



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

El anillo de Burnside para grupos nilpotentes finitos

Tesis presentada como requisito parcial para la obtención del título de

LICENCIADO EN MATEMÁTICAS

por

Diego Mora Antonio

Director de tesis

Dr. David Villa Hernández

Puebla Pue.
07 de junio de 2024

Título: El anillo de Burnside para grupos nilpotentes finitos
Estudiante: DIEGO MORA ANTONIO

COMITÉ

Dr. César Cejudo Castilla
Presidente

Dr. Carlos Alberto López Andrade
Secretario

Mtro. Cristhian Vázquez Rosas
Vocal

Agradecimientos

Agradezco sinceramente a mis padres, Jose Luis y Martina, quienes han sido la fuente inagotable de apoyo y aliento a lo largo de mi travesía académica. Su dedicación incansable y confianza en mí han sido el cimiento sobre el cual he construido mi camino hacia este logro significativo.

A mis hermanos, Jose Luis, Rocio y Rodrigo, les agradezco por ser mi red de respaldo constante. Su presencia ha iluminado mi viaje, haciendo que cada desafío se vuelva más llevadero y cada triunfo más significativo.

A mis adoradas mascotas, quienes con su presencia han llenado de alegría y calma mis días de estudio. Su apoyo emocional ha sido un regalo invaluable que ha hecho más placentera esta travesía académica.

Mi más sincero reconocimiento al Dr. David Villa, mi asesor de tesis, cuya paciencia, enseñanzas y orientación experta han sido pilares fundamentales en la culminación de este proyecto. Además de ser mi guía académica, agradezco el haber compartido con él uno de mis primeros cursos, una experiencia que despertó en mí un profundo interés por el álgebra.

Agradezco también a los distinguidos sinodales, el Dr. Cesar, el Dr. Carlos Alberto y el Mtro. Cristhian, por su valioso tiempo, revisión crítica y contribuciones que han enriquecido mi trabajo de investigación.

La culminación de una etapa de mi vida no sería completa sin reconocer a todas las personas extraordinarias que he tenido el privilegio de conocer a lo largo de mis estudios. A mis profesores, compañeros de clase y a quienes forman parte de mi red académica, les expreso mi gratitud por compartir conocimientos, experiencias y amistades que han contribuido significativamente a mi formación.

Quiero expresar mi agradecimiento a mis compañeros de vivienda por su apoyo constante, los momentos compartidos y la compañía que ha hecho más ligera esta travesía, quienes con su presencia han convertido mi espacio de vivienda en un hogar lleno de experiencias y aprendizajes compartidos.

Además, agradezco a todas las personas que de alguna manera han influido en mi desarrollo académico y personal. Desde los profesionales en la universidad hasta aquellos que, de manera indirecta, han dejado huella en mi camino, reconozco y agradezco la diversidad de experiencias que han contribuido a forjar la persona en la que me he convertido hoy en día.

Mi agradecimiento se extiende también a la Facultad de Ciencias Fisico Matemáticas y a la Benemérita Universidad Autónoma de Puebla. Este entorno académico ha sido el escenario donde he cultivado mis estudios, encontrando inspiración y recursos que han sido fundamentales para mi crecimiento.

Este logro no habría sido posible sin el apoyo de cada una de estas personas. Agradezco sinceramente por formar parte de este capítulo extraordinario en mi vida académica.

Índice general

1. Acciones de grupos en conjuntos	3
2. Teoremas de Sylow	11
3. Grupos nilpotentes finitos	15
4. El anillo de Burnside	21
5. El anillo de Burnside para grupos nilpotentes finitos	33
Bibliografía	39

Introducción

El objetivo principal de esta tesis se enfoca en el estudio de los grupos nilpotentes finitos y su anillo de Burnside, el cual es un invariante del grupo. Se pretende utilizar un resultado conocido, el Teorema 5.2, que caracteriza a un grupo nilpotente finito como el producto de sus subgrupos de Sylow. Para tal propósito se continúa el trabajo previo realizado en [1] proporcionando ejemplos adicionales y profundizando en el tema.

En el primer capítulo se presenta el teorema de Cayley, daremos un repaso a los principales conceptos en la teoría de los G -conjuntos introduciendo el concepto de acción de grupos en conjuntos, donde un grupo actúa sobre un conjunto a través de una operación que cumple ciertas propiedades. Se establece el marco teórico para comprender estas acciones y se presentan ejemplos ilustrativos de ellas, también introduciremos conceptos como órbitas y estabilizadores.

Para el segundo capítulo nos enfocaremos en los teoremas de Sylow, explorando resultados importantes como el Teorema de Cauchy y la ecuación de clase por mencionar algunos. Específicamente, el Teorema 2.11 desempeña un papel crucial en este trabajo, ya que permite caracterizar cuándo un grupo es el producto directo de sus subgrupos de Sylow.

En el tercer capítulo, se introducen la serie central inferior, la serie central superior y los grupos nilpotentes de clase c , con el propósito de demostrar que un grupo finito es nilpotente si y sólo si es el producto directo de sus subgrupos de Sylow (ver el Teorema 3.21).

El cuarto capítulo ofrece una revisión de los conceptos principales en la teoría de los anillos de Burnside, cubriendo la noción de marca y el anillo fantasma.

Finalmente, en el capítulo 5, se aplican los conceptos teóricos establecidos previamente y se explora cómo se pueden visualizar los anillos de Burnside utilizando las tablas de marcas, lo que proporciona una comprensión más intuitiva de estas estructuras algebraicas.

Capítulo 1

Acciones de grupos en conjuntos

En el contexto de este trabajo, la notación $H \leq G$ denotará que H es un subgrupo de G .

Teorema 1.1 (Cayley). *Sea G un grupo. Entonces, existe $H \leq S_G$ tal que $H \cong G$. En particular si $|G| = n$, entonces, $G \cong H \leq S_n$.*

Demostración. Recordemos que el grupo simétrico está definido como:

$$S_G = \{\alpha : G \rightarrow G \mid \alpha \text{ es función biyectiva}\}$$

Sea $a \in G$ arbitrario pero fijo, definamos:

$$\begin{aligned}\tau_a : G &\rightarrow G \\ g &\mapsto ag\end{aligned}$$

Veamos que $\tau_a \in S_G$. Sean $a, b \in G$ entonces:

$$\begin{aligned}\tau_b \circ \tau_a(g) &= \tau_b(ag) \\ &= b(ag) \\ &= (ba)g \\ &= \tau_{ba}(g)\end{aligned}$$

Por lo tanto $\tau_b \circ \tau_a = \tau_{ba}$. De aquí que $\tau_a \circ \tau_{a^{-1}} = \tau_e = 1_G = \tau_e = \tau_{a^{-1}} \circ \tau_a$, en donde:

$$\begin{aligned}1_G : G &\rightarrow G \\ g &\mapsto g\end{aligned}$$

es decir $\tau_a \in S_G$. Lo anterior nos permite definir:

$$\begin{aligned}\varphi : G &\rightarrow S_G \\ a &\mapsto \tau_a.\end{aligned}$$

En efecto φ es un homomorfismo inyectivo de grupos:

Como $\varphi(ab) = \tau_{ab} = \tau_a \circ \tau_b = \varphi(a)\varphi(b)$ para todo $a, b \in G$, tenemos que $\varphi(ab) = \varphi(a)\varphi(b)$.

Por lo anterior φ es un homomorfismo de grupos. Ahora, consideremos $a_1, a_2 \in G$ tales que $\tau_{a_1} = \tau_{a_2}$, entonces $a_1g = a_2g$, para toda $g \in G$, en particular $a_1e = a_2e$, por lo tanto $a_1 = a_2$, es decir, φ es inyectiva. Así, por el primer Teorema de isomorfismos de grupos, para:

$$\begin{aligned}\varphi : G &\rightarrow S_G \\ a &\mapsto \tau_a\end{aligned}$$

tenemos que $G \cong \frac{G}{\{0\}} = \frac{G}{\text{Ker}(\varphi)} \cong \text{Im}(\varphi) \leq S_G$.

■

Teorema 1.2. Sea G un grupo y $H \leq G$ con $[G : H] = n$, entonces existe un homomorfismo $\varphi : G \rightarrow S_n$ tal que $\text{Ker}(\varphi) \leq H$.

Demostración. Observemos que S_n y $S_{\frac{G}{H}}$ tienen $n!$ elementos cada uno por lo que $S_n \cong S_{\frac{G}{H}}$, donde:

$$\frac{G}{H} = \{gH \mid g \in G\}.$$

Sea $a \in G$ arbitrario pero fijo, definamos:

$$\begin{aligned} \tau_a : \frac{G}{H} &\rightarrow \frac{G}{H} \\ gH &\mapsto (ag)H \end{aligned}$$

Veamos que τ_a es una biyección. Sea $a, b \in G$, entonces:

$$\tau_b \circ \tau_a(gH) = b(ag)H = (ba)gH = \tau_{ba}(gH)$$

para cada $gH \in \frac{G}{H}$, por lo tanto:

$$\tau_b \circ \tau_a = \tau_{ba}$$

y de manera análoga al teorema anterior, obtenemos que τ_a es una biyección para cada a en G . De lo anterior, el siguiente es un homomorfismo de grupos:

$$\begin{aligned} \varphi : G &\rightarrow S_{\frac{G}{H}} \\ a &\mapsto \tau_a \end{aligned}$$

Probemos que $\text{ker}\varphi \subseteq H$. Sea $a \in \text{Ker}\varphi$, entonces $\tau_a = 1_{\frac{G}{H}}$, por lo que $\tau_a(gH) = gH$ para todo $gH \in \frac{G}{H}$, en particular:

$$\begin{aligned} aeH = eH &\Leftrightarrow aH = H \\ &\Leftrightarrow a \in H. \end{aligned}$$

Así $\text{ker}\varphi \leq H$. ■

Definición 1.3. Sea G un grupo y X un conjunto. Decimos que G actúa en X si existe una función:

$$* : G \times X \rightarrow X$$

tal que:

1. $e * x = x$, para todo $x \in X$ y $e \in G$ el elemento identidad.
2. $(g_1 g_2) * x = g_1 * (g_2 * x)$, para todo $x \in X$ y para todo $g_1, g_2 \in G$.

Ejemplo. Sea $a \in G$ arbitrario pero fijo y X un G -conjunto, veamos que G actúa en G con acción $a * g = ag$ y en $\frac{G}{H}$ con acción $a(gH) = (ag)H$. Definamos:

$$\begin{aligned} \tau_a : X &\rightarrow X \\ x &\mapsto a * x \end{aligned}$$

En efecto $\tau_a \in S_X$, sea $x \in X$:

$$\begin{aligned}\tau_b \circ \tau_a(x) &= \tau_b(a * x) \\ &= b * (a * x) \\ &= (ba) * x \\ &= \tau_{ba}(x).\end{aligned}$$

De este modo tenemos que:

$$\tau_b \circ \tau_a = \tau_{ba},$$

de donde:

$$\tau_a \circ \tau_{a^{-1}} = \tau_e.$$

Además $\tau_e(x) = e * x = x = 1_X(x)$, por lo que $\tau_e = 1_X$. De aquí que:

$$(\tau_a)^{-1} = \tau_{a^{-1}}.$$

Por lo tanto τ_a es biyección, es decir $\tau_a \in S_X$. Lo cual nos permite definir:

$$\begin{aligned}\varphi : G &\rightarrow S_X \\ a &\mapsto \tau_a\end{aligned}$$

El cual es un homomorfismo de grupos. Por otro lado, supongamos que existe $\varphi : G \rightarrow S_X$ un homomorfismo de grupos, veamos que G actúa en X con la siguiente acción:

$$\begin{aligned}* : G \times X &\rightarrow X \\ (a, x) &\mapsto a * x = (\varphi(a))(x) \text{ (} x \text{ evaluado en } \varphi(a)\text{)}\end{aligned}$$

tenemos que $\varphi(e) = 1_X$, por lo que para cada $x \in X$:

$$\begin{aligned}e * x &= (\varphi(e))(x) \\ &= 1_X(x) \\ &= x.\end{aligned}$$

Sean $a, b \in G$, entonces:

$$\begin{aligned}(ba) * x &= \varphi(ba)(x) \\ &= (\varphi(b) \circ \varphi(a))(x) \\ &= \varphi(b)(\varphi(a)(x)) \\ &= b * (\varphi(a)(x)) \\ &= b * (a * x).\end{aligned}$$

Por el Teorema 1.1 tenemos que G actúa en G con acción $a * g = ag$.

Por el Teorema 1.2 tenemos que G actúa en $\frac{G}{H}$ con acción $a(gH) = (ag)H$.

