal{Q}) \simeq \langle \alpha_1\alpha_2 \rangle \simeq \mathbb{Z}_{p_j^{a_j}}$. ∎

Hagamos ahora unas observaciones y definiciones previas a la demostración del teorema.

Definición 4.1.18: Un *multiconjunto* de números naturales es un par (A, ν_A) donde A es un conjunto de números naturales y $\nu_A : A \to \mathbb{N}$ es una función de multiplicidad asociada. Informalmente, es un conjunto con repeticiones: si $a \in A$, $\nu_A(a)$ me dice cuántas veces aparece a en el multiconjunto.

En general vamos a cometer un abuso de notación y, dado un multiconjunto (L, ν_L), vamos a escribirlo como $L = \{l_1, l_2, \ldots, l_N\}$ donde $N = \sum_{l \in L} \nu_L(l)$ y $l_1, \ldots, l_N$ son los elementos de L incluyendo repeticiones.

Ejemplo: Si (L, ν_L) se define como $L = \{1, 2\}$ con $\nu_L(1) = 2$ y $\nu_L(2) = 3$, vamos a escribir $L = \{1, 1, 2, 2, 2\}$; aunque no nos va a interesar en qué orden están, también podríamos escribir $L = \{2, 1, 2, 1, 2\}$.

Recordemos que en la Desigualdad Fundamental, dados $a_1, \ldots, a_n \in \mathbb{N}$ definíamos $D = \{d_1, \ldots, d_m\}$ como el conjunto de potencias de primos que dividen exactamente a algún a_i con $1 \leqslant i \leqslant n$. También definíamos $(k_i)_{1 \leqslant i \leqslant m}$ de modo que
$k_i = |\{1 \leqslant j \leqslant n : d_i \mid a_j\}|$ y probamos que se cumplía

$$a_1 + \ldots + a_n \geqslant k_1 d_1 + \ldots + k_m d_m.$$

En particular, dado un multiconjunto $L = \{l_1, \ldots, l_N\}$, podemos aplicar esta desigualdad a sus elementos con repetición $l_1, l_2, \ldots, l_N \in \mathbb{N}$.

Teniendo en mente esto, definimos una función $f : \text{Mult}(\mathbb{N}) \times \mathbb{N} \to \mathbb{N}_0$ de manera que, si $L = \{l_1, l_2, \ldots, l_N\}$ es un multiconjunto y $(k_i)_{1 \leqslant i \leqslant m_L}$ y $(d_i)_{1 \leqslant i \leqslant m_L}$ son los de la desigualdad fundamental aplicada a $l_1, \ldots, l_N \in \mathbb{N}$:

$$f(L, d) = \begin{cases} k_i & \text{si } d = d_i \text{ para algún } 1 \leqslant i \leqslant m_L \\ 0 & \text{si no} \end{cases}$$

Además, denotaremos D_L al conjunto D que queda definido en esta aplicación de la desigualdad fundamental y $m_L = |D_L|$.

Con esta definición dada, podemos reescribir el resultado de la desigualdad fundamental aplicada sobre los elementos con repetición del multiconjunto L como:

$$l_1 + \cdots + l_N \geqslant f(L, d_1) d_1 + \cdots + f(L, d_{m_L}) d_{m_L}.$$

Con esto dicho, podemos hacer una definición que será crucial para la demostración del teorema final de esta sección.

Definición 4.1.19: Sea $L = \{l_1, \cdots, l_N\}$ un multiconjunto de números naturales y f la función recién definida. Decimos que aplicamos una *transformación elemental* al multiconjunto L si lo cambiamos por otro multiconjunto L', que se construye reemplazando algunos elementos de L, $l_{i_1}, \ldots, l_{i_s}$ por otros $\overline{l_1}, \ldots, \overline{l_k}$ y cumple:

- $\sum_{j=1}^{s} l_{i_j} \geqslant \sum_{j=1}^{k} \overline{l_j}$.
- $D_{L'} \subseteq D_L$.
- $f(L', d) \geqslant f(L, d)$ para todo $d \in \mathbb{N}$, $d \neq 2$.

Vamos a denotar como

$$\{l_{i_1}, \ldots, l_{i_s}\} \mapsto \{\overline{l_1}, \ldots, \overline{l_r}\}$$

a la transformación elemental que reemplaza los $l_{i_1}, \ldots, l_{i_s}$ por los $\overline{l_1}, \ldots, \overline{l_r}$.

Ejemplo: si $L = \{2, 3, 3, 6\}$ es un multiconjunto podemos aplicar

$$\{2, 6\} \mapsto \{2, 2, 3\}$$

que convierte a L en un nuevo multiconjunto $L' = \{2, 2, 3, 3, 3\}$. Notar que es efectivamente una transformación elemental pues $2 + 6 \geqslant 2 + 2 + 3$, $D_L = D_{L'} = \{2, 3\}$, $f(L', 2) = 2 \geqslant 1 = f(L, 2)$ y $f(L', 3) = 3 \geqslant 2 = f(L, 3)$.

4.2 El teorema del caso cíclico

Ahora, estamos en condiciones de enunciar el teorema principal de este capítulo que, dado $n \in \mathbb{N}$, calcula el menor cardinal que debe tener un poset $\mathcal{P}$ con $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n$.

Teorema 4.2.1: Sea $n = p_1^{a_1} \cdots p_r^{a_r}$ donde los p_i son primos distintos.
Entonces, si $12 \nmid n$, o $8 \mid n$ o $9 \mid n$, se cumple que:

$$\beta(\mathbb{Z}_n) = \sum_{i=1}^{r} \beta(\mathbb{Z}_{p_i^{a_i}}) = \sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i}.$$

En cambio, si $4 \parallel n$ y $3 \parallel n$, se cumple que:

$$\beta(\mathbb{Z}_n) = \left(\sum_{i=1}^{r} \beta(\mathbb{Z}_{p_i^{a_i}})\right) - 1 = \left(\sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i}\right) - 1.$$

Demostración. Sea $\mathcal{P}$ un poset finito con $\beta(\mathbb{Z}_n)$ puntos y $\mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_n$.
Por la construcción ya hecha en los Lemas 4.1.14 y 4.1.16, basta ver que

$$|\mathcal{P}| \geqslant \begin{cases} \displaystyle\sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i} & \text{si } 12 \nmid n \text{ o } 8 \mid n \text{ o } 9 \mid n \\ \displaystyle\left(\sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i}\right) - 1 & \text{si } 4 \parallel n \text{ y } 3 \parallel n \end{cases}$$

El hecho de que $3, 4, 5$ y 7 sean los únicos cuyo coeficiente en la cota no es menor o igual a 2, porque $b(3) = b(4) = b(5) = b(7) = 3$, motiva la siguiente definición.

Definición 4.2.2: Decimos que $a \in \{3, 4, 5, 7\}$ es una *potencia problemática* si $a \parallel n$.

Los argumentos utilizados en la demostración del Lema 4.1.1 nos permiten afirmar que, si $L = \{l_1, \cdots, l_N\}$ es el multiconjunto de las longitudes de todos los ciclos contenidos en g — por supuesto, incluyendo repeticiones — vale que

$$l_1 + \cdots + l_N \geqslant f(L, d_1)d_1 + \cdots + f(L, d_{m_L})d_{m_L}$$

donde $f(L, d_i) \geqslant 2$ para todo $1 \leqslant i \leqslant m_L$ con $d_i \neq 2$ y $f(L, d_i) \geqslant 1$ si $d_i = 2$.

Sin embargo, si aplicásemos una transformación elemental, convirtiendo este multiconjunto L en otro L', obtendríamos

$$|\mathcal{P}| = \sum_{l \in L} l \geqslant \sum_{l' \in L'} l' \geqslant f(L', d_1)d_1 + \cdots + f(L', d_{m_L})d_{m_L}.$$

Observar que tiene sentido usar los $(d_i)_{1 \leqslant i \leqslant m_L}$ de D_L en vez de los de $D_{L'}$, ya que $D_{L'} \subseteq D_L$ y si algún d_j no está en $D_{L'}$ su coeficiente será $f(L', d_j) = 0$. Más aún, por definición de transformación elemental, valdrá que $f(L', d_i) \geqslant 2$ para todo $1 \leqslant i \leqslant m_L$ con $d_i \neq 2$, ya que $f(L', d_i) \geqslant f(L, d_i)$.
Esto nos sugiere que podemos realizar una sucesión de transformaciones elementales al multiconjunto L — de manera que los coeficientes de las potencias problemáticas aumenten — hasta conseguir que la desigualdad fundamental nos devuelva la cota deseada.

Para lograr esto, vamos a presentar esta sucesión de transformaciones como un algoritmo, pero antes vamos a necesitar hacer dos observaciones claves para el desarrollo del mismo.

Observación 4.2.3: Para cada potencia problemática, o bien existe un tercer ciclo con tamaño divisible por p_j o bien alguno de los dos ciclos en cuestión tiene longitud $p_j^{a_j} m$ con $m \geqslant 2$.

En efecto, consideremos una potencia problemática fija $p_j^{a_j}$ y supongamos, a modo de contradicción, que entre los ciclos de g hay exactamente dos ciclos de longitud $p_j^{a_j}$, que llamaremos α y β, y todos los demás ciclos tienen longitud no divisible por p_j.
Por el Lema 3.7, el subposet $\mathcal{Q}$ inducido por los puntos de α y β cumple $\mathrm{Aut}(\mathcal{Q}) \simeq \mathbb{Z}_{p_j^{a_j}}$.
Pero esto no puede ocurrir, ya que las potencias problemáticas cumplen $\beta(\mathbb{Z}_{p_j^{a_j}}) = 3p_j^{a_j}$, de donde se sigue el resultado de la observación.

Observación 4.2.4: Sea c un entero positivo cuya factorización en primos es $c = q_1^{c_1} \cdots q_s^{c_s}$. Si existen enteros positivos coprimos a y b tales que $c = ab$ y $(a-2)(b-2) \geqslant 4$, entonces

$$c \geqslant 2q_1^{c_1} + \cdots + 2q_s^{c_s}.$$

Empecemos probando que $ab \geqslant 2a+2b$. En efecto, esto ocurre sí y sólo si $ab-2a-2b \geqslant 0$, que sumando 4 a ambos lados es equivalente a:

$$(a-2)(b-2) = ab - 2a - 2b + 4 \geqslant 4$$

que se cumple por hipótesis. Ahora, si $a = q_{i_1}^{c_{i_1}} \cdots q_{i_k}^{c_{i_k}}$ y $b = q_{i_{k+1}}^{c_{i_{k+1}}} \cdots q_{i_s}^{c_{i_s}}$ donde

$$\{q_1^{c_1}, \ldots, q_s^{c_s}\} = \left\{q_{i_1}^{c_{i_1}}, \ldots, q_{i_s}^{c_{i_s}}\right\},$$

por el Lema 4.1.2 se cumple que

$$ab \geqslant 2a + 2b \geqslant 2q_{i_1}^{c_{i_1}} + \cdots + 2q_{i_k}^{c_{i_k}} + 2q_{i_{k+1}}^{c_{i_{k+1}}} + \cdots + 2q_{i_s}^{c_{i_s}} = 2q_1^{c_1} + \cdots + 2q_s^{c_s}$$

como queríamos.

Definición 4.2.5: A un ciclo cuya longitud cumpla las condiciones de la observación anterior, lo llamaremos *ciclo rebosante*.

Si la longitud de un ciclo rebosante contenido en g es $c = q_1^{c_1} \cdots q_s^{c_s}$ — y por lo tanto $q_j^{c_j} \mid n$ para todo $1 \leqslant j \leqslant s$ — podemos recolectar $q_j^{c_j}$ puntos extra para cada $1 \leqslant j \leqslant s$. Para esto, basta con aplicar la transformación elemental:

$$\{c\} \mapsto \{q_1^{c_1}, q_1^{c_1}, q_2^{c_2}, q_2^{c_2}, \ldots, q_s^{c_s}, q_s^{c_s}\}$$

es decir, cambiando c por dos copias de cada una de $q_1^{c_1}, \ldots, q_s^{c_s}$. Esto funciona ya que:

$$\sum_{l \in L} l \geqslant \sum_{l' \in L'} l' \geqslant f(L', d_1)d_1 + \cdots + f(L', d_{m_L})d_{m_L} = \sum_{j=1}^{s} q_j^{c_j} + \sum_{j=1}^{m_L} f(L, d_j)d_j.$$

Dicho de otra forma, $f\left(L', q_j^{c_j}\right) = f\left(L, q_j^{c_j}\right) + 1$ para todo $1 \leqslant j \leqslant s$ y, para todo d_i que no sea una de estas potencias, se cumplirá $f(L', d_i) = f(L, d_i)$.

Definición 4.2.6: Dado un ciclo rebosante contenido en g, diremos que le estamos aplicando una *transformación rebosante* si le aplicamos la transformación elemental recién descripta.

Vamos a describir un algoritmo en cuatro pasos, y cada uno tendrá un objetivo.
Cuando hablemos de *aumentar* el coeficiente $f(L, d)$ para algún $d \in \mathbb{N}$ nos estaremos refiriendo a realizar una transformación elemental al multiconjunto L tranformándolo en otro L' de modo que $f(L', d) > f(L, d)$.
En cada paso, llamamos L' al multiconjunto actual — es decir, al multiconjunto que proviene de haber aplicado la correspondiente sucesión de transformaciones elementales al multiconjunto inicial L en pasos anteriores — y L'' al multiconjunto obtenido una vez realizado el paso.

- **Paso 1:** tiene como objetivo realizar una transformación elemental a L que, si 3 es potencia problemática, logre $f(L'', 3) \geqslant 3$ o $f(L'', 3) \geqslant 4$ según el caso.
- **Paso 2:** tiene como objetivo realizar una transformación elemental a L' que, si 5 es potencia problemática, logre que $f(L'', 5) \geqslant 3$.
- **Paso 3:** tiene como objetivo realizar una transformación elemental a L' que, si 7 es potencia problemática, logre que $f(L'', 7) \geqslant 3$.
- **Paso 4:** tiene como objetivo realizar una transformación elemental a L' que, si 4 es potencia problemática, logre $f(L'', 4) \geqslant 3$ o $f(L'', 2) \geqslant 2$ según el caso.

Para entender a qué nos referimos con "según el caso", hay que entender el objetivo final del algoritmo, que dependerá de cuáles son las potencias problemáticas de n.

Si 4 no es potencia problemática, nuestro objetivo será aplicar una sucesión de transformaciones elementales hasta llegar a un multiconjunto L'' que cumpla $f(L'', d_i) \geqslant 3$ para todo $1 \leqslant i \leqslant m_L$ tal que d_i es una potencia problemática.

Importante: Si, además, n es par pero no múltiplo de 4, debemos asegurarnos que todas las transformaciones elementales que pasan de un multiconjunto L' a otro L'' cumplan $f(L'', 2) \geqslant 1$.

Si 4 es potencia problemática pero 3 no lo es, nuestro objetivo será aplicar una sucesión de transformaciones elementales hasta llegar a un multiconjunto L'' que cumpla $f(L'', d_i) \geqslant 3$ para todo $1 \leqslant i \leqslant m_L$ tal que d_i es una potencia problemática distinta de 4 y además, o bien $f(L'', 4) \geqslant 3$, o bien $f(L'', 2) \geqslant 2$ y $f(L'', 4) \geqslant 2$.

Esto último nos sirve porque, como 4 es potencia problemática, 2 no sería una potencia que divide exactamente a n y, por lo tanto, podemos usar el término $f(L'', 2) \cdot 2$ para complementar a $f(L'', 4) \cdot 4$. En particular, $f(L'', 2) \cdot 2 + f(L'', 4) \cdot 4 \geqslant 2 \cdot 2 + 2 \cdot 4 = b(4) \cdot 4$.

Importante: En el caso recién descripto, exigiremos que todas las transformaciones elementales que pasan de un multiconjunto L' a otro L'' cumplan $f(L'', 2) \geqslant f(L', 2)$.

Si 3 y 4 son potencias problemáticas, nuestro objetivo será, idealmente, aplicar una sucesión de transformaciones elementales hasta llegar a un multiconjunto L'' que cumpla $f(L'', d_i) \geqslant 3$ para todo $1 \leqslant i \leqslant m_L$ tal que d_i es una potencia problemática distinta de 4 y además, o bien $f(L'', 4) \geqslant 3$, o bien $f(L'', 2) \geqslant 2$ y $f(L'', 4) \geqslant 2$.
Pero habrá un caso particular en el que no podremos lograr esto: si hay exactamente dos ciclos con longitud divisible por 3 contenidos en g y estas longitudes son ambas iguales a 6, nos alcanzará con que cumpla $f(L'', 3) \geqslant 4$ y $f(L'', d_i) \geqslant 3$ para todo $1 \leqslant i \leqslant m_L$ tal que d_i es una potencia problemática distinta de 4.
Notar que $f(L'', 3) \cdot 3 + f(L'', 4) \cdot 4 \geqslant 4 \cdot 3 + 2 \cdot 4 = b(3) \cdot 3 + b(4) \cdot 4 - 1$; este es precisamente el caso del teorema en el que la respuesta es un punto menos de "lo esperado".

Ahora sí, pasamos a la descripción completa del algoritmo.

Paso 1: mirando las potencias de 3.

Primero, notar que en este primer paso es $L = L'$.

Si 3 no es una potencia problemática o bien hay tres ciclos de longitud divisible por 3, entonces ya se cumple $f(L, 3) \geqslant 3$ como queríamos, por lo que salteamos este paso.
Notar que en ninguno de estos casos necesitamos lograr $f(L'', 3) \geqslant 4$ — en un caso 3 no es potencia problemática y en el otro hay más de dos ciclos con longitud divisible por 3.

Por lo tanto, podemos suponer que 3 es una potencia problemática y que hay exactamente dos ciclos de longitud divisible por 3 en L. Por la Observación 4.2.3, alguno de los dos ciclos es de la forma $3m$ con $m \geqslant 2$.

Si alguno de los dos ciclos es rebosante, elegimos uno de los dos y recolectamos los puntos extra aplicándole una transformación rebosante. Más aún, luego de aplicar dicha transformación, $f(L'', q_j^{a_j}) = f(L', q_j^{a_j}) + 1$ para cada potencia $q_j^{a_j}$ que divida exactamente a la longitud de este ciclo, en particular, para todas las potencias problemáticas que lo hagan.

Si no, los ciclos son de la forma $3m$ y $3t$ con $2 \leqslant m \leqslant 5$ y $1 \leqslant t \leqslant 5$ — pues de otro modo alguno de los dos sería rebosante. Más aún, como 3 es potencia problemática, m y t son coprimos con 3, ya que de lo contrario la longitud de alguno de los dos sería divisible por 9 y entonces 3 no sería potencia problemática. Dicho esto, las posibles combinaciones restantes son:

(1) $(3m, 3t) = (6, 3)$

(2) $(3m, 3t) = (6, 6)$

(3) $(3m, 3t) = (6, 12)$

(4) $(3m, 3t) = (6, 15)$

(5) $(3m, 3t) = (12, 3)$

(6) $(3m, 3t) = (12, 12)$

(7) $(3m, 3t) = (12, 15)$

(8) $(3m, 3t) = (15, 3)$

(9) $(3m, 3t) = (15, 15)$

Los casos 1, 5 y 8 no son posibles por el Lema 4.1.9, ya que estamos suponiendo que existen exactamente dos ciclos en g con longitud múltiplo de 3.

En el **caso 2**, si 4 es una potencia problemática, aplicamos la transformación elemental

$$\{6, 6\} \mapsto \{3, 3, 3, 3\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 2 \geqslant 4$ y $f(L'', 2) = f(L, 2) - 2$. Notar que las restricciones que atañen a $f(L, 2)$ sólo aplican en los casos donde 4 o 3 no son potencias problemáticas, y no en este donde 3 y 4 son ambas potencias problemáticas.
Recordar que este será el único caso en el que debemos lograr $f(L'', 3) \geqslant 4$.

Es interesante destacar que, cuando aplicamos el algoritmo con $n = 12$, este es el caso que nos sugiere el ejemplo con 20 puntos que exhibimos en la Figura 4.6.
En particular, las longitudes de ciclos en ese ejemplo son $\{4, 4, 6, 6\}$ y nuestro algoritmo hace la transformación elemental

$$\{4, 4, 6, 6\} \mapsto \{4, 4, 3, 3, 3, 3\}$$

logrando nuestro objetivo de $f(L', 3) \geqslant 4$ y $f(L', 4) \geqslant 2$.

Si 4 no es una potencia problemática, aplicamos la transformación elemental

$$\{6, 6\} \mapsto \{2, 3, 3, 3\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 1 \geqslant 3$ y $f(L'', 2) = f(L, 2) - 1 \geqslant 1$. Como n es par por contener un $6-$ciclo pero podría no ser múltiplo de 4, es importante que se cumpla $f(L', 2) \geqslant 1$, ya que exigimos esto antes de empezar el algoritmo.

En el **caso 3**, aplicamos en L' la transformación elemental:

$$\{6, 12\} \mapsto \{3, 3, 3, 4, 4\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 1 \geqslant 3$, $f(L'', 4) = f(L, 4) + 1$ y $f(L'', 2) = f(L, 2) - 1$. Notar que en este caso no aplican las restricciones a $f(L, 2)$, ya que aquí 3 es potencia problemática y n es múltiplo de 4 por contener un $12-$ciclo.

En el **caso 4**, aplicamos en L' la transformación elemental:

$$\{6, 15\} \mapsto \{2, 3, 3, 3, 5, 5\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 1 \geqslant 3$, $f(L'', 5) = f(L, 5) + 1$ y manteniendo el valor de $f(L, 2)$, es decir, $f(L'', 2) = f(L, 2)$.

En el **caso 6**, aplicamos en L' la transformación elemental:

$$\{12, 12\} \mapsto \{3, 3, 3, 4, 4, 4\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 1 \geqslant 3$ y $f(L'', 4) = f(L, 4) + 1$.

En el **caso 7**, aplicamos en L' la transformación elemental:

$$\{12, 15\} \mapsto \{3, 3, 3, 4, 4, 5, 5\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 1 \geqslant 3$, $f(L'', 4) = f(L, 4) + 1$ y $f(L'', 5) = f(L, 5) + 1$.

En el **caso 9**, aplicamos en L' la transformación elemental:

$$\{15, 15\} \mapsto \{3, 3, 3, 5, 5, 5\}$$

provocando los cambios $f(L'', 3) = f(L, 3) + 1 \geqslant 3$ y $f(L'', 5) = f(L, 5) + 1$.

Notar que en todos los casos, además de lograr $f(L'', 3) = f(L', 3) + 1 \geqslant 3$ o $f(L'', 3) = f(L', 3) + 2 \geqslant 4$ según el caso, siempre que aplicamos una transformación elemental a un ciclo con longitud divisible exactamente por $4, 5$ o 7 también aumentamos en 1 los coeficientes $f(L, 4)$, $f(L, 5)$ y/o $f(L, 7)$ respectivamente.

Paso 2: mirando las potencias de 5.

Si 5 no es una potencia problemática o bien hay tres ciclos de longitud divisible por 5 en L, entonces ya se cumple $f(L, 5) \geqslant 3$ como queríamos, por lo que salteamos este paso.

Por lo tanto, podemos suponer que 5 es una potencia problemática y que hay exactamente dos ciclos contenidos en g con longitud múltiplo de 5.

Si en el Paso 1 le aplicamos alguna transformación elemental a alguno de estos dos ciclos, entonces ya conseguimos aumentar en 1 el valor de $f(L, 5)$, es decir, logramos $f(L', 5) \geqslant 3$.

Si ese fuese el caso, también salteamos este paso, pues no hay nada que hacer.
A partir de ahora podemos suponer también que hasta el momento no le aplicamos una transformación elemental a estos dos ciclos — que son los únicos con longitud múltiplo de 5.

Por la Observación 4.2.3, alguno de los dos ciclos es de la forma $5t$ con $t \geqslant 2$.

Si alguno de los dos ciclos es rebosante, elegimos uno de los dos y recolectamos los puntos extra aplicándole una transformación rebosante. Más aún, luego de aplicar dicha transformación, $f(L'', q_j^{a_j}) = f(L', q_j^{a_j}) + 1$ para cada potencia $q_j^{a_j}$ que divida exactamente a la longitud de este ciclo, en particular, para todas las potencias problemáticas que lo hagan.

Entonces supongamos que no.
Los ciclos son de la forma $5m$ y $5t$ con $t \geqslant 2$ y m y t coprimos con 5, ya que de lo contrario la longitud de alguno de los dos sería divisible por 25 y eso contradice que 5 sea potencia problemática. Como $(5-2)(k-2) \geqslant 4$ para todo $k \geqslant 4$ — por lo que todo $5k$—ciclo con $k \geqslant 4$ y k coprimo con 5 sería rebosante — los únicos casos posibles son:

(1) $(5m, 5t) = (5, 10)$

(2) $(5m, 5t) = (5, 15)$

(3) $(5m, 5t) = (10, 10)$

(4) $(5m, 5t) = (10, 15)$

(5) $(5m, 5t) = (15, 15)$

Por el Lema 4.1.11, el **caso 1** no es posible.

En el **caso 2**, como no necesitamos aumentar el valor de $f(L', 3)$ (pues si 3 fuese potencia problemática, esto ya lo hubiésemos hecho en el paso 1), aplicamos en L' la transformación elemental:

$$(5, 15) \mapsto (3, 5, 5, 5)$$

provocando que $f(L'', 5) = f(L', 5) + 1 \geqslant 3$ y manteniendo el valor de $f(L', 3)$, es decir, $f(L'', 3) = f(L', 3)$.

En el **caso 3**, aplicamos en L' la transformación elemental:

$$\{10, 10\} \mapsto \{2, 2, 5, 5, 5\}$$

provocando que $f(L'', 5) = f(L', 5) + 1 \geqslant 3$ y manteniendo el valor de $f(L', 2)$, es decir, $f(L'', 2) = f(L', 2)$.

En el **caso 4**, como no necesitamos aumentar el valor de $f(L', 3)$ (pues si 3 fuese potencia problemática, esto ya lo hubiésemos hecho en el paso 1), aplicamos en L' la transformación elemental:

$$\{10, 15\} \mapsto \{2, 3, 5, 5, 5\}$$

provocando que $f(L'', 5) = f(L', 5) + 1 \geqslant 3$ y manteniendo los valores de $f(L', 2)$ y $f(L', 3)$, es decir, $f(L'', 2) = f(L', 2)$ y $f(L'', 3) = f(L', 3)$.

En el **caso 5**, aplicamos en L' la transformación elemental:

$$\{15, 15\} \mapsto \{3, 3, 5, 5, 5\}$$

provocando que $f(L'',5) = f(L',5) + 1 \geqslant 3$ y manteniendo el valor de $f(L',3)$, es decir, $f(L'',3) = f(L',3)$.

Notar que en todos los casos, además de lograr $f(L'',5) = f(L',5) + 1 \geqslant 3$, siempre que aplicamos una transformación elemental a un ciclo con longitud divisible exactamente por 4 o 7 también aumentamos en 1 los coeficientes $f(L',4)$ y/o $f(L',7)$ respectivamente. Además, siempre que aplicamos una transformación elemental a un ciclo con longitud múltiplo de 3, mantuvimos o aumentamos el coeficiente $f(L',3)$.

Paso 3: mirando las potencias de 7.

Si 7 no es una potencia problemática o bien hay tres ciclos de longitud divisible por 7 en L, entonces ya se cumple $f(L,7) \geqslant 3$ como queríamos, por lo que salteamos este paso.

Por lo tanto, podemos suponer que 7 es una potencia problemática y que hay exactamente dos ciclos de longitud divisible por 7 en L.

Si en el Paso 1 o en el Paso 2 le aplicamos alguna transformación elemental a alguno de estos dos ciclos, entonces ya conseguimos aumentar en 1 el valor de $f(L,7)$, es decir, logramos $f(L',7) \geqslant 3$.

Si ese fuese el caso, también salteamos este paso, pues no hay nada que hacer.
A partir de ahora podemos suponer también que hasta el momento no le aplicamos una transformación elemental a estos dos ciclos — que son los únicos con longitud múltiplo de 7.

Por la Observación 4.2.3, alguno de los dos ciclos es de la forma $7t$ con $t \geqslant 2$.

Si alguno de los dos ciclos es rebosante, elegimos uno de los dos y recolectamos los puntos extra aplicándole una transformación rebosante. Más aún, luego de aplicar dicha transformación, $f(L'', q_j^{a_j}) = f(L', q_j^{a_j}) + 1$ para cada potencia $q_j^{a_j}$ que divida exactamente a la longitud de este ciclo, en particular, para todas las potencias problemáticas que lo hagan.

Entonces supongamos que no.
Las longitudes de estos dos ciclos son de la forma $7m$ y $7t$ con $t \geqslant 2$ y m y t coprimos con 7; de lo contrario la longitud de alguno de los dos sería divisible por 49 y eso contradice que 7 sea potencia problemática. Como cualquier ciclo de longitud $7k$ con $k \geqslant 3$ y k coprimo con 7 es rebosante — ya que en ese caso $(7-2)(k-2) \geqslant 4$, los únicos casos posibles son:

(1) 7 y 14

(2) 14 y 14

Por el Lema 4.1.11, el **caso 1** no es posible.

En el **caso 2**, aplicamos en L' la transformación elemental:

$$\{14, 14\} \mapsto \{2, 2, 7, 7, 7\}$$

provocando que $f(L'', 7) = f(L', 7) + 1 \geqslant 3$ y manteniendo el valor de $f(L', 2)$, es decir, $f(L'', 2) = f(L', 2)$.

Notar que en todos los casos, además de lograr $f(L'', 7) = f(L', 7) + 1 \geqslant 3$, siempre que aplicamos una transformación elemental a un ciclo con longitud divisible exactamente por 4 también aumentamos en 1 el coeficiente $f(L', 4)$. Además, siempre que aplicamos una transformación elemental a un ciclo con longitud múltiplo de 3 o 5, mantuvimos o aumentamos el coeficiente $f(L', 3)$ y/o $f(L', 5)$ respectivamente.

Paso 4: mirando las potencias de 4.

Si 4 no es una potencia problemática o bien hay tres ciclos de longitud divisible por 4 en L, entonces ya se cumple $f(L, 4) \geqslant 3$ como queríamos, por lo que salteamos este paso.

Por lo tanto, podemos suponer que 4 es una potencia problemática y que hay exactamente dos ciclos de longitud divisible por 4 en L.

Si existe algún otro ciclo de longitud par, por el Lema 4.1.3 existe otro ciclo de longitud par más. Y de aquí se desprenden dos situaciones que analizamos en el próximo párrafo.

Si $f(L', 2) \geqslant f(L, 2)$, tenemos $f(L', 2) \geqslant 2$ y $f(L', 4) \geqslant 2$, por lo que terminamos. Si no, quiere decir que en el paso 1 pasamos por el caso 2 — donde conseguimos $f(L', 3) \geqslant 4$ y $f(L', 4) \geqslant 2$ como queríamos — o bien por el caso 3 — donde conseguimos $f(L', 3) \geqslant 3$ y $f(L', 4) \geqslant 3$ como queríamos — ya que estos son los únicos casos en los que disminuimos el valor de $f(L, 2)$; así que en este segundo caso tampoco hay nada que hacer.

A partir de ahora, podemos suponer también que no existe un ciclo de longitud par distinto de los dos 4−ciclos.

Si en el Paso 1, el Paso 2 o el Paso 3 le aplicamos alguna transformación elemental a alguno de estos dos ciclos con longitud múltiplo de 4, entonces ya conseguimos aumentar en 1 el valor de $f(L, 4)$, es decir, logramos $f(L', 4) \geqslant 3$.

Si ese fuese el caso, también salteamos este paso, pues no hay nada que hacer.
Entonces, a todas las suposiciones anteriores podemos agregar la suposición de que hasta el momento no le aplicamos una transformación elemental a estos dos ciclos — que son los únicos con longitud múltiplo de 4.

Por la Observación 4.2.3, alguno de los dos 4−ciclos es de la forma $4m$ con $m \geqslant 2$. Más aún, $m \neq 2$ por que ningún ciclo puede tener longitud múltiplo de 8, ya que 8 no es potencia problemática por serlo 4. Así que $m \geqslant 3$.

Si alguno de los dos ciclos es rebosante, elegimos uno de los dos y recolectamos los puntos extra aplicándole una transformación rebosante. Más aún, luego de aplicar dicha transformación, $f(L'', q_j^{a_j}) = f(L', q_j^{a_j}) + 1$ para cada potencia $q_j^{a_j}$ que divida exactamente a la longitud de este ciclo, en particular, para todas las potencias problemáticas que lo hagan.

Entonces supongamos que no.
Las longitudes de los ciclos son de la forma $4m$ y $4t$ con $t \geqslant 2$ y m y t impares; de lo contrario la longitud de alguno sería divisible por 8 y eso contradice que 4 sea potencia problemática. Como $(4-2)(k-2) \geqslant 4$ para todo $k \geqslant 4$ — por lo que todo $4k$−ciclo con $k \geqslant 4$ y k impar sería rebosante — los únicos casos posibles son:

(1) 4 y 12

(2) 12 y 12

En el **caso 1**, aplicamos en L' la transformación elemental:

$$\{4, 12\} \mapsto \{4, 4, 4, 3\}$$

provocando que $f(L'', 4) = f(L', 4) + 1 \geqslant 3$ y manteniendo el valor de $f(L', 3)$, es decir, $f(L'', 3) = f(L', 3)$.

En el **caso 2**, aplicamos en L' la transformación elemental:

$$\{12, 12\} \mapsto \{3, 3, 4, 4, 4\}.$$

provocando que $f(L'', 4) = f(L', 4)+1$ y manteniendo el valor de $f(L', 3)$, es decir, $f(L'', 3) = f(L'3)$.

Al finalizar este último paso, terminamos el algoritmo.

Finalmente, si L'' es la lista final, mediante una sucesión de transformaciones elementales obtuvimos:

$$|\mathcal{P}| = \sum_{l \in L} l \geqslant \sum_{l'' \in L''} l'' \geqslant f(L'', d_1)d_1 + \cdots + f(L'', d_{m_L})d_{m_L}$$

Si $12 \nmid n$, o $8 \mid n$ o $9 \mid n$,

$$|\mathcal{P}| \geqslant \sum_{i=1}^{r} b\,(p_i^{a_i})\,p_i^{a_i}.$$

En cambio, si $3 \parallel n$ y $4 \parallel n$,

$$|\mathcal{P}| \geqslant \left(\sum_{\substack{1 \leqslant i \leqslant r \\ p_i^{a_i} \neq 3,4}} b\left(p_i^{a_i}\right) p_i^{a_i} \right) + 4 \cdot 3 + 2 \cdot 4 = \left(\sum_{i=1}^{r} b\left(p_i^{a_i}\right) p_i^{a_i} \right) - 1$$

que es precisamente el resultado deseado. ■

Capítulo 5

El caso p-grupo

El objetivo principal de este capítulo es calcular $\beta(G)$ para todo G que sea $p-$grupo con $p \geqslant 11$, sin embargo de las demostraciones se podrán deducir cotas para $p = 5$ y $p = 7$. Los resultados preliminares de este capítulo son algunos originales y muchos otros extraídos de [Arl85], aunque parte de nuestro aporte fue completar sus demostraciones — que no están completas. En las demás secciones, todos los resultados — si bien tienen ideas inspiradas en los resultados de Arlinghaus — son originales.

Lo último que haremos es probar el siguiente resultado:

Teorema 5.0.1: Sea $\mathcal{P}$ un poset con $\mathrm{Aut}(\mathcal{P}) \simeq \prod_{i=1}^{n} \mathbb{Z}_{p^{a_i}}$ con p primo, y $a_i \geqslant a_j$ si $i \leqslant j$. Entonces, si $p \geqslant 5$, se cumple que:

$$|\mathcal{P}| \geqslant \sum_{i=1}^{n} 2p^{a_i}.$$

Con el fin de hacer más organizada la solución, vamos a probar algunos resultados y definiciones preliminares sobre permutaciones. Vamos a fijar $n \in \mathbb{N}$ y los enteros $a_1, \ldots, a_n$, que son arbitrarios, por el resto del capítulo.

5.1 Preliminares

En esta sección vamos a probar algunos resultados sobre permutaciones. Todas las permutaciones con las que trabajemos en esta sección serán sobre un conjunto C arbitrario.

Varios de los siguientes lemas y corolarios fueron demostrados o enunciados por Arlinghaus en [Arl85] y otros fueron agregados porque serán necesarios para las demostraciones de este capítulo. Concretamente, extrajimos el Lema 5.1.1 y sus corolarios, el Lema 5.1.12 y su corolario, la definición 5.1.10 y algunas ideas usadas en sus demostraciones que inspiraron parte de las nuestras a lo largo de este capítulo.

También, en esta sección completamos las demostraciones de todos los lemas que Arlinghaus no demostró o bien dejó con una demostración incompleta.

Vale la pena observar que, si bien los enunciados están demostrados para permutaciones en general, cuando trabajemos con un poset $\mathcal{P}$ con grupo de automorfismos $G = Aut(\mathcal{P})$ y $|G| = |C|$, podemos aplicar estos resultados a los elementos de G. Esto es porque, como mencionamos en capítulos anteriores, pensamos a los automorfismos embebidos en $\mathbb{S}_{|\mathcal{P}|}$, es decir, como permutaciones del conjunto subyacente de $\mathcal{P}$.

Lema 5.1.1 (Arlinghaus)**:** Sean g y h dos permutaciones de C que conmutan. Supongamos que g contiene un p^i—ciclo α y h contiene un p^j—ciclo β con $i \geqslant j$ tales que $|\mathcal{O}_\alpha \cap \mathcal{O}_\beta| = t \geqslant 1$. Entonces:

a) $t = p^k$, para cierto $0 \leqslant k \leqslant j$

b) g contiene p^i—ciclos $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_{p^{j-k}}$ y h contiene p^j—ciclos $\beta_1 = \beta, \beta_2, \ldots, \beta_{p^{i-k}}$, con $|\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{\beta_s}| = t$, para todo $1 \leqslant r \leqslant p^{j-k}$ y para todo $1 \leqslant s \leqslant p^{i-k}$. Más aún, estos ciclos quedan determinados por g, h y α (también por g, h y β).

Demostración. Empezamos probándolo para $t = 1$.
Vamos a etiquetar $\alpha = (1\ 2\ \cdots\ p^i)$ y vamos a suponer sin pérdida de la generalidad que $1 \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$. En ese caso, nos quedaría que $\beta = \left(1\ \ h\cdot 1\ \ h^2\cdot 1\ \ \cdots\ \ h^{p^j-1}\cdot 1\right)$. Definamos, para cada $1 \leqslant s \leqslant p^i$ y cada $1 \leqslant r \leqslant p^j$ los ciclos:

$$\alpha_r = \left(h^{r-1}\cdot 1\ \ h^{r-1}\cdot 2\ \ \cdots\ \ h^{r-1}\cdot p^i\right)$$
$$\beta_s = \left(s\ \ h\cdot s\ \ \cdots\ \ h^{p^j-2}\cdot s\ \ h^{p^j-1}\cdot s\right).$$

Empecemos viendo que α_r es un ciclo contenido en g para todo $1 \leqslant r \leqslant p^j$.
Para ver esto primero hay que ver que, dado un punto x de α_r, $g\cdot x$ es el siguiente elemento a x en el ciclo α_r. Si tomamos un punto arbitrario de α_r, $x = h^{r-1}\cdot w$ con $1 \leqslant w \leqslant p^k$, no es difícil notar que, por la conmutatividad de g y h y que α es un ciclo de g, $gh^{r-1}\cdot w = h^{r-1}g\cdot w = h^{r-1}\alpha\cdot w = h^{r-1}\cdot(w+1)$ donde $w+1$ debe ser visto módulo p^k.
Lo otro que debemos ver es que, para cada $1 \leqslant r \leqslant p^j$ los puntos de α_r son distintos dos a dos, pero esto es inmediato ya que para cualquier par $1 \leqslant w, w' \leqslant p^k$, $h^{r-1}\cdot w = h^{r-1}\cdot w'$ es equivalente a $w = w'$; se puede ver aplicando h^{1-r} a ambos lados. Por lo tanto, α_r es un ciclo contenido en g.

Observación 5.1.2: $h^m \cdot x$ toma valores distintos para cada $0 \leqslant m \leqslant p^j - 1$ y $1 \leqslant x \leqslant p^k$.

En efecto, si $1 \leqslant x, y \leqslant p^i$ y $h^m \cdot x = h^k \cdot y$ para algún par $0 \leqslant m, k \leqslant p^j - 1$, debe suceder que $m = k$ y $x = y$. Si no fuese así, tendríamos que $x = h^{k-m} \cdot y$ que, como α es un ciclo de g, equivale a $x = h^{k-m} g^{y-1} \cdot 1$, que gracias a la conmutatividad de g y h es $g^{-y+1} \cdot x = h^{k-m} \cdot 1$; pero esto es absurdo: como $x \in \mathcal{O}_\alpha$, entonces $\mathcal{O}_\beta \ni h^{m-k} \cdot 1 = g^{-y+1} \cdot x \in \mathcal{O}_\alpha$, pero 1 era el único punto que estaba en α y β a la vez, así que debe ser $m = k$.

Por definición de β_s, dado un elemento arbitrario y de β_s, $h \cdot y$ nos devuelve el siguiente elemento en β_s. Además, la observación anterior nos asegura que los elementos de β_s son distintos dos a dos. Por lo tanto, β_s es un ciclo contenido en h.

La observación anterior también nos asegura que, para todo $1 \leqslant r, r' \leqslant p^j$ y $1 \leqslant s \leqslant p^i$ vale $|\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{\beta_s}| = 1$ y además que $\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{\alpha_{r'}} = \emptyset$. Esto termina de probar el resultado.

Pasamos a probarlo para $t > 1$.
Vamos a etiquetar temporalmente $\alpha = (1\ 2\ \cdots\ p^i)$ y vamos a suponer sin pérdida de la generalidad que $1 \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$. Sea $m+1$ el menor entero mayor que 1 tal que $m+1 \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$. Si $n \in \mathbb{N}$ es tal que $h^n \cdot 1 = m + 1$, entonces $g^m \cdot 1 = h^n \cdot 1$.

Observación 5.1.3: Más aún, vale que $(h^n)^t \cdot x = (g^m)^t \cdot x$ para todo $x \in \mathcal{O}_\alpha$ y $t \in \mathbb{N}$.

En efecto, $g^{x+1} \cdot 1 = \alpha^{x+1} \cdot 1 = x$. Luego, esta igualdad equivale a $(h^n)^t \cdot g^{x+1} \cdot 1 = (g^m)^t \cdot g^{x+1} \cdot 1$, pero como g y h conmutan, esto es equivalente a $(h^n)^t \cdot 1 = (g^m)^t \cdot 1$.
Esta última igualdad podemos probarla por inducción en t. Por hipótesis vale para $t = 1$, así que supongamos que vale para algún $t_0 \in \mathbb{N}$ y vamos a probar que vale para $t = t_0 + 1$. Lo que debemos probar se puede reescribir como $h^n \cdot \left((h^n)^{t_0} \cdot 1\right) = g^m \cdot \left((g^m)^{t_0} \cdot 1\right)$, y esto es cierto gracias a la hipótesis inductiva y al hecho de que $(g^m)^{t_0} \cdot 1 \in \mathcal{O}_\alpha$.

Un caso particular de esta observación es que $(h^n)^t \cdot 1 = (g^m)^t \cdot 1$ para todo $t \in \mathbb{N}$.
Por lo tanto, h^n y g^m contienen un mismo ciclo γ con $1 \in \mathcal{O}_\gamma$ y $\mathcal{O}_\gamma \subseteq \mathcal{O}_\alpha \cap \mathcal{O}_\beta$; donde la última contención vale porque β está contenido en h y α está contenido en g. Como γ es un ciclo de α^m por ser un ciclo de g^m que no deja fijo al 1, $|\mathcal{O}_\gamma| = \frac{p^i}{mcd(m, p^i)} = p^k$ para algún $k \in \mathbb{N}$.

Como $m < p^i$, podemos escribir $m = d \cdot mcd(m, p^i) = d \cdot p^{i-k}$ con $mcd(d, p) = 1$.
Por lo tanto, mirando las etiquetas módulo p^i, tenemos que

$$\alpha^{p^{i-k}} = \prod_{r=1}^{p^{i-k}} \left(r\ \ r + p^{i-k}\ \ r + 2p^{i-k}\ \ \cdots\ \ r + (p^k - 1)p^{i-k}\right)$$

y luego, elevando a la d ambos lados, tenemos que

$$\alpha^m = \prod_{r=1}^{p^{i-k}} \left(r\ \ r + p^{i-k}\ \ r + 2p^{i-k}\ \ \cdots\ \ r + (p^k - 1)p^{i-k}\right)^d$$

donde los p^{i-k} ciclos que fueron elevados a la d, como d es coprimo con p, siguen siendo ciclos en los mismos puntos.

Observación 5.1.4: La minimalidad de m nos dice que $\mathcal{O}_\alpha \cap \mathcal{O}_\beta = \mathcal{O}_\gamma$.

En efecto, supongamos que existe $y \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$ con $y \notin \mathcal{O}_\gamma$; este punto debe pertenecer a un ciclo contenido en α^m de la forma $\left(r \;\; r+p^{i-k} \;\; r+2p^{i-k} \;\; \cdots \;\; r+(p^k-1)p^{i-k}\right)^d$ para algún $1 < r \leqslant p^{i-k}$, ya que el ciclo que contiene al 1 es γ. En particular, para algún $s \in \mathbb{N}$ se cumple que $y = (g^m)^s \cdot r = (h^n)^s \cdot r$; la última igualdad vale por la Observación 5.1.3. Pero esto implicaría que $r = (h^n)^{-s} \cdot y$ lo cual, como $y \in \mathcal{O}_\beta$, implica $r = (\beta^n)^{-s} \cdot y$; así que $r \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$, contradiciendo la minimalidad de $m = dp^{i-k}$.

Una vez probado esto, como γ es $\left(1 \;\; 1+p^{i-k} \;\; \cdots \;\; 1+(p^k-1)p^{i-k}\right)^d$, podemos asegurar que m es exactamente p^{i-k}. Por otro lado, como γ también está contenido en h^n, es $|\mathcal{O}_\gamma| = \frac{p^j}{mcd(n,p^j)}$; así que $mcd(n,p^j) = p^{j-k}$.

Observación 5.1.5: Podemos afirmar que si $g^t \cdot 1 \in \mathcal{O}_\gamma$ para algún $t \in \mathbb{N}$, entonces $p^{i-k} \mid t$.

Supongamos que no, entonces podríamos escribir $t = q \cdot mcd(t, p^{i-k})$ con $mcd(q,p) = 1$ y $mcd(t,p^{i-k}) < p^{i-k}$. Como $mcd(q,p) = 1$, existe un $q' \in \mathbb{N}$ tal que $qq' \equiv 1 \pmod{p^i}$ y

$$\left(g^t\right)^{q'} \cdot 1 = \alpha^{mcd(t,p^{i-k})qq'} \cdot 1 = \alpha^{mcd(t,p^{i-k})} \cdot 1 = g^{mcd(t,p^{i-k})} \cdot 1$$

contradiciendo la minimalidad de p^{i-k}.

Para lo que sigue, por comodidad, reetiquetamos los puntos de C de manera que la etiqueta 1 siga etiquetando el mismo punto y que $g^{p^{i-k}}$ contenga al ciclo $(1\,2\,3\,\ldots\,p^k)$; y, por lo tanto, $\mathcal{O}_\gamma = \{1, 2, \ldots, p^k\}$.
Ahora definimos, para cada $1 \leqslant s \leqslant p^{i-k}$ y para cada $1 \leqslant r \leqslant p^{j-k}$,

$$\alpha_r = \Big(h^{r-1} \cdot 1 \;\; h^{r-1}g \cdot 1 \;\cdots\; h^{r-1}g^{p^{i-k}-1} \cdot 1 \;\; h^{r-1} \cdot 2 \;\; h^{r-1}g \cdot 2 \;\cdots$$
$$\cdots \;\; h^{r-1}g^{p^{i-k}-1} \cdot 2 \;\cdots\; h^{r-1} \cdot p^k \;\; \cdots \; h^{r-1}g^{p^{i-k}-1} \cdot p^k\Big)$$

$$\beta_s = \Big(g^{s-1} \cdot 1 \;\; g^{s-1}h \cdot 1 \;\; \cdots \;\; g^{s-1}h^{p^j-1} \cdot 1\Big).$$

Veamos que los $\{\alpha_r\}_{1 \leqslant r \leqslant p^{j-k}}$ son efectivamente ciclos disjuntos contenidos en g.
Para ver esto primero hay que ver que, dado un punto x de α_r, $g \cdot x$ es el siguiente elemento a x en el ciclo α_r. Si tomamos un punto de la forma $x = h^{r-1}g^t \cdot w$ con $t < p^{i-k} - 1$ y $1 \leqslant w \leqslant p^k$, es fácil ver que $g \cdot x = h^{r-1}g^{t+1} \cdot w$, por lo que se cumple lo que necesitamos. Si, en cambio, es un punto de la forma $x = h^{r-1}g^{p^{i-k}-1} \cdot w$ para algún $1 \leqslant w \leqslant p^k$, podemos

ver que $g \cdot x = h^{r-1}g^{p^{i-k}} \cdot w = h^{r-1} \cdot (w+1)$ por cómo hicimos el reetiquetado; aquí $w+1$ es visto módulo p^k.

Lo otro que debemos ver es que todos los puntos de α_r son distintos dos a dos. Probaremos este hecho junto al hecho de que $\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{\alpha_{r'}} = \emptyset$ para todo par $1 \leqslant r, r' \leqslant p^{j-k}$ con $r \neq r'$.
Supongamos por un momento que, dados $1 \leqslant r, r' \leqslant p^{j-k}$, existen $0 \leqslant s, s' \leqslant p^{i-k} - 1$ y $1 \leqslant w, w' \leqslant p^k$ tales que $h^{r-1}g^s \cdot w = h^{r'-1}g^{s'} \cdot w'$. En ese caso, debería ocurrir que $h^{r-1}g^s g^{p^{i-k}(w-1)} \cdot 1 = h^{r'-1}g^{s'}g^{p^{i-k}(w'-1)} \cdot 1$.

Despejando, nos queda $\mathcal{O}_\beta \ni h^{r-r'} \cdot 1 = g^{s'-s+p^{i-k}(w'-w)} \cdot 1 \in \mathcal{O}_\alpha$; por lo que se trata de un punto de γ, y mirando el lado derecho esto nos dice que $p^{i-k} \mid s - s' + p^{i-k}(w - w')$. Luego, $p^{i-k} \mid s - s'$ y, como $|s - s'| < p^{i-k}$, es $s = s'$. Ahora, por la Observación 5.1.3, la igualdad es equivalente a $h^{r-r'} \cdot 1 = g^{p^{i-k}(w'-w)} \cdot 1 = h^{n(w-w')}$ y, despejando, nos queda $h^{r-r'+n(w'-w)} \cdot 1 = 1$. Como $1 \in \mathcal{O}_\beta$ — que es un p^j ciclo contenido en h — tenemos que $p^j \mid r - r' + n(w' - w)$ y en particular $p^{j-k} \mid r - r' + n(w' - w)$. Como $p^{j-k} \mid n$, esto se reduce a $p^{j-k} \mid r - r'$ pero, como $|r - r'| < p^{j-k}$, esto implica que $r = r'$.
Esto muestra que para cada $1 \leqslant r \leqslant p^{j-k}$ los puntos de α_r son distintos dos a dos, y que si $1 \leqslant r' \leqslant p^{j-k}$ con $r' \neq r$ entonces $\mathcal{O}_{\alpha_{r'}} \cap \mathcal{O}_{\alpha_r} = \emptyset$.

Veamos que los $\{\beta_s\}_{1 \leqslant s \leqslant p^{i-k}}$ son efectivamente ciclos contenidos en g.
Dado un elemento en β_s, por definición el siguiente proviene de aplicarle exactamente h. Además, los elementos de β_s son distintos dos a dos porque 1 es un punto de β — que justamente es un p^j—ciclo de h — así que $h^t \cdot 1$, en particular también $g^{s-1}h^t$, toma todos valores distintos para $0 \leqslant t \leqslant p^j - 1$.

Nos queda analizar $\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{\beta_s}$. Dados $1 \leqslant s \leqslant p^{i-k}$ y $1 \leqslant r \leqslant p^{j-k}$ fijos, supongamos que existen $0 \leqslant t \leqslant p^j - 1, 0 \leqslant t' \leqslant p^i - 1$ y $1 \leqslant w \leqslant p^k$ tales que $g^{s-1}h^t \cdot 1 = h^{r-1}g^{t'} \cdot w$. Esta igualdad es equivalente a $g^{s-t'-1} \cdot 1 = h^{r-t-1} \cdot w$. Como el lado izquierdo es un punto de α y el derecho un punto de β, se trata de un punto de γ; esto nos dice que $p^{i-k} \mid s - t' - 1$. Como $|s - t' - 1| < p^{i-k}$, debe ser $s = t' + 1$.

Volviendo a la ecuación, como $w = g^{p^{i-k}(w-1)} = h^{n(w-1)}$ nos queda que $1 = h^{r-t-1} \cdot w = h^{r-t-1+n(w-1)} \cdot 1$. Como $1 \in \mathcal{O}_\beta$, se cumple $p^j \mid r - t - 1 + n(w - 1)$.
En particular $p^{j-k} \mid r - t - 1 + n(w - 1)$. Como $p^{j-k} \mid n$, entonces $p^{j-k} \mid r - t - 1$, y como $|r - t - 1| < p^{j-k}$, debe ser $r = t + 1$.
Logramos probar que si la igualdad incial se cumple, entonces $t' = s - 1$ y $t = r - 1$, pero no es difícil notar (reemplazando) que si t y t' toman esos valores la igualdad se cumple; por lo tanto es una condición equivalente.
Todos los valores excepto w están fijos, por lo que podemos concluir que hay exactamente p^k puntos en $\mathcal{O}_\alpha \cap \mathcal{O}_\beta$ (uno por cada valor de w). ■

Corolario 5.1.6 (Arlinghaus)**:** Bajo las condiciones anteriores, $|\mathcal{O}_g \cap \mathcal{O}_h| \geqslant p^{i+j-k}$.