Ejemplo. Sea G un grupo. G actúa en G por conjugación, es decir, si $a, g \in G$, definimos:

$$a * g = aga^{-1}$$

1. $e * g = ege^{-1} = g$.

2.

$$\begin{aligned}(ab) * g &= abg(ab)^{-1} \\ &= a(bgb^{-1})a^{-1} \\ &= a * (b * g).\end{aligned}$$

Definición 1.4. Sea G un grupo y (X, \cdot) un G -conjunto. Sea $x_0 \in X$, definimos y denotamos el estabilizador como:

$$\text{Stab}_G(x_0) = \{g \in G \mid g \cdot x_0 = x_0\}.$$

Proposición 1.5. Sea G un grupo y (X, \cdot) un G -conjunto. Entonces, para $x_0 \in X$ se tiene que $\text{Stab}_G(x_0) \leq G$.

Demostración. 1. $e \cdot x_0 = x_0$, por lo que $e \in \text{Stab}_G(x_0)$.

2. Sean $a, b \in \text{Stab}_G(x_0)$,

$$\begin{aligned} (ab) \cdot x_0 &= a \cdot (b \cdot x_0) \\ &= a \cdot (x_0) \\ &= x_0. \end{aligned}$$

Entonces $ab \in \text{Stab}_G(x_0)$.

3. Si $a \in \text{Stab}_G(x_0)$, tenemos que $a^{-1} \cdot (a \cdot x_0) = a^{-1} \cdot x_0$, entonces $(a^{-1}a) \cdot x_0 = a^{-1} \cdot x_0$, es decir $x_0 = a^{-1} \cdot x_0$, por lo tanto $a^{-1} \in \text{Stab}_G(x_0)$.

Por lo tanto $\text{Stab}_G(x_0) \leq G$. ■

Definición 1.6. Sean X y Y dos G -conjuntos con acciones $*$, \cdot , respectivamente. Una funcion

$$\varphi : X \rightarrow Y$$

es un homomorfismo de G -conjuntos si $\varphi(a * x) = a \cdot \varphi(x)$ para cada $a \in G$ y para cada $x \in X$. Un isomorfismo de G -conjuntos es un homomorfismo de G -conjuntos biyectivo. En lo sucesivo utilizaremos esta notación $X \cong Y$ y diremos que X e Y son isomorfos como G -conjuntos.

Proposición 1.7. Sea G un grupo y (X, \cdot) un G -conjunto. La siguiente es una relacion de equivalencia en X :

Sean $x, y \in X$, $x \sim y$, si y solo si, existe $g \in G$ tal que $g \cdot x = y$.

Demostración. 1. $e \cdot x = x$, por lo que $x \sim x$.

2. Si $x \sim y$, entonces existe $g \in G$ tal que $g \cdot x = y$, por lo que $x = g^{-1} \cdot y$, de aquí que $y \sim x$.

3. Si además $y \sim z$, entonces existe $h \in G$ tal que $h \cdot y = z$, de este modo:

$$\begin{aligned} (hg) \cdot x &= h \cdot (g \cdot x) \\ &= h \cdot y \\ &= z. \end{aligned}$$

Por lo anterior $x \sim z$.

Así \sim es una relacion de equivalencia en X . ■

Definición 1.8. Sea X un G -conjunto y $x \in X$. Definimos y denotamos la órbita de x en G como:

$$\mathcal{O}_G(x) = \{y \in X \mid y = g \cdot x, \text{ con } g \in G\}.$$

Corolario 1.9. Las órbitas de un G -conjunto son ajenas y $X = \bigcup_{i \in I} \mathcal{O}(x_i)$ para algún conjunto de índices I .

Proposición 1.10. Sea X un G -conjunto y $x_0 \in X$. Entonces se cumple que como G -conjuntos:

$$\mathcal{O}_G(x_0) \cong \frac{G}{\text{Stab}_G(x_0)}.$$

Demostración. Si $(X, *)$ es un G -conjunto, observemos que $\mathcal{O}_G(x_0) \subseteq X$ de donde $\mathcal{O}_G(x_0)$ es un G -conjunto con la acción restringida a la órbita. Llamemos $H = \text{Stab}_G(x_0)$, entonces G actúa en $\frac{G}{H}$ con acción $a \cdot (gH) = agH$, donde $a \in G$ y $gH \in \frac{G}{H}$. Definamos:

$$\begin{aligned} \varphi : \mathcal{O}_G(x_0) &\rightarrow \frac{G}{H} \\ g * x_0 &\mapsto gH. \end{aligned}$$

Veamos que φ es un homomorfismo biyectivo de G -conjuntos. Tenemos que para cada $g_1, g_2 \in G$:

$$\begin{aligned} \varphi(g_1 * x_0) = \varphi(g_2 * x_0) &\Leftrightarrow g_1H = g_2H \\ &\Leftrightarrow g_2^{-1}g_1 \in H \\ &\Leftrightarrow (g_2^{-1}g_1) * x_0 = x_0 \\ &\Leftrightarrow g_1 * x_0 = g_2 * x_0. \end{aligned}$$

De lo anterior φ es inyectiva y está bien definida. Notemos que para cada $gH \in \frac{G}{H}$ se tiene que $\varphi(g * x_0) = gH$, por lo que φ es sobreyectiva. Por último, sea $a \in G$ y $g * x_0 \in \mathcal{O}_G(x_0)$

$$\begin{aligned} \varphi(a * (g * x_0)) &= \varphi((ag) * x_0) \\ &= agH \\ &= a \cdot (gH) \\ &= a \cdot (\varphi(g * x_0)). \end{aligned}$$

De aquí que φ es un homomorfismo biyectivo de G -conjuntos y por lo tanto:

$$\mathcal{O}_G(x_0) \cong \frac{G}{H}.$$

■

Corolario 1.11. *Sea X un G -conjunto y $x_0 \in X$ entonces:*

$$|\mathcal{O}_G(x_0)| = [G : \text{Stab}_G(x_0)].$$

Definición 1.12. *Sea G un grupo, $a \in G$ y $H \leq G$. Definimos y denotamos:*

1. El subgrupo centralizador de a en G :

$$C_G(a) = \{g \in G \mid ga = ag\}.$$

2. El subgrupo normalizador de H en G :

$$N_G(H) = \{g \in G \mid gH = Hg\}.$$

Ejemplos. *Calculemos las órbitas y los estabilizadores bajo distintas acciones de grupos en los siguientes ejemplos:*

1. Recordemos que G actúa en $\frac{G}{H}$:

$$\begin{aligned} \cdot : G \times \frac{G}{H} &\rightarrow \frac{G}{H} \\ (a, gH) &\mapsto a \cdot gH = agH. \end{aligned}$$

Sea $gH \in \frac{G}{H}$, observemos que:

$$gH = g \cdot eH \in \mathcal{O}_G(eH),$$

ademas, notemos que cada elemento en $\mathcal{O}_G(eH)$ es una clase lateral de H en G , lo que implica que $\mathcal{O}_G(eH) \subseteq \frac{G}{H}$, por lo que $\frac{G}{H} = \mathcal{O}_G(eH)$. Por otro lado, tenemos que:

$$\begin{aligned} \text{Stab}_G(gH) &= \{a \in G \mid agH = gH\} \\ &= \{a \in G \mid g^{-1}agH = H\} \\ &= \{a \in G \mid a \in gHg^{-1}\} \subseteq gHg^{-1}. \end{aligned}$$

Sea $ghg^{-1} \in gHg^{-1}$, entonces:

$$\begin{aligned} (ghg^{-1})gH &= (ghg^{-1}g)H \\ &= (gh)H \\ &= gH. \end{aligned}$$

Así $\frac{G}{H} = \mathcal{O}_G(eH)$ y $\text{Stab}(gH) = gHg^{-1}$.

2. G actúa en G con acción:

$$\begin{aligned} \cdot : G \times G &\rightarrow G \\ (a, g) &\mapsto a \cdot g = ag \end{aligned}$$

Notemos que $g = g \cdot e \in \mathcal{O}_G(e)$, por lo que:

$$G = \mathcal{O}_G(e).$$

Sea $g \in G$ entonces:

$$\text{Stab}_G(g) = \{a \in G \mid ag = g\} = \{e\}.$$

3. G actúa en G por conjugación:

$$\begin{aligned} \cdot : G \times G &\rightarrow G \\ (a, g) &\mapsto a \cdot g = aga^{-1} \end{aligned}$$

donde

$$\begin{aligned} \mathcal{O}_G(g) &= \{y \in G \mid y = a \cdot g, \text{ para algún } a \in G\} \\ &= \{y \in G \mid y = aga^{-1}, \text{ para algún } a \in G\}. \end{aligned}$$

$\mathcal{O}_G(g)$ es la clase de conjugación de g en G . Por otro lado, tenemos que:

$$\begin{aligned} \text{Stab}_G(g) &= \{a \in G \mid a \cdot g = g\} \\ &= \{a \in G \mid aga^{-1} = g\} \\ &= \{a \in G \mid ag = ga\} \\ &= C_G(g). \end{aligned}$$

4. Sea $X = \{H \subseteq G \mid H \text{ es subgrupo de } G\}$. G actúa en X por conjugación:

$$\begin{aligned} \cdot : G \times X &\rightarrow X \\ (a, H) &\mapsto a \cdot H = aHa^{-1} \end{aligned}$$

Tenemos que:

$$\begin{aligned}\mathcal{O}_G(H) &= \{K \subseteq X \mid K = a \cdot H \text{ para algún } a \in G\} \\ &= \{K \subseteq X \mid K = aHa^{-1} \text{ para algún } a \in G\}.\end{aligned}$$

De aquí que $\mathcal{O}_G(H)$ es la clase de conjugación de H . Por otro lado, tenemos que:

$$\begin{aligned}\text{Stab}_G(H) &= \{a \in G \mid a \cdot H = H\} \\ &= \{a \in G \mid aHa^{-1} = H\} \\ &= \{a \in G \mid aH = Ha\} \\ &= N_G(H).\end{aligned}$$

Teorema 1.13. Sea X un G -conjunto finito, con G un grupo finito. Si $X = \bigcup_{i=1}^N \mathcal{O}_G(x_i)$ entonces:

$$N = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|,$$

en donde $\text{fix}(g) = \{x \in X \mid gx = x\}$.

Demostración. Sea $\mathcal{A} = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Para cada $g \in G$ arbitrario pero fijo definamos:

$$\mathcal{A}_g = \{(g, x) \in G \times X \mid x \in \text{fix}(g)\}.$$

Observemos que $|\mathcal{A}_g| = |\text{fix}(g)|$, además $\mathcal{A} = \bigcup_{g \in G} \mathcal{A}_g$, donde esta unión es disjunta, es decir, los

conjuntos \mathcal{A}_g son disjuntos dos a dos. Por lo que $|\mathcal{A}| = \sum_{g \in G} |\text{fix}(g)|$. Ahora, para cada $x \in X$

arbitrario pero fijo definamos $\mathcal{A}_x = \{(g, x) \in G \times X \mid g \in \text{Stab}_G(x)\}$. Tenemos que $\mathcal{A} = \bigcup_{x \in X} \mathcal{A}_x$,

además $|\mathcal{A}_x| = |\text{Stab}_G(x)|$, por lo que:

$$\begin{aligned}|\mathcal{A}| &= \sum_{x \in X} |\mathcal{A}_x| \\ &= \sum_{x \in X} |\text{Stab}_G(x)| \\ &= \sum_{i=1}^N \sum_{x \in \mathcal{O}_G(x_i)} |\text{Stab}_G(x)| \\ &= \sum_{i=1}^N \sum_{x \in \mathcal{O}_G(x_i)} |\text{Stab}_G(x_i)|.\end{aligned} \tag{1.1}$$

Veamos que (1.1) se cumple. Sea $x \in \mathcal{O}_G(x_i)$, entonces existe $g \in G$ tal que $x = g \cdot x_i$, de este modo $\text{Stab}_G(x) = \text{Stab}_G(g \cdot x_i)$, notemos que:

$$\begin{aligned}a \in \text{Stab}_G(gx_0) &\Leftrightarrow a(gx_0) = gx_0 \\ &\Leftrightarrow (ag)x_0 = gx_0 \\ &\Leftrightarrow g^{-1}agx_0 = x_0 \\ &\Leftrightarrow g^{-1}ag \in \text{Stab}_G(x_0) \\ &\Leftrightarrow a \in g(\text{Stab}_G(x_0))g^{-1},\end{aligned}$$

por lo que $Stab_G(gx_0) = g(Stab_G(x_0))g^{-1}$, tomando lo anterior si $x \in \mathcal{O}_G(x_i)$ tenemos que $|Stab_G(x)| = |gStab_G(x_i)g^{-1}| = |Stab_G(x_i)|$. Por otro lado, recordemos que:

$$|\mathcal{O}_G(x_i)| = [G : Stab_G(x_i)] = \frac{|G|}{|Stab_G(x_i)|},$$

por consiguiente $|Stab_G(x_i)| = \frac{|G|}{|\mathcal{O}_G(x_i)|}$. Entonces:

$$\begin{aligned} |\mathcal{A}| &= \sum_{i=1}^N \sum_{x \in \mathcal{O}_G(x_i)} \frac{|G|}{|Stab_G(x_i)|} \\ &= |G| \sum_{i=1}^N \left(\sum_{x \in \mathcal{O}_G(x_i)} \frac{1}{|Stab_G(x_i)|} \right) \\ &= |G|N. \end{aligned}$$

De aquí que $|G|N = \sum_{g \in G} |fix(g)|$. Así:

$$N = \frac{1}{|G|} \sum_{g \in G} fix(g).$$

■

Para más detalles puede consultar [4] y [2, capítulo 2, sección 2.7].

Capítulo 2

Teoremas de Sylow

Teorema 2.1. (Cauchy) Sea G un grupo finito y $p \in \mathbb{Z}$ primo. Si p divide al orden de G , entonces existe $a \in G$ tal que a tiene orden p .

Demostración. Sea $|G| = pm$ con $m \geq 1$ y $p \in \mathbb{Z}$ primo.

Veamos que existe $a \in G$ tal que a tiene orden p (por inducción en m):

1. Si $m = 1$, tenemos que $|G| = p$, por lo que para todo $a \in G$, con $a \neq e$, a tiene orden p , es decir, $\langle a \rangle = G$.
2. Si $m > 1$, sabemos que G actúa en G por conjugación. Para cada $g \in G$ tenemos que $\mathcal{O}_G(g) = \{h \in G \mid h = aga^{-1} \text{ para algún } a \in G\}$, además $Stab_G(g) = C_G(g)$.

De aquí que:

$$|\mathcal{O}_G(g)| = [G : C_G(g)].$$

Observemos que, si $g \in Z(G) = \{a \in G \mid ab = ba, \text{ para toda } b \in G\}$, entonces tenemos que $aga^{-1} = gaa^{-1} = g$, por lo que:

$$|\mathcal{O}_G(g)| = 1, \text{ para cada } g \in Z(G).$$

Por otro lado, si $g \notin Z(G)$, entonces existe $a_0 \in G$ tal que $a_0g \neq ga_0$, tomando de lo anterior $a_0ga_0^{-1} \neq g = ege^{-1}$, notemos que hay al menos dos clases de conjugación de g , es decir:

$$|\mathcal{O}_G(g)| > 1, \text{ para cada } g \notin Z(G),$$

entonces $C_G(g) \subset G$. De aquí que:

- Si G es abeliano, existe $a \in G$ tal que a tiene orden p .
- Si $p \mid |C_G(g)|$ para algún $g \notin Z(G)$, entonces $|C_G(g)| = pm'$ con $m' < m$. Así, por hipótesis de inducción existe $a \in C_G(g) < G$ de orden p .
- Si $p \nmid |C_G(g)|$ para cada $g \notin Z(G)$, entonces, dado que $|\mathcal{O}_G(g)| = \frac{|G|}{|C_G(g)|}$, tenemos que $|G| = |C_G(g)||\mathcal{O}_G(g)|$. En consecuencia si $p \mid |G|$ implica que $p \mid |\mathcal{O}_G(g)|$ para cada $g \notin Z(G)$. Puesto que G es la unión de sus órbitas, al separar sus órbitas de tamaño 1 (una por cada elemento en el $Z(G)$) y las de tamaño mayor que 1 (para los elementos que no pertenecen al $Z(G)$), obtenemos la ecuación de clase:

$$|G| = |Z(G)| + \sum_{i \in I} [G : C_G(g_i)].$$

Donde I es un conjunto finito apropiado de índices tal que $g_i \notin Z(G)$. Así:

$$|G| - \sum_{i \in I} [G : C_G(g_i)] = |Z(G)|.$$

Recordemos $p \mid |G|$ y $p \mid [G : C_G(g_i)]$ para cada $g_i \notin Z(G)$, por lo que $p \mid |Z(G)|$. Por lo tanto existe $a \in Z(G) \subset G$ de orden p . ■

Corolario 2.2. Sea $p \in \mathbb{Z}$ primo. Si G es un grupo de orden p^2 , entonces G es abeliano.

Teorema 2.3. Si G es un grupo finito de orden p^n entonces para cada $1 \leq k \leq n$ existe $H \trianglelefteq G$ tal que $|H| = p^k$.

Definición 2.4. Un grupo finito G es un p -grupo con $p \in \mathbb{Z}$ primo si $|G| = p^n$ para algún $n \in \mathbb{N}$.

Definición 2.5. Sea G un grupo finito. Un subgrupo $P < G$ es un p -subgrupo de Sylow si P es un p -grupo máximo, es decir, si $H < G$ es un p -grupo tal que $P \subseteq H$, entonces $P = H$.

Proposición 2.6. Sea G un grupo finito y $S < G$ un p -subgrupo (posiblemente $S = \{e\}$). Entonces existe $P < G$ un p -subgrupo de Sylow tal que $S \subseteq P$.

Demostración. Si S es un p -subgrupo máximo, entonces es de Sylow y tenemos que $S \subseteq P$. En caso contrario, como S no es un p -subgrupo máximo existe $P_1 < G$ un p -subgrupo tal que $S \subsetneq P_1$, si P_1 es de Sylow hemos terminado la demostración. De no ser así existe $P_2 < G$ un p -subgrupo tal que $S \subsetneq P_1 \subsetneq P_2$, si P_2 es de Sylow hemos terminado la demostración.

Puesto que G es finito, el proceso también es finito (no mayor a $|G|$) de este modo eventualmente obtenemos $P_r < G$ un p -subgrupo máximo tal que:

$$S \subsetneq P_1 \subsetneq P_2 \subsetneq \dots \subsetneq P_r < G.$$

Por lo que P_r es un p -subgrupo de Sylow. ■

Lema 2.7. Sea G un grupo finito y $P < G$ un p -subgrupo de Sylow, entonces:

1. Para toda $a \in G$, aPa^{-1} es un p -subgrupo de Sylow.
2. $p \nmid |\frac{N_G(P)}{P}|$.
3. Sea $a \in G$ con $a \neq e$, tal que el orden(a) = p^m y $aPa^{-1} = P$ entonces $a \in P$.

Demostración. 1. Sea $a \in G$ arbitraria pero fija, definamos:

$$\begin{aligned} \gamma_a : P &\rightarrow aPa^{-1} \\ x &\mapsto axa^{-1} \end{aligned}$$

Tenemos que γ_a es biyectiva (con inversa $\gamma_{a^{-1}}$), entonces $|aPa^{-1}| = |P|$. Observemos que $aPa^{-1} < G$ es un p -subgrupo. Supongamos que aPa^{-1} no es p -subgrupo de Sylow, entonces existe $Q < G$ un p -subgrupo tal que $aPa^{-1} \subset Q$, así $P \subset a^{-1}Qa$ lo cual es una contradicción. Por lo tanto aPa^{-1} es un p -subgrupo de Sylow.

2. Supongamos que p divide a $|\frac{N_G(P)}{P}|$. Observemos (en general) que $P \trianglelefteq N_G(P)$, por lo que $\frac{N_G(P)}{P}$ es un grupo, entonces (por el Teorema de Cauchy) existe $aP \in \frac{N_G(P)}{P}$ de orden p . Sea $S^* = \langle aP \rangle \leq \frac{N_G(P)}{P}$ (es un subgrupo de orden p), por el Teorema de la Correspondencia para grupos tenemos que $S^* = \frac{S}{P}$, para algún $S \leq N_G(P)$, tal que $P \leq S$. Notemos que $|S^*| = \frac{|S|}{|P|}$, entonces $|S| = |S^*||P|$, por lo que S es un p -grupo tal que $P \subset S$ lo cual es una contradicción. Por lo tanto $p \nmid |\frac{N_G(P)}{P}|$.

3. Notemos que $a \in N_G(P)$. Supongamos que $a \notin P$, entonces $aP \neq P$ en $\frac{N_G(P)}{P}$, de lo anterior $(aP)^{p^m} = P$, donde el orden de aP divide a p^m , entonces p divide al orden de aP , en consecuencia $p \mid \left| \frac{N_G(P)}{P} \right|$ lo que contradice el inciso anterior. Por lo tanto $a \in P$. ■

Teorema 2.8. (Sylow) Sea G un grupo finito de orden $|G| = p_1^{e_1} \cdots p_t^{e_t}$. Sea P un p -subgrupo de Sylow con $p = p_i$ para algún $i \in \{1, \dots, t\}$. Entonces:

1. Todo p -subgrupo de Sylow es conjugado de P .
2. Sea r el número de p -subgrupos de Sylow, entonces:

$$r \text{ divide a } \frac{|G|}{p^e}, r \equiv 1 \pmod{p}.$$

Demostración. Sea $\mathbb{X} = \{P_1, \dots, P_r\}$ el conjunto de todos los conjugados de $P_1 = P$. Sea Q un p -subgrupo de Sylow. Veamos que Q actúa en \mathbb{X} por conjugación:

Sea $q \in Q$, observemos que $P_j = gPg^{-1}$ para algún $g \in G$, entonces $q \cdot P_j = (qg)P(qg)^{-1} \in \mathbb{X}$. Además:

$$|\mathcal{O}_Q(P_i)| = \left| \frac{Q}{\text{Stab}_Q(P_i)} \right| = \frac{|Q|}{|\text{Stab}_Q(P_i)|},$$

por lo que $|\mathcal{O}_Q(P_i)|$ divide a $|Q|$ la cual es una potencia de p . Supongamos que existe una órbita de tamaño 1, es decir existe $j \in \{1, \dots, r\}$ tal que $|\mathcal{O}_Q(P_j)| = 1 = \frac{|Q|}{|\text{Stab}_Q(P_j)|}$, entonces $\text{Stab}_Q(P_j) = Q$, en consecuencia $qP_jq^{-1} = P_j$ para toda $q \in Q$. Por 3) de el Lema 2.8 tenemos $q \in P_j$ para todo $q \in Q$, así $Q \subseteq P_j$, por lo que $Q = P_j$ (Q es p -subgrupo de Sylow). Ahora veamos que P_j es el único con órbita de tamaño 1. Supongamos que existe $l \neq j$ tal que $|\mathcal{O}_G(P_l)| = 1$, de lo anterior $P_l = Q$, entonces $P_l = P_j$ lo cual es una contradicción. Tenemos en particular que P actúa en $\mathbb{X} = \{P_1, \dots, P_r\}$ con $P = P_1$ y $\mathcal{O}_P(P)$ es la única órbita de tamaño 1. Por lo tanto $p \mid |\mathcal{O}_P(P_j)|$ para toda $j = 2, \dots, r$. $\mathbb{X} = \mathcal{O}_P(P_1) \bigcup_{i \in I} \mathcal{O}_P(P_{j_i})$ (donde I es un conjunto apropiado de índices),

entonces:

$$r \equiv 1 \pmod{p}.$$

Supongamos que existe Q un p -subgrupo de Sylow tal que $Q \notin \mathbb{X}$. Entonces Q actúa en \mathbb{X} por conjugación y p divide a $|\mathcal{O}_Q(P_j)|$ para toda $j = 1, \dots, n$. De aquí que $r \equiv 0 \pmod{p}$ lo cual es una contradicción. De este modo r es el número de p -subgrupos de Sylow. Por último, observemos que el número de conjugados de P esta dado por:

$$r = [G : N_G(P)] = \frac{|G|}{|N_G(P)|},$$

por lo que r divide a $|G|$. Además $r \equiv 1 \pmod{p}$ si y sólo si $(r, p) = 1$, tambien notemos que $|G| = \frac{|G|}{p^e} p^e$, así tenemos que r divide a m . ■

Corolario 2.9. Sea G un grupo finito y P un p -subgrupo de Sylow para algún $p \in \mathbb{Z}$ primo. Entonces P es único, si y sólo si, $P \triangleleft G$.

Demostración. (\Rightarrow) Sea $g \in G$, entonces gPg^{-1} es un p -subgrupo Sylow, lo que implica que $gPg^{-1} = P$ para todo $g \in G$, por lo que $P \triangleleft G$.