En general, a lo largo del capítulo, vamos a referirnos al *conjunto de puntos compartidos* proveniente de la intersección entre dos ciclos α y β como el conjunto que nos provee el lema anterior. Si lo llamamos S, sería $S = \bigcup_{r=1}^{p^{j-k}} \mathcal{O}_{\alpha_r} = \bigcup_{r=1}^{p^{i-k}} \mathcal{O}_{\beta_r}$.
Notemos que este conjunto queda determinado por g, h y α: como $\{\beta_r\}_{1 \leqslant r \leqslant p^{i-k}}$ son los únicos ciclos de h que mueven puntos de α, podemos decir que S es la unión de los complementos de los puntos fijos de todos los ciclos de h que mueven puntos de α.
De manera análoga también podemos ver que queda determinado por g, h y β.

Observación 5.1.7: Si $a = \prod_{r=1}^{p^{j-k}} \alpha_r$ y $b = \prod_{r=1}^{p^{i-k}} \beta_r$, como $g = ag'$ y $h = bh'$ — con g' y h' permutaciones disjuntas con S — la acción de $\langle a, b\rangle$ como permutaciones en C restringida a S es transitiva. En particular, la acción de $\langle g, h\rangle$ en C restringida a S es transitiva.

En efecto, dado cualquier par $x, y \in S$, si $x \in \mathcal{O}_{\alpha_r}$ e $y \in \mathcal{O}_{\beta_s}$, como $\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{\beta_s} \neq \emptyset$ y α_r es un ciclo contenido en g, existe $k_1 \in \mathbb{N}$ tal que $g^{k_1} x \in \mathcal{O}_{\beta_s}$. Finalmente, como β_s es un ciclo contenido en h, existe $k_2 \in \mathbb{N}$ tal que $h^{k_2} g^{k_1} x = y$.

Corolario 5.1.8 (Arlinghaus)**:** Si $k = j$, entonces

$$\prod_{r=1}^{p^{i-k}} \beta_r = \alpha^m$$

para algún $m = dp^{i-k}$ con $mcd(d, p) = 1$.

Demostración. Si miramos los ciclos formados al final de la demostración del Lema 5.1.1, podemos ver que nos queda, para cada $1 \leqslant s \leqslant p^{i-k}$,

$$\alpha = \Big(1 \quad g\cdot 1 \quad \cdots \quad g^{p^{i-k}-1}\cdot 1 \quad 2 \quad g\cdot 2 \quad \cdots \quad \cdots \quad g^{p^{i-k}-1}\cdot 2 \quad \cdots \quad p^k \quad g\cdot p^k \quad \cdots \quad g^{p^{i-k}-1}\cdot p^k\Big)$$

$$\beta_s = \Big(g^{s-1}\cdot 1 \quad g^{s-1}h\cdot 1 \quad g^{s-1}h^2\cdot 1 \quad \cdots \quad g^{s-1}h^{p^j-1}\cdot 1\Big).$$

Recordemos que $g^{p^{i-k}} \cdot 1 = h^n \cdot 1$ y que γ era el p^k—ciclo contenido en $g^{p^{i-k}}$ y h^n respectivamente que no deja fijo al 1.

Observación 5.1.9: n debe ser coprimo con p

Supongamos que no. En ese caso existiría $k' < k$ tal que $(h^n)^{p^{k'}} \cdot 1 = 1$.
Usando la Observación 5.1.3 obtenemos

$$\left(g^{p^{i-k}}\right)^{p^{k'}} \cdot 1 = (h^n)^{p^{k'}} \cdot 1 = 1$$

lo cual es absurdo pues $1 \in \mathcal{O}_\gamma$ y γ es un p^k—ciclo de $g^{p^{i-k}}$ con $k > k'$.

Ahora podemos asegurar que existe un $n' \in \mathbb{N}$ también coprimo con p de modo que $nn' \equiv 1 \pmod{p^j}$, y por lo tanto, como $1 \in \mathcal{O}_\beta$,

$$\left(g^{p^{i-k}}\right)^{n'} \cdot 1 = (h^n)^{n'} \cdot 1 = \beta^{nn'} \cdot 1 = \beta \cdot 1 = h \cdot 1.$$

Finalmente, dado $1 \leqslant s \leqslant p^{i-k}$, para todo $0 \leqslant t \leqslant p^j - 1$, usando que $g^{s-1+p^{i-k}n't} \cdot 1 \in \mathcal{O}_\alpha$ y, de forma inductiva, la igualdad $g^{p^{i-k}n'} \cdot 1 = h \cdot 1$, tenemos

$$\begin{aligned}\beta_s\left(g^{s-1}h^t \cdot 1\right) &= g^{s-1}h^{t+1} \cdot 1 = g^{s-1}g^{p^{i-k}n'(t+1)} \cdot 1 = g^{s-1+p^{i-k}n'(t+1)} \cdot 1 \\ &= g^{p^{i-k}n'} \cdot \left(g^{s-1+p^{i-k}n't} \cdot 1\right) = \alpha^{p^{i-k}n'} \cdot \left(g^{s-1+p^{i-k}n't} \cdot 1\right) \\ &= \alpha^{p^{i-k}n'} \cdot \left(g^{s-1}h^t \cdot 1\right)\end{aligned}$$

Observando que $\left|\mathcal{O}_{\alpha^{p^{i-k}n'}}\right| = \sum_{s=1}^{p^{i-k}} |\mathcal{O}_{\beta_s}|$ y tomando $d = n'$ podemos concluir. ■

Estos resultados motivan la siguiente definición:

Definición 5.1.10: Si se da la situación del Lema 5.1.1, y $k < j$, diremos que α y β tienen *intersección rara*.

Antes de empezar a lidiar con las intersecciones raras, vamos a ver algunos lemas que son, de algún modo, consecuencias del Lema 5.1.1.

Lema 5.1.11: Sean $f_1, f_2, \ldots, f_k$ permutaciones de C que conmutan dos a dos. Supongamos que existen ciclos $\eta_1, \eta_2, \ldots, \eta_k$ de modo que, para todo $1 \leqslant i \leqslant k$, η_i es un p^{l_i}—ciclo de f_i para algún $l_i \in \mathbb{N}$ y además $\mathcal{O}_{\eta_i} \cap \mathcal{O}_{\eta_{i+1}} \neq \emptyset$ para todo $1 \leqslant i \leqslant k-1$.

Entonces, cada punto de η_1 pertenece a algún p^{l_k}—ciclo de f_k.
Además, aplicando el mismo resultado a $f_k, f_{k-1}, \ldots, f_1$ tenemos que cada punto de η_k pertenece a algún p^{l_1}—ciclo de f_1.

Demostración. Vamos a probarlo por inducción en k.

Caso base $k = 2$**:** Como $\mathcal{O}_{\eta_1} \cap \mathcal{O}_{\eta_2} \neq \emptyset$, el Lema 5.1.1 aplicado a la intersección entre η_1 y η_2 como ciclos de f_1 y f_2 respectivamente nos dice que $|\mathcal{O}_{\eta_1} \cap \mathcal{O}_{\eta_2}| = p^a$ para algún $a \in \mathbb{N}$ y que existen p^{l_1}— ciclos de f_1 $\eta_1 = \tilde{\eta}_{1,1}, \ldots, \tilde{\eta}_{1,p^{l_2-a}}$ y p^{l_2}—ciclos de f_2 $\eta_2 = \tilde{\eta}_{2,1}, \ldots, \tilde{\eta}_{2,p^{l_1-a}}$ tales que $\bigcup_{r=1}^{p^{l_2-a}} \mathcal{O}_{\eta_{1,r}} = \bigcup_{s=1}^{p^{l_1-a}} \mathcal{O}_{\eta_{2,s}}$. Por lo tanto, cualquier punto de η_1 pertenece a algún p^{l_2}—ciclo de f_2 y cualquier punto de η_2 pertenece a algún p^{l_1}—ciclo de f_1, como queríamos.

Paso inductivo: Supongamos que el resultado vale para $k = k_0$ y veamos que vale para $k = k_0 + 1$. Sean $f_1, f_2, \dots, f_{k_0+1}$ permutaciones con ciclos $\eta_1, \dots, \eta_{k_0+1}$ tales que para todo $1 \leqslant i \leqslant k_0 + 1$, η_i es un p^{l_i}—ciclo de f_i para algún $l_i \in \mathbb{N}$ y además $\mathcal{O}_{\eta_i} \cap \mathcal{O}_{\eta_{i+1}}$ para todo $1 \leqslant i \leqslant k_0$. Por hipótesis inductiva aplicada a $f_2, \dots, f_{k_0+1}$ con los ciclos $\eta_2, \dots, \eta_{k_0+1}$, sabemos que cada punto de η_2 pertenece a algún $p^{l_{k_0+1}}$—ciclo de f_{k_0+1}. En particular, como $\mathcal{O}_{\eta_1} \cap \mathcal{O}_{\eta_2} \neq \emptyset$, debe suceder que $\mathcal{O}_{\eta_1} \cap \mathcal{O}_\delta \neq \emptyset$ para algún $p^{l_{k_0+1}}$—ciclo δ de f_{k_0+1}. Luego, aplicando el caso $k = 2$ a f_1 y f_{k_0+1} con los ciclos η_1 y δ, tenemos que cada punto de η_1 pertenece a algún $p^{l_{k_0+1}}$—ciclo de f_{k_0+1}, como queríamos. ∎

Antes de enunciar el siguiente lema, viene bien recordar que dado un conjunto X, un desarreglo de los puntos de X es una biyección $\phi : X \to X$ que no tiene puntos fijos.

Lema 5.1.12 (Arlinghaus)**:** Sean g, h, α y β como en el Lema 5.1.1, siendo S el conjunto de puntos compartidos. Sea f una permutación que conmuta con g y h y contiene un p^l—ciclo γ que cumple $|\mathcal{O}_\gamma \cap \mathcal{O}_\alpha| \geqslant 1$.

Entonces existe un conjunto T y un entero z con $S \subseteq T$, $|T| = p^{l-z}|S|$ y α_T, β_T y γ_T desarreglos de T tales que $g = \alpha_T g_3, h = \beta_T h_3$ y $f = \gamma_T f_3$ con α_T producto de p^i—ciclos, β_T producto de p^j—ciclos y γ_T producto de p^l—ciclos.

En particular, si $\gamma_T \notin \langle \alpha_T, \beta_T \rangle$, entonces $|T| \geqslant p|S|$.

Demostración. El Lema 5.1.11 con $k = 2$ aplicado a g y f con ciclos α y γ respectivamente nos dice, en particular, que $\mathcal{O}_\alpha \subseteq \mathcal{O}_f$. Sean $\beta_1, \dots, \beta_{p^{i-k}}$ los p^j- ciclos de h que cumplen $\bigcup_{s=1}^{p^{i-k}} \beta_s = S$ siendo $k \in \mathbb{N}$ el que cumple $|\mathcal{O}_\alpha \cap \mathcal{O}_\beta| = p^k$.
Para cada $1 \leqslant s \leqslant p^{i-k}$, como $\mathcal{O}_\alpha \cap \mathcal{O}_{\beta_s} \neq \emptyset$, aplicamos el Lema 5.1.11 con $k = 3$ a h, g, f con ciclos β_s, α y γ respectivamente. Esto nos dice que, para todo $1 \leqslant s \leqslant p^{i-k}$, cada punto de β_s pertenece a algún p^l—ciclo de f. En particular, como $S = \bigcup_{s=1}^{p^{i-k}} \mathcal{O}_{\beta_s}$, nos dice que cualquier punto de S pertenece a algún p^l—ciclo de f.
Consideramos

$$\Gamma = \{\delta \ : \ \delta \text{ es un } p^l\text{—ciclo de } f \text{ con } \mathcal{O}_\delta \cap S \neq \emptyset\}.$$

Para cualquier ciclo $\delta \in \Gamma$, existe s_0 tal que $\mathcal{O}_\delta \cap \mathcal{O}_{\beta_{s_0}} \neq \emptyset$; y una aplicación del Lema 5.1.11 a h y f con ciclos β_{s_0} y δ nos dice que cada punto de δ pertenece a algún p^j—ciclo de h. Luego, si también consideramos

$$B_2 = \{\eta \ : \ \eta \text{ es un } p^j\text{—ciclo de } h \text{ con } \mathcal{O}_\eta \cap \mathcal{O}_\delta \neq \emptyset \text{ para algún } \delta \in \Gamma\}$$

podemos afirmar que $\bigcup_{\delta \in \Gamma} \mathcal{O}_\delta \subseteq \bigcup_{\eta \in B_2} \mathcal{O}_\eta$.

Además, si consideramos

$$B_1 = \{\epsilon \ : \ \epsilon \text{ es un } p^i\text{—ciclo de } h \text{ con } \mathcal{O}_\epsilon \cap \mathcal{O}_\delta \neq \emptyset \text{ para algún } \delta \in \Gamma\}.$$

Dado $\delta \in \Gamma$, como $S \subseteq \mathcal{O}_g$, existe ϵ un p^i—ciclo de g tal que $\mathcal{O}_\delta \cap \mathcal{O}_\epsilon \neq \emptyset$, en particular $\epsilon \in B_1$. Aplicando el Lema 5.1.11 a f y g con ciclos δ y ϵ respectivamente, deducimos que cada punto de δ pertenece a algún p^i—ciclo de g y, más aún, pertenece a algún p^i—ciclo en B_1, ya que todos estos p^i—ciclos tienen intersección no vacía con δ. Esto nos dice que $\bigcup_{\delta\in\Gamma} \mathcal{O}_\delta \subseteq \bigcup_{\epsilon\in B_1} \mathcal{O}_\epsilon$.

Probemos las inclusiones opuestas.
Definimos $b_1 = i$ y $b_2 = j$ y tomamos $t \in \{1, 2\}$ arbitrario.
Dado $\rho \in B_t$, existe $\delta_0 \in \Gamma$ tal que $\mathcal{O}_\rho \cap \mathcal{O}_{\delta_0} \neq \emptyset$. Aplicar el Lema 5.1.1 a la intersección de ρ y δ_0 como ciclos de h y f respectivamente, asegura que $|\mathcal{O}_\rho \cap \mathcal{O}_{\delta_0}| = p^{k'}$ para algún $k' \in \mathbb{N}_0$ y que existen p^{b_t}—ciclos $\rho = \rho_1, \rho_2, \ldots, \rho_{p^{l-k'}}$ y p^l—ciclos $\delta_0 = \delta_1, \delta_2, \ldots, \delta_{p^{b_t-k'}}$ con $|\mathcal{O}_{\rho_r} \cap \mathcal{O}_{\delta_s}| = p^{k'}$ y $\bigcup_{r=1}^{p^{l-k'}} \mathcal{O}_{\rho_r} = \bigcup_{s=1}^{p^{b_t-k'}} \mathcal{O}_{\delta_s}$, para todo $1 \leqslant r \leqslant p^{l-k'}$ y $1 \leqslant s \leqslant p^{b_t-k'}$.
Como $\mathcal{O}_{\delta_0} \cap S \neq \emptyset$, deberá existir $1 \leqslant r_0 \leqslant p^{l-k'}$ tal que $\mathcal{O}_{\rho_{r_0}} \cap S \neq \emptyset$, más aún, por la definición de S sería $\mathcal{O}_{\rho_{r_0}} \subseteq S$. Como cada uno de los δ_s con $1 \leqslant s \leqslant p^{b_t-k'}$ comparte puntos con ρ_{r_0}, terminamos probando que $\delta_s \cap S \neq \emptyset$, y por lo tanto $\delta_s \in \Gamma$, para todo $1 \leqslant s \leqslant p^{b_t-k'}$ como queríamos. Esto termina de probar $\bigcup_{\delta\in\Gamma} \mathcal{O}_\delta = \bigcup_{\rho\in B_t} \mathcal{O}_\rho$.

Como los ciclos contenidos en una misma permutación son disjuntos, tomamos

$$\begin{aligned} T &= \bigcup_{\delta\in\Gamma} \mathcal{O}_\delta = \bigcup_{\eta\in B} \mathcal{O}_\eta = \bigcup_{\epsilon\in A} \mathcal{O}_\epsilon \supseteq S \\ \alpha_T &= \prod_{\epsilon\in A} \epsilon \\ \beta_T &= \prod_{\eta\in B} \eta \\ \gamma_T &= \prod_{\delta\in\Gamma} \delta \end{aligned}$$

y los proponemos como candidatos para el resultado final.

Veamos que la acción de $\langle \alpha_T, \beta_T, \gamma_T \rangle$ es transitiva en T. Tomemos dos puntos $x, y \in T$ arbitrarios y vamos a probar que existe $q \in \langle \alpha_T, \beta_T, \gamma_T \rangle$ tal que $q \cdot x = y$.
Como $x, y \in T$, existen ciclos $\delta_x, \delta_y \in \Gamma$ tales que $x \in \mathcal{O}_{\delta_x}$ e $y \in \mathcal{O}_{\delta_y}$.
Por definición de Γ, existe s_x tal que $\delta_x^{s_x} \cdot x \in S$; y como la acción de $\langle g, h \rangle$ es transitiva en S y $\mathcal{O}_{\delta_y} \cap S \neq \emptyset$, existen $a, b \in \mathbb{N}$ tales que $g^a h^b \cdot (\delta_x^{s_x} \cdot x) \in \mathcal{O}_{\delta_y}$.
Luego, existe $s_y \in \mathbb{N}$ tal que $y = \delta_y^{s_y} \cdot \left(g^a h^b \cdot (\delta_x^{s_x} \cdot x)\right) = \gamma_T^{s_y} \alpha_T^a \beta_T^b \gamma_T^{s_x} \cdot x$.
Tomando $q = \gamma_T^{s_y} \alpha_T^a \beta_T^b \gamma_T^{s_x}$ obtenemos el resultado deseado.

Para terminar de probar lo que falta, tenemos que inspeccionar un poco más.
Vamos a etiquetar $\gamma = (1\ 2\ \cdots\ p^l)$ y vamos a suponer sin pérdida de la generalidad que $1 \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta \cap \mathcal{O}_\gamma$ (si $\mathcal{O}_\gamma \cap \mathcal{O}_\beta = \emptyset$, cambiamos a β por algún ciclo $\overline{\beta}$ de h que contenga un punto de $\mathcal{O}_\alpha \cap \mathcal{O}_\gamma \neq \emptyset$).

Definimos $m+1$ como el menor entero mayor que 1 tal que $\mathcal{O}_\gamma \cap S \neq \emptyset$; si sucede que $\mathcal{O}_\gamma \cap S = \{1\}$ definimos $m = p^l$. Como $\langle g, h\rangle$ actúa transitivamente sobre S, debe existir una permutación $c \in \langle g, h\rangle$ de modo que $c \cdot 1 = f^m \cdot 1$.

Observación 5.1.13: Más aún, vale que $c^t \cdot x = (f^m)^t \cdot x$ para todo $x \in S$ y $t \in \mathbb{N}$.

En efecto, como la acción de $\langle g, h\rangle$ es transitiva en S, existen exponentes $e_1, e_2 \in \mathbb{N}$ tales que $g^{e_1}h^{e_2} \cdot 1 = x$. Luego, esta igualdad equivale a $c^t \cdot g^{e_1}h^{e_2} \cdot 1 = (f^m)^t \cdot g^{e_1}h^{e_2} \cdot 1$, pero como c, f, h y g conmutan dos a dos esto es equivalente a $c^t \cdot 1 = (f^m)^t \cdot 1$.
Esta última igualdad podemos probarla por inducción en t. Por hipótesis vale para $t = 1$, así que supongamos que vale para algún $t_0 \in \mathbb{N}$ y vamos a probar que vale para $t = t_0 + 1$. Lo que debemos probar se puede reescribir como $c \cdot (c^{t_0} \cdot 1) = f^m \cdot \left((f^m)^{t_0} \cdot 1\right)$, por hipótesis inductiva es $c \cdot (c^{t_0} \cdot 1) = f^m \cdot (c^{t_0} \cdot 1)$ y es cierto por conmutatividad e hipótesis inicial.

Como consecuencia de esta observación tenemos que tanto c como f^m contienen un mismo ciclo $\tilde{\gamma}$ que no deja fijo al 1, de modo que $\mathcal{O}_{\tilde{\gamma}} \subseteq \mathcal{O}_\gamma \cap S$. Por supuesto, como $\tilde{\gamma}$ es un ciclo de γ^m por ser un ciclo de f^m que no deja fijo al 1, $|\mathcal{O}_{\tilde{\gamma}}| = \frac{p^l}{mcd(m,p^l)} = p^z$ para algún $z \in \mathbb{N}_0$.

Como $m \leqslant p^l$, podemos escribir $m = d \cdot mcd(m, p^l) = d \cdot p^{l-z}$ con $mcd(d, p) = 1$.
Por lo tanto, mirando las etiquetas módulo p^l, tenemos que

$$\gamma^{p^{l-z}} = \prod_{r=1}^{p^{l-z}} \left(r \;\; r + p^{l-z} \;\; r + 2p^{l-z} \;\; \cdots \;\; r + (p^z - 1)p^{l-z}\right)$$

y luego, elevando a la d ambos lados, tenemos que

$$\gamma^m = \prod_{r=1}^{p^{l-z}} \left(r \;\; r + p^{l-z} \;\; r + 2p^{l-z} \;\; \cdots \;\; r + (p^z - 1)p^{l-z}\right)^d$$

donde los p^{l-z} ciclos que fueron elevados a la d, como d es coprimo con p, siguen siendo ciclos en los mismos puntos.

Observación 5.1.14: La minimalidad de m nos dice que $\mathcal{O}_\gamma \cap S = \mathcal{O}_{\tilde{\gamma}}$.

Supongamos que existe $y \in \mathcal{O}_\gamma \cap S$ con $y \notin \mathcal{O}_{\tilde{\gamma}}$; este punto debe pertenecer a un ciclo contenido en γ^m de la forma $\left(r \;\; r + p^{l-z} \;\; r + 2p^{l-z} \;\; \cdots \;\; r + (p^z - 1)p^{l-z}\right)^d$ con $1 < r < p^{l-z}$. En particular, para algún $s \in \mathbb{N}$ se cumple que $y = (f^m)^s \cdot r = c^s \cdot r$, pero esto implicaría que $r = c^{-s} \cdot y$ lo cual, como $c^{-s} \cdot y \in S$ por ser $y \in S$, implica que $r \in \mathcal{O}_\gamma \cap S$; contradiciendo la minimalidad de m.

Una vez probado esto, como $\tilde{\gamma}$ es $\left(1 \;\; 1 + p^{l-z} \;\; \cdots \;\; 1 + (p^z - 1)p^{l-z}\right)^d$, podemos asegurar que m es exactamente p^{l-z}.

Observación 5.1.15: Dado $x \in S$, $f^t \cdot x \in S$ si y sólo si $p^{l-z} \mid t$.

Para la ida, como la acción de $\langle g, h\rangle$ es transitiva en S, existe $c' \in \langle g, h\rangle$ tal que $c' \cdot 1 = x$. Como c' y f conmutan y $f^t \cdot x \in S$, tenemos que $(c')^{-1} f^t \cdot x = f^t \cdot 1 \in S$. Supongamos que $p^{l-z} \nmid t$ y escribimos $t = \tilde{d} \cdot mcd(t, p^{l-z})$ con $mcd\left(\tilde{d}, p\right) = 1$ y $mcd(t, p^{l-z}) < p^{l-z}$.
Como $mcd\left(\tilde{d}, p\right) = 1$, existe un $\tilde{d}' \in \mathbb{N}$ tal que $\tilde{d}\tilde{d}' \equiv 1 \pmod{p^l}$ y

$$\left(f^t\right)^{\tilde{d}'} \cdot 1 = \gamma^{mcd(t,p^{l-z})\tilde{d}\tilde{d}'} \cdot 1 = \gamma^{mcd(t,p^{l-z})} \cdot 1 = f^{mcd(t,p^{l-z})} \cdot 1$$

contradiciendo la minimalidad de p^{l-z}.
Para la vuelta, si $t = p^{l-z}t'$ con $t' \in \mathbb{N}_0$, $f^t \cdot x = \left(f^{p^{l-z}}\right)^{t'} \cdot x = c^{t'} \cdot x \in S$.

Notemos que, como T está conformado por todos los p^l—ciclos de f que intersecan con S,

$$T = \{f^t \cdot x : 1 \leqslant t \leqslant p^l,\ x \in S\} = \bigcup_{x \in S} \{f^t \cdot x : 1 \leqslant t \leqslant p^l\}.$$

Por la Observación 5.1.15, podemos notar que para cada $x_0 \in S$ hay exactamente $\frac{p^l}{p^{l-z}} = p^z$ elementos $x \in S$ tales que $x_0 \in \{f^t \cdot x : 1 \leqslant t \leqslant p^l\}$. Luego $|T| = \frac{p^l p^{i+j-k}}{p^z} = p^{l-z}|S|$.

Finalmente, supongamos que $\gamma_T \notin \langle \alpha_T, \beta_T\rangle$ y veamos que $|T| \geqslant p|S|$.
Supongamos, a modo de contradicción, que $|T| = |S|$ — que como está uno contenido en el otro, implica $T = S$. En ese caso, como $\mathcal{O}_\gamma \subseteq T = S$, debe ser $m = 1$.
Por lo tanto, se cumple que $c \cdot x = f \cdot x$ para todo $x \in S = T$. Esto, como $c = g^a h^b$ para algún par $a, b \in \mathbb{N}$, es equivalente a $\alpha_T^a \beta_T^b \cdot x = \gamma_T \cdot x$ para todo $x \in S = T$.
Como $\mathcal{O}_{\alpha_T^a \beta_T^b} \subseteq \mathcal{O}_{\alpha_T} \cup \mathcal{O}_{\beta_T} = T = S$, concluimos que $\alpha_T^a \beta_T^b = \gamma_T$; pero esto es absurdo.
Luego, debe suceder que $|T| > |S|$ y, $|T|$ es potencia de p, es $|T| \geqslant p|S|$ como queríamos. ■

Podemos probar usando las mismas ideas el siguiente corolario.

Corolario 5.1.16 (Arlinghaus)**:** Sean $f_1, \dots, f_k$ permutaciones de C que conmutan dos a dos, de modo que para todo $1 \leqslant i \leqslant k-1$:

- $f_i = \gamma_{T_{k-1}^{(i)}} f_i'$ con f_i' una permutación disjunta con T_{k-1}.
- $\gamma_{T_{k-1}^{(i)}}$ es producto de p^{b_i}—ciclos para algún $b_i \in \mathbb{N}$ y $\mathcal{O}_{\gamma_{T_{k-1}^{(i)}}} = T_{k-1}$.
- La acción de $\left\langle \gamma_{T_{k-1}}^{(1)}, \dots, \gamma_{T_{k-1}}^{(k-1)} \right\rangle$ como permutaciones en C restringida a T_{k-1} es transitiva.