(\Leftarrow) Sea Q un p -subgrupo de Sylow, por el Teorema de Sylow existe $g \in G$ tal que $Q = gPg^{-1} = P$, por lo que P es el único p -subgrupo de Sylow. ■

Teorema 2.10. Sea G un grupo finito de orden $|G| = p^e m$ tal que $p \in \mathbb{Z}$ primo y p no divide a m . Si P es un p -subgrupo de Sylow de G . Entonces $|P| = p^e$.

Demostración. Veamos que $p \nmid [G : P]$. Tenemos que:

$$[G : P] = [G : N(P)][N(P) : P],$$

$$[G : N(P)] = r \text{ el número de conjugados de } P,$$

entonces $p \nmid [G : N(P)]$ y por 2. de el Lema 2.8 $p \nmid \left| \frac{N(P)}{P} \right|$, de este modo tenemos que p no divide a $[G : P]$. Ahora, sea $|P| = p^n$ para algún $n \in \mathbb{N}$, entonces $\left| \frac{G}{P} \right| = \frac{p^e m}{p^n} = p^{e-n} m$, así $e - n = 0$, por lo que $|P| = p^e$. ■

Ejemplos.

1. Sea G un grupo de orden 42, notemos que $|G| = (2)(3)(7)$. Si P es un 7-subgrupo de Sylow, entonces $|P| = 7$. Sea r el número de 7-subgrupos de Sylow, tenemos que $r \mid 6$ y $r \equiv 1 \pmod{7}$, así $r = 1$, por lo que $P \triangleleft G$.
2. Sea G un grupo de orden 30, notemos que $|G| = (2)(3)(5)$. Si $r_5 \mid 6$ y $r_5 \equiv 1 \pmod{5}$, entonces $r_5 = 1$ o $r_5 = 6$.

Teorema 2.11. *Sea G un grupo finito, tal que todos sus subgrupos de Sylow son normales. Entonces G es el producto directo de sus subgrupos de Sylow.*

Demostración. Sean $|G| = p_1^{e_1} \cdots p_t^{e_t}$ y P_i el p_i -subgrupo de Sylow. Sea S el subgrupo generado por los P_i con $i = 1, \dots, t$. Tenemos que para cada $i = 1, \dots, t$; $P_i \leq S$, entonces $|P_i| = p_i^{e_i}$ el cual divide a $|S|$, así $p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ divide a $|S|$, por lo que $S = G$. Veamos que $P_i \cap \langle \bigcup_{j \neq i} P_j \rangle = \{e\}$.

Observación. Sean $H, K \leq G$ tal que $H \cap K = \{e\}$ y sean $h \in H, k \in K$. Tenemos que $h^{-1}k^{-1}hk \in H \cap K$, por lo que $h^{-1}k^{-1}hk = e$, entonces $hk = kh$.

Por lo anterior $xy = yx$ para todo $x \in P_i$ y $y \in P_j, i \neq j \in \{1, \dots, t\}$. Sea $x \in P_i \cap \langle \bigcup_{j \neq i} P_j \rangle$,

entonces existe $p_i^{l_i}$ tal que $x^{p_i^{l_i}} = e$. Ahora $x \in \langle \bigcup_{j \neq i} P_j \rangle$, entonces $x = \prod_{j \neq i} (s_j)$ donde $s_j \in P_j$. Sea

$p_j^{l_j} = \text{orden}(s_j)$ y sea $q = \prod_{j \neq i} (p_j)^{l_j}$, tenemos que $x^q = \prod_{j \neq i} (s_j)^q = e$. Además, observemos que q y $p_i^{l_i}$

son coprimos, entonces existe $a, b \in \mathbb{Z}$ tales que $aq + bp_i^{l_i} = 1$, así $x^1 = x^{aq + bp_i^{l_i}} = (x^q)^a (x^{p_i^{l_i}})^b = e$, por lo que:

$$P_i \cap \langle \bigcup_{j \neq i} P_j \rangle = \{e\} \quad \text{para cada } i \in \{1, \dots, t\}$$

■

Teorema 2.12. *Sea $p \in \mathbb{Z}$ primo y sea G un p -grupo tal que $G \neq \{e\}$. Entonces $Z(G) \neq \{e\}$.*

Demostración. ■ Si G es abeliano, entonces $G = Z(G)$.

- Si G no es abeliano, para cada $x_i \notin Z(G)$, de la demostración del Teorema de Cauchy tenemos que $C_G(x_i) < G$, entonces p divide a $[G : C_G(x_i)]$, por la ecuación de clase tenemos que:

$$|Z(G)| = |G| - \sum_{i \in I} [G : C_G(x_i)].$$

Además p divide a $|G|$, así p divide a $|Z(G)|$, por lo que $Z(G) \neq \{e\}$. ■

Para más detalles puede consultar [2, capítulo 5, sección 5.2].

Capítulo 3

Grupos nilpotentes finitos

Definición 3.1. Sean H, K subgrupos de G . El subgrupo conmutador de H y K lo definimos y denotamos por:

$$[H, K] = \langle [h, k] \mid h \in H \text{ y } k \in K \rangle,$$

donde $[h, k] = hkh^{-1}k^{-1}$ el cual es llamado el conmutador de h y k .

Nota.

- En general $\{[h, k] \mid h \in H \text{ y } k \in K\}$ no es un subgrupo de G .
- $[H, K] = [K, H]$.

Notación. Denotamos al subgrupo conmutador $G' = [G, G]$ y de manera mas general:

$$G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Definición 3.2. Sean H, K subgrupos de G . Decimos que K normaliza a H si $K \leq N_G(H)$.

Proposición 3.3. Sean H, K subgrupos de G . K normaliza a H , si y solo si, $[H, K] \leq H$.

Demostración. (\Rightarrow) Es suficiente demostrar que $[k, h] \in H$ para todo $k \in K$ y para todo $h \in H$. Como $kHk^{-1} = H$, entonces existe $h_0 \in H$ tal que $khk^{-1} = h_0$, así:

$$[k, h] = khk^{-1}h^{-1} = h_0h^{-1} \in H.$$

(\Leftarrow) Sea $k \in K$, es suficiente probar que $khk^{-1} \in H$ para todo $h \in H$.

Por hipótesis tenemos que $khk^{-1}h^{-1} \in H$, por lo que existe $h' \in H$ tal que $khk^{-1}h^{-1} = h'$, entonces:

$$khk^{-1} = h'h \in H. \quad \blacksquare$$

Definición 3.4. Sea $H \leq G$, el centralizador de H en G se define y denota como:

$$C_G(H) = \{x \in G \mid xh = hx \ \forall h \in H\}.$$

Observación. Notemos que $C_G(H) = \{x \in G \mid [x, h] = 1 \ \forall h \in H\}$.

Definición 3.5. Decimos que K centraliza a H si $K \leq C_G(H)$.

Observación.

- Podemos ver que K centraliza a H , si y solo si, $[H, K] = 1$.
- Si $a, b \in G$ y $[a, b] \in K$, donde $K \triangleleft G$, puesto que $aba^{-1}b^{-1} = (ab)(ba)^{-1} \in K$, entonces:

$$\begin{aligned} (ba)^{-1}K &= (ab)^{-1}K \\ \Leftrightarrow (ba)K &= (ab)K \\ \Leftrightarrow bKaK &= aKbK. \end{aligned}$$

Es decir, "a y b conmutan módulo K ".

Lema 3.6.

1. Sea $K \triangleleft G$ y $K \leq H \leq G$, entonces $[H, G] \leq K$ si y solo si $H/K \leq Z(G/K)$.
2. Si $H, K \leq G$ y $f : G \rightarrow L$ es un homomorfismo, entonces $f([H, K]) = [f(H), f(K)]$.

Demostración. 1. Sea $h \in H$ y $g \in G$, tenemos que:

$$\begin{aligned} hKgK &= gKhK \Leftrightarrow h^{-1}Kg^{-1}K = g^{-1}Kh^{-1}K \\ &\Leftrightarrow (h^{-1}g^{-1})K = (g^{-1}h^{-1})K \\ &\Leftrightarrow hgh^{-1}g^{-1} \in K. \end{aligned}$$

2. Sea $[h, k] \in [H, K]$, observemos que:

$$\begin{aligned} f([h, k]) &= f(hkh^{-1}k^{-1}) \\ &= f(h)f(k)f(h^{-1})f(k^{-1}) \\ &= [f(h), f(k)]. \end{aligned}$$

Por lo tanto $f([H, K]) = [f(H), f(K)]$ ya que ambos tienen los mismos generadores. ■

Definición 3.7. Definimos los subgrupos característicos $\gamma_i(G)$ de G de forma inductiva:

$$\gamma_1(G) = G;$$

$$\gamma_{i+1}(G) = [\gamma_i(G), G].$$

Nota. $\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G' \leq G$. Observemos que $\gamma_2(G) \leq \gamma_1(G)$.

Proposición 3.8. Sea G un grupo. Entonces $\gamma_{i+1}(G) \leq \gamma_i(G)$ para cada $i \in \mathbb{N}$.

Demostración. Veamos por inducción en $i \geq 1$

- $\gamma_2(G) \leq \gamma_1(G)$.
- Supongamos que $\gamma_{i+1}(G) \leq \gamma_i(G)$, tenemos que $\gamma_{i+2}(G) = [\gamma_{i+1}(G), G]$. Consideremos a $x \in \gamma_{i+1}(G)$, $g \in G$, tenemos que $[x, g] = xgx^{-1}g^{-1}$, como $x \in \gamma_{i+1}(G) \leq \gamma_i(G)$ entonces $xgx^{-1}g^{-1} \in [\gamma_i(G), G] = \gamma_{i+1}(G)$. Por lo tanto:

$$\gamma_{i+2}(G) \leq \gamma_{i+1}(G).$$

Por otro lado, como $[\gamma_i(G), G] = \gamma_{i+1}(G)$, entonces $[\gamma_i(G), G] \leq \gamma_i(G)$, por la Proposición 3.3 tenemos que $G = N_G(\gamma_i(G))$, es decir $\gamma_i(G) \trianglelefteq G$ para cada $i \geq 1$, entonces $\gamma_{i+1}(G) \trianglelefteq G$ y 1. del Lema 3.6 nos dice que $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$. ■

Definición 3.9. Con la notación anterior se define la serie central inferior de G como

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \dots$$

Definición 3.10. El centro superior $\zeta^i(G)$ es el subgrupo característico de G definido de forma inductiva:

$$\begin{aligned} \zeta^0(G) &= 1; \\ \frac{\zeta^{i+1}(G)}{\zeta^i(G)} &= Z\left(\frac{G}{\zeta^i(G)}\right). \end{aligned}$$

Esto es, si

$$\begin{aligned} v_i : G &\rightarrow G/\zeta^i(G) \\ g &\mapsto g\zeta^i(G), \end{aligned}$$

entonces $\zeta^{i+1}(G)$ es la preimagen bajo v_i de $Z\left(\frac{G}{\zeta^i(G)}\right)$,

Nota. $\zeta^1(G) = \frac{\zeta^1(G)}{\zeta^0(G)} = Z\left(\frac{G}{\zeta^0(G)}\right) = Z(G)$.

Definición 3.11. Con la notación anterior definimos la serie central superior de G como:

$$1 = \zeta^0(G) \leq \zeta^1(G) \leq \zeta^2(G) \leq \dots$$

Si no causa confusión, abreviaremos $\zeta^i(G)$ por ζ^i y $\gamma_i(G)$ por γ_i .

Proposición 3.12. Sean G y H grupos, $f : G \rightarrow H$ un homomorfismo sobreyectivo. Si $A \leq Z(G)$, entonces $f(A) \leq Z(H)$.

Demostración. Sea $x \in f(A)$ y $y \in H$, como f es sobreyectiva existe $g \in G$ tal que $f(g) = y$, además existe $a \in A$ tal que $f(a) = x$, así:

$$\begin{aligned} x \cdot y &= f(a) \cdot f(g) \\ &= f(ag) \\ &= f(ga) \\ &= f(g) \cdot f(a) \\ &= y \cdot x. \end{aligned}$$

Por lo que $x \in Z(H)$. ■

Teorema 3.13. Sea G un grupo, entonces existe un entero c tal que $\zeta^c = G$, si y solo si, $\gamma_{c+1} = 1$. Más aún, $\gamma_{i+1} \leq \zeta^{c-i}$ para todo $i \in \mathbb{N}$.

Demostración. (\Rightarrow) Supongamos que $\zeta^c = G$, veamos que $\gamma_{i+1} \leq \zeta^{c-i}$ (por inducción en $i \geq 0$).

- Si $i = 0$, tenemos que: $\gamma_1 = G = \zeta^c$.
- Supongamos que $\gamma_{i+1} \leq \zeta^{c-i}$, tenemos que:

$$\gamma_{i+2} = [\gamma_{i+1}, G] \leq [\zeta^{c-i}, G] \leq \zeta^{c-i-1}.$$

Esta última desigualdad se da gracias a 1. de el Lema 3.6 ya que $\zeta^{c-i}/\zeta^{c-i-1} = Z(G/\zeta^{c-i-1})$, por lo que $\gamma_{i+1} \leq \zeta^{c-i}$ para todo i , en particular si $i = c$ tenemos que:

$$\gamma_{c+1} \leq \zeta^0 = 1.$$

(\Leftarrow) Supongamos que $\gamma_{c+1} = 1$, vamos a probar que $\gamma_{c+1-j} \leq \zeta^j$ (por inducción en $j \geq 0$).

- $\gamma_{c+1} = 1 = \zeta^0$.
- Supongamos que $\gamma_{c+1-j} \leq \zeta^j$, observemos que $\gamma_{c+1-j} = [\gamma_{c-j}, G]$, por 1. de el Lema 3.7 tenemos que $\gamma_{c-j}/\gamma_{c+1-j} \leq Z(G/\gamma_{c+1-j})$. Por hipótesis de inducción podemos construir el siguiente homomorfismo sobreyectivo:

$$\begin{aligned} G/\gamma_{c+1-j} &\rightarrow G/\zeta^j \\ g\gamma_{c+1-j} &\mapsto g\zeta^j. \end{aligned}$$

De la proposición anterior tenemos que:

$$\gamma_{c-j}\zeta^j/\zeta^j \leq Z(G/\zeta^j) = \zeta^{j+1}/\zeta^j.$$

Entonces $\gamma_{c-j} \leq \gamma_{c-j}\zeta^j \leq \zeta^{j+1}$.

Por último, en particular tenemos que: $\gamma_1 = G \leq \zeta^c$, así:

$$\zeta^c = G. \quad \blacksquare$$

Definición 3.14. *Un grupo G es nilpotente si existe un entero c tal que $\gamma_{c+1} = 1$. Si c es el menor entero positivo que cumple esta condición, diremos que G es nilpotente de clase c .*

Teorema 3.15. *Cada p -grupo finito G es nilpotente.*

Demostración. Recordemos que un p -grupo finito no trivial tiene centro no trivial. Por lo que si para algún entero positivo i , $\zeta^i(G) < G$, entonces $G/\zeta^i(G) \neq 1$ es un p -grupo finito, luego $Z(G/\zeta^i(G)) \neq 1$, así $\zeta^i(G) < \zeta^{i+1}(G)$, entonces como G es finito debe existir c tal que $\zeta^c(G) = G$, por el Teorema 3.13 $\gamma_{c+1}(G) = 1$, es decir, G es nilpotente. ■

Teorema 3.16. *Todo subgrupo H de un grupo nilpotente es nilpotente. Más aún, si G es nilpotente de clase c , entonces H es nilpotente de clase menor o igual que c .*

Demostración. Veamos que si $H \leq G$ entonces $\gamma_i(H) \leq \gamma_i(G)$ para todo i (por inducción sobre $i \geq 1$).

- Si $i = 1$, tenemos que $\gamma_1(H) = H \leq G = \gamma_1(G)$.
- Supongamos que $\gamma_i(H) \leq \gamma_i(G)$, tenemos que $\gamma_{i+1}(H) = [\gamma_i(H), H]$. Sea $x \in \gamma_i(H)$ y $h \in H$, entonces $[x, h] \in [\gamma_i(G), G]$, por lo que todo generador del grupo $[\gamma_i(H), H]$ pertenece al grupo $[\gamma_i(G), G]$, por lo tanto $[\gamma_i(H), H] \leq [\gamma_i(G), G]$, es decir $\gamma_{i+1}(H) \leq \gamma_{i+1}(G)$.

Como G es nilpotente existe c tal que $\gamma_{c+1}(G) = 1$, por lo anterior $\gamma_{c+1}(H) = 1$, por lo que H es nilpotente de clase menor o igual que c . ■

Teorema 3.17. *Si G es nilpotente de clase c y $H \triangleleft G$, entonces $\frac{G}{H}$ es nilpotente de clase menor o igual que c .*

Demostración. Tomemos $f : G \rightarrow L$ un homomorfismo de grupos sobreyectivo, veamos por inducción en $i \geq 1$, que:

$$\gamma_i(L) \leq f(\gamma_i(G)).$$

- Si $i = 1$, tenemos que $\gamma_1(L) = L = f(G) = f(\gamma_1(G))$.

- Supongamos que $\gamma_i(L) \leq f(\gamma_i(G))$, por 2. del Lema 3.6 tenemos que:

$$\begin{aligned}\gamma_{i+1}(L) &= [\gamma_i(L), L] \\ &\leq [f(\gamma_i(G)), L] \\ &= [f(\gamma_i(G)), f(G)] \\ &= f[\gamma_i(G), G] \\ &= f(\gamma_{i+1}(G)).\end{aligned}$$

Sea:

$$\begin{aligned}\Pi : G &\rightarrow G/H \\ a &\mapsto aH,\end{aligned}$$

el cual es un homomorfismo sobreyectivo de grupos, tenemos que $\gamma_i(G/H) \leq \Pi(\gamma_i(G))$, como G es nilpotente, existe c tal que $\gamma_{c+1}(G) = 1$, lo cual implica que $\gamma_{c+1}(G/H) \leq \Pi(1) = 1$, por lo que $\gamma_{c+1}(G/H) = 1$, es decir, G/H es nilpotente de clase menor o igual a c . ■

Teorema 3.18. *Si H y K son grupos nilpotentes, entonces su producto directo $H \times K$ es nilpotente.*

Demostración. Veamos que $\gamma_i(H \times K) \leq \gamma_i(H) \times \gamma_i(K)$ para toda i (por inducción sobre $i \geq 1$).

- Si $i = 1$, tenemos que $\gamma_1(H \times K) = \gamma_1(H) \times \gamma_1(K)$.
- Supongamos que $\gamma_i(H \times K) \leq \gamma_i(H) \times \gamma_i(K)$, tenemos que:

$$\gamma_{i+1}(H \times K) = [\gamma_i(H \times K), H \times K] \leq [\gamma_i(H) \times \gamma_i(K), H \times K].$$

Por otro lado, sea $(x, y) \in \gamma_i(H) \times \gamma_i(K)$ y $(h, k) \in H \times K$, observemos que un generador arbitrario de $[\gamma_i(H) \times \gamma_i(K), H \times K]$ es:

$$\begin{aligned}(x, y)(h, k)(x, y)^{-1}(h, k)^{-1} &= (xh, yk)(x^{-1}, y^{-1})(h^{-1}, k^{-1}) \\ &= (xhx^{-1}h^{-1}, yky^{-1}k^{-1})\end{aligned}$$

el cual pertenece a $[\gamma_i(H), H] \times [\gamma_i(K), K]$, por lo anterior:

$$[\gamma_i(H) \times \gamma_i(K), H \times K] \leq [\gamma_i(H), H] \times [\gamma_i(K), K],$$

obteniendo que $\gamma_{i+1}(H \times K) \leq \gamma_{i+1}(H) \times \gamma_{i+1}(K)$.

Como H y K son nilpotentes existe c y d tales que $\gamma_{c+1}(H) = 1$ y $\gamma_{d+1}(K) = 1$, así tomando a $M = \max\{c, d\}$ tenemos que $\gamma_{M+1}(H \times K) \leq \gamma_{M+1}(H) \times \gamma_{M+1}(K) = 1$, por lo que:

$$\gamma_{M+1}(H \times K) = 1,$$

así $H \times K$ es nilpotente de clase menor o igual a M . ■

Teorema 3.19. *Si G es nilpotente y $H < G$, entonces $H < N_G(H)$.*

Demostración. Observemos que $\gamma_{c+1}(G) = 1 \leq H < \gamma_1(G) = G$ para algún $c \in \mathbb{N}$, podemos elegir $i \in \{1, \dots, c\}$ tal que $\gamma_i(G) \not\leq H$ y $\gamma_{i+1}(G) \leq H$. Ahora:

$$[\gamma_i(G), H] \leq [\gamma_i(G), G] = \gamma_{i+1}(G) \leq (H),$$

entonces $[\gamma_i(G), H] \leq H$, equivalentemente $[H, \gamma_i(G)] \leq H$ si y solo si $\gamma_i(G)$ normaliza a H , es decir $\gamma_i(G) \leq N_G(H)$, concluyendo que $H < N_G(H)$, ya que de lo contrario $\gamma_i(G) \leq N_G(H) = H$ (lo cual sería una contradicción). ■

Teorema 3.20. *Sea $P \leq G$ un subgrupo de Sylow. Si $N_G(P) \leq H \leq G$, entonces H es igual a su propio normalizador, esto es $H = N_G(H)$.*

Demostración. Sea $x \in N_G(H)$, por hipótesis $P \leq N_G(P) \leq H$, entonces $xPx^{-1} \leq xHx^{-1} = H$, obteniendo que P y xPx^{-1} son p -subgrupos de Sylow de H , esto implica que existe $h \in H$ tal que:

$$\begin{aligned} P &= h(xPx^{-1})h^{-1} \\ &= (hx)P(x^{-1}h^{-1}) \\ &= (hx)P(hx)^{-1}, \end{aligned}$$

por lo que $hx \in N_G(P) \leq H$, lo que implica que existe $h' \in H$ tal que $hx = h'$, así $x = h^{-1}h' \in H$, de aquí que $N_G(H) \leq H$, por lo tanto $H = N_G(H)$. ■

Teorema 3.21. *Un grupo finito G es nilpotente si y solo si es el producto de sus subgrupos de Sylow.*

Demostración. (\Rightarrow) Sea $p \in \mathbb{Z}$ primo tal que p divide a $|G|$ y sea P un p -subgrupo de Sylow de G , tenemos que $N_G(P) \leq N_G(P) \leq G$, entonces por el Teorema 3.19 $N_G(P)$ es igual a su propio normalizador. Por otro lado, si $N_G(P) < G$, por el Teorema 3.18 tenemos que $N_G(P) < N_G(P)$ (lo cuales una contradicción), por lo que $N_G(P) = G$, así $P \triangleleft G$, lo que es equivalente a que P es el unico p -subgrupo de Sylow, por lo tanto del Teorema 2.11 obtenemos que G es el producto directo de sus subgrupos de Sylow.

(\Leftarrow) Recordemos que todo p -subgrupo finito es nilpotente para cada $p \in \mathbb{Z}$ primo, además el producto de grupos nilpotentes es nilpotente, así, si G es el producto directo de sus subgrupos de Sylow entonces G es nilpotente. ■

Teorema 3.22. *Sean P y K grupos finitos tales que $G = P \times K$ y $(|P|, |K|) = 1$. Sea $H \leq G$, entonces existe $S \leq P$ y $T \leq K$ subgrupo tales que $H = S \times T$.*

Demostración. Definamos $S = \{s \in P \mid (s, 1) \in H\}$ y $T = \{t \in K \mid (1, t) \in H\}$. Veamos que $S \leq P$.

- $(1, 1) \in H$, entonces $1 \in S$.
- Sean $s_1, s_2 \in S$, tenemos que $(s_1, 1), (s_2, 1) \in H$, entonces $(s_1s_2, 1) \in H$, así $s_1s_2 \in S$.
- Sea $s \in S$, tenemos que $(s, 1) \in H$, entonces $(s, 1)^{-1} = (s^{-1}, 1) \in H$, así $s^{-1} \in S$.

Por lo que $S \leq P$, de manera análoga $T \leq K$. Ahora observemos que si $(s, t) \in S \times T$, entonces $(s, t) = (s, 1)(1, t) \in H$, por lo que $S \times T \leq H$. Basta con demostrar que $|S \times T| = |H|$, así $H = S \times T$. Veamos que $H = (S \times \{1\})(\{1\} \times T)$:

Sea $h \in H$, tenemos que $h = (a, b) \in P \times K$, entonces $h = (a, 1)(1, b) = (1, b)(a, 1)$. Por otro lado, sea $l = \text{orden}(a)$ el cual divide a $|P|$ y $r = \text{orden}(b)$ el cual divide a $|K|$, entonces $(l, r) = 1$, por lo que $h^l = (a^l, b^l) = (1, b^l) \in H$, de aquí que $b^l \in T$, así $\langle b \rangle = \langle b^l \rangle \leq T$, por lo tanto $b \in T$. Similarmente $a \in S$, entonces $h = (a, 1)(1, b) \in (S \times \{1\})(\{1\} \times T)$, por lo que $H = (S \times \{1\})(\{1\} \times T)$, además $(S \times \{1\}) \cap (\{1\} \times T) = \{(1, 1)\}$. Veamos que $S \times \{1\} \trianglelefteq H$. Si $s \in S$, entonces $(s, 1) \in H$, si $(a, b) \in H$, tenemos que $(a, b)(s, 1)(a^{-1}, b^{-1}) = (asa^{-1}, 1) \in H$, en consecuencia $asa^{-1} \in S$, así $(asa^{-1}, 1) \in S \times \{1\}$, por lo tanto $S \times \{1\} \trianglelefteq H$. De manera análoga $\{1\} \times T \trianglelefteq H$, de aquí que $H \cong (S \times \{1\}) \times (\{1\} \times T)$, así $|H| = |S||T| = |S \times T|$. ■

Para más detalles puede consultar [3, capítulo 5, sección 5.5].