Si ρ es un p^{b_k}—ciclo de f_k con $b_k \in \mathbb{N}$ que cumple $\mathcal{O}_\rho \cap T_{k-1} \neq \emptyset$, entonces existe un conjunto $T_k \supseteq T_{k-1}$ de manera que para todo $1 \leqslant i \leqslant k$:

- $f_i = \gamma_{T_k^{(i)}} f_i''$ con f_i'' una permutación disjunta con T_k.
- $\gamma_{T_k^{(i)}}$ es producto de p^{b_i}—ciclos y $\mathcal{O}_{\gamma_{T_k^{(i)}}} = T_k$.
- La acción de $\left\langle \gamma_{T_k}^{(1)}, \dots, \gamma_{T_k}^{(k)} \right\rangle$ como permutaciones en C restringida a T_k es transitiva.

Más aún, si $\gamma_{T_k}^{(k)} \notin \left\langle \gamma_{T_k}^{(1)}, \dots, \gamma_{T_k}^{(k-1)} \right\rangle$, tenemos que $|T_k| \geqslant p|T_{k-1}|$.

Demostración. Comenzaremos viendo que cada punto de T_{k-1} pertenece a algún p^{b_k}—ciclo de f_k. Sea $y \in T_{k-1}$ arbitrario y tomemos un punto x de ρ. Como $\mathcal{O}_\rho \cap T_{k-1} \neq \emptyset$, sabemos que existe s_x de modo que $f_k^{s_x} \cdot x \in T_{k-1}$. Además, como la acción de $\langle f_1, \dots, f_{k-1} \rangle$ es transitiva en T_{k-1} — por serlo la acción de $\left\langle \gamma_{T_{k-1}}^{(1)}, \dots, \gamma_{T_{k-1}}^{(k-1)} \right\rangle$ — existen $1 \leqslant i_1, \dots, i_N \leqslant k-1$ distintos y $s_1, \dots, s_N \in \mathbb{N}$ tales que

$$y = \left(\prod_{r=1}^{N} f_{i_r}^{s_r} \right) \cdot (f_k^{s_x} \cdot x) = \left(\prod_{r=1}^{N} \epsilon_r^{s_r} \right) \cdot (\rho^{s_x} \cdot x)$$

donde ϵ_r es un ciclo de f_{i_r} con $\mathcal{O}_{\epsilon_r} \subseteq T_{k-1}$ para todo $1 \leqslant r \leqslant N$.
Esto quiere decir que $y \in \mathcal{O}_{\epsilon_1}$, que para todo $1 \leqslant r \leqslant N-1$ es $\mathcal{O}_{\epsilon_r} \cap \mathcal{O}_{\epsilon_{r+1}} \neq \emptyset$, y que $\mathcal{O}_{\epsilon_N} \cap \mathcal{O}_\rho \neq \emptyset$. Luego, aplicando el Lema 5.1.11 a $f_{i_1}, \dots, f_{i_N}$ y f_k con ciclos $\epsilon_1, \dots, \epsilon_N$ y ρ respectivamente, tenemos que cada punto de ϵ_1 pertenece a algún p^{b_k}—ciclo de f_k; en particular, y pertenece a un p^{b_k}—ciclo de f_k. Como $y \in T_{k-1}$ es arbitrario, probamos lo que queríamos.

Consideramos

$$\Gamma = \left\{ \delta \,:\, \delta \text{ es un } p^{b_k}\text{—ciclo de } f_k \text{ con } \mathcal{O}_\delta \cap T_{k-1} \neq \emptyset \right\}.$$

Fijamos $1 \leqslant i \leqslant k-1$ arbitrario. Para cualquier ciclo $\delta \in \Gamma$, existe un p^{b_i}—ciclo β de f_i tal que $\mathcal{O}_\delta \cap \mathcal{O}_\beta \neq \emptyset$; y una aplicación del Lema 5.1.11 a f_i y f_k con ciclos β y δ nos dice que cada punto de δ pertenece a algún p^{b_i}—ciclo de f_i. Luego, si también consideramos

$$B_i = \{\eta \ : \ \eta \text{ es un } p^{b_i}\text{—ciclo de } f_i \text{ con } \mathcal{O}_\eta \cap \mathcal{O}_\delta \neq \emptyset \text{ para algún } \delta \in \Gamma \ \}$$

podemos afirmar que $\bigcup_{\delta\in\Gamma} \mathcal{O}_\delta \subseteq \bigcup_{\eta\in B_i} \mathcal{O}_\eta$. Probemos la otra inclusión.

Dado $\eta \in B$, existe $\delta_0 \in \Gamma$ tal que $\mathcal{O}_\eta \cap \mathcal{O}_{\delta_0} \neq \emptyset$. Aplicando el Lema 5.1.1 a la intersección de η y δ_0 como ciclos de f_i y f_k respectivamente, tenemos que $|\mathcal{O}_\eta \cap \mathcal{O}_{\delta_0}| = p^{a'}$ para algún $a' \in \mathbb{N}$ y que existen p^{b_i}—ciclos $\eta = \eta_1, \eta_2, \ldots, \eta_{p^{b_k-a'}}$ y p^{b_k}—ciclos $\delta_0 = \delta_1, \delta_2, \ldots, \delta_{p^{b_i-a'}}$ de modo que $|\mathcal{O}_{\eta_r} \cap \mathcal{O}_{\delta_s}| = p^{a'}$, para todo $1 \leqslant r \leqslant p^{b_k-a'}$ y para todo $1 \leqslant s \leqslant p^{b_i-a'}$.
Como $\mathcal{O}_{\delta_0} \cap T_{k-1} \neq \emptyset$, deberá existir $1 \leqslant r_0 \leqslant p^{b_k-a'}$ tal que $\mathcal{O}_{\eta_{r_0}} \cap T_{k-1} \neq \emptyset$, más aún, por la definición de T_{k-1} sería $\mathcal{O}_{\eta_{r_0}} \subseteq T_{k-1}$. Como cada uno de los δ_s con $1 \leqslant s \leqslant p^{b_i-a'}$ comparte puntos con η_{r_0}, terminamos probando que $\delta_s \cap T_{k-1} \neq \emptyset$ y, por lo tanto, $\delta_s \in \Gamma$, para todo $1 \leqslant s \leqslant p^{b_i-a''}$ como queríamos. Esto termina de probar $\bigcup_{\delta\in\Gamma} \mathcal{O}_\delta = \bigcup_{\eta\in B_i} \mathcal{O}_\eta$.

Como los ciclos contenidos en una misma permutación son disjuntos, tomamos

$$T_k = \bigcup_{\delta\in\Gamma} \mathcal{O}_\delta = \bigcup_{\eta\in B_i} \mathcal{O}_\eta \supseteq T_{k-1} \quad \text{para todo } i = 1, 2, \ldots, k-1$$

$$\gamma_{T_k}^{(i)} = \prod_{\eta\in B_i} \eta \quad \text{para todo } i = 1, 2, \ldots, k-1$$

y los proponemos como candidatos para el resultado final.

Veamos que la acción de $\left\langle \gamma_{T_k}^{(1)}, \ldots, \gamma_{T_k}^{(k)} \right\rangle$ es transitiva en T_k. Tomemos dos puntos $x, y \in T_k$ arbitrarios y vamos a probar que existe $q \in \left\langle \gamma_{T_k}^{(1)}, \ldots, \gamma_{T_k}^{(k)} \right\rangle$ tal que $q \cdot x = y$.
Como $x, y \in T_k$, existen ciclos $\delta_x, \delta_y \in \Gamma$ tales que $x \in \mathcal{O}_{\delta_x}$ e $y \in \mathcal{O}_{\delta_y}$.
Por definición de Γ, existe s_x tal que $\delta_x^{s_x} \cdot x \in T_{k-1}$; y como la acción de $\langle f_1, \ldots, f_{k-1}\rangle$ es transitiva en T_{k-1} y $\mathcal{O}_{\delta_y} \cap T_{k-1} \neq \emptyset$, existen $l_1, \ldots, l_{k-1} \in \mathbb{N}$ tales que

$$\prod_{i=1}^{k-1} (f_i)^{l_i} \cdot (\delta_x^{s_x} \cdot x) \in \mathcal{O}_{\delta_y}.$$

Luego, existe $s_y \in \mathbb{N}$ tal que

$$y = \delta_y^{s_y} \cdot \left(\prod_{i=1}^{k-1} (f_i)^{l_i} \cdot (\delta_x^{s_x} \cdot x) \right) = \left(\gamma_{T_k}^{(k)}\right)^{s_y} \prod_{i=1}^{k-1} \left(\gamma_{T_k}^{(i)}\right)^{l_i} \left(\gamma_{T_k}^{(k)}\right)^{s_x} \cdot x.$$

Tomando $q = \left(\gamma_{T_k}^{(k)}\right)^{s_y} \prod_{i=1}^{k-1} \left(\gamma_{T_k}^{(i)}\right)^{l_i} \left(\gamma_{T_k}^{(k)}\right)^{s_x}$ obtenemos el resultado deseado.

Para terminar, vamos a probar que si $\gamma_{T_k}^{(k)} \notin \left\langle \gamma_{T_k}^{(1)}, \dots, \gamma_{T_k}^{(k-1)} \right\rangle$ entonces $|T_k| \geqslant p|T_{k-1}|$.
Vamos a etiquetar $\rho = (1\ 2\ \cdots\ p^{b_k})$ y vamos a suponer sin pérdida de la generalidad que $1 \in \mathcal{O}_\rho \cap T_{k-1}$
Definimos $m+1$ como el menor entero mayor que 1 tal que $\mathcal{O}_\rho \cap T_{k-1} \neq \emptyset$; si sucede que $\mathcal{O}_\rho \cap T_{k-1} = \{1\}$ definimos $m = p^{b_k}$. Como $\langle f_1, \dots, f_{k-1}\rangle$ actúa transitivamente sobre T_{k-1}, debe existir una permutación $c \in \langle f_1, \dots, f_{k-1}\rangle$ de modo que $c \cdot 1 = f_k^m \cdot 1$.

Observación 5.1.17: Más aún, vale que $c^t \cdot x = (f_k^m)^t \cdot x$ para todo $x \in T_{k-1}$ y $t \in \mathbb{N}$.

En efecto, como la acción de $\langle f_1, \dots, f_{k-1}\rangle$ es transitiva en T_{k-1}, existen $e_1, \dots, e_{k-1} \in \mathbb{N}_0$ tales que, llamando $\tilde{c} = \prod_{i=1}^{k-1} f_i^{e_i}$, vale $\tilde{c} \cdot 1 = x$. Luego, esta igualdad equivale a $c^t \cdot \tilde{c} \cdot 1 = (f_k^m)^t \cdot \tilde{c} \cdot 1$, pero como $f_1, \dots, f_k$ y c conmutan dos a dos — y por lo tanto también conmutan con $\tilde{c}$ — esto es equivalente a $c^t \cdot 1 = (f_k^m)^t \cdot 1$.
Esta última igualdad podemos probarla por inducción en t. Por hipótesis vale para $t = 1$, así que supongamos que vale para algún $t_0 \in \mathbb{N}$ y vamos a probar que vale para $t = t_0 + 1$. Lo que debemos probar se puede reescribir como $c \cdot (c^{t_0} \cdot 1) = f_k^m \cdot \left((f_k^m)^{t_0} \cdot 1\right)$, por hipótesis inductiva es $c \cdot (c^{t_0} \cdot 1) = f_k^m \cdot (c^{t_0} \cdot 1)$ y es cierto por conmutatividad e hipótesis inicial.

Como consecuencia de esta observación tenemos que tanto c como f_k^m contienen un mismo ciclo $\tilde{\rho}$ que no deja fijo al 1, de modo que $\mathcal{O}_{\tilde{\rho}} \subseteq \mathcal{O}_\gamma \cap T_{k-1}$. Por supuesto, como $\tilde{\rho}$ es un ciclo de ρ^m por ser un ciclo de f_k^m que no deja fijo al 1, $|\mathcal{O}_{\tilde{\rho}}| = \frac{p^{b_k}}{mcd(m, p^{b_k})} = p^z$ para algún $z \in \mathbb{N}_0$.

Como $m \leqslant p^{b_k}$, podemos escribir $m = d \cdot mcd(m, p^{b_k}) = d \cdot p^{b_k - z}$ con $mcd(d, p) = 1$.
Por lo tanto, mirando las etiquetas módulo p^{b_k}, tenemos que

$$\rho^{p^{b_k - z}} = \prod_{r=1}^{p^{b_k - z}} \left(r\ \ r + p^{b_k - z}\ \ r + 2p^{b_k - z}\ \ \cdots\ \ r + (p^z - 1)p^{b_k - z}\right)$$

y luego, elevando a la d ambos lados, tenemos que

$$\rho^m = \prod_{r=1}^{p^{b_k - z}} \left(r\ \ r + p^{b_k - z}\ \ r + 2p^{b_k - z}\ \ \cdots\ \ r + (p^z - 1)p^{b_k - z}\right)^d$$

donde los $p^{b_k - z}$ ciclos que fueron elevados a la d, como d es coprimo con p, siguen siendo ciclos en los mismos puntos.

Observación 5.1.18: La minimalidad de m nos dice que $\mathcal{O}_\rho \cap T_{k-1} = \mathcal{O}_{\tilde{\rho}}$.

Supongamos que existe $y \in \mathcal{O}_\rho \cap T_{k-1}$ con $y \notin \mathcal{O}_{\tilde{\rho}}$; este punto debe pertenecer a un ciclo contenido en ρ^m de la forma $\left(r\ \ r + p^{b_k - z}\ \ r + 2p^{b_k - z}\ \ \cdots\ \ r + (p^z - 1)p^{b_k - z}\right)^d$ con $1 < r < p^{b_k - z}$. En particular, para algún $s \in \mathbb{N}$ se cumple que $y = (f_k^m)^s \cdot r = c^s \cdot r$, pero esto implicaría que $r = c^{-s} \cdot y$ lo cual, como $c^{-s} \cdot y \in T_{k-1}$, implica que $r \in \mathcal{O}_\rho \cap T_{k-1}$; contradiciendo la minimalidad de m.

Una vez probado esto, como $\tilde{\rho}$ es $\begin{pmatrix} 1 & 1+p^{b_k-z} & \cdots & 1+(p^z-1)p^{b_k-z} \end{pmatrix}^d$, podemos asegurar que m es exactamente p^{b_k-z}.

Observación 5.1.19: Dado $x \in T_{k-1}$, $f_k^t \cdot x \in T_{k-1}$ si y sólo si $p^{b_k-z} \mid t$.

Para la ida, como la acción de $\langle f_1, \dots, f_{k-1} \rangle$ es transitiva en T_{k-1}, existe $c' \in \langle f_1, \dots, f_{k-1} \rangle$ tal que $c' \cdot 1 = x$. Como c' y f_k conmutan y $f_k^t \cdot x \in T_{k-1}$, tenemos que $(c')^{-1} f_k^t \cdot x = f_k^t \cdot 1 \in T_{k-1}$. Supongamos que $p^{b_k-z} \nmid t$ y escribimos $t = \tilde{d} \cdot mcd(t, p^{b_k-z})$ con $mcd\left(\tilde{d}, p\right) = 1$ y $mcd(t, p^{b_k-z}) < p^{b_k-z}$. Como $mcd\left(\tilde{d}, p\right) = 1$, existe $\tilde{d}' \in \mathbb{N}$ tal que $\tilde{d}\tilde{d}' \equiv 1 \pmod{p^{b_k}}$ y

$$\left(f_k^t\right)^{\tilde{d}'} \cdot 1 = \rho^{mcd(t,p^{b_k-z})\tilde{d}\tilde{d}'} \cdot 1 = \rho^{mcd(t,p^{b_k-z})} \cdot 1 = f_k^{mcd(t,p^{b_k-z})} \cdot 1$$

contradiciendo la minimalidad de p^{b_k-z}.
Para la vuelta, si $t = p^{b_k-z}t'$ con $t' \in \mathbb{N}_0$, $f_k^t \cdot x = \left(f_k^{p^{b_k-z}}\right)^{t'} \cdot x = c^{t'} \cdot x \in T_{k-1}$.

Notar que, como T_k consiste de los puntos de todos los p^{b_k}–ciclos de f_k que intersecan con T_{k-1} y $T_{k-1} \subseteq T_k$,

$$T_k = \{f_k^t \cdot x : 1 \leqslant t \leqslant p^{b_k},\ x \in T_{k-1}\} = \bigcup_{x \in T_{k-1}} \{f_k^t \cdot x : 1 \leqslant t \leqslant p^{b_k}\}.$$

Por la Observación 5.1.19, notar que para cada $x_0 \in T_{k-1}$ hay exactamente $\frac{p^{b_k}}{p^{b_k-z}} = p^z$ elementos $x \in T_{k-1}$ tales que $x_0 \in \{f^t \cdot x : 1 \leqslant t \leqslant p^{b_k}\}$. Luego $|T_k| = \frac{p^{b_k}|T_{k-1}|}{p^z} = p^{b_k-z}|T_{k-1}|$.

Finalmente, supongamos que $\gamma_T \notin \left\langle \gamma_{T_k}^{(1)}, \dots, \gamma_{T_k}^{(k-1)} \right\rangle$ y veamos que $|T_k| \geqslant p|T_{k-1}|$.
Supongamos, a modo de contradicción, que $|T_k| = |T_{k-1}|$ — que como está uno contenido en el otro, implica $T_k = T_{k-1}$. En ese caso, como $\mathcal{O}_\rho \subseteq T_k = T_{k-1}$, debe ser $m = 1$.
Por lo tanto, se cumple que $c \cdot x = f_k \cdot x$ para todo $x \in T_{k-1} = T_k$.
Esto, como $c = \prod_{i=1}^{k-1} f_i^{t_i}$ para ciertos $t_1, \dots, t_{k-1} \in \mathbb{N}_0$ ya que los f_i conmutan dos a dos, es equivalente a

$$\prod_{i=1}^{k-1} \left(\gamma_{T_k}^{(i)}\right)^{t_i} \cdot x = \gamma_{T_k}^{(k)} \cdot x$$

para todo $x \in T_{k-1} = T_k$. Como $\mathcal{O}_{\prod_{i=1}^{k-1}\left(\gamma_{T_k}^{(i)}\right)^{t_i}} \subseteq \bigcup_{i=1}^{k-1} \left(\gamma_{T_k}^{(i)}\right)^{t_i} = T_k = T_{k-1}$, concluimos que

$$\prod_{i=1}^{k-1} \left(\gamma_{T_k}^{(i)}\right)^{t_i} = \gamma_{T_k}^{(k)};$$

pero esto es absurdo. Luego, debe suceder que $|T_k| > |T_{k-1}|$ y, como $|T_k|$ es potencia de p, es $|T_k| \geqslant p|T_{k-1}|$. ∎

El siguiente lema nos dice un poco más sobre la estructura de los conjuntos provenientes de intersecciones que nos provee el Lema 5.1.1.

Lema 5.1.20: Sean g y h permutaciones de C que conmutan y S el conjunto de puntos compartidos que nos provee el Lema 5.1.1, proveniente de una intersección entre un p^i-ciclo α de g y un p^j-ciclo β de h. Si f es una permutación de C que conmuta con g y h y $\mathcal{O}_f \cap S \neq \emptyset$, entonces $\mathcal{O}_S \subseteq \mathcal{O}_f$.

Demostración. Sean $\alpha_1, \alpha_2, \ldots, \alpha_{p^{j-k}}$ y $\beta_1, \ldots, \beta_{p^{i-k}}$ los ciclos del Lema 5.1.1, que cumplen $S = \bigcup_{r=1}^{p^{j-k}} \mathcal{O}_{\alpha_r} = \bigcup_{r=1}^{p^{i-k}} \mathcal{O}_{\beta_r}$. Como $\mathcal{O}_f \cap S \neq \emptyset$, debe existir algún $1 \leqslant d \leqslant p^{j-k}$ y un ciclo γ de f tal que $\mathcal{O}_\gamma \cap \mathcal{O}_{\alpha_d} \neq \emptyset$. Como el conjunto S proveniente de la intersección entre α y β es el mismo que el proveniente de la intersección entre α_d y β — pues, como α_d es un ciclo de g, S está determinado por g, h y β —, el Lema 5.1.12 nos dice que existe un conjunto $T \supseteq S$ tal que $f = \gamma_T f'$ con γ_T un desarreglo de los puntos de T y f' una permutación disjunta con T; así que $S \subseteq \mathcal{O}_f$. ∎

En los siguientes dos lemas, trabajaremos con permutaciones sobre C que tengan orden potencia de p, a las cuales llamaremos $p-$*permutaciones* para abreviar.
Decimos que un ciclo α contenido en una $p-$permutación $g \in \mathbb{S}_{|C|}$, con $|g| = p^k$ para algún $k \in \mathbb{N}$, es de *longitud máxima* si $|\alpha| = p^k$.
En las demostraciones será de vital importancia identificar dos posibles casos: si hay intersecciones raras que involucren ciclos de longitud máxima, o si no.

Lema 5.1.21: Sean f_0, f_1 y f_2 $p-$permutaciones de C que conmutan dos a dos.
Si algún ciclo γ_1 de f_1 con $|f_0| \geqslant |\gamma_1|$ tiene intersección rara con un ciclo γ_2 de f_2 con $|f_0| \geqslant |\gamma_2|$, con conjunto de puntos compartidos S, y $\mathcal{O}_{\beta_0} \cap S \neq \emptyset$ para algún ciclo de longitud máxima β_0 de f_0, entonces, β_0 tiene intersección rara con un ciclo δ de f_1 o de f_2, con $\mathcal{O}_\delta \subseteq S$.

Demostración. Supongamos que β_0 no tiene intersección rara con ningún ciclo de f_1 ni de f_2. Por cumplirse $\mathcal{O}_{\beta_0} \cap S \neq \emptyset$, debe existir un ciclo β_2 de f_2 con $\mathcal{O}_{\beta_2} \subseteq S$ tal que $\mathcal{O}_{\beta_0} \cap \mathcal{O}_{\beta_2} \neq \emptyset$ y, análogamente, un ciclo β_1 de f_1 con $\mathcal{O}_{\beta_1} \subseteq S$ tal que $\mathcal{O}_{\beta_0} \cap \mathcal{O}_{\beta_1} \neq \emptyset$.
Además, notemos que $|\beta_1| = |\gamma_1|$ y $|\beta_2| = |\gamma_2|$, ya que β_1 es un ciclo de f_1 con $\mathcal{O}_{\beta_1} \subseteq S$, β_2 es un ciclo de f_2 con $\mathcal{O}_{\beta_2} \subseteq S$, y S es el conjunto de puntos compartidos que nos provee el Lema 5.1.1 aplicado a la intersección entre γ_1 y γ_2 como ciclos de f_1 y f_2 respectivamente.
Por lo tanto $|\beta_0| \geqslant |\beta_1|$ y $|\beta_0| \geqslant |\beta_2|$.
Gracias a la suposición, por el Corolario 5.1.8, deberán existir $m_1, m_2 \in \mathbb{N}$ tales que $\beta_0^{m_1} = \beta_1 q_1$ y $\beta_0^{m_2} = \beta_2 q_2$ con q_1 y q_2 permutaciones disjuntas con β_1 y β_2 respectivamente.

Concretamente, si $|\beta_0| = p^{i_0}$, $|\beta_1| = p^{i_1}$ y $|\beta_2| = p^{i_2}$, podemos escribir $m_1 = p^{i_0-i_1}d_1$ y $m_2 = p^{i_0-i_2}d_2$ con $mcd(d_1, p) = mcd(d_2, p) = 1$. Vamos a suponer sin pérdida de la generalidad que $i_1 \leqslant i_2$.
En particular, como $mcm(m_1, m_2) = p^{i_0-i_2}mcm(d_1, d_2)$ elevando la primer ecuación al exponente $\overline{d}$ y la segunda al exponente e, obtenemos

$$\beta_2^{\overline{d}}q_2^{\overline{d}} = \beta_0^{mcm(m_1,m_2)} = \beta_1^e q_1^e$$

$$\text{donde} \quad e = \frac{mcm(m_1, m_2)}{m_1} \quad \text{y} \quad \overline{d} = \frac{mcm(m_1, m_2)}{m_2} = \frac{mcm(d_1, d_2)}{d_2}.$$

Como $\overline{d}$ es coprimo con p, $\beta_2^{\overline{d}}$ es un ciclo con $\mathcal{O}_{\beta_2} = \mathcal{O}_{\beta_{\overline{d}}}$.
Como β_1^e y q_1^e son permutaciones disjuntas, $\beta_2^{\overline{d}}$ debe ser un ciclo contenido en β_1^e o un ciclo contenido en q_1^e. Concretamente, $\mathcal{O}_{\beta_2^{\overline{d}}} \subseteq \mathcal{O}_{\beta_1^e}$ o $\mathcal{O}_{\beta_2^{\overline{d}}} \subseteq \mathcal{O}_{q_1^e}$.
Como el conjunto S proviene de una intersección rara entre un ciclo de f_1 y otro de f_2 y $\mathcal{O}_{\beta_1} \subseteq S$ y $\mathcal{O}_{\beta_2} \subseteq S$, sabemos que $\mathcal{O}_{\beta_1} \cap \mathcal{O}_{\beta_2} \neq \emptyset$, pero también que $\mathcal{O}_{\beta_1} \not\subseteq \mathcal{O}_{\beta_2}$ y $\mathcal{O}_{\beta_2} \not\subseteq \mathcal{O}_{\beta_1}$.
Como $\mathcal{O}_{\beta_1} \cap \mathcal{O}_{\beta_2} \neq \emptyset$, debe ser $\mathcal{O}_{\beta_2^{\overline{d}}} \subseteq \mathcal{O}_{\beta_1^e}$ pero, como $\mathcal{O}_{\beta_1^e} \subseteq \mathcal{O}_{\beta_1}$, tenemos $\mathcal{O}_{\beta_2^{\overline{d}}} \subseteq \mathcal{O}_{\beta_1^e} \subseteq \mathcal{O}_{\beta_1}$, lo cual es absurdo. ■

Para hacer más amena la escritura de las próximas demostraciones, introducimos una nueva noción.

Definición 5.1.22: Sean a, b y c permutaciones de C que conmutan dos a dos, α un ciclo de a, β un ciclo de b y γ un ciclo de c, de modo que β y γ tienen intersección rara y S es el conjunto de puntos compartidos que nos provee el Lema 5.1.1. Decimos que α tiene puntos involucrados en la intersección rara entre β y γ si $\mathcal{O}_\alpha \cap S \neq \emptyset$.

En la definición anterior, incluimos aquellos casos en los que $a = b$ y $\alpha = \beta$.

Lema 5.1.23: Sean $f_0, f_1, \ldots, f_m$ $p-$permutaciones de C que conmutan dos a dos, con $|f_0| \geqslant |f_i|$ para todo $1 \leqslant i \leqslant m$ y supongamos que ningún ciclo de longitud máxima β de f_0 tiene puntos involucrados en alguna intersección rara entre un ciclo de f_k y uno de $f_{k'}$ para ningún par $k, k' \in \{0, \ldots m\}$.

Entonces, si $1 \leqslant d \leqslant m$, cambiando f_d por $\overline{f_d} = f_{i_1}^{-x_1} \ldots f_{i_s}^{-x_s} f_d$, para cualesquiera $x_1, \ldots, x_s \in \mathbb{N}$ y $i_1, \ldots, i_s \in \{1, \ldots, m\}$, sigue valiendo la afirmación análoga: ningún ciclo de longitud máxima β de f_0 tiene puntos involucrados en alguna intersección rara entre un ciclo de f y un ciclo de f' para ningún par $f, f' \in \{f_0, \ldots, \widehat{f_d}, \ldots, f_m\} \cup \{\overline{f_d}\}$.