Capítulo 4

El anillo de Burnside

Definición 4.1. Sean X y Y conjuntos. Consideremos los conjuntos $X' = X \times \{1\}$ y $Y' = Y \times \{2\}$ donde $1 \notin Y$ y $2 \notin X$, entonces definimos y denotamos la unión ajena de X y Y como:

$$X \sqcup Y = X' \cup Y'.$$

De manera más general, dada $\{X_i\}_{i \in I}$ una familia de conjuntos, la unión ajena de dicha familia es:

$$\bigsqcup_{i \in I} X_i = \bigcup_{i \in I} X'_i, \text{ donde } X'_i = X \times \{i\}.$$

Ejemplos. 1. Si $\{X_i\}_{i \in I}$ es una familia de G -conjuntos, entonces $\bigsqcup_{i \in I} X_i$ es un G -conjunto con la siguiente acción:

$$\begin{aligned} * : G \times \bigsqcup_{i \in I} X_i &\rightarrow \bigsqcup_{i \in I} X_i \\ (g, (x, i)) &\mapsto (g *_i x, i) \end{aligned}$$

donde $*_i$ es la acción de G en X_i con $x \in X_i$, para algún $i \in I$.

2. Si $\{X_i\}_{i \in I}$ es una familia de G -conjuntos, entonces el producto cartesiano de la familia $\{X_i\}_{i \in I}$ es un G -conjunto con la siguiente acción:

$$\begin{aligned} * : G \times \prod_{i \in I} X_i &\rightarrow \prod_{i \in I} X_i \\ (g, (x_i)_{i \in I}) &\mapsto (g *_i x_i)_{i \in I} \end{aligned}$$

donde $*_i$ es la acción de G en X_i , para cada $i \in I$.

3. Si X y Y son dos G -conjuntos, entonces:

$$\text{Hom}(X, Y) = \{f : X \rightarrow Y \mid f \text{ es función}\}.$$

es un G -conjunto con la siguiente acción:

$$\begin{aligned} * : G \times \text{Hom}(X, Y) &\rightarrow \text{Hom}(X, Y) \\ (g, f) &\mapsto g * f \end{aligned}$$

donde $(g * f)(x) = g *_Y f(g^{-1} *_X x)$, para todo $x \in X$, $f \in \text{Hom}(X, Y)$ y $g \in G$. Notemos que $*$ está bien definida, puesto que f es una función y $*_Y, *_X$ son las acciones de G en Y y X , respectivamente.

Veamos que $*$ es una acción:

- Sea $f \in \text{Hom}(X, Y)$, entonces $(e * f)(x) = e *_{\mathcal{Y}} f(e *_{\mathcal{X}} x) = f(x)$ para todo $x \in X$, por lo que $e * f = f$.
- Sean $g, g' \in G$. Entonces para $x \in X$ se tiene que:

$$\begin{aligned} ((g'g) * f)(x) &= (g'g) *_{\mathcal{Y}} [f(g^{-1}g'^{-1} *_{\mathcal{X}} x)] \\ &= g' *_{\mathcal{Y}} [g *_{\mathcal{Y}} f(g^{-1}g'^{-1} *_{\mathcal{X}} x)] \\ &= g' *_{\mathcal{Y}} [(g * f)(g'^{-1} *_{\mathcal{X}} x)] \\ &= (g' * (g * f)). \end{aligned}$$

$$\text{Así, } g'g * f = g' * (g * f).$$

Definición 4.2. Sean X, Y dos G -conjuntos con acciones $*_{\mathcal{X}}$ y $*_{\mathcal{Y}}$, respectivamente. Diremos que $f \in \text{Hom}(X, Y)$ es un morfismo de G -conjuntos si satisface que $f(g *_{\mathcal{X}} x) = g *_{\mathcal{Y}} f(x)$ para todo $g \in G$ y $x \in X$.

Denotamos a la colección de morfismos de G -conjuntos de X a Y por $\text{Hom}_G(X, Y)$.

Definición 4.3. Sean X, Y dos G -conjuntos diremos que X y Y son isomorfos como G -conjuntos si existe $f \in \text{Hom}_G(X, Y)$ biyectivo. Si X y Y son isomorfos lo denotaremos por $X \cong_G Y$.

Ejemplos. 1. Sean $H \leq K \leq G$ entonces:

$$\begin{aligned} \Pi: \frac{G}{H} &\rightarrow \frac{G}{K} \\ aH &\mapsto aK \end{aligned}$$

es un morfismo sobreyectivo de G -conjuntos.

- Veamos que Π está bien definida. Sean $aH, a'H \in \frac{G}{H}$ tales que $aH = a'H$, así $(a')^{-1}a \in H \leq K$, en consecuencia $aK = a'K$.
- Veamos que Π es un morfismo de G -conjuntos. Primero, notemos que la acción de G en $\frac{G}{H}$ y en $\frac{G}{K}$ es la definida en la demostración de la Proposición 1.8, así:

$$\Pi(g * aH) = \Pi((ga)H) = (ga)K = g * (aK) = g * \Pi(aH).$$

2. Sea X un G -conjunto, la identidad:

$$\begin{aligned} \text{Id}_X: X &\rightarrow X \\ x &\mapsto x \end{aligned}$$

es un morfismo de G -conjuntos.

Observación.

1. La composición de morfismos de G -conjuntos es nuevamente un morfismo de G -conjuntos.
2. El inverso de un isomorfismo de G -conjuntos es también un isomorfismo de G -conjuntos.
3. Un morfismo de G -conjuntos manda órbitas en órbitas:

Sean $f \in \text{Hom}_G(X, Y)$, $x \in X$ y $\mathcal{O}_G(x)$ la órbita de x en G . Luego, $f(gx) = g(f(x))$, así $f(\mathcal{O}_G(x)) \subseteq \mathcal{O}_G(f(x))$. Por otro lado, $gf(x) = f(gx) \in f(\mathcal{O}_G(x))$, por tanto $\mathcal{O}_G(f(x)) \subseteq f(\mathcal{O}_G(x))$, concluyendo que:

$$\mathcal{O}_G(f(x)) = f(\mathcal{O}_G(x)).$$

De aquí en adelante si no hay lugar a confusión, vamos a abreviar la notación y escribiremos gx en lugar de $g * x$.

Definición 4.4. Diremos que un G -conjunto es transitivo si este tiene una única órbita; es decir, si para cada $x, y \in X$ existe $g \in G$ tal que $y = gx$.

Teorema 4.5. Si G es un grupo, X un G -conjunto y $x_0 \in X$ entonces:

1. $Stab_G(gx_0) = g(Stab_G(x_0))g^{-1}$.
2. Si H es un subgrupo de G , entonces G/H es transitivo.
3. Si X es un G -conjunto transitivo, entonces $X \cong_G \frac{G}{H}$ para algún $H \leq G$.

Demostración. 1.

$$\begin{aligned} a \in Stab_G(gx_0) &\Leftrightarrow a(gx_0) = gx_0 \\ &\Leftrightarrow (ag)x_0 = gx_0 \\ &\Leftrightarrow g^{-1}agx_0 = x_0 \\ &\Leftrightarrow g^{-1}ag \in Stab_G(x_0) \\ &\Leftrightarrow a \in g(Stab_G(x_0))g^{-1}. \end{aligned}$$

2. Como G actúa en $\frac{G}{H}$ por medio de la multiplicación por la izquierda, tenemos que:

$$\frac{G}{H} = \mathcal{O}_G(H).$$

Por lo tanto, $\frac{G}{H}$ es transitivo.

3. Como X es transitivo, este tiene una única órbita la cual, por la Proposición 1.8 es isomorfa como G -conjunto a:

$$\frac{G}{Stab_G(x)}$$

para cada $x \in X$. ■

Teorema 4.6. Si X es un G -conjunto finito, entonces existe un conjunto de índices I tal que:

$$X \cong_G \bigsqcup_{i \in I} G/H_i \text{ donde } H_i \leq G \text{ para cada } i \in I.$$

Demostración. Sea X un G -conjunto y $\{x_i | i \in I\}$ un conjunto de representantes de las órbitas de G en X . Entonces:

$$X = \bigcup_{i \in I} \mathcal{O}_G(x_i),$$

por la Proposición 1.8 sabemos que $\mathcal{O}_G(x_i) \cong \frac{G}{Stab_G(x_i)}$ para cada $i \in I$, llamemos f_i al isomorfismo de $\mathcal{O}_G(x_i)$ a $\frac{G}{Stab_G(x_i)}$. Así, definimos:

$$\begin{aligned} f : \bigcup_{i \in I} \mathcal{O}_G(x_i) &\rightarrow \bigsqcup_{i \in I} \left(\frac{G}{Stab_G(x_i)} \right) \\ x &\mapsto (f_i(x), i) \end{aligned}$$

el cual es un isomorfismo de G -conjuntos. Finalmente denotando $H_i = Stab_G(x_i)$, obtenemos:

$$X \cong_G \bigsqcup_{i \in I} \frac{G}{H_i}. \quad \blacksquare$$

Lema 4.7. Si $H, K \leq G$, entonces $\frac{G}{H} \cong_G \frac{G}{K}$ si y sólo si $H = gKg^{-1}$ para algún $g \in G$.

Demostración. (\Leftarrow) Sabemos que existe $g \in G$ tal que $H = gKg^{-1}$, definamos:

$$f : \frac{G}{H} \rightarrow \frac{G}{K}$$

$$aH \mapsto agK$$

Veamos que f es un morfismo biyectivo. Sean $aH, bH \in G/H$. Entonces:

$$aH = bH \Leftrightarrow agKg^{-1} = bgKg^{-1}$$

$$\Leftrightarrow agK = bgK.$$

Por lo tanto f está bien definida y es inyectiva. Ahora, sea $bK \in \frac{G}{K}$ con $b \in G$, notemos que $bg^{-1}H \in \frac{G}{H}$, luego:

$$f(bg^{-1}H) = bg^{-1}gK$$

$$= bK.$$

De aquí, f es suprayectiva y, por tanto, biyectiva. Por último:

$$f(g_1(aH)) = f(g_1aH)$$

$$= (g_1ag)K$$

$$= g_1(ag)K$$

$$= g_1(aH)K$$

$$= g_1f(aH),$$

con lo que f es morfismo de G -conjuntos. Por lo tanto $\frac{G}{H} \cong_G \frac{G}{K}$.

(\Rightarrow) Sea f un isomorfismo de G -conjuntos tal que:

$$f : \frac{G}{H} \rightarrow \frac{G}{K}$$

$$aH \mapsto agK$$

para algún $g \in G$. Veamos que $H \subseteq gKg^{-1}$. Sea $h \in H$:

$$gK = f(H)$$

$$= f(hH)$$

$$= hgK,$$

entonces $gK = hgK$, luego $g^{-1}hg \in K$, de aquí que $g^{-1}Hg \subseteq K$, es decir:

$$H \subseteq gKg^{-1}.$$

Ahora consideremos:

$$f^{-1} : \frac{G}{K} \rightarrow \frac{G}{H}$$

$$aK \mapsto ag^{-1}H$$

el cual sabemos que es morfismo de G -conjuntos. Veamos que $gKg^{-1} \subseteq H$. Note que para cada $k \in K$ se tiene que:

$$kg^{-1}H = kf^{-1}(K)$$

$$= f^{-1}(kK)$$

$$= f^{-1}(K)$$

$$= g^{-1}H,$$

así $gkg^{-1} \in H$ para cada $k \in K$, luego $gKg^{-1} \subseteq H$, por tanto:

$$H = gKg^{-1}.$$

■

Definición 4.8. Sea G un grupo, $H \leq G$ un subgrupo y X un G -conjunto finito. Definimos X^H como el conjunto de todos los puntos de X que quedan fijos bajo la acción de H ; es decir:

$$X^H = \{x \in X \mid h * x = x \text{ para todo } h \in H\}.$$

Definamos la Marca de H en X como el número de elementos de X^H y la denotamos por:

$$\varphi_H(X) = |X^H|.$$

Teorema 4.9. Si $H, K \leq G$ son subgrupos y X, Y son G -conjuntos finitos, entonces:

1. $\varphi_H(X \sqcup Y) = \varphi_H(X) + \varphi_H(Y)$.
2. $\varphi_H(X \times Y) = \varphi_H(X)\varphi_H(Y)$.
3. Si $H = gKg^{-1}$ para algún $g \in G$, entonces $\varphi_H(X) = \varphi_K(X)$ para todo G -conjunto finito X .

Demostración. 1.

$$\begin{aligned} (X \sqcup Y)^H &= \{z \in X \sqcup Y \mid h * z = z, \forall h \in H\} \\ &= \{z \mid (z \in X \times \{1\} \vee z \in Y \times \{2\}) \wedge h * z = z, \forall h \in H\} \\ &= \{z \mid (z \in X \times \{1\} \wedge h * z = z) \vee (z \in Y \times \{2\} \wedge h * z = z), \forall h \in H\} \\ &= \{z \in X \times \{1\} \vee z \in Y \times \{2\} \mid h * z = z, \forall h \in H\} \\ &= X^H \sqcup Y^H. \end{aligned}$$

$$\text{Por lo tanto } |(X \sqcup Y)^H| = |X^H \sqcup Y^H| = |X^H| + |Y^H|.$$

2.

$$\begin{aligned} (X \times Y)^H &= \{(x, y) \in X \times Y \mid h * (x, y) = (x, y), \forall h \in H\} \\ &= \{(x, y) \in X \times Y \mid (h * x, h * y) = (x, y), \forall h \in H\} \\ &= \{(x, y) \mid x \in X^H \wedge y \in Y^H, \forall h \in H\} \\ &= X^H \times Y^H. \end{aligned}$$

$$\text{Por lo tanto } |(X \times Y)^H| = |X^H \times Y^H| = |X^H||Y^H|.$$

3. Sea X un G -conjunto. Supongamos que existe $g \in G$ tal que $H = gKg^{-1}$, entonces tenemos que:

$$\begin{aligned} X^H &= \{x \in X \mid h * x = x, \forall h \in H\} \\ &= \{x \in X \mid gkg^{-1} * x = x, \forall k \in K\} \\ &= \{x \in X \mid k(g^{-1} * x) = g^{-1} * x, \forall k \in K\} \\ &= \{x \in X \mid g^{-1} * x \in X^K\} \\ &= \{x \in X \mid x \in gX^K\} \\ &= gX^K. \end{aligned}$$

Del párrafo anterior tenemos que $|X^H| = |gX^K|$.

Ahora definimos:

$$\begin{aligned}\psi : X^K &\rightarrow gX^K \\ x &\mapsto gx\end{aligned}$$

Observe que ψ es una biyección, por lo que $|X^K| = |gX^K|$, y con ello se tiene que $|X^H| = |X^K|$. Por lo tanto, para todo G -conjunto X tenemos que:

$$\varphi_H(X) = \varphi_K(X).$$

■

Definición 4.10. Sean $H, K \leq G$. Diremos que H es subconjugado de K si existe $g \in G$ tal que:

$$gHg^{-1} \subseteq K.$$

Teorema 4.11. Si $H, K \leq G$ son subgrupos, entonces $\text{Hom}_G(\frac{G}{H}, \frac{G}{K}) \neq \emptyset$ si y sólo si H es subconjugado de K .

Demostración. (\Rightarrow) Sea $f \in \text{Hom}_G(\frac{G}{H}, \frac{G}{K})$ entonces $f(eH) = aK$ para alguna $a \in G$. Para cada $h \in H$ tenemos que $hH = H$, entonces se tiene que $f(hH) = f(eH) = aK$ lo anterior implica que $aK = f(hH) = hf(eH) = haK$, de aquí que $a^{-1}ha \in K$, por lo tanto $a^{-1}Ha \subseteq K$.

(\Leftarrow) Sabemos que existe $a \in G$ tal que $a^{-1}Ha \subseteq K$, por el ejemplo 1. Pagina 22 tenemos el morfismo de G -conjuntos $\Pi : \frac{G}{a^{-1}Ha} \rightarrow \frac{G}{K}$. Por otro lado, sea $\alpha : \frac{G}{H} \rightarrow \frac{G}{a^{-1}Ha}$ un isomorfismo de G -conjuntos, así:

$$(\Pi \circ \alpha) \in \text{Hom}_G(\frac{G}{H}, \frac{G}{K}).$$

■

Teorema 4.12. Sean $H, K \leq G$ subgrupos, entonces existe una biyección entre:

$$\left(\frac{G}{K}\right)^H \text{ y } \text{Hom}_G\left(\frac{G}{H}, \frac{G}{K}\right).$$

Demostración. ■ Supongamos que H no es subconjugado de K , entonces por el teorema anterior:

$$\text{Hom}_G\left(\frac{G}{H}, \frac{G}{K}\right) = \emptyset.$$

Por otro lado tenemos que:

$$\begin{aligned}\left(\frac{G}{K}\right)^H &= \{gK \in G/K \mid (hg)K = gK \text{ para todo } h \in H\} \\ &= \{gK \in G/K \mid g^{-1}hgK = K \text{ para todo } h \in H\} \\ &= \{gK \in G/K \mid g^{-1}Hg \subseteq K\} \\ &= \emptyset.\end{aligned}$$

■ Supongamos que H es subconjugado de K . Definamos:

$$\begin{aligned}\gamma : \left(\frac{G}{K}\right)^H &\rightarrow \text{Hom}_G\left(\frac{G}{H}, \frac{G}{K}\right) \\ aK &\mapsto \gamma_a.\end{aligned}$$

donde:

$$\begin{aligned}\gamma_a : \frac{G}{H} &\rightarrow \frac{G}{K} \\ gH &\mapsto gaK.\end{aligned}$$

1. Veamos que γ_a está bien definida:

Sean $g_1H = g_2H$, así $g_1 = g_2h$ para algún $h \in H$. Luego:

$$\begin{aligned}\gamma_a(g_1H) &= g_1aK \\ &= g_2(h(aK)) \\ &= g_2(aK) \\ &= \gamma_a(g_2H).\end{aligned}$$

2. Ahora veamos que γ_a es un morfismo de G -conjuntos:

Sean $g' \in G$ y $gH \in \frac{G}{H}$, entonces:

$$\begin{aligned}\gamma_a(g'(gH)) &= \gamma_a((g'g)H) \\ &= g'gaK \\ &= g'\gamma_a(gH).\end{aligned}$$

3. Veamos que γ está bien definida:

Sean $aK, bK \in (\frac{G}{K})^H$ tales que $aK = bK$. Entonces $b = ak$ para algún $k \in K$. Luego:

$$\begin{aligned}\gamma_b(gH) &= gbK \\ &= gakK \\ &= gaK \\ &= \gamma_a(gH),\end{aligned}$$

para toda $gH \in \frac{G}{H}$, por tanto $\gamma_a = \gamma_b$.

Por otro lado, definamos:

$$\begin{aligned}\gamma' : \text{Hom}_G\left(\frac{G}{H}, \frac{G}{K}\right) &\rightarrow \left(\frac{G}{K}\right)^H \\ \alpha &\mapsto \alpha(H).\end{aligned}$$

4. Veamos que γ' está bien definida:

Sea $h \in H$, tenemos que $h\alpha(H) = \alpha(hH) = \alpha(H)$, lo cual implica que $\alpha(H) \in (\frac{G}{K})^H$.

5. Ahora veamos que $\gamma \circ \gamma' = \text{Id}_{\text{Hom}_G(\frac{G}{H}, \frac{G}{K})}$:

Tenemos que:

$$\begin{aligned}(\gamma \circ \gamma')(\alpha) &= \gamma(\gamma'(\alpha)) \\ &= \gamma(\alpha(H)) \\ &= \gamma(gK) \\ &= \gamma_g,\end{aligned}$$

donde $\alpha(H) = gK$. Por otro lado:

$$\begin{aligned}((\gamma \circ \gamma')(\alpha))(xH) &= \alpha_g(xH) \\ &= xgK \\ &= x\alpha(H) \\ &= \alpha(xH),\end{aligned}$$

para todo $xH \in \frac{G}{H}$. Por lo que $(\gamma \circ \gamma')(\alpha) = \alpha$, de aquí:

$$\gamma \circ \gamma' = \text{Id}_{\text{Hom}_G\left(\frac{G}{H}, \frac{G}{K}\right)}.$$

6. Por último veamos que $\gamma' \circ \gamma = Id(\frac{G}{K})^H$:

Sea $aK \in (\frac{G}{K})^H$, tenemos que:

$$\begin{aligned} (\gamma' \circ \gamma)(aK) &= \gamma(\gamma_a) \\ &= \gamma_a(H) \\ &= aK. \end{aligned}$$

Así:

$$\gamma' \circ \gamma = Id(\frac{G}{K})^H.$$

Por lo tanto, γ es una biyección. ■

Corolario 4.13. Sean $H, K \in G$ subgrupos. Entonces $\varphi_H(\frac{G}{K}) \neq 0$ si y sólo si H es subconjugado de K .

Lema 4.14. Sean $H, K \in G$ subgrupos, entonces:

$$\varphi_H(\frac{G}{K}) = \frac{|N_G(K)|}{|K|} \alpha(H, K)$$

donde:

$$\alpha_H(H, K) = |\{E \leq G \mid H \subseteq E \text{ y } E = aKa^{-1} \text{ para algún } a \in G\}|.$$

Demostración. Primero, llamemos $\mathcal{U} = \{E \leq G \mid H \subseteq E \text{ y } E = aKa^{-1} \text{ para algún } a \in G\}$. Luego, sabemos que:

$$\begin{aligned} (\frac{G}{K})^H &= \{aK \mid haK = aK \text{ para toda } h \in H\} \\ &= \{aK \mid a^{-1}ha \in K \text{ para toda } h \in H\} \\ &= \{aK \mid a^{-1}Ha \subseteq K\} \\ &= \{aK \mid H \subseteq aKa^{-1}\}. \end{aligned}$$

Ahora, tomemos:

$$\begin{aligned} f : \{aK \mid H \subseteq aKa^{-1}\} &\rightarrow \mathcal{U} \\ aK &\mapsto aKa^{-1} \end{aligned}$$

1. Veamos que f está bien definida:

Sean $aK = bK$, entonces existe $k \in K$ tal que $a = bk$, por lo tanto $aKa^{-1} = bkKk^{-1}b^{-1} = bKb^{-1}$.

2. Veamos que f es sobreyectiva:

Sea $E \in \mathcal{U}$, así existe $a \in G$ tal que $E = aKa^{-1}$. Sólo falta ver que $aK \in (\frac{G}{K})^H$. Sea $h \in H \leq E$, entonces $h = aka^{-1}$ para algún $k \in K$, por lo que $haK = aka^{-1}aK = aK$. Por lo tanto, $\{aK \mid H \leq aKa^{-1}\} = \bigcup_{E \in \mathcal{U}} f^{-1}(E)$, donde $f^{-1}(E)$ es la imagen inversa de E bajo f .

3. Sea $E = bKb^{-1}$. Veamos que $f^{-1}(E) = \{abK : bK \in \frac{N_G(K)}{K}\}$:

⊆) Sea $cK \in \{aK : H \subseteq aKa^{-1}\}$ tal que $f(cK) = bKb^{-1}$, de aquí que $cKc^{-1} = bKb^{-1}$, así $b^{-1}cKc^{-1}b = K$, con lo que $b^{-1}c \in N_G(K)$, en consecuencia $b^{-1}c = d \in N_G(K)$, entonces $c = bd$ tal que $dK \in \frac{N_G(K)}{K}$.

⊇) Sea bdK con $dK \in \frac{N_G(K)}{K}$, en consecuencia $f(bdK) = bdKd^{-1}b^{-1} = bKb^{-1} = E$, entonces $bdK \in f^{-1}(E)$.