Demostración. Sea β un ciclo de longitud máxima de f_0 y definimos $i_0 := d$. Como $|\beta| = |f_0| \geqslant |f_{i_w}|$ para todo $0 \leqslant w \leqslant s$, sabemos que para cada $0 \leqslant w \leqslant s$ existe un exponente e_w tal que $f_{i_w} = \beta^{e_w} f'_{i_w}$ con f'_{i_w} una permutación disjunta con β. En efecto, si β tiene intersección no vacía con algún ciclo de f_{i_w}, esto es consecuencia del Corolario 5.1.8 y, si no, sería $\mathcal{O}_\beta \cap \mathcal{O}_{f_{i_w}} = \emptyset$ así que tomamos $e_w = |\beta|$.
Luego, si $e = e_0 - x_1 e_1 - \ldots - x_s e_s$, como β conmuta con f'_{i_w} para todo $0 \leqslant w \leqslant s$ por ser permutaciones disjuntas con β, podemos escribir

$$\overline{f_d} = \beta^e (f'_{i_1})^{-x_1} \cdots (f'_{i_s})^{-x_s} f'_d$$

y entonces la intersección entre β y los ciclos de $\overline{f_d}$ no puede ser rara.

Por otro lado supongamos que existe un $d^* \in \{0, \ldots, m\}$ de modo que hay un ciclo de $\overline{f_d}$ que tiene intersección rara con un ciclo de f_{d^*}, con conjunto de puntos compartidos S, y $\mathcal{O}_\beta \cap S \neq \emptyset$. Por lo antes probado, deberá ser $d^* > 0$.
Como los órdenes de todas estas permutaciones son potencias de p y conmutan,

$$\left|\overline{f_d}\right| \leqslant \operatorname{mcm}\left(\left|f_{i_1}^{-x_1}\right|, \ldots, \left|f_{i_s}^{-x_s}\right|, |f_d|\right) \leqslant \max\{|f_{i_1}|, \ldots, |f_{i_w}|, |f_d|\} \leqslant |f_0|$$

y además, por definición, $|f_0| \geqslant |f_{d^*}|$.

Por el Lema 5.1.21, β deberá tener intersección rara o bien con un ciclo de $\overline{f_d}$ o bien con un ciclo de f_{d^*}, pero ninguna de las dos cosas ocurre — la primera por lo antes probado, y la segunda por hipótesis. Por lo tanto, no puede existir tal d^*.
Por último, gracias a la hipótesis, es claro que β no tiene puntos involucrados en una intersección rara entre ciclos de f_i y f_j para ningún par $i, j \in \left\{1, \ldots, \widehat{d}, \ldots, m\right\}$.
Como β es un ciclo de longitud máxima de f_0 arbitrario, terminamos. ∎

5.2 Esquivando las intersecciones raras

Definamos $\bigoplus_{i=1}^{n} \mathbb{Z}_{p^{a_i}} \simeq \langle h_1, \ldots, h_n \rangle$ donde $|h_i| = p^{a_i}$ para todo $1 \leqslant i \leqslant n$. Vamos a asumir sin pérdida de la generalidad que los a_i están ordenados de forma decreciente.

Observación 5.2.1: Notemos que cada h_i debe contener al menos un p^{a_i}—ciclo en su descomposición en ciclos disjuntos.

Recordemos que un ciclo contenido en una p—permutación es de *longitud máxima* si tiene el mismo orden que la permutación. En particular, un ciclo de longitud máxima de un generador h_i es un ciclo contenido en h_i de tamaño p^{a_i}.

La Afirmación 5.2.3 nos será útil en el futuro, así como la idea de su demostración, que volveremos a utilizar.

Sea M el menor índice tal que algún ciclo de longitud máxima de h_M tiene puntos involucrados en alguna intersección rara y tomemos un ciclo de longitud máxima α_i de h_i para cada $1 \leqslant i < M$. En lo que sigue, si $g \in G$ y α es un ciclo, vamos a decir que g *contiene* una potencia de α, digamos α^k con $k \in \mathbb{N}$, si podemos escribir $g = \alpha^k g'$ con g' una permutación disjunta con α y $|\alpha| \nmid k$.

Observación 5.2.2: Sean $1 \leqslant i, j \leqslant n$ y α un p^a—ciclo de h_i para algún $a \in \mathbb{N}$.
Si existe $1 \leqslant k \leqslant p^a$ tal que α^k está contenida en h_j, entonces $k = dp^{a-k'}$ para algún d con $mcd(d, p) = 1$, siendo k' el orden de los ciclos contenidos en α^k.

En efecto, si δ es un $p^{k'}$—ciclo contenido en α^k, como $|\delta| \leqslant |\alpha|$ por estar δ contenido en una potencia de α, el Corolario 5.1.8 aplicado a la intersección de α y δ como ciclos de h_i y h_j respectivamente nos dice que existe m tal que α^m es un producto de ciclos distintos contenidos en h_j y, más aún, que $m = dp^{a-k'}$ para algún d con $mcd(d, p) = 1$.
Por último, notar que no puede haber dos valores distintos de k tal que α^k está contenida en h_j. Si hubiese dos valores $1 \leqslant k, k^* \leqslant p^a$ distintos tales que $h_j = \alpha^k h_j' = \alpha^{k^*} h_j''$ con h_j' y h_j'' permutaciones disjuntas con α, tendríamos que $\alpha^k = \alpha^{k^*}$; un claro absurdo. Luego $k = dp^{a-k'}$.

Afirmación 5.2.3: Cambiando los generadores $\{h_i\}_{1 \leqslant i \leqslant n}$ de ser necesario, podemos suponer que para todo par $i < j$ con $i < M$, h_j no contiene potencias de α_i, es decir, que no podemos escribir a $h_j = \alpha_i^k q$ con $k \in \mathbb{N}$ y q una permutación disjunta con α_i.

Demostración. Para cada $1 \leqslant i < M$, empezando por $i = 1$ y siguiendo en orden creciente, realizamos el siguiente proceso: si h_j contiene una potencia $\alpha_i^{k_j}$ (suponemos k_j reducido módulo p^{a_i}), cambiamos el generador h_j por $h_i^{-k_j} h_j$, que no contiene potencias de α_i. Resta ver que $|h_j| = \left|h_i^{-k_j} h_j\right|$.
Cualquier ciclo δ contenido en $\alpha_i^{k_j}$ cumple $\mathcal{O}_\delta \subseteq \mathcal{O}_{\alpha_i}$ y $|\delta| = p^k \leqslant p^{a_j}$ para algún k, así que la Observación 5.2.2 aplicada a h_i, h_j, α_i y k_j nos dice que $k_j = dp^{a_i - k}$ con $mcd(d, p) = 1$.
Como G es abeliano y $|h_i| = p^{a_i}$,

$$\left|h_i^{-k_j} h_j\right| \leqslant mcm\left(\left|h_i^{-k_j}\right|, |h_j|\right) = mcm\left(p^k, p^{a_j}\right) = p^{a_j}.$$

Como $\left\langle h_1, \ldots, \widehat{h_j}, \ldots, h_n \right\rangle + \left\langle h_i^{-k_j} h_j \right\rangle \simeq \mathrm{Aut}(\mathcal{P})$, no puede ocurrir que $\left|h_i^{-k_j} h_j\right| < p^{a_j}$ ya que, si así fuese, lo anterior sería falso — basta mirar la cardinalidad a ambos lados.
Por lo tanto $\left|h_i^{-k_j} h_j\right| = p^{a_j} = |h_j|$, como queríamos. ∎

Notemos que la demostración anterior puede realizarse para todo par $i < j$, sin la restricción de M, pero ponemos esta restricción en pos de hacer más cómoda la demostración principal de esta sección.

A partir de ahora vamos a suponer que ya fueron aplicados los cambios de la Afirmación 5.2.3, de modo que ahora, si $s < t$ y $s < M$, entonces h_t no contiene potencias de α_s.

El siguiente lema está bien relacionado con la afirmación anterior, ya que nos provee de un resultado más fuerte: si $t > s$ y $s < M$, h_t deja fijos los puntos de α_s.

Lema 5.2.4: Sea τ_i un ciclo de longitud máxima de h_i que no tiene intersección rara con ningún ciclo de h_j para algún $j > i$ y, además, h_j no contiene potencias de τ_i. En estas condiciones, se cumple $\mathcal{O}_{\tau_i} \cap \mathcal{O}_{h_j} = \emptyset$.

Demostración. Supongamos, a modo de contradicción que $\mathcal{O}_{\tau_i} \cap \mathcal{O}_{h_j} \neq \emptyset$. Esto quiere decir que, para algún $k \in \mathbb{N}$, existe un p^k—ciclo γ contenido en h_j tal que $\mathcal{O}_{\tau_i} \cap \mathcal{O}_\gamma \neq \emptyset$.
Como no hay intersecciones raras involucrando τ_i, y $k \leqslant a_i$ por ser $|h_j| = p^{a_j} \leqslant p^{a_i}$, el Lema 5.1.1 nos dice que $|\mathcal{O}_{\tau_i} \cap \mathcal{O}_\gamma| = p^k$ y el Corolario 5.1.8 que existen $\gamma_1 = \gamma, \gamma_2, \ldots, \gamma_{p^{a_i-k}}$ ciclos de tamaño p^k contenidos en h_j tales que

$$\prod_{r=1}^{p^{a_i-k}} \gamma_r = \tau_i^m$$

para algún $m \in \mathbb{N}$.
Esto es absurdo, ya que el lado izquierdo es un producto de ciclos disjuntos contenidos en h_j y el derecho es una potencia de τ_i, y sabemos que no hay potencias de τ_i contenidas en h_j. Como el absurdo provino de suponer que $\mathcal{O}_{\tau_i} \cap \mathcal{O}_{h_j} \neq \emptyset$, concluimos que $\mathcal{O}_{\tau_i} \cap \mathcal{O}_{h_j} = \emptyset$ como queríamos. ∎

Gracias a este lema, como suponemos ya hechos los cambios de la Afirmación 5.2.3, podemos afirmar que, si $s < t$ y $s < M$, entonces $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{h_t} = \emptyset$.

La siguiente definición será crucial para la demostración principal de esta sección.

Definición 5.2.5: Diremos que un subconjunto de índices $I \subseteq \{1, \ldots, n\}$ es *bueno* si:

- Si $i \in I$, ningún ciclo de longitud máxima de h_i tiene puntos involucrados en alguna intersección rara entre ciclos de algún par h_j y $h_{j'}$ con $j, j' \in I$.
- Para cada $s \in I$ existe un ciclo de longitud máxima α_s de h_s de modo que, dado cualquier par $r, t \in I$ con $r < t$, $\mathcal{O}_{\alpha_r} \cap \mathcal{O}_{h_t} = \emptyset$.
- $\langle h_i : i \notin I \rangle$ mueve un conjunto de puntos $J(I)$ con $|J(I)| \geqslant \sum_{i \in [n]-I} 2|h_i|$.
- $J(I)$ no contiene puntos de ciclos de longitud máxima de ningún h_i con $i \in I$.

En lo que sigue, vamos a probar que — haciendo algunos cambios en el conjunto de generadores — podemos extraer un subconjunto *bueno* de índices $I \subseteq \{1, \dots, n\}$.

Lema 5.2.6: Existe un conjunto de generadores $\left\{\widetilde{h_1}, \dots, \widetilde{h_n}\right\}$ de $\mathrm{Aut}(\mathcal{P})$ de modo que $\left|\widetilde{h_i}\right| = |h_i|$ para todo $1 \leqslant i \leqslant n$ y tal que existe un subconjunto bueno de índices $I \subseteq \{1, \dots, n\}$ respecto a estos nuevos generadores

Concretamente, vamos a probar por inducción en k que, para todo $0 \leqslant k \leqslant n+1$, podemos modificar el conjunto de generadores $\{h_1, \dots, h_n\}$ de modo que se siga cumpliendo $\langle h_1, \dots, h_n \rangle = \mathrm{Aut}(\mathcal{P})$ y $|h_i| = p^{a_i}$ para todo $1 \leqslant i \leqslant n$, y existan una familia de subconjuntos de $\{1, \dots, n\}$, $\{A(i)\}_{i=0}^{k}$ y una familia de subconjuntos del conjunto subyacente de $\mathcal{P}$, $\{\mathcal{S}(i)\}_{i=0}^{k}$ cumpliendo cinco hipótesis que llamaremos $H_1(k), H_2(k), H_3(k), H_4(k)$ y $H_5(k)$; las describimos más abajo.

Para entender mejor la idea de la demostración, es bueno tener presente que, en la instancia k de la inducción, vamos a tener dadas las familias $\{A(i)\}_{i=0}^{k}$ y $\{\mathcal{S}(i)\}_{i=0}^{k}$; y nuestro objetivo será, luego de modificar adecuadamente el conjunto de generadores — pero sin modificar las familias recién mencionadas —, construir conjuntos $A(k+1)$ y $\mathcal{S}(k+1)$ para poder agregarlos a estas familias.

En lo que sigue $M(k)$ es, si existe, el menor índice en $A(k)$ tal que algún ciclo de longitud máxima de $h_{M(k)}$ tiene puntos involucrados en alguna intersección rara entre ciclos de dos generadores h_i y h_{i^*} con $i, i^* \in A(k)$ — el conjunto que nos provee el Lema 5.1.1. Si no existe tal índice, definimos $M(k) := n+1$. Ahora sí, describimos las cinco hipótesis:

- Hipótesis $H_1(k)$: Para todo $i \geqslant M(k)$ con $i \in A(k)$, vale que $\mathcal{O}_{h_i} \cap \bigcup_{r=0}^{k} \mathcal{S}(r) = \emptyset$.
- Hipótesis $H_2(k)$: Para cada $1 \leqslant s < M(k)$ con $s \in A(k)$ existe un ciclo de longitud máxima α_s de h_s, de modo que dado cualquier $t \in A(k)$ con $s < t$, $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{h_t} = \emptyset$.
- Hipótesis $H_3(k)$: Si $i \in A(k)$, no hay puntos de ciclos de longitud máxima de h_i que pertenezcan a $\bigcup_{r=0}^{k} \mathcal{S}(r)$.
- Hipótesis $H_4(k)$: Se cumple $\left|\bigcup_{r=0}^{k} \mathcal{S}(r)\right| \geqslant \sum_{i \notin A(k)} 2|h_i|$.
- Hipótesis $H_5(k)$: $M(k) \geqslant k$.

Vale la pena mencionar que, en la instancia k de la inducción, las modificaciones al conjunto de generadores las haremos sólo en aquellos h_i con $i \geqslant M(k)$ e $i \in A(k)$.

Por lo tanto, los ciclos α_i con $1 \leqslant i < M(k)$ e $i \in A(k)$ que aparecen en la hipótesis inductiva $H_2(k)$ no serán modificados, y parte de nuestro trabajo será definir ciclos α_i con $M(k) \leqslant i < M(k+1)$ e $i \in A(k+1)$ en pos de intentar que se cumpla $H_2(k+1)$.

Demostración. **Caso base:** Empezamos definiendo

$$\mathcal{S}(0) = \emptyset \text{ y } A(0) = \{1, \dots, n\}.$$

Notar que $H_1(0)$, $H_3(0)$, $H_4(0)$ y $H_5(0)$ valen trivialmente y, como $M(0)$ es el M mencionado en la Afirmación 5.2.3, ya probamos que también vale $H_2(0)$, como indicamos debajo de la demostración del Lema 5.2.4.

Paso inductivo:

Supongamos que tenemos dados $\{A(i)\}_{i=0}^{k}$ y $\{\mathcal{S}(i)\}_{i=0}^{k}$ de modo que el conjunto de generadores $h_1, \dots, h_n$ cumple las hipótesis $H_i(k)$ para cada $1 \leqslant i \leqslant 5$.

Si $M(k) > k$, definimos $\mathcal{S}(k+1) := \emptyset$ y $A(k+1) := A(k)$ y no modificamos el conjunto de generadores. Si no, será $M(k) = k$ y procedemos de la siguiente manera.

Vamos a definir un valor fijo $M := k$, el valor actual de $M(k)$.
Lo hacemos porque eventualmente modificaremos el conjunto de generadores permitiendo que el valor de $M(k)$ se modifique.

En la siguiente afirmación (5.2.7), vamos a probar que ciertas modificaciones en el conjunto de generadores no afectan la validez de las hipótesis planteadas, salvo la de $H_2(k)$. Sin embargo, mantendrán la validez de una hipótesis más débil que esta última, pero que nos será igual de útil.

Hipótesis $\widetilde{H_2}(k)$: Para cada $1 \leqslant s < M$ con $s \in A(k)$ existe un ciclo de longitud máxima α_s de h_s, de modo que dado cualquier $t \in A(k)$ con $s < t$, $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{h_t} = \emptyset$.

Notar que es la misma que $H_2(k)$ pero cambiando $M(k)$ — que podría modificarse eventualmente — por M que está fijo.
Por otro lado, no sólo se mantendrá la validez de la hipótesis $H_1(k)$ sino que, a lo largo de las modificaciones, se mantendrá la validez de una hipótesis que la implica si $M(k) \geqslant M$.

Hipótesis $\widetilde{H_1}(k)$: Para todo $i \geqslant M$ con $i \in A(k)$, vale que $\mathcal{O}_{h_i} \cap \bigcup_{r=0}^{k} \mathcal{S}(r) = \emptyset$.

Notar que coincide con $H_1(k)$ pero cambiando $M(k)$ por M.
Tener presente que las hipótesis $\widetilde{H_1}(k)$, $\widetilde{H_2}(k)$ y $H_i(k)$ para todo $i \in \{3, 4, 5\}$ son actualmente válidas.

Afirmación 5.2.7: Si cambiamos en el conjunto de generadores un h_r con $r \in A(k)$ y $r \geqslant M$ por $\overline{h_r} = h_{r_1}^{-x_1} \dots h_{r_s}^{-x_s} h_r$ con $r_1, \dots, r_s \in \{t \in A(k) : t \neq r \text{ y } t \geqslant M\}$, $x_1, \dots, x_s \in \mathbb{N}$ y se cumple que $|\overline{h_r}| = |h_r|$, entonces, luego del cambio, $M(k) \geqslant M$ y no se ve afectada la validez de la hipótesis $H_i(k)$ para ningún $i \in \{3,4,5\}$ ni la de $\widetilde{H_1}(k)$ ni la de $\widetilde{H_2}(k)$.

Demostración. Lo primero a destacar es que

$$\left\langle h_1, \dots, \widehat{h_r}, \dots, h_n \right\rangle + \langle \overline{h_r} \rangle = \mathrm{Aut}(\mathcal{P})$$

y que por hipótesis $|\overline{h_r}| = |h_r|$, así que el nuevo conjunto de generadores sigue generando, y siguen ordenados de la misma forma ya que el orden de ese generador se mantiene.

Vale que $M(k) \geqslant M$: Como no modificamos ningún h_i con $i < M$, sabemos que ningún h_i con $1 \leqslant i < M$ e $i \in A(k)$ tiene puntos de ciclos de longitud máxima involucrados en alguna intersección rara entre un ciclo de h_w y un ciclo de h_{w^*} con $w, w^* < M$.
Aplicando el Lema 5.1.23 para cada $1 \leqslant t < M$ con $t \in A(k)$, tomando $f_0 = h_t$ y $\{f_1, \dots, f_m\} = \{h_r : r \geqslant M \text{ y } r \in A(k)\}$ nos aseguramos que, si $1 \leqslant i < M$ e $i \in A(k)$, h_i no tiene puntos de ciclos de longitud máxima involucrados en alguna intersección rara entre un ciclo de h_w y un ciclo de h_{w^*} con $w, w^* \in A(k)$ y, o bien $w \geqslant M$, o bien $w^* \geqslant M$, o ambas.

Vale $\widetilde{H_1}(k)$: Llamando temporalmente $\Lambda = \{t \in A(k) : t \geqslant M\}$, la hipótesis $\widetilde{H_1}(k)$ — antes de la modificación — nos decía que $\left(\bigcup_{i \in \Lambda} \mathcal{O}_{h_i}\right) \cap \bigcup_{i=0}^{k} \mathcal{S}(i) = \emptyset$.
Como $\mathcal{O}_{\overline{h_r}} \subseteq \bigcup_{i=1}^{s} \mathcal{O}_{h_{r_i}} \cup \mathcal{O}_{h_r} \subseteq \bigcup_{i \in \Lambda} \mathcal{O}_{h_i}$ y no modificamos ningún otro generador, podemos asegurar que luego de redefinir h_r como $\overline{h_r}$, valdrá $\mathcal{O}_{h_t} \cap \bigcup_{i=0}^{k} \mathcal{S}(i) = \emptyset$ para todo $t \in \Lambda$; por lo que sigue valiendo $\widetilde{H_1}(k)$.

Vale $\widetilde{H_2}(k)$: Se deduce de que valía $\widetilde{H_2}(k)$ antes de la modificación, y de que sólo modificamos un h_r cambiándolo por un $\overline{h_r}$ que cumple $\mathcal{O}_{\overline{h_r}} \subseteq \bigcup_{i \in \Lambda} \mathcal{O}_{h_i}$ (y por $\widetilde{H_2}(k)$ esta unión era disjunta con $\mathcal{O}_{\alpha_i}$ para todo $i \in A(k)$ con $i < M$).

Vale $H_3(k)$: Previo a la modificación valía $H_3(k)$; y el único generador modificado fue h_r. Como ya vimos que $\mathcal{O}_{\overline{h_r}} \cap \bigcup_{i=0}^{k} \mathcal{S}(i) = \emptyset$, podemos afirmar que sigue valiendo $H_3(k)$.

Vale $H_4(k)$: Esto se verifica trivialmente, ya que no modificamos $A(k)$, ni los h_i con $i \notin A(k)$, ni los conjuntos $S(i)$ para ningún $0 \leqslant i \leqslant k$.

Vale $H_5(k)$: Esto vale porque $M(k) \geqslant M \geqslant k$. ∎

Por definición de M, algún ciclo β_M de longitud máxima de h_M tiene puntos involucrados en alguna intersección rara entre un ciclo η_1 de h_w y un ciclo η_2 de h_{w^*} para algún par $w, w^* \in A(k)$.

Si alguno de los dos ciclos, η_1 o η_2, tiene orden mayor o igual a p^{a_M}, llamaremos $\mathcal{S}'(k)$ al conjunto de puntos compartidos en cuestión, por el Corolario 5.1.6, valdrá $|\mathcal{S}'(k)| \geqslant p^{a_M+1}$.

Si ambos ciclos, η_1 y η_2, tienen orden menor a p^{a_M}, una aplicación del Lema 5.1.21 nos dice que β_M tiene intersección rara con algún ciclo δ de h_w o de h_{w*}; y en ese caso llamamos $\mathcal{S}'(k)$ al conjunto de puntos compartidos que nos provee el Lema 5.1.1 aplicado a la intersección entre β_M y δ, el primero como ciclo de h_M y el segundo como ciclo de h_w o h_w^*, según corresponda. Por el Corolario 5.1.6, nuevamente podríamos asegurar que $|\mathcal{S}'(k)| \geqslant p^{a_M+1}$.

Sean $h_{i_1}, \dots, h_{i_m}$, con $i_a < i_b$ si $a < b$, todos los generadores h_t con $t \in A(k)$ que cumplen $\mathcal{O}_{h_t} \cap \mathcal{S}'(k) \neq \emptyset$ — que, como $\mathcal{S}'(k)$ es un conjunto de puntos compartidos, por el Lema 5.1.20 cumplirán $\mathcal{S}'(k) \subseteq \mathcal{O}_{h_t}$. Llamamos j al subíndice que cumple $h_{i_j} = h_M$.

Afirmación 5.2.8: Haciendo cambios en el conjunto de generadores, podemos suponer que para todo $s > j$ y todo ρ ciclo de longitud máxima de h_M con $\mathcal{O}_\rho \cap \mathcal{S}'(k) \neq \emptyset$, existe un ciclo ρ' de h_{i_s} con $\mathcal{O}_{\rho'} \cap \mathcal{S}'(k) \neq \emptyset$ de modo que ρ y ρ' tienen intersección rara.

Demostración. Tomamos un ciclo ρ de longitud máxima de h_M con $\mathcal{O}_\rho \cap \mathcal{S}'(k) \neq \emptyset$ y consideramos, si existe, un generador h_{i_s} con $s > j$. Como $\mathcal{S}'(k) \subseteq \mathcal{O}_{h_{i_s}}$, existe un ciclo ρ' de h_{i_s} de modo que $\mathcal{O}_\rho \cap \mathcal{O}_{\rho'} \neq \emptyset$; llamaremos a su tamaño $|\rho'| = p^N$.
Supongamos que ρ y ρ' no tienen intersección rara.
En ese caso, como $|\rho| = |h_M| \geqslant |h_{i_s}| \geqslant |\rho'|$, por el Corolario 5.1.8 aplicado a la intersección entre ρ y ρ' como ciclos de h_M y h_{i_s} respectivamente, podemos afirmar que $h_{i_s} = \rho^x h'_{i_s}$ con h'_{i_s} una permutación disjunta con ρ y $x = dp^{a_M - N}$ con $mcd(d, p) = 1$.
Dicho esto, definiendo $\overline{h_{i_s}} = h_M^{-x} h_{i_s}$ podemos observar que

$$\left\langle h_1, \dots, \widehat{h_{i_s}}, \dots h_n \right\rangle + \langle \overline{h_{i_s}} \rangle = Aut(\mathcal{P}).$$

Mirando la cardinalidad a ambos lados, vemos que no puede ocurrir que $\left|\overline{h_{i_s}}\right| < |h_{i_s}|$ y, como G es abeliano y $|h_M| = p^{a_M}$,

$$|h_M^{-x} h_{i_s}| \leqslant mcm\left(|h_M^{-x}|, |h_{i_s}|\right) = mcm\left(p^N, p^{a_{i_s}}\right) = p^{a_{i_s}} = |h_{i_s}|.$$

Por lo tanto, $\left|\overline{h_{i_s}}\right| = |h_M^{-x} h_{i_s}| = |h_{i_s}|$.
Gracias a la Afirmación 5.2.7, esto nos dice que podemos redefinir a h_{i_s} como $\overline{h_{i_s}}$.
Por último, podemos afirmar que $\mathcal{S}'(k) \cap \mathcal{O}_{\overline{h_{i_s}}} = \emptyset$; de darse lo contrario, gracias al Lema 5.1.20 sería $\mathcal{S}'(k) \subseteq \mathcal{O}_{\overline{h_{i_s}}}$, lo cuál es absurdo porque $\mathcal{O}_\rho \cap \mathcal{S}'(k) \neq \emptyset$ y $\overline{h_{i_s}}$ deja fijos a todos los puntos de ρ. Luego, redefinimos h_{i_s} como $\overline{h_{i_s}}$ y este nuevo generador ya no pertenece al subconjunto en cuestión. ∎

A partir de ahora, vamos a suponer que se cumplen las condiciones de la afirmación anterior.
Si, luego de los cambios, se cumple que $j = m$, definimos $\mathcal{S}(k+1) := \mathcal{S}'(k)$ y $A(k+1) := A(k) - \{i_j\}$. Veremos luego, junto con el otro caso, que de esta forma se satisfacen las cinco hipótesis requeridas.

En cambio, si luego de los cambios de la Afirmación 5.2.8 termina siendo $m > j$, significa que existen un ciclo ρ de longitud máxima de h_M con $\mathcal{O}_\rho \cap \mathcal{S}'(k) \neq \emptyset$ y un ciclo ρ' de h_{i_m} con $\mathcal{O}_{\rho'} \cap \mathcal{S}'(k) \neq \emptyset$ tales que ρ y ρ' tienen intersección rara. Llamamos $\mathcal{S}''(k)$ al conjunto de puntos compartidos y notamos que $\mathcal{S}'(k) \cap \mathcal{S}''(k) \neq \emptyset$ y que $|\mathcal{S}''(k)| \geqslant p^{a_M+1}$ gracias al Corolario 5.1.6.

Afirmación 5.2.9: Podemos afirmar, salvo modificaciones, que existe un conjunto T de puntos de $\mathcal{P}$ con $T \subseteq \mathcal{O}_{h_{i_r}}$ para todo $j \leqslant r \leqslant m$ y $|T| \geqslant p^{m-j-1}|\mathcal{S}''(k)| \geqslant p^{a_M+m-j}$ y, además, que ningún otro generador h_r con $r \in A(k)$ y $r \notin \{i_1, \ldots, i_m\}$ cumple $\mathcal{O}_{h_r} \cap T \neq \emptyset$.

Demostración. Vamos a probar por inducción invertida en R que para todo $j+1 \leqslant R \leqslant m$ podemos afirmar, salvo modificaciones, que h_{i_j} y $h_{i_m}, h_{i_{m-1}}, \ldots, h_{i_R}$ comparten un conjunto de puntos T_R de modo que:

(1) Para todo $r \in \{j, m, m-1, \ldots, R\}$ podemos escribir $h_{i_r} = \gamma_{T_R}^{(r)} h'_{i_r}$ con $\gamma_{T_R}^{(r)}$ un desarreglo de los puntos de T_R que es producto de p^{l_r}— ciclos de h_{i_r} para algún $l_r \in \mathbb{N}$ y h'_{i_r} una permutación disjunta con T_R.

(2) $\mathcal{S}''(k) \subseteq T_R$ y $|T_R| \geqslant p^{m-R}|\mathcal{S}''(k)| \geqslant p^{a_M+m-R+1}$.

(3) La acción de $\left\langle \gamma_{T_R}^{(j)}, \gamma_{T_R}^{(m)}, \gamma_{T_R}^{(m-1)} \ldots, \gamma_{T_R}^{(R)} \right\rangle$ — como permutaciones en el conjunto subyacente de $\mathcal{P}$ — restringida a T_R es transitiva.

(4) Ningún generador h_r con $r \in A(k)$ y $r \notin \{i_1, \ldots, i_m\}$ cumple $\mathcal{O}_{h_r} \cap T_R \neq \emptyset$.

Caso base $R = m$:
Empezamos definiendo $T_m := \mathcal{S}''(k)$ que es el conjunto de puntos compartidos que proviene de la intersección rara entre un ciclo de $h_M = h_{i_j}$ y uno de h_{i_m}.
En este caso $T_R = \mathcal{S}''(k)$, $\gamma_{\mathcal{S}''(k)}^{(j)}$ es el producto de todos los ciclos de h_{i_j} que tienen sus puntos contenidos en $\mathcal{S}''(k)$ y $\gamma_{\mathcal{S}''(k)}^{(m)}$ es el producto de todos los ciclos de h_{i_m} que tienen sus puntos contenidos en $\mathcal{S}''(k)$.

Paso inductivo:
Supongamos que h_{i_j} y $h_{i_m}, h_{i_{m-1}}, \ldots, h_{i_R}$ comparten un conjunto T_R cumpliendo las cuatro condiciones antes mencionadas.

Tomamos un ciclo δ_{R-1} en $h_{i_{R-1}}$ que cumpla $\mathcal{O}_{\delta_{R-1}} \cap \mathcal{S}'(k) \neq \emptyset$ y $\mathcal{O}_{\delta_{R-1}} \cap \mathcal{S}''(k) \neq \emptyset$, que existe pues $\mathcal{S}'(k) \cap \mathcal{S}''(k) \neq \emptyset$ y $\mathcal{S}'(k) \subseteq \mathcal{O}_{h_{i_{R-1}}}$. Llamaremos T_{R-1} al conjunto que nos provee el Corolario 5.1.16 al aplicarlo con este ciclo δ_{R-1} de $h_{i_{R-1}}$, el conjunto T_R y los elementos $h_{i_j}, h_{i_m}, \ldots, h_{i_R}$, que cumplirá $\mathcal{S}''(k) \subseteq T_R \subseteq T_{R-1}$.
Ahora, para cada $r \in \{j, m, m-1, \ldots, R-1\}$, podemos escribir $h_{i_r} = \gamma^{(r)}_{T_{R-1}} h'_{i_s}$ con $\gamma^{(r)}_{T_{R-1}}$ un desarreglo de los puntos de T_{R-1}, producto de p^{l_r}—ciclos para algún $l_r \in \mathbb{N}$ y h'_{i_s} una permutación disjunta con T_{R-1}. Y la acción de $\left\langle \gamma^{(j)}_{T_{R-1}}, \gamma^{(m)}_{T_{R-1}}, \gamma^{(m-1)}_{T_{R-1}} \ldots, \gamma^{(R-1)}_{T_{R-1}} \right\rangle$ como permutaciones en el conjunto subyacente de $\mathcal{P}$ restringida a T_{R-1} es transitiva.
Como vamos a trabajar con exponentes, con el fin de no sobrecargar la notación vamos a nombrar temporalmente $S_r = \gamma^{(r)}_{T_{R-1}}$.

Si $S_{R-1} \notin \langle S_j, S_m, \ldots, S_R \rangle$, por el Corolario 5.1.16, $|T_{R-1}| \geqslant p^{m-1-(R-1)+1} |\mathcal{S}''(k)|$.
Además, ningún otro generador h_r con $r \in A(k)$ y $r \notin \{i_1, \ldots, i_m\}$ cumple $\mathcal{O}_{h_r} \cap T_{R-1} \neq \emptyset$, ya que de lo contrario, por el Corolario 5.1.16, $T_{R-1} \subseteq \mathcal{O}_{h_r}$, lo cuál no puede ocurrir pues $\mathcal{S}'(k) \cap T_{R-1} \neq \emptyset$ y sabemos que h_r deja fijos todos los puntos de $\mathcal{S}'(k)$ por ser $r \in A(k)$ y $r \notin \{i_1, \ldots, i_m\}$. Esto completaría el paso inductivo.

Si $S_{R-1} \in \langle S_j, S_m, \ldots, S_R \rangle$, vamos a ver que podemos cambiar al generador $h_{i_{R-1}}$ por otro generador que deje fijos todos los puntos de $\mathcal{S}'(k)$ — y por lo tanto no pertenecería al subconjunto de generadores con el que estamos trabajando — y volveremos a considerar el conjunto T_R y los elementos $h_{i_1}, \ldots, h_{i_R}$ para realizar desde el comienzo este mismo proceso pero, en vez de con $h_{i_{R-1}}$, con $h_{i_{R-2}}$ que es el siguiente generador en la lista.

Para ver eso, empecemos notando que existen $\{r_1, \ldots, r_s\} \subseteq \{j, m, m-1, \ldots, R\}$ tales que

$$S_{R-1} = S_{r_1}^{x_1} \cdots S_{r_s}^{x_s}$$

para algunos $x_1, \ldots, x_s \in \mathbb{N}$ con $1 \leqslant x_i < p^{l_{r_i}}$ para todo $1 \leqslant i \leqslant s$.
Sean $\{g_1, \ldots, g_t\} \subseteq \{h_{i_{r_1}}, \ldots, h_{i_{r_s}}\}$ todos los generadores de ese conjunto que sean distintos de h_{i_j} e $y_1, \ldots, y_t$ definidos de forma que $y_w = x_{w'}$ si y sólo si $g_w = h_{i_{w'}}$.
Definiendo $\overline{h_{i_{R-1}}} = g_1^{-y_1} \cdots g_t^{-y_t} h_{i_{R-1}}$, podemos observar que

$$\left\langle h_1, \ldots, \widehat{h_{i_{R-1}}}, \ldots, h_n \right\rangle + \left\langle \overline{h_{i_{R-1}}} \right\rangle = \mathrm{Aut}(\mathcal{P}).$$

Mirando la cardinalidad a ambos lados, vemos que no puede ocurrir que $\left|\overline{h_{i_{R-1}}}\right| < \left|h_{i_{R-1}}\right|$.
Además, como los órdenes de los generadores son potencias de p y G es abeliano,

$$\left|\overline{h_{i_{R-1}}}\right| \leqslant \mathrm{mcm}\left(\left|g_1^{-y_1}\right|, \ldots, \left|g_t^{-y_t}\right|, \left|h_{i_{R-1}}\right|\right) \leqslant \left|h_{i_{R-1}}\right|,$$

ya que $|g_1|, \ldots, |g_t| \leqslant \left|h_{i_{R-1}}\right|$ por ser $\{g_1, \ldots, g_t\} \subseteq \{h_{i_R}, \ldots, h_{i_m}\}$.
Por lo tanto, $\left|\overline{h_{i_{R-1}}}\right| = \left|h_{i_{R-1}}\right|$.

Si $h_{i_j} \notin \{h_{i_{r_1}}, \ldots, h_{i_{r_s}}\}$ entonces $\overline{h_{i_{R-1}}}$ es una permutación disjunta con T_{R-1}.

Si no, observemos que será $\overline{h_{i_{R-1}}} = S_j^x h''_{i_{R-1}}$ para algún $1 \leqslant x < p^{l_j}$, con $h''_{i_{R-1}}$ una permutación disjunta con T_{R-1}. Tomamos un ciclo γ de longitud máxima de h_{i_j} con $\mathcal{O}_\gamma \subseteq \mathcal{S}''(k) \subseteq T_{R-1}$ (podemos por cómo está definido $\mathcal{S}''(k)$), y notemos que no puede tener intersección rara con ningún ciclo de $\overline{h_{i_{R-1}}}$ ya que podemos escribir $\overline{h_{i_{R-1}}} = \gamma^x q$ con q una permutación disjunta con γ; pues γ es, en particular, un ciclo contenido en S_j.
De hecho, por la Observación 5.2.2 aplicada a h_{i_j}, $\overline{h_{i_{R-1}}}$ y γ^x, debe ser $x = dp^{a_M - y}$ con $mcd(d,p) = 1$, siendo $p^y \leqslant \left|\overline{h_{i_{R-1}}}\right| = \left|h_{i_{R-1}}\right|$ el orden de los ciclos contenidos en γ^x.

Dicho esto, definiendo $\overline{\overline{h_{i_{R-1}}}} = h_M^{-x}\overline{h_{i_{R-1}}}$, podemos observar que

$$\left\langle h_1, \dots, \widehat{h_{i_{R-1}}}, \dots h_n \right\rangle + \left\langle \overline{\overline{h_{i_{R-1}}}} \right\rangle \simeq Aut(\mathcal{P}).$$

Mirando la cardinalidad a ambos lados, vemos que no puede ocurrir que $\left|\overline{\overline{h_{i_{R-1}}}}\right| < \left|h_{i_{R-1}}\right|$ y, como G es abeliano y $|h_M| = p^{a_M}$,

$$\left|h_M^{-x}\overline{h_{i_{R-1}}}\right| \leqslant mcm\left(|h_M^{-x}|, \left|\overline{h_{i_{R-1}}}\right|\right) = mcm\left(p^y, p^{a_{i_{R-1}}}\right) = p^{a_{i_{R-1}}} = \left|h_{i_{R-1}}\right|.$$

Por lo tanto, $\left|\overline{\overline{h_{i_{R-1}}}}\right| = \left|h_M^{-x}h_{i_{R-1}}\right| = \left|h_{i_{R-1}}\right|$. Por último, notar que gracias al Lema 5.1.20 podemos afirmar que $\mathcal{S}''(k) \cap \mathcal{O}_{\overline{\overline{h_{i_{R-1}}}}} = \emptyset$, ya que de lo contrario sería $\mathcal{O}_\gamma \subseteq \mathcal{S}''(k) \subseteq \mathcal{O}_{\overline{\overline{h_{i_{R-1}}}}}$, lo cuál es absurdo porque $\overline{\overline{h_{i_{R-1}}}}$ deja fijos a todos los puntos de γ.

Por lo tanto, en ambos casos, la Afirmación 5.2.7 nos dice que podemos redefinir a $h_{i_{R-1}}$ como $\overline{h_{i_{R-1}}}$ o $\overline{\overline{h_{i_{R-1}}}}$ respectivamente.
Una vez hecho el cambio, como ahora $h_{i_{R-1}}$ es disjunto con $\mathcal{S}'(k)$, volvemos a considerar el conjunto T_R y los elementos $h_{i_1}, \dots, h_{i_R}$ para realizar desde el comienzo este mismo proceso pero, en vez de con $h_{i_{R-1}}$, con $h_{i_{R-2}}$.

Ahora sí, esto completa el paso inductivo.

Para concluír el resultado de la afirmación, basta con tomar $T = T_{j+1}$. ∎

Definimos entonces $\mathcal{S}(k+1) := T$ y $A(k+1) := A(k) - \{i_r \in A(k) : j \leqslant r \leqslant m\} \subsetneq A(k)$.
Si cuando $j = m$ definimos artificialmente $T = \mathcal{S}'(k)$ entonces esta definición coincide con la que ya dimos para dicho caso, por lo que podemos tratarlas como una única definición.

También notar que $M(k+1) > M$ ya que, como sólo eliminamos índices de $A(k)$, debe suceder que $M(k+1) \geqslant M(k) \geqslant M$, pero $M \notin A(k+1)$.
Una consecuencia de esto es que $M(k+1) \geqslant M + 1 = k + 1$, que implica $H_5(k+1)$.
Por cómo definimos $A(k+1)$, es $\mathcal{O}_{h_t} \cap \mathcal{S}(k+1) = \emptyset$ para todo $t \geqslant M$ tal que $t \in A(k+1)$.
Como vale $\widetilde{H_1}(k)$ y $M(k+1) \geqslant M$, esto implica $H_1(k+1)$; nos será de utilidad recordar que sigue valiendo $\widetilde{H_1}(k)$.

Por otro lado, si $m-j>0$, como $p \geqslant 5$ tenemos que

$$|\mathcal{S}(k+1)| \geqslant p^{a_M+m-j} = p^{m-j} \cdot p^{a_M} \geqslant 2(m-j+1) \cdot p^{a_M} \geqslant \sum_{r=j}^{m} 2|h_{i_r}|$$

Y si $m=j$

$$|\mathcal{S}(k+1)| = |\mathcal{S}'(k)| \geqslant p^{a_M+1} \geqslant 2p^{a_M} = 2|h_M|$$

por lo que podemos recolectar $2|h_{i_r}|$ puntos para cada h_{i_r} con $j \leqslant r \leqslant m$.
También podemos observar que

$$\mathcal{S}(k+1) \cap \bigcup_{i=1}^{k} \mathcal{S}(i) = \emptyset$$

ya que vale $\widetilde{H_1}(k)$ y $\mathcal{S}(k+1) \subseteq \mathcal{O}_{h_M}$. Esto y la cota anterior nos aseguran que

$$\left|\bigcup_{i=1}^{k+1} \mathcal{S}(i)\right| = \left|\bigcup_{i=1}^{k} \mathcal{S}(i)\right| + |\mathcal{S}(k+1)| \geqslant \sum_{i \notin A(k)} 2|h_i| + \sum_{i \in (A(k)-A(k+1))} 2|h_i| = \sum_{i \notin A(k+1)} 2|h_i|,$$

por lo que vale $H_4(k+1)$.

Notar que, si $r \in \{1, \dots, j-1\}$, h_{i_r} no contiene ciclos de longitud máxima δ que cumplan $\mathcal{O}_\delta \cap \mathcal{S}(k+1) \neq \emptyset$. Si así fuese, habría un ciclo δ' de h_M con $\mathcal{O}_{\delta'} \subseteq \mathcal{S}(k+1)$ tal que $\mathcal{O}_\delta \cap \mathcal{O}_{\delta'} \neq \emptyset$ y, por el Corolario 5.1.16, podríamos escribir $h_{i_r} = \gamma_F h'_{i_r}$ con γ_F un desarreglo de los puntos de un conjunto $F \supseteq \mathcal{S}(k+1)$ que es producto de p^{a_r}—ciclos (por ser δ uno de ellos y $|\delta| = p^{a_r}$); y h'_{i_r} una permutación disjunta con F. Esto no puede ocurrir ya que, como $\mathcal{S}'(k) \cap \mathcal{S}(k+1) \neq \emptyset$, existiría un ciclo δ'' de longitud máxima de h_{i_r} que cumpla $\mathcal{O}_{\delta''} \cap \mathcal{S}'(k) \neq \emptyset$; pero eso es absurdo por la definición del índice j.

Estos son los únicos generadores h_i con $i \in A(k+1)$ que cumplen $\mathcal{O}_{h_i} \cap \mathcal{S}(k+1) \neq \emptyset$, así que lo recién probado junto a la validez de $H_3(k)$ nos asegura que se cumple $H_3(k+1)$.

Finalmente, consideramos el conjunto

$$\{h_t : t \in A(k+1) \text{ y } t \geqslant M\} = \{h_{t_1}, \dots, h_{t_d}\} \text{ con } |h_{t_s}| \geqslant \left|h_{t_{s'}}\right| \text{ si } s \leqslant s'.$$

Para cada h_t en el conjunto, tomamos un ciclo de longitud máxima de h_t que llamaremos η_t y vamos a realizar un procedimiento análogo al de la Afirmación 5.2.3.

Para cada $1 \leqslant r \leqslant d$, empezando por $r=1$ y siguiendo en orden creciente, realizamos el siguiente proceso: si $r^* > r$ y $h_{t_{r^*}}$ contiene la potencia $\eta_{t_r}^{k_r}$ (supondremos k_r reducido módulo $|\eta_{k_r}|$), definimos $\overline{h_{t_{r^*}}} = h_{t_r}^{-k_r} h_{t_{r^*}}$. Veamos que vale $\left|\overline{h_{t_{r^*}}}\right| = |h_{t_{r^*}}|$.

En efecto, cualquier ciclo δ contenido en $\eta_{t_r}^{k_r}$ cumple $\mathcal{O}_\delta \subseteq \mathcal{O}_{\eta_{t_r}}$ y $|\delta| = p^N \leqslant p^{a_{t_{r^*}}}$ para algún N, así que la Observación 5.2.2 aplicada a $h_{t_r}, h_{t_{r^*}}, \eta_{t_r}$ y k_r nos dice que $k_r = dp^{a_{t_r}-N}$ con $mcd(d,p) = 1$. Como G es abeliano y $|h_r| = p^{a_{t_r}}$,

$$\left|h_{t_r}^{-k_r} h_{t_{r^*}}\right| \leqslant mcm\left(\left|h_{t_r}^{-k_r}\right|, |h_{t_{r^*}}|\right) = mcm\left(p^N, p^{a_{t_{r^*}}}\right) = p^{a_{t_{r^*}}} = |h_{t_{r^*}}|.$$

Como $\left\langle h_1, \ldots, \widehat{h_{t_{r^*}}}, \ldots, h_n \right\rangle + \left\langle \overline{h_{t_{r^*}}} \right\rangle = \mathrm{Aut}(\mathcal{P})$, no puede ocurrir que $\left|\overline{h_{t_{r^*}}}\right| < |h_{t_{r^*}}|$ ya que, si así fuese, lo anterior sería falso por un argumento de cardinalidad.
Por lo tanto $\left|\overline{h_{t_{r^*}}}\right| = |h_{t_{r^*}}|$. Dicho esto, cambiamos al generador $h_{t_{r^*}}$ por $\overline{h_{t_{r^*}}}$.

Observación 5.2.10: Luego de cada uno de estos cambios, sigue valiendo $M(k+1) > M$.

En efecto, como no modificamos ningún h_i con $i < M$, sabemos que ningún h_i con $1 \leqslant i < M$ e $i \in A(k+1)$ tiene puntos de ciclos de longitud máxima involucrados en alguna intersección rara entre un ciclo de h_w y un ciclo de h_{w^*} con $w, w^* < M$.
Aplicando reiteradas veces el Lema 5.1.23 — para cada cambio, una aplicación por cada $t < M$ con $t \in A(k+1)$, siguiendo la notación anterior, tomando $f_0 = h_t, f_1 = h_{t_r}$ y $f_2 = h_{t_{r^*}}$ — nos aseguramos que, si $1 \leqslant i < M$ e $i \in A(k+1)$, h_i no tiene puntos de ciclos de longitud máxima involucrados en alguna intersección rara entre un ciclo de h_w y un ciclo de h_{w^*} con $w, w^* \in A(k+1)$ y, o bien $w \geqslant M$, o bien $w^* \geqslant M$, o ambas.

Para cada $M \leqslant i < M(k+1)$ con $i \in A(k+1)$ definimos $\alpha_i = \eta_i$.
Gracias a los cambios hechos y al Lema 5.2.4 podemos asegurar que dado cualquier par $i, t \in A(k+1)$ con $M \leqslant i < M(k+1)$ e $i < t$, $\mathcal{O}_{\alpha_i} \cap \mathcal{O}_{h_t} = \emptyset$. Esto sumado a la validez de $\widetilde{H_2}(k)$ nos asegura que vale $H_2(k+1)$.
Sin embargo, resta chequear que luego de estos cambios se siguen cumpliendo las hipótesis $H_i(k+1)$ para $i \in \{1,3,4,5\}$.

Afirmación 5.2.11: Luego de cada uno de estos cambios, siguen valiendo las hipótesis $H_i(k+1)$ con $i \in \{1,3,4,5\}$.

Demostración. En lo que sigue, tener presente que $M(k+1) > M$.

Vale $H_1(k+1)$: Llamando temporalmente $\Lambda = \{t \in A(k+1) : t \geqslant M\}$, como $A(k+1) \subseteq A(k)$, la hipótesis $\widetilde{H_1}(k)$ — antes de la modificación — nos decía que $\left(\bigcup_{i\in\Lambda} \mathcal{O}_{h_i}\right) \cap \bigcup_{i=0}^{k+1} \mathcal{S}(i) = \emptyset$. Como $\mathcal{O}_{\overline{h_{t_{r^*}}}} \subseteq \mathcal{O}_{h_{t_{r^*}}} \cup \mathcal{O}_{h_{t_r}} \subseteq \bigcup_{i\in\Lambda} \mathcal{O}_{h_i}$ y no modificamos ningún otro generador, podemos asegurar que luego de redefinir $h_{t_{r^*}}$ como $\overline{h_{t_{r^*}}}$, valdrá $\mathcal{O}_{h_t} \cap \bigcup_{i=0}^{k+1} \mathcal{S}(i) = \emptyset$ para todo $t \in \Lambda$. Como $M(k+1) > M$, $\{t \in A(k+1) : t \geqslant M(k+1)\} \subseteq \Lambda$, por lo que sigue valiendo $H_1(k+1)$.

Vale $H_3(k+1)$: Previo a la modificación valía $H_3(k+1)$; y el único generador modificado fue $h_{t_{r^*}}$. Como ya vimos que $\mathcal{O}_{\overline{h_{t_{r^*}}}} \cap \bigcup_{i=0}^{k+1} \mathcal{S}(i) = \emptyset$, podemos afirmar que sigue valiendo $H_3(k+1)$.

Vale $H_4(k+1)$**:** Esto se verifica trivialmente, ya que no modificamos $A(k+1)$, ni los h_i con $i \notin A(k+1)$, ni los conjuntos $S(i)$ para ningún $0 \leqslant i \leqslant k+1$.

Vale $H_5(k+1)$**:** Como $M(k+1) > M$, sigue valiendo que $M(k+1) \geqslant k+1$. ■

Para terminar con la demostración, basta con tomar $I = A(n+1)$ y $J = \bigcup_{i=1}^{n+1} S(i)$. ■

5.3 Entendiendo las intersecciones no raras

Aplicamos el Lema 5.2.6 para obtener un subconjunto bueno $A \subseteq \{1, 2, \ldots, n\}$.
Si $A = \emptyset$ entonces no hay nada que hacer, habremos probado el resultado del teorema ya que $|J(A)| \geqslant \sum_{i \in [\![n]\!]} 2p^{a_i}$. En lo que sigue, asumiremos $A \neq \emptyset$.

Vamos a analizar qué pasa con los puntos de $\mathcal{P}$ que no deja fijos el subgrupo $\langle h_j \rangle_{j \in A}$.

Por comodidad, llamaremos $g_1, \ldots, g_N$ a los generadores h_j tales que $j \in A$, y para cada $1 \leqslant i \leqslant N$, si $g_i = h_j$, nos permitiremos hacer el abuso de notación de renombrar como α_i al ciclo α_j. Los asumiremos ordenados, de forma que $|g_i| \geqslant |g_j|$ si $i \leqslant j$.
Vamos a denotar $|g_i| = p^{c_i}$. Respecto a los órdenes de los generadores, la única hipótesis que necesitamos en esta sección es $|g_i| \neq 2$ para todo $1 \leqslant i \leqslant N$, que se cumple ampliamente si pedimos $p \geqslant 5$ para ser consistentes con la sección anterior.

Para hacer más amena la notación en esta sección, vamos a usar con frecuencia una frase cuyo significado podría no quedar claro, así que lo explicamos en la siguiente definición.

Definición 5.3.1: Dado $1 \leqslant i \leqslant N$ y un ciclo α de g_i, vamos a decir que *no hay intersecciones raras involucrando puntos de* α si no existe ningún par $1 \leqslant r, r^* \leqslant N$ tal que un ciclo de g_r y un ciclo de g_{r^*} tienen intersección rara con conjunto de puntos compartidos S y $\mathcal{O}_\alpha \cap S \neq \emptyset$.

En particular, vamos a decir que *no hay intersecciones raras involucrando puntos de ciclos de longitud máxima* para referirnos a que no hay intersecciones raras involucrando puntos de algún ciclo de longitud máxima β de g_i para ningún $1 \leqslant i \leqslant N$; que se cumple por ser A un subconjunto bueno. Pasamos a hacer otras observaciones importantes.

Observación 5.3.2: Dados $1 \leqslant i, j \leqslant N$, si un ciclo β_i de g_i cumple $\mathcal{O}_{\beta_i} \cap \mathcal{O}_{g_j} \neq \emptyset$, entonces $\mathcal{O}_{\beta_i} \subseteq \mathcal{O}_{g_j}$.

En efecto, si $\mathcal{O}_{\beta_i} \cap \mathcal{O}_{g_j} \neq \emptyset$, debe existir un ciclo β_j de g_j tal que $\mathcal{O}_{\beta_i} \cap \mathcal{O}_{\beta_j} \neq \emptyset$. Si S es el conjunto de puntos compartidos que provee el Lema 5.1.1 aplicado a la intersección entre β_i y β_j como ciclos de g_i y g_j respectivamente, tenemos $\mathcal{O}_{\beta_i} \subseteq S \subseteq \mathcal{O}_{g_j}$, como queríamos.

Observación 5.3.3: Sean $1 \leqslant i, j \leqslant N$. Si δ es un ciclo de g_i, β un ciclo de longitud máxima de g_j y $\mathcal{O}_\delta \cap \mathcal{O}_\beta \neq \emptyset$, entonces todos los puntos de δ pertenecen a algún ciclo de longitud máxima de g_j y, por lo tanto, no hay intersecciones raras involucrando puntos de δ.

En efecto, teniendo en cuenta que no hay intersecciones raras involucrando puntos de ciclos de longitud máxima, esto es una consecuencia del Lema 5.1.11 aplicado a la intersección entre δ y β como ciclos de g_i y g_j respectivamente.

Observación 5.3.4: Para cada par $1 \leqslant i < j \leqslant N$ o bien g_i contiene una potencia de α_j o bien sucede que $\mathcal{O}_{\alpha_j} \cap \mathcal{O}_{g_i} = \emptyset$ o bien existe un ciclo $\gamma_{i,j}$ de g_i de longitud $p^k \geqslant p^{c_j+1}$ y p^{c_j}—ciclos $\alpha_j = \overline{\alpha_{i,1}}, \ldots, \overline{\alpha_{i,p^{k-c_j}}}$ contenidos en g_j tales que:

$$\prod_{r=1}^{p^{k-c_j}} \overline{\alpha_{i,r}} = \gamma_{i,j}^m$$

para algún $m \in \mathbb{N}$ tal que $p \mid m$.

En efecto, como no hay intersecciones raras involucrando ciclos de longitud máxima, si g_i no contiene potencias de α_j, el resultado es una consecuencia directa del Lema 5.1.1 y el Corolario 5.1.8 aplicado a la intersección entre α_j como ciclo de g_j y algún ciclo de g_i que comparta puntos con α_j.

Motivados por esta observación y para hacer más amena la redacción de la solución, hacemos la siguiente definición:

Definición 5.3.5: A los ciclos $\gamma_{i,j}$ que se generan cada vez que $\mathcal{O}_{\alpha_j} \cap \mathcal{O}_{\beta_i} \neq \emptyset$ para algún par $1 \leqslant i < j \leqslant n$ y β_i un ciclo de g_i de longitud mayor a la de α_j, los llamaremos *ciclos de tipo* γ

Como $\mathcal{O}_{\alpha_j} \subseteq \mathcal{O}_{\gamma_{i,j}}$ para cualquier par $1 \leqslant i < j \leqslant N$, por la Observación 5.3.3 sabemos que no hay intersecciones raras involucrando puntos de ciclos de tipo γ. Además, se cumple $\mathcal{O}_{\gamma_{i,j}} \cap \mathcal{O}_{g_s} = \emptyset$ para todo $s > j$, ya que de lo contrario por la Observación 5.3.2 sería $\mathcal{O}_{\alpha_j} \subseteq \mathcal{O}_{\gamma_{i,j}} \subseteq \mathcal{O}_{g_s}$, contradiciendo la segunda condición de conjunto bueno.

Observación 5.3.6: Dado un ciclo de tipo γ, digamos γ_{i_1,j_1}, este es disjunto con γ_{i_2,j_2} para todo $1 \leqslant i_2 \leqslant n$ y $j_1 \neq j_2$. Además, γ_{i_1,j_1} es disjunto con α_t para todo $t \neq j_1$.

Sin pérdida de la generalidad asumamos que $j_1 < j_2$ y supongamos que $\mathcal{O}_{\gamma_{i_1,j_1}} \cap \mathcal{O}_{\gamma_{i_2,j_2}} \neq \emptyset$. Como $\mathcal{O}_{\gamma_{i_2,j_2}} \cap \mathcal{O}_{g_{j_2}} \neq \emptyset$, por la Observación 5.3.2 sabemos que $\mathcal{O}_{\gamma_{i_2,j_2}} \subseteq \mathcal{O}_{g_{j_2}}$. Esto nos dice que $\mathcal{O}_{\gamma_{i_1,j_1}} \cap \mathcal{O}_{g_{j_2}} \neq \emptyset$ y, nuevamente por la Observación 5.3.2, $\mathcal{O}_{\gamma_{i_1,j_1}} \subseteq \mathcal{O}_{g_{j_2}}$. En particular, $\mathcal{O}_{\alpha_{j_1}} \subseteq \mathcal{O}_{\gamma_{i_1,j_1}} \subseteq \mathcal{O}_{g_{j_2}}$; pero esto contradice la segunda condición de conjunto bueno, ya que $j_2 > j_1$. Llegamos a un absurdo, lo que prueba la primera parte de la observación.
La segunda parte es similar, supongamos que existe $t \neq j_1$ tal que $\mathcal{O}_{\gamma_{i_1,j_1}} \cap \mathcal{O}_{\alpha_t} \neq \emptyset$.
Si $t < j_1$, como $\mathcal{O}_{\gamma_{i_1,j_1}} \subseteq \mathcal{O}_{g_{j_1}}$, se cumple $\mathcal{O}_{\alpha_t} \cap \mathcal{O}_{g_{j_1}} \neq \emptyset$, que contradice la segunda condición de conjunto bueno.
Si $t > j_1$, como α_t es un ciclo de g_t, la Observación 5.3.2 nos dice que $\mathcal{O}_{\gamma_{i_1,j_1}} \subseteq \mathcal{O}_{g_t}$; esto implica que $\mathcal{O}_{\alpha_{j_1}} \subseteq \mathcal{O}_{\gamma_{i_1,j_1}} \subseteq \mathcal{O}_{g_t}$, lo que contradice la segunda condición de conjunto bueno. Llegamos a una contradicción, probando la segunda parte de la observación.

El siguiente resultado es trivial bajo la hipótesis de $p \geqslant 5$, ya que $\mathrm{Aut}(\mathcal{P})$ no puede contener elementos de orden par por ser un grupo de orden impar. Sin embargo, con esperanzas de una futura reutilización de estas ideas para $p = 2$ y 3, hacemos la siguiente observación.

Observación 5.3.7: No existen trasposiciones $\tau = (a\ b) \in \mathrm{Aut}(\mathcal{P})$ con $a, b \in \mathcal{O}_\beta$ para algún ciclo β que no sea una trasposición y esté contenido en g_i para algún $1 \leqslant i \leqslant N$.

Sea $\tau = (a\ b) \in \mathrm{Aut}(\mathcal{P})$ tal que $a, b \in \mathcal{O}_\beta$ para algún ciclo β que no sea una trasposición y esté contenido en g_i para algún $1 \leqslant i \leqslant N$. Consideramos S el conjunto de puntos compartidos que nos provee el Lema 5.1.1 aplicado a la intersección entre β y τ como ciclos de g_i y τ respectivamente. Como $S \subseteq \mathcal{O}_\tau$ y $|S| \geqslant |\mathcal{O}_\beta| > 2$, llegamos a un absurdo.

En particular, como $|\alpha_i| = |g_i| \neq 2$ para todo $1 \leqslant i \leqslant N$, no existen trasposiciones $\tau \in \mathrm{Aut}(\mathcal{P})$ que intercambien dos puntos de α_i. Más aún, como todo ciclo de tipo γ tiene orden mayor que α_i para algún $1 \leqslant i \leqslant N$, no existen trasposiciones $\tau \in \mathrm{Aut}(\mathcal{P})$ que intercambien dos puntos de un ciclo de tipo γ.

Antes de pasar a probar una proposición, necesitamos hacer la siguiente definición:

Definición 5.3.8: Dado $1 \leqslant j \leqslant N$, diremos que un ciclo η de g_j es un *ciclo dominante* si para todo $t > j$, η es disjunto con todos los ciclos de g_t de longitud mayor o igual que la de η y para todo $t < j$, η es disjunto con todos los ciclos de g_t de longitud mayor que la de η.

Observación 5.3.9: Sean $1 \leqslant i < j \leqslant N$, y sean η_i y η_j un ciclo dominante de g_i y un ciclo dominante de g_j respectivamente. Entonces $\mathcal{O}_{\eta_i} \cap \mathcal{O}_{\eta_j} = \emptyset$.

En efecto, supongamos que $\mathcal{O}_{\eta_i} \cap \mathcal{O}_{\eta_j} \neq \emptyset$. Si $|\eta_i| > |\eta_j|$, llegamos a un absurdo por ser η_j ciclo dominante de g_j. Luego $|\eta_i| \leqslant |\eta_j|$, pero es absurdo por ser η_i ciclo dominante de g_i.

Dicho esto, estamos en condiciones de probar el siguiente resultado por inducción en i:

Lema 5.3.10: Para todo $1 \leqslant i \leqslant N$ el complemento de los puntos fijos de la acción del subgrupo $\langle g_j : j \geqslant i \rangle \leqslant \mathrm{Aut}(\mathcal{P})$ tiene al menos

$$\sum_{j=i}^{N} 2p^{c_j}$$

puntos. Más aún, ninguno de estos puntos pertenece a $J(A)$.

Demostración. Vamos a probar por inducción invertida en i, empezando por $i = N+1$ y yendo en orden decreciente, que para todo $1 \leqslant i \leqslant N+1$ podemos conseguir un conjunto $C(i)$ de puntos de $\mathcal{P}$ que cumpla las siguientes condiciones:

(1) $|C(i)| \geqslant \sum_{k=i}^{N} 2p^{c_k}$.

(2) Si $j < i \leqslant r$ y $\gamma_{j,r}$ es un ciclo dominante de tipo γ de g_j, $\left|\mathcal{O}_{\gamma_{j,r}} \cap C(i)\right| \leqslant 2p^{c_r}$.

(3) Si $j < i$ y ϵ_j es un ciclo dominante de g_j que no es de tipo γ, $\mathcal{O}_{\epsilon_j} \cap C(i) = \emptyset$.

(4) $C(i) \cap J(A) = \emptyset$.

(5) Si $i \leqslant n$, $C(i+1) \subseteq C(i)$.

(6) Si $x \in C(i)$, entonces $x \in \mathcal{O}_\epsilon$ para algún ciclo dominante ϵ con $\mathcal{O}_\epsilon \subseteq \mathcal{O}_{g_r}$ para algún $i \leqslant r \leqslant N$. Notar que ϵ no es necesariamente un ciclo de g_r.

Nuestro caso base será cuando $i = N+1$, en cuyo caso definimos $C(N+1) = \emptyset$ y cumple las seis hipótesis trivialmente.

Ahora vamos a realizar el paso inductivo. Dado $s \in \mathbb{N}$, supongamos que tenemos definido $C(i)$ para todo $i \geqslant s+1$, cumpliendo las seis propiedades descriptas anteriormente. Veamos que podemos definir $C(s)$ de modo que cumpla las seis propiedades.

Caso 1: Si α_s no es dominante.

Como no comparte puntos con ciclos de $g_{t'}$ para ningún $t' > s$, debe existir un $t < s$ tal que α_s tiene intersección no vacía con algún ciclo de g_t de longitud mayor que p^{c_s}, o sea, un ciclo de tipo γ.

Observación 5.3.11: Existe un ciclo dominante $\gamma_{d,s}$ de tipo γ para algún $d < s$.

Recordemos que, para cualquier $1 \leqslant r \leqslant N$, si un ciclo de g_r tiene longitud mayor a la de α_s y tiene intersección no vacía con α_s, entonces es un ciclo de tipo γ.
Sean $\gamma_{t_1,s}, \dots, \gamma_{t_k,s}$ todos los ciclos de tipo γ que tienen intersección no vacía con α_s y consideramos $w = \max\{|\gamma_{t_r,s}| : 1 \leqslant r \leqslant k\}$ y $d = \max\{t_r : |\gamma_{t_r,s}| = w\}$.
No es difícil observar que $\gamma_{d,s}$ es un ciclo dominante de tipo γ: si para algún $1 \leqslant r \leqslant N$ existe un ciclo β_r de g_r de longitud mayor o igual que la de $\gamma_{d,s}$ tal que $\mathcal{O}_{\beta_r} \cap \mathcal{O}_{\gamma_{d,s}} \neq \emptyset$ entonces, como no hay intersecciones raras involucrando puntos de $\gamma_{d,s}$, por el Corolario 5.1.8 aplicado a la intersección entre $\gamma_{d,s}$ y β_r como ciclos de g_d y g_r, tendríamos que $\mathcal{O}_{\gamma_{d,s}} \subseteq \mathcal{O}_{\beta_r}$, y entonces $\mathcal{O}_{\alpha_s} \subseteq \mathcal{O}_{\beta_r}$.
Luego, como $|\beta_r| \geqslant |\gamma_{d,s}| > |\alpha_s|$, β_r debe ser un ciclo de tipo γ que tenga intersección no vacía con α_s. Si $|\beta_r| > |\gamma_{d,s}|$, es absurdo por definición de $\gamma_{d,s}$; así que $|\beta_r| = |\gamma_{d,s}|$, pero por definición de $\gamma_{d,s}$ es $r < d$, así que $\gamma_{d,s}$ es dominante.

Por definición, $\gamma_{d,s}$ tendrá longitud al menos $p^{c_s+1} \geqslant 2p^{c_s}$ y, por la Observación 5.3.4, cumplirá $\mathcal{O}_{\gamma_{d,s}} \subseteq \mathcal{O}_{g_s}$. Gracias a esto, podemos definir $C(s) = C(s+1) \cup D$ donde D es cualquier subconjunto de $\mathcal{O}_{\gamma_{s,d}}$ de cardinal $2p^{c_s}$. Veamos que cumple las seis condiciones:

(1) Como $\mathcal{O}_{\alpha_s} \cap \bigcup_{j=s+1}^{N} \mathcal{O}_{g_j} = \emptyset$, por la Observación 5.3.2 tenemos que $\mathcal{O}_{\gamma_{d,s}} \cap \bigcup_{j=s+1}^{N} \mathcal{O}_{g_j} = \emptyset$ y en particular $D \cap \bigcup_{j=s+1}^{N} \mathcal{O}_{g_j} = \emptyset$. Por lo tanto, como por la condición 6 con $i = s+1$ es $C(s+1) \subseteq \bigcup_{j=s+1}^{N} \mathcal{O}_{g_j}$,

$$|C(s+1) \cup D| = |C(s+1)| + |D| = \sum_{j=s}^{N} 2p^{c_j}.$$

(2) Dado $\gamma_{j,r}$ con $j < s \leqslant r$, sabemos que $|\mathcal{O}_{\gamma_{j,r}} \cap C(s+1)| \leqslant 2p^{c_r}$ si $r \geqslant s+1$ por la condición 2 con $i = s+1$, y además $|\mathcal{O}_{\gamma_{j,s}} \cap D| = \emptyset$ si $j \neq d$ ya que los ciclos de tipo γ son disjuntos dos a dos como observamos en 5.3.6. Por último notar que $|\mathcal{O}_{\gamma_{d,s}} \cap D| = 2p^{c_s}$ y $\gamma_{d,s} \cap C(s+1) = \emptyset$ por ser $\gamma_{d,s}$ dominante — y por lo tanto disjunto con los demás ciclos dominantes — y la condición 6 con $i = s+1$.

(3) Como D no contiene puntos de ciclos dominantes que no sean de tipo γ por ser $\gamma_{d,s}$ disjunto con los demás ciclos dominantes, esta propiedad — que se cumple para $i = s+1$ — se mantiene para $i = s$.

(4) No hay puntos de ciclos de longitud máxima de ningún g_r con $1 \leqslant r \leqslant N$ en $J(A)$, por lo que, gracias a la Observación 5.3.3, $\mathcal{O}_{\gamma_{d,s}} \cap J(A) = \emptyset$. Por la condición 4 en $i = s+1$, $C(s+1) \cap J(A) = \emptyset$.

(5) $C(s+1) \subseteq C(s+1) \cup D$.

(6) Todos los puntos de D pertenecen a $\gamma_{d,s}$ que es dominante, de tipo γ y $\mathcal{O}_{\gamma_{d,s}} \subseteq \mathcal{O}_{g_s}$, y la condición 6 con $i = s+1$ nos dice que los puntos de $C(s+1)$ también cumplen.

Esto completa el paso inductivo en el Caso 1.

Caso 2: Si α_s es un ciclo dominante de g_s.

En esta situación, α_s no interseca con ciclos de tipo γ. Sólo necesitamos recolectar los p^{c_s} puntos que faltan usando puntos de otros ciclos dominantes.

Observación 5.3.12: Dado $1 \leqslant r \leqslant N$, g_r contiene al menos un ciclo de longitud máxima distinto de α_s.

Si no fuese así, la acción de $\langle g_r^{p^{c_r-1}} \rangle$ en $\mathcal{P}$ deja fijos todos los puntos excepto los de α_s. Como los puntos de α_s forman una anticadena, esto implica que para todo $x \in \mathcal{O}_{\alpha_s}$

$$\mathcal{P}_{<x} = \mathcal{P}_{<g_r^{p^{c_r-1}}x} \quad \text{y} \quad \mathcal{P}_{>x} = \mathcal{P}_{>g_r^{p^{c_r-1}}x}$$

y por lo tanto existe un automorfismo de $\mathcal{P}$ que intercambia dos puntos de α_s, contradiciendo la Observación 5.3.7.

Afirmación 5.3.13: Debe existir al menos un ciclo dominante de longitud máxima en g_s distinto de α_s.

Demostración. Llamemos $\beta_1, \ldots, \beta_{m_s}$ a los ciclos de longitud máxima de g_s distintos de α_s. Ahora supongamos, a modo de contradicción, que para todo $1 \leqslant r \leqslant m_s$ sucede que β_r tiene intersección no vacía con algún ciclo de longitud más grande η_r de g_{t_r} para algún $t_r \neq s$ o bien con un ciclo de igual longitud η_r de g_{t_r} para algún $t_r > s$.

Para lo que sigue será importante notar que no hay intersecciones raras involucrando puntos de ningún β_r por ser de longitud máxima. Vamos a probar que, para cada uno de estos ciclos, todos sus puntos se relacionan de la misma forma con todos los puntos de α_s — es decir, que dado $y_0 \in \mathcal{O}_{\alpha_s}$, si $x_0 \geqslant y_0$ (respectivamente $\leqslant$ o incomparable) para algún $x_0 \in \mathcal{O}_{\beta_r}$, entonces $x \geqslant y_0$ (respectivamente $\leqslant$ o incomparable) para todo $x \in \mathcal{O}_{\beta_r}$.
Para esto alcanza con, para cada β_r, encontrar un automorfismo de $\mathcal{P}$ que actúe transitivamente restringido a β_r y deje fijos todos los puntos de α_s.

Caso 1: β_r interseca con un ciclo de longitud más grande Δ_r en g_{t_r} para algún $t_r \neq s$.

En este caso, el Corolario 5.1.8 aplicado a β_r y Δ_r como ciclos de g_s y g_{t_r} respectivamente nos dice que $\mathcal{O}_{\beta_r} \subseteq \mathcal{O}_{\Delta_r}$. Más aún, nos dice que existe $l \in \mathbb{N}$ con $p \mid l$ tal que β_r es un ciclo de Δ_r^l, quien a su vez es una potencia contenida en g_s.

Si α_s no interseca con $\mathcal{O}_{g_{t_r}}$ entonces la acción de $\langle g_{t_r}^l \rangle$ es transitiva si se la restringe a $\mathcal{O}_{\beta_r}$ y además deja fijos los puntos de $\mathcal{O}_{\alpha_s}$, obteniendo el resultado esperado.

Si α_s interseca con un ciclo δ de g_{t_r}, como no puede haber intersecciones raras involucrando α_s por ser un ciclo de longitud máxima y $|\alpha_s| \geqslant |\delta|$ por ser α_s dominante, por el

Corolario 5.1.8 aplicado a la intersección de α_s y δ como ciclos de g_s y g_{t_r} respectivamente, sabemos que existe $k \in \mathbb{N}$ tal que la potencia α_s^k está contenida en g_{t_r}.

Notemos que $g_s^{-k} g_{t_r}$ deja fijos los puntos de α_s pero sí contiene al ciclo Δ_r^{1-kl}, que es un único ciclo por ser $mcd(p, 1-kl) = 1$. Luego, la acción de $\langle (g_s^{-k} g_{t_r})^l \rangle$ es transitiva si se la restringe a $\mathcal{O}_{\beta_r}$ (ya que contiene la potencia $(\Delta^l)^{1-kl}$ y $1-kl$ es coprimo con p), y además deja fijos los puntos de $\mathcal{O}_{\alpha_s}$, como queríamos.

Caso 2: β_r no interseca con un ciclo más grande Δ_r en g_{t_r} para ningún $t_r \neq s$.

Por hipótesis, sucede que β_r tiene intersección no vacía con un ciclo de igual longitud η_r de g_{t_r} para algún $t_r > s$ y con $\mathcal{O}_{\eta_r} = \mathcal{O}_{\beta_r}$, ya que no hay intersecciones raras involucrando puntos de β_r. Luego, como $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{g_t} = \emptyset$ para todo $t > s$, la acción de $\langle g_{t_r} \rangle$ es transitiva en $\mathcal{O}_{\eta_r}$ (luego en $\mathcal{O}_{\beta_r}$), y deja fijos los puntos de $\mathcal{O}_{\alpha_s}$.

En ambos casos logramos probar que, dados $1 \leqslant r \leqslant m_s$ e $y_0 \in \mathcal{O}_{\alpha_s}$, si un punto x_0 en β_r cumple $x_0 \geqslant y_0$ (respectivamente $\leqslant$ o incomparable), entonces $x \geqslant y_0$ (respectivamente $\leqslant$ o incomparable) para todo x punto de β_r.

Ahora, dado cualquier punto $y \in \mathcal{O}_{\alpha_s}$, sabemos que existe z de modo que $g_s^z \cdot y_0 = y$.
Por lo tanto, aplicando g_s^z a la desigualdad anterior, obtenemos $g_s^z \cdot x \geqslant g_s^z \cdot y_0 = y$ (respectivamente $\leqslant$ o incomparable). Por lo probado en el párrafo anterior, como $g_s^z \cdot x \in \mathcal{O}_{\beta_r}$, esto implica que $x \geqslant y$ (respectivamente $\leqslant$ o incomparable) para cualquier $x \in \mathcal{O}_{\beta_r}$.

Esto último prueba que, para cada $1 \leqslant r \leqslant m_s$, todos los puntos de α_s se relacionan de la misma forma con todos los puntos de β_r. $(\star)$

Ahora, consideramos la acción de $\langle g_s^{p^{c_s-1}} \rangle$ que deja fijos todos los puntos de $\mathcal{O}_{g_s}$ que no pertenecen a ciclos de longitud máxima.

Dado que los puntos de α_s forman una anticadena, y además se cumple $(\star)$, para todo $x \in \mathcal{O}_{\alpha_s}$ se cumplen:

$$\mathcal{P}_{<x} = \mathcal{P}_{<g_s^{p^{c_s-1}} x} \quad \text{y} \quad \mathcal{P}_{>x} = \mathcal{P}_{>g_s^{p^{c_s-1}} x}.$$

Por lo tanto, existe un automorfismo de $\mathcal{P}$ que intercambia dos puntos de α_s, digamos x y $g_s^{p^{c_s-1}} x$ y deja a todos los demás fijos. Esto es absurdo ya que $\mathrm{Aut}(\mathcal{P})$ no contiene trasposiciones involucrando dos puntos de α_s. ∎

Subcaso 2.1: Si este nuevo ciclo no es de tipo γ.

De ser así, obtenemos el resultado deseado, ya que tendremos p^{c_s} puntos para recolectar de un segundo ciclo dominante que no es de tipo γ. Es decir, podemos definir $C(s) = C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \mathcal{O}_\eta$, donde η es el ciclo en cuestión. Veamos que cumple las seis condiciones:

(1) Como η es dominante y no es de tipo γ, por la condición 3, $\mathcal{O}_\eta \cap C(s+1) = \emptyset$.

Recordemos que $\mathcal{O}_{\alpha_s} \cap C(s+1) = \emptyset$, por cumplirse $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{g_r} = \emptyset$ para todo $r > s$.

Luego, como α_s y η también son disjuntos,

$$|C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \mathcal{O}_\eta| = |C(s+1)| + |\mathcal{O}_{\alpha_s}| + |\mathcal{O}_\eta| \geqslant \sum_{j=s+1}^{N} 2p^{c_j} + 2p^{c_s}.$$

(2) No usamos puntos de ciclos dominantes de tipo γ, pues los ciclos dominantes son disjuntos dos a dos y usamos dos ciclos dominantes que no son de tipo γ; y, además, vale la condición 2 con $i = s+1$.

(3) No usamos puntos de ciclos de g_j con $j < s$ que sean dominantes y no de tipo γ, pues los ciclos dominantes son disjuntos y usamos dos ciclos dominantes de g_s; y, además vale la condición 3 con $i = s+1$.

(4) Por ser η y α_s de longitud máxima y A subconjunto bueno, la Observación 5.3.3 nos dice que $\mathcal{O}_\eta \cap J(A) = \emptyset$ y $\mathcal{O}_{\alpha_s} \cap J(A) = \emptyset$.

Además, por la condición 4 con $i = s+1$, $C(s+1) \cap J(A) = \emptyset$

(5) $C(s+1) \subseteq C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \mathcal{O}_\eta$.

(6) Tanto α_s como η son ciclos dominantes de g_s, eso sumado a la condición 6 con $i = s+1$ prueba que se cumple para $i = s$

Esto concluye la demostración en el Subcaso 2.1.

Subcaso 2.2: Si el ciclo que nos provee la Afirmación 5.3.13 es de tipo γ, es decir, es $\gamma_{s,q}$ para algún $q > s$.

Afirmación 5.3.14: Dado un ciclo $\gamma_{s,b}$ de g_s dominante y de tipo γ, debe existir al menos un ciclo dominante ϵ de g_s distinto de $\gamma_{s,b}$ que cumpla $\mathcal{O}_\epsilon \cap \mathcal{O}_\beta \neq \emptyset$ para algún ciclo β de longitud máxima en g_b.

Demostración. Empecemos probando que existe algún ciclo de g_s distinto de $\gamma_{s,b}$ que interseca con algún ciclo de longitud máxima de g_b.

Supongamos, a modo de contradicción, que todos los ciclos distintos de $\gamma_{s,b}$ de g_s intersecan sólo con ciclos de longitud no máxima de g_b o bien con ningún ciclo de g_b.
Por un lado, sabemos que todos los puntos de $\gamma_{s,b}$ se relacionan de la misma forma con cada punto de $\mathcal{P} - \mathcal{O}_{g_s}$, ya que la acción de $\langle g_s \rangle$ restringida a $\gamma_{s,b}$ es transitiva y deja fijos todos los puntos de dicho conjunto.
Por otro lado, la acción de $\langle g_b^{p^{c_b-1}} \rangle$ tiene al menos dos puntos de $\gamma_{s,b}$ en una misma órbita, pero deja fijos los puntos de los ciclos de g_s distintos de $\gamma_{s,b}$ ya que $\mathcal{O}_{\alpha_b} \subseteq \mathcal{O}_{\gamma_{s,b}}$ y α_b es de

longitud máxima (así que todos los puntos de $\gamma_{s,b}$ pertenecen a ciclos de longitud máxima de g_b). Luego, estos dos puntos se relacionan de la misma forma con cada puntos de $\mathcal{O}_{g_s} - \mathcal{O}_{\gamma_{s,b}}$. Esto sumado a lo visto en el párrafo anterior implica que existe un automorfismo de $\mathcal{P}$ que intercambia dos puntos de $\gamma_{s,b}$ y deja todos los demás fijos, lo cuál es absurdo pues $\mathrm{Aut}(\mathcal{P})$ no contiene trasposiciones de dos puntos de un ciclo de tipo γ. Por lo tanto, existe al menos un ciclo de g_s distinto de $\gamma_{s,b}$ que interseca con algún ciclo de longitud máxima de g_b.

Ahora, probemos que no puede suceder que todos los ciclos de g_s distintos de $\gamma_{s,b}$ que intersecan con ciclos de longitud máxima de g_b no sean dominantes.

Llamemos $\delta_1, \dots, \delta_{d_s}$ a los ciclos de g_s distintos de $\gamma_{s,b}$ que intersecan con algún ciclo de longitud máxima de g_b. Ahora supongamos, a modo de contradicción, que para todo $1 \leqslant r \leqslant d_s$ sucede que δ_r tiene intersección no vacía con algún ciclo más grande η_r de g_{t_r} para algún $t_r \neq s$ o bien con un ciclo de igual longitud η_r de g_{t_r} para algún $t_r > s$.

Para lo que sigue será importante notar que, gracias a la Observación 5.3.3, podemos afirmar que no hay intersecciones raras involucrando puntos de ningún δ_r.
Vamos a probar que, para cada uno de estos ciclos, todos sus puntos se relacionan de la misma forma con cada punto de $\gamma_{s,b}$. Para esto alcanza con, para cada δ_r, encontrar un automorfismo de $\mathcal{P}$ que actúe transitivamente restringido a δ_r y deje fijos todos los puntos de $\gamma_{s.b}$.

Caso 1: δ_r interseca con un ciclo de longitud más grande Δ_r en g_{t_r} para algún $t_r \neq s$.

En este caso, el Corolario 5.1.8 aplicado a δ_r y Δ_r como ciclos de g_s y g_{t_r} respectivamente nos dice que $\mathcal{O}_{\delta_r} \subseteq \mathcal{O}_{\Delta_r}$. Más aún, nos dice que existe $l \in \mathbb{N}$ con $p \mid l$ tal que δ_r es un ciclo de Δ_r^l, quien a su vez está contenido en g_s.

Si $\gamma_{s,b}$ no interseca con g_{t_r} entonces la acción de $\langle g_{t_r}^l \rangle$ es transitiva si se la restringe a $\mathcal{O}_{\delta_r}$ y además deja fijos los puntos de $\mathcal{O}_{\gamma_{s,b}}$, obteniendo el resultado esperado.

Si $\gamma_{s,b}$ interseca con un ciclo μ de g_{t_r}, como no puede haber intersecciones raras involucrando $\gamma_{s,b}$ por la Observación 5.3.3, como $\gamma_{s,b}$ es dominante, por el Corolario 5.1.8 aplicado a la intersección de $\gamma_{s,b}$ y μ como ciclos de g_s y g_{t_r} respectivamente, sabemos que existe $k \in \mathbb{N}$ tal que la potencia $\gamma_{s,b}^k$ está contenida en g_{t_r}.

Notemos que $g_s^{-k} g_{t_r}$ deja fijos los puntos de $\gamma_{s,b}$ pero sí contiene al ciclo Δ_r^{1-kl}, que es un único ciclo por ser $mcd(p, 1-kl) = 1$. Luego, la acción de $\langle (g_s^{-k} g_{t_r})^l \rangle$ es transitiva si se la restringe a $\mathcal{O}_{\delta_r}$ (ya que contiene la potencia $(\Delta^l)^{1-kl}$ y $1-kl$ es coprimo con p), y además deja fijos los puntos de $\gamma_{s,b}$ como queríamos.

Caso 2: δ_r no interseca con un ciclo de longitud más grande Δ_r en g_{t_r} para ningún $t_r \neq s$.

Por hipótesis, sucede que δ_r tiene intersección no vacía con un ciclo de igual longitud η_r de g_{t_r} para algún $t_r > s$ y con $\mathcal{O}_{\eta_r} = \mathcal{O}_{\delta_r}$, ya que no hay intersecciones raras involucrando puntos de β_r.

Más aún, por el Corolario 5.1.8 aplicado a la intersección entre δ_r y η_r como ciclos de g_s y g_{t_r} respectivamente, existe $l \in \mathbb{N}$ tal que δ_r es un ciclo de η_r^l, quien a su vez es una potencia contenida en g_s.

Si $\gamma_{s,b}$ no interseca con $\mathcal{O}_{g_{t_r}}$ entonces la acción de $\langle g_{t_r} \rangle$ es transitiva en $\mathcal{O}_{\delta_r}$ y deja fijos los puntos de $\mathcal{O}_{\gamma_{s,b}}$, obteniendo el resultado esperado.

Si $\gamma_{s,b}$ interseca con un ciclo μ de g_{t_r}, como no puede haber intersecciones raras involucrando $\gamma_{s,b}$ por la Observación 5.3.3, $t_r > s$ y $\gamma_{s,b}$ es un ciclo dominante, el Corolario 5.1.8 aplicado a la intersección de $\gamma_{s,b}$ y μ como ciclos de g_s y g_{t_r} respectivamente nos dice que existe $k \in \mathbb{N}$ con $p \mid k$ tal que la potencia $\gamma_{s,b}^k$ está contenida en g_{t_r}.

Notemos que $g_s^{-k} g_{t_r}$ deja fijos los puntos de $\gamma_{s,b}$ pero sí contiene al ciclo η_r^{1-kl}, que es un único ciclo por ser $mcd(p, 1-kl) = 1$. Luego, la acción de $\langle (g_s^{-k} g_{t_r})^l \rangle$ es transitiva si se la restringe a $\mathcal{O}_{\delta_r}$ (ya que contiene la potencia $(\eta^l)^{1-kl}$ y $1-kl$ es coprimo con p) y deja fijos los puntos de $\mathcal{O}_{\gamma_{s,b}}$ como queríamos.

En ambos casos logramos probar que, dados $1 \leqslant r \leqslant d_s$ e $y_0 \in \mathcal{O}_{\gamma_{s,b}}$, si un punto x_0 en δ_r cumple $x_0 \geqslant y_0$ (respectivamente $\leqslant$ o incomparable), entonces $x \geqslant y_0$ (respectivamente $\leqslant$ o incomparable) para todo x punto de δ_r.

Ahora, dado cualquier punto $y \in \mathcal{O}_{\gamma_{s,b}}$, sabemos que existe z de modo que $g_s^z \cdot y_0 = y$.
Por lo tanto, aplicando g_s^z a la desigualdad anterior, obtenemos $g_s^z \cdot x \geqslant g_s^z \cdot y_0 = y$ (respectivamente $\leqslant$ o incomparable). Por lo probado en el párrafo anterior, como $g_s^z \cdot x \in \mathcal{O}_{\delta_r}$, esto implica que $x \geqslant y$ (respectivamente $\leqslant$ o incomparable) para cualquier $x \in \mathcal{O}_{\delta_r}$.

Esto último prueba que, para cada $1 \leqslant r \leqslant m_s$, todos los puntos de $\gamma_{s,b}$ se relacionan de la misma forma con todos los puntos de δ_r. $(\star\star)$

Finalmente, la acción de $\langle g_b^{p^{c_b-1}} \rangle$ en $\mathcal{P}$ tiene al menos dos puntos de $\mathcal{O}_{\gamma_{s,b}}$ en una misma órbita, pero deja fijos los puntos de $\mathcal{O}_{\alpha_s}$ (pues $b > s$) y los de los ciclos de g_s que sólo intersecan con ciclos de longitud no máxima (o ninguno) de g_b.
Además, todos los puntos de $\gamma_{s,b}$ se relacionan de la misma forma con cada punto de $\mathcal{P} - \mathcal{O}_{g_s}$ ya que la acción de $\langle g_s \rangle$ es transitiva si se la restringe a $\mathcal{O}_{\gamma_{s,b}}$ y deja fijos los puntos de $\mathcal{P} - \mathcal{O}_{g_s}$.
Como los puntos de $\gamma_{s,b}$ forman una anticadena y vale $(\star\star)$, si x e y son los puntos en la misma órbita, se cumplirá que

$$\mathcal{P}_{<x} = \mathcal{P}_{<y} \quad \text{y} \quad \mathcal{P}_{>x} = \mathcal{P}_{>y}.$$

Por lo tanto, existe un automorfismo que intercambia dos puntos de $\gamma_{s,b}$ y deja a todos los demás fijos. Esto es absurdo ya que $\mathrm{Aut}(\mathcal{P})$ no contiene trasposiciones involucrando ciclos

de tipo γ. Esto quiere decir que existe al menos un ciclo dominante de g_s distinto de $\gamma_{s,b}$ que interseca con un ciclo de longitud máxima de g_b. ■

Aplicando la afirmación anterior con $b = q$, vemos que debe existir al menos un ciclo dominante ϵ_1 de g_s distinto de $\gamma_{s,q}$, y cumpliendo $\mathcal{O}_{\epsilon_1} \cap \mathcal{O}_{\beta_1} \neq \emptyset$ para algún ciclo β_1 de longitud máxima en g_q. Como ϵ_1 es un ciclo dominante de g_s y $\mathcal{O}_{\epsilon_1} \cap \mathcal{O}_{\beta_1} \neq \emptyset$ con β_1 un ciclo de longitud máxima de g_q, deberá ser $|\mathcal{O}_{\epsilon_1}| \geqslant p^{c_q+1}$.

Subcaso 2.2.1: Si este ciclo ϵ_1 no es de tipo γ.

Podemos definir $C(s) = C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \mathcal{O}_{\gamma_{s,q}} \cup \mathcal{O}_{\epsilon_1}$. Veamos que cumple las cinco condiciones:

(1) Por la condición 3 con $i = s+1$, se cumple que $\mathcal{O}_{\epsilon_1} \cap C(s+1) = \emptyset$.

Recordemos que $\mathcal{O}_{\alpha_s} \cap C(s+1) = \emptyset$, por cumplirse $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{g_r} = \emptyset$ para todo $r > s$.

Luego, por la condición 2 con $i = s+1$, y por ser $\alpha_s, \gamma_{s,q}$ y ϵ_1 ciclos disjuntos,

$$\begin{aligned}\left|C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \mathcal{O}_{\gamma_{s,q}} \cup \mathcal{O}_{\epsilon_1}\right| &\geqslant |C(s+1)| + |\mathcal{O}_{\alpha_s}| + \left|\mathcal{O}_{\gamma_{s,q}}\right| - 2p^{c_q} + |\mathcal{O}_{\epsilon_1}| \\ &\geqslant \left(\sum_{j=s+1}^{N} 2p^{c_j}\right) + p^{c_s} + p^{c_s} - 2p^{c_q} + p^{c_q+1} \\ &\geqslant \left(\sum_{j=s+1}^{N} 2p^{c_j}\right) + 2p^{c_s}.\end{aligned}$$

(2) No usamos puntos de ciclos de g_j con $j < s$ que sean dominantes, ya que sólo usamos ciclos dominantes de g_s, que por definición tienen intersección vacía con cualquier ciclo dominante de g_j con $j < s$.

(3) Por la misma razón que el ítem anterior.

(4) Por ser $\epsilon_1 \cap \beta_1 \neq \emptyset$ con β_1 ciclo de longitud máxima de g_q, la Observación 5.3.3 nos asegura que todos los puntos de ϵ_1 pertenecen a ciclos de longitud máxima de g_q. Como A es un subconjunto bueno, $\mathcal{O}_{\epsilon_1} \cap J(A) = \emptyset$.

Además, como $\mathcal{O}_{\gamma_{s,q}}$ y α_s, son de longitud máxima, por ser A un subconjunto bueno, $\mathcal{O}_{\gamma_{s,q}} \cap J(A) = \mathcal{O}_{\alpha_s} \cap J(A) = \emptyset$.

Por último, la condición 4 con $i = s+1$ nos dice que $C(s+1) \cap J(A) = \emptyset$.

(5) $C(s+1) \subseteq C(s+1) \cup D$.

(6) Tanto $\gamma_{s,q}$ como ϵ_1 son ciclos dominantes de g_s, eso sumado a la condición 6 con $i = s+1$ prueba que se cumple para $i = s$

Esto termina la demostración en el Subcaso 2.2.1.

Subcaso 2.2.2: Si ϵ_1 es de tipo γ.

Para ser consistentes con la notación, será $\epsilon_1 = \gamma_{s,\nu_1}$ para algún $\nu_1 > q$. Esta última desigualdad se da porque la Observación 5.3.2 nos dice que $\mathcal{O}_{\gamma_{s,\nu_1}} \subseteq \mathcal{O}_{g_q}$ y entonces $\mathcal{O}_{\alpha_{\nu_1}} \subseteq \mathcal{O}_{\gamma_{s,\nu_1}} \subseteq \mathcal{O}_{g_q}$; eso sólo puede ocurrir si $\nu_1 \geqslant q$, pero como γ_{s,ν_1} es un ciclo disjunto con los puntos de α_q — porque están contenidos en $\gamma_{s,q}$ — no puede ser $\nu_1 = q$, así que $\nu_1 > q$.

Como $\gamma_{s,q}$ es disjunto con g_{ν_1} (por ser $\nu_1 > q$, $\mathcal{O}_{\alpha_q} \subseteq \mathcal{O}_{\gamma_{s,q}}$ y la Observación 5.3.2), podemos aplicar la Afirmación 5.3.14 para probar que existe al menos un ciclo dominante ϵ_2 de g_s distinto de γ_{s,ν_1} y $\gamma_{s,q}$, y cumpliendo $\mathcal{O}_{\epsilon_2} \cap \mathcal{O}_{\beta_2} \neq \emptyset$ para algún ciclo β_2 de longitud máxima en g_{ν_1}.

A partir de ahora, comenzando con $i = 2$, siempre que ϵ_i sea un ciclo de tipo γ, digamos γ_{s,ν_i}, podemos definir ϵ_{i+1} como el ciclo que nos provee la Afirmación 5.3.14, que es un ciclo dominante de g_s que cumple $\mathcal{O}_{\epsilon_{i+1}} \cap \mathcal{O}_{\beta_{i+1}} \neq \emptyset$ para algún ciclo β_{i+1} de longitud máxima en g_{ν_i}. Es distinto de γ_{s,ν_i} según la afirmación, pero también será distinto de $\gamma_{s,q}, \gamma_{s,\nu_1}, \ldots, \gamma_{s,\nu_{i-1}}$. En efecto, por un argumento análogo al que usamos para probar que $\nu_1 > q$, podemos probar que $\nu_{j+1} > \nu_j$ para todo j, así que basta con notar que $\mathcal{O}_{\gamma_{s,\nu_j}} \cap \mathcal{O}_{g_{\nu_i}} = \emptyset$ para todo $j < i$ y $\mathcal{O}_{\gamma_{s,q}} \cap \mathcal{O}_{g_{\nu_i}} = \emptyset$. Además, por ser dominante, deberá cumplirse que $\left|\mathcal{O}_{\epsilon_{i+1}}\right| \geqslant p^{c_{\nu_i}+1}$.

Como hay finitos generadores y $\nu_{i+1} > \nu_i$ para todo i (por un argumento análogo al que usamos para probar que $\nu_1 > q$), eventualmente nos encontraremos por primera vez con un índice, digamos j, de modo que ϵ_j no es un ciclo de tipo γ, y en esa situación detenemos el proceso de definición.

Ahora, afirmamos que entre los ciclos $\alpha_s, \gamma_{s,q}, \epsilon_1, \epsilon_2, \ldots, \epsilon_j$ juntamos la cantidad de puntos necesaria.

En efecto, definamos

$$C(s) = C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \mathcal{O}_{\gamma_{s,q}} \cup \bigcup_{i=1}^{j} \mathcal{O}_{\epsilon_i}$$

y veamos que se cumplen las seis condiciones:

(1) Definamos $\nu_0 = q$ y recordemos que $\epsilon_r = \gamma_{s,\nu_r}$ para todo $1 \leqslant r \leqslant j-1$.

Recordemos que $\mathcal{O}_{\alpha_s} \cap C(s+1) = \emptyset$, por cumplirse $\mathcal{O}_{\alpha_s} \cap \mathcal{O}_{g_r} = \emptyset$ para todo $r > s$.

Además, por la condición 3 con $i = s+1$, $\mathcal{O}_{\epsilon_j} \cap C(s+1) = \emptyset$.

Por la condición 2 con $i = s+1$, para todo $0 \leqslant r \leqslant j-1$ sabemos que

$$\left|C(s+1) \cap \mathcal{O}_{\gamma_{s,\nu_r}}\right| \leqslant 2p^{c_{\nu_r}}$$

y como todos estos ciclos son disjuntos dos a dos, tenemos

$$\begin{aligned}
|C(s)| &= \left|C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \bigcup_{r=0}^{j-1} \mathcal{O}_{\gamma_{s,\nu_r}} \cup \mathcal{O}_{\epsilon_j}\right| \\
&= |C(s+1)| + |\mathcal{O}_{\alpha_s}| + \left|\mathcal{O}_{\gamma_{s,q}}\right| + \left|\bigcup_{r=1}^{j-1} \mathcal{O}_{\gamma_{s,\nu_r}}\right| - \sum_{r=0}^{j-1} 2p^{c_{\nu_r}} + \left|\mathcal{O}_{\epsilon_j}\right| \\
&\geqslant \left(\sum_{r=s+1}^{N} 2p^{c_r}\right) + 2p^{c_s} + \left(\sum_{r=1}^{j-1} p^{c_{\nu_{r-1}+1}}\right) - \sum_{r=0}^{j-1} 2p^{c_{\nu_r}} + p^{c_{\nu_{j-1}+1}} \\
&= \left(\sum_{r=s+1}^{N} 2p^{c_r}\right) + 2p^{c_s} + \left(\sum_{r=0}^{j-1} p^{c_{\nu_r+1}} - \sum_{r=0}^{j-1} 2p^{c_{\nu_r}}\right) \\
&\geqslant \left(\sum_{r=s+1}^{N} 2p^{c_r}\right) + 2p^{c_s}.
\end{aligned}$$

(2) No usamos puntos de ciclos de g_j con $j < s$ que sean dominantes, ya que sólo usamos ciclos dominantes de g_s, que por definición son disjuntos con cualquier ciclo dominante de g_j con $j < s$.

(3) Por la misma razón que el ítem anterior.

(4) Para todo $1 \leqslant r \leqslant j$, por ser $\epsilon_r \cap \beta_r \neq \emptyset$ con β_r algún ciclo de longitud máxima de $g_{\nu_{r-1}}$, la Observación 5.3.3 nos asegura que todos los puntos de ϵ_r pertenecen a ciclos de longitud máxima de $g_{\nu_{r-1}}$. Como A es un subconjunto bueno, $\mathcal{O}_{\epsilon_r} \cap J(A) = \emptyset$.

Además, como $\mathcal{O}_{\gamma_{s,q}}$ y α_s son de longitud máxima, por ser A un subconjunto bueno, $\mathcal{O}_{\gamma_{s,q}} \cap J(A) = \mathcal{O}_{\alpha_s} \cap J(A) = \emptyset$.

Por último, la condición 4 con $i = s+1$ nos dice que $C(s+1) \cap J(A) = \emptyset$.

(5) $C(s+1) \subseteq C(s+1) \cup \mathcal{O}_{\alpha_s} \cup \bigcup_{r=0}^{j-1} \mathcal{O}_{\gamma_{s,\nu_r}} \cup \mathcal{O}_{\epsilon_j}$.

(6) Tanto α_s, como ϵ_j, como γ_{s,ν_r} para todo $1 \leqslant r \leqslant j-1$ son ciclos dominantes de g_s; eso sumado a la condición 6 con $i = s+1$ prueba que se cumple para $i = s$

Habiendo agotado todos los casos, la demostración de la proposición está completa. ■

Aplicando el resultado anterior con $i = 1$, conseguimos probar que el tamaño del complemento de los puntos fijos de la acción de $\mathrm{Aut}(\mathcal{P})$ en $\mathcal{P}$ es al menos

$$|J(A)| + \sum_{i=1}^{N} 2|g_i| \geqslant \sum_{i \notin A} 2|h_i| + \sum_{i \in A} 2|h_i| = \sum_{i=1}^{n} 2|h_i|.$$

Esto prueba, en particular, el Teorema 5.0.1, y tiene la siguiente consecuencia.

Teorema 5.3.15: Para todo $p \geqslant 11$ primo y $a_1, \dots a_n \in \mathbb{N}$,

$$\beta\left(\bigoplus_{i=1}^{n} \mathbb{Z}_{p^{a_i}}\right) = \sum_{i=1}^{n} 2p^{a_i}.$$

Demostración. Probar que $\beta\left(\prod_{i=1}^{n} \mathbb{Z}_{p^{a_i}}\right) \geqslant \sum_{i=1}^{n} 2p^{a_i}$ es el trabajo que hicimos a lo largo de este capítulo. Para la otra desigualdad alcanza con encontrar un ejemplo.
Por el caso cíclico, como $p \geqslant 11$, para cada $1 \leqslant i \leqslant n$ existe un poset $\mathcal{P}_i$ con $2p^{a_i}$ puntos y $\mathrm{Aut}(\mathcal{P}_i) \simeq \mathbb{Z}_{p^{a_i}}$. Luego, podemos considerar el join

$$\mathcal{P} = \mathcal{P}_1 \oplus \cdots \oplus \mathcal{P}_n$$

que cumple exactamente lo necesario. ∎

Bibliografía

[Arl85] William C. Arlinghaus, *The classification of minimal graphs with given abelian automorphism group*, Mem. Amer. Math. Soc. **57** (1985), no. 330, viii+86, DOI 10.1090/memo/0330. MR803975 ↑6, 7, 9, 29, 73

[Arl79] William Charles Arlinghaus, *THE STRUCTURE OF MINIMAL GRAPHS WITH GIVEN ABELIAN AUTOMORPHISM GROUP*, ProQuest LLC, Ann Arbor, MI, 1979. Thesis (Ph.D.)–Wayne State University. MR2630418 ↑7

[Bab74] László Babai, *On the minimum order of graphs with given group*, Canad. Math. Bull. **17** (1974), no. 4, 467–470, DOI 10.4153/CMB-1974-082-9. MR406855 ↑5

[Bab78] László Babai, *Infinite digraphs with given regular automorphism groups*, J. Combin. Theory Ser. B **25** (1978), no. 1, 26–46, DOI 10.1016/S0095-8956(78)80008-2. MR0498225 ↑6, 17

[Bab80] ———, *Finite digraphs with given regular automorphism groups*, Period. Math. Hungar. **11** (1980), no. 4, 257–270, DOI 10.1007/BF02107568. MR603394 ↑6, 8, 11, 12, 18, 19, 21, 24, 26, 28

[BM09] Jonathan Ariel Barmak and Elias Gabriel Minian, *Automorphism groups of finite posets*, Discrete Math. **309** (2009), no. 10, 3424–3426, DOI 10.1016/j.disc.2008.09.026. MR2528204 ↑8

[Bar20] Jonathan Ariel Barmak, *Automorphism groups of finite posets II*, arXiv:2008.04997 (2020). ↑8

[Bir46] Garrett Birkhoff, *On groups of automorphisms*, Rev. Un. Mat. Argentina **11** (1946), 155–157 (Spanish). MR15387 ↑8

[Fru39] R. Frucht, *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. **6** (1939), 239–250 (German). MR1557026 ↑5

[Fru50] Robert Frucht, *On the construction of partially ordered systems with a given group of automorphisms*, Amer. J. Math. **72** (1950), 195–199, DOI 10.2307/2372146. MR32628 ↑8

[God81] C. D. Godsil, *GRRs for nonsolvable groups*, Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), Colloq. Math. Soc. János Bolyai, vol. 25, North-Holland, Amsterdam-New York, 1981, pp. 221–239. MR642043 ↑6

[HP66] Frank Harary and Ed Palmer, *The smallest graph whose group is cyclic*, Czechoslovak Math. J. **16(91)** (1966), 70–71 (English, with Russian summary). MR194353 ↑7

[Hem78] Robert L. Hemminger, *Directed graphs with transitive abelian groups* (1978). ↑6

[Het76] D Hetzel, *Über reguläre graphische Darstellung von auflösbaren Gruppen* (1976). ↑5

[Imr69] Wilfried Imrich, *Graphen mit transitiver Automorphismengruppe*, Monatsh. Math. **73** (1969), 341–347, DOI 10.1007/BF01298984. MR255446 ↑5, 6

[Imr70] ———, *Graphs with transitive abelian automorphism group*, Combinatorial theory and its applications, Coll. Math. Soc. János Bolyai **4** (1970), 651–656. ↑5, 6

[Imr78] W. Imrich, *Graphical regular representations of groups of odd order*, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Amsterdam-New York, 1978, pp. 611–621. MR519296 ↑5

[Kön86] D. König, *Theorie der endlichen und unendlichen Graphen*, Teubner-Archiv zur Mathematik [Teubner Archive on Mathematics], vol. 6, BSB B. G. Teubner Verlagsgesellschaft, Leipzig, 1986 (German). Mit einer Abhandlung von L. Euler. [With a monograph by L. Euler]; With an introduction by Paul Erdős; Edited and with comments and an introduction by H. Sachs; With a biography of König by T. Gallai; With English, French and Russian summaries. MR886676 ↑5

[Mer63] R. L. Meriwether, *Smallest graphs with a given cyclic group* (1963).Unpublished, but see MR 33 (1967) #2563 ↑6

[McA65] M. H. McAndrew, *On graphs with transitive automorphism groups*, Notices Amer. Math. Soc. **12** (1965), 575. ↑5, 6

[MS17] Joy Morris and Pablo Spiga, *Classification of finite groups that admit an oriented regular representation*, Bulletin of the London Mathematical Society **50** (2017), DOI 10.1112/blms.12177. ↑6

[NW72a] Lewis A. Nowitz and Mark E. Watkins, *Graphical regular representations of non-abelian groups. I, II*, Canadian J. Math. **24** (1972), 993–1008; ibid. 24 (1972), 1009–1018, DOI 10.4153/CJM-1972-101-5. MR319804 ↑5

[NW72b] ———, *Graphical regular representations of non-abelian groups. I, II*, Canadian J. Math. **24** (1972), 993–1008; ibid. 24 (1972), 1009–1018, DOI 10.4153/CJM-1972-101-5. MR319804 ↑5

[Sab59] Gert Sabidussi, *On the minimum order of graphs with given automorphism group*, Monatsh. Math. **63** (1959), 124–127, DOI 10.1007/BF01299094. MR104596 ↑5, 6

[Sab58] ———, *On a class of fixed-point-free graphs*, Proc. Amer. Math. Soc. **9** (1958), 800–804, DOI 10.2307/2033090. MR97068 ↑5

[TSD19] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.9)* (2019), https://www.sagemath.org. ↑

[Tho72] M. C. Thornton, *Spaces with given homeomorphism groups*, Proc. Amer. Math. Soc. **33** (1972), 127–131, DOI 10.2307/2038184. MR292054 ↑8