Observemos que si $dK, d'K \in \frac{N_G(K)}{K}$ entonces $dK = d'K$ si y sólo si $bdK = bd'K$ por lo que de la igualdad anterior de conjuntos obtenemos que $|f^{-1}(E)| = |N_G(K)/K|$. Así:

$$\varphi_H(G/K) = \frac{|N_G(K)|}{|K|} \alpha(H, K).$$

■

Dado G un grupo finito, sea \mathbb{A} la clase de todos los G -conjuntos finitos; es decir:

$$\mathbb{A} = \{X \mid X \text{ es un } G\text{-conjunto finito}\}$$

Observación. En \mathbb{A} hay una relación de equivalencia \sim . A saber, dados $X, Y \in \mathbb{A}$ se tiene que:

$$X \sim Y \text{ si y sólo si } X \cong_G Y.$$

Definición 4.15. Sea $X \in \mathbb{A}$. Denotaremos por $[X]$ a la clase de equivalencia de $X \in \mathbb{A}$, es decir:

$$[X] = \{Y \in \mathbb{A} \mid X \cong_G Y\},$$

y la llamaremos la clase de G -isomorfismo de X . Así, definimos:

$$B^+(G) = \{[X] \mid X \in \mathbb{A}\}.$$

Teorema 4.16. Sea G un grupo finito, entonces $(B^+(G), +, \cdot)$ es un semianillo conmutativo con unidad, con las siguientes operaciones binarias de suma y producto:

1.

$$\begin{aligned} + : B^+(G) \times B^+(G) &\rightarrow B^+(G) \\ ([X], [Y]) &\mapsto [X \sqcup Y]. \end{aligned}$$

2.

$$\begin{aligned} \cdot : B^+(G) \times B^+(G) &\rightarrow B^+(G) \\ ([X], [Y]) &\mapsto [X \times Y]. \end{aligned}$$

Observación. Dados $G = \{e\}$ y X un conjunto. Entonces X es un $\{e\}$ -conjunto con acción trivial. Además, dos G -conjuntos con la acción trivial son isomorfos si y sólo si existe una biyección entre ellos. De aquí que

$$\begin{aligned} \phi : B^+(\{e\}) &\rightarrow \mathbb{N} \\ [X] &\mapsto |X| \end{aligned}$$

es un isomorfismo de semianillos, con lo cual $\mathbb{N} \cong B^+(\{e\})$. En este capítulo consideramos al cero como un elemento de los números naturales.

Teorema 4.17. Sean $[X], [Y], [Z] \in B^+(G)$ tales que $[X] + [Y] = [Z] + [Y]$, entonces $[X] = [Z]$. Es decir, hay cancelación con la suma en $B^+(G)$.

Demostración. Sean $[X], [Y]$ y $[Z] \in B^+(G)$ tales que $[X] + [Y] = [Z] + [Y]$. Sin pérdida de generalidad podemos asumir que X, Y, Z son ajenos dos a dos, por lo que las siguientes uniones son ajenas. Sean $X = \bigcup_{i=1}^m \mathcal{O}_G(x_i)$, $Y = \bigcup_{j=1}^l \mathcal{O}_G(y_j)$ y $Z = \bigcup_{k=1}^n \mathcal{O}_G(z_k)$, puesto que $[X \sqcup Y] = [Z \sqcup Y]$ hay una correspondencia biyectiva entre las órbitas de $X \sqcup Y$ y $Z \sqcup Y$, esto implica que $m + l = n + l$, por lo que $m = n$. Por lo tanto $Z = \bigcup_{i=1}^m \mathcal{O}_G(z_i)$. Finalmente, se puede demostrar por inducción en $l \geq 1$ que se pueden cancelar las órbitas de Y . ■

Observación. El Teorema anterior nos permite definir una relación de equivalencia en:

$$B^+(G) \times B^+(G).$$

A saber, dados $([X_1], [Y_1])$ y $([X_2], [Y_2]) \in B^+(G) \times B^+(G)$ tenemos que $([X_1], [Y_1]) \sim ([X_2], [Y_2])$ si y sólo si $[X_1] + [Y_2] = [X_2] + [Y_1]$. Denotaremos a la clase de equivalencia de $([X], [Y])$ que pertenece a $B^+(G) \times B^+(G)$ por $[X] - [Y]$

Definición 4.18. Definimos el Anillo de Burnside $B(G)$ de un grupo finito G como:

$$B(G) = \{[X] - [Y] \mid ([X], [Y]) \in B^+(G) \times B^+(G)\}$$

dotado de las siguientes operaciones binarias de suma y producto:

$$([X_1] - [Y_1]) + ([X_2] - [Y_2]) = ([X_1] + [X_2]) - ([Y_1] + [Y_2]).$$

$$([X_1] - [Y_1])([X_2] - [Y_2]) = ([X_1][X_2] + [Y_1][Y_2]) - ([X_1][Y_2] + [X_2][Y_1]).$$

Observación. $B(G)$ es el anillo de Grothendieck de $B^+(G)$, donde:

1. El neutro de la suma es $[\emptyset] - [\emptyset] = [X] - [X]$ con $[X] \in B^+(G)$.
2. Dado $[X] - [Y] \in B(G)$ su inverso aditivo es $[Y] - [X]$.
3. En el producto la unidad es $[\frac{G}{G}] - [\emptyset]$.

Notación. Dado un grupo finito G , denotaremos por $\mathcal{C}(G)$ a un conjunto completo de representantes de las clases de conjugación de los subgrupos de G .

Teorema 4.19. Dado un grupo finito G . Entonces $B(G)$ como grupo abeliano es libre como \mathbb{Z} -módulo, generado por los elementos de la forma $[\frac{G}{H}]$, donde $H \in \mathcal{C}(G)$.

Demostración. Sea G un grupo finito y X un G -conjunto finito. Por el Teorema 4.6:

$$X \cong_G \bigsqcup_{i \in I} \frac{G}{H_i},$$

donde $H_i \leq G$ para cada $i \in I$. Así,

$$[X] = [\bigsqcup_{i \in I} \frac{G}{H_i}] = \sum_{i \in I} [\frac{G}{H_i}] \in B^+(G).$$

Ahora, por el Lema 4.7 podemos tener repeticiones de algunos $[\frac{G}{H_i}]$, ya que dos de estos se identifican si y sólo si los subgrupos son conjugados. Por lo que denotaremos con $a_{H_i} \in \mathbb{N}$ al número de veces que se repite el elemento $[\frac{G}{H_i}]$. En consecuencia, si $[X] \in B^+(G)$, entonces:

$$[X] = \sum_{H \in \mathcal{C}(G)} a_H [\frac{G}{H}],$$

con $a_H \in \mathbb{N}$. Por lo que, abusando de la notación tenemos que los elementos de $B(G)$ son de la forma:

$$\sum_{H \in \mathcal{C}(G)} a_H [\frac{G}{H}], \text{ con } a_H \in \mathbb{Z}.$$

Veamos que esta expresión es única. Supongamos que:

$$\sum_{H \in \mathcal{C}(G)} a_H [\frac{G}{H}] = 0$$

y que no todos los a_H son cero, así tenemos la siguiente igualdad en $B^+(G)$:

$$\sum_{a_K > 0} a_K [\frac{G}{K}] = \sum_{a_L < 0} (-a_L) [\frac{G}{L}].$$

Llamemos $[Y] = \sum_{a_K > 0} a_K [\frac{G}{K}]$ y $[Z] = \sum_{a_L < 0} (-a_L) [\frac{G}{L}]$. Ahora, si $[Y] = [\emptyset]$, entonces \emptyset tendría una órbita distinta del vacío, lo que no es posible. De aquí que, sin pérdida de generalidad, podemos suponer que $[Y] \neq [\emptyset]$ y $[Z] \neq [\emptyset]$. Entonces si $a_{K_0} > 0$ existe $\mathcal{O}_G(y_0) \subseteq Y$ tal que $\mathcal{O}_G(y_0) \cong_G \frac{G}{K_0}$. Por otro lado, $[Y] = [Z]$, entonces $\mathcal{O}_G(y_0) \cong_G \mathcal{O}_G(z_0)$ para algún $z_0 \in Z$ que a su vez $\mathcal{O}_G(z_0) \cong_G \frac{G}{L_0}$ para algún L_0 tal que $a_{L_0} < 0$, en consecuencia $\frac{G}{K_0} \cong_G \frac{G}{L_0}$, así K_0 y L_0 son conjugados, lo que no es posible. Por tanto:

$$B(G) = \bigoplus_{H \in \mathcal{C}(G)} \mathbb{Z}[\frac{G}{H}].$$

■

Observación.

- Hay una inclusión $B^+(G) \rightarrow B(G)$ tal que $[X] \mapsto [X] - [\emptyset]$.
- Dados G un grupo finito, R un anillo conmutativo y:

$$f : B^+(G) \rightarrow R$$

un morfismo de semianillos, tenemos que f se extiende de manera única a $B(G)$; es decir, existe:

$$F : B(G) \rightarrow R$$

un morfismo de anillos tal que $F|_{B^+(G)} = f$. Además, F esta dada por:

$$F([X] - [Y]) = f([X]) - f([Y]).$$

Lema 4.20. *Sea:*

$$\begin{aligned} \varphi : B^+(G) &\rightarrow \prod_{H \in \mathcal{C}(G)} \mathbb{Z} \\ [X] &\mapsto (\varphi_H(X))_{H \in \mathcal{C}(G)}, \end{aligned}$$

entonces φ es un morfismo inyectivo de semianillos. De aquí que, φ se extiende de manera única a un morfismo inyectivo de anillos:

$$\tilde{\varphi} : B(G) \rightarrow \prod_{H \in \mathcal{C}(G)} \mathbb{Z}.$$

Para más información acerca del anillo de Burnside y de las demostraciones que se omiten en este capítulo puede consultar [4].

Capítulo 5

El anillo de Burnside para grupos nilpotentes finitos

Sea G un grupo finito, recordemos que el anillo de Burnside $B(G)$ denotado en esta sección como $B(G)$, es el anillo de Grothendieck de las clases de isomorfismo de los G -conjuntos con la suma dada por la unión disjunta y el producto dado por el producto cartesiano. $B(G)$ es libre como grupo abeliano con base dada por las clases de isomorfismo de G -conjuntos transitivos de la forma $\frac{G}{H}$ con $H \leq G$, en donde dos de estos se identifican si sus estabilizadores H son conjugados en G , esto es:

$$B(G) = \bigoplus_{H \in \mathcal{C}(G)} \mathbb{Z}[\frac{G}{H}]$$

donde $\mathcal{C}(G)$ es un conjunto completo de representantes de las clases de conjugación de subgrupos de G .

A menudo $B(G)$ se estudia a través del homomorfismo inyectivo de anillos, llamado marca:

$$\varphi : B(G) \rightarrow \mathbb{Z}^{|\mathcal{C}(G)|}$$

en donde, para cada K en $\mathcal{C}(G)$ la K -ésima coordenada de φ se define por:

$$\varphi_K(X) = |X^K|,$$

donde X es un G -conjunto, extendiéndose de manera lineal a todo $B(G)$. Denotamos por $\tilde{B}(G) = \mathbb{Z}^{|\mathcal{C}(G)|}$ el cual es llamado el anillo fantasma de G , con la suma y producto entrada a entrada. Sea $p \in \mathbb{Z}$ primo y sea \mathbb{Z}_p el anillo de los enteros p -ádicos. Denotamos los siguientes productos tensoriales:

$$B_p(G) = \mathbb{Z}_p \otimes B(G) = \bigoplus_{H \in \mathcal{C}(G)} \mathbb{Z}_p[\frac{G}{H}].$$

$$\tilde{B}_p(G) = \mathbb{Z}_p \otimes \tilde{B}(G) = \mathbb{Z}_p^{|\mathcal{C}(G)|}.$$

Aquí tenemos que $B_p(G)$ es un \mathbb{Z}_p -orden con $\tilde{B}_p(G)$ su orden máximo.

Observación. Sea $q \in \mathbb{Z}$ primo, notemos que $B_q(G) \subseteq \tilde{B}_q(G)$ (a través de la marca).

Sabemos que para cada $a \in \tilde{B}_q(G)$, se cumple que $|G|a \in B_q(G)$, en el caso en que $q \nmid |G|$ tenemos que $|G| \in \mathbb{Z}_q$ es unidad, esto implica $a \in B_q(G)$. Concluyendo que: si $q \nmid |G|$ entonces $B_q(G) = \tilde{B}_q(G)$.

Ejemplo. Sea $n \in \mathbb{N}$ y C_{p^n} un grupo cíclico de orden p^n con $p \in \mathbb{Z}$ primo. Entonces:

$$\mathcal{C}(C_{p^n}) = \{H_0, \dots, H_n\},$$

en donde $H_i \leq C_{p^n}$ de orden p^i para $i = 0, \dots, n$. Por lo anterior una base para $B_p(C_{p^n})$ sería a_0, \dots, a_n , donde:

$$a_i = C_{p^n}/H_i \text{ para } i = 0, \dots, n,$$

es decir que:

$$B_p(C_{p^n}) = \bigoplus_{i=0}^n \mathbb{Z}_p a_i$$

y su \mathbb{Z}_p -orden máximo es \mathbb{Z}_p^{n+1} . Recordemos que:

$$\varphi_H(C_{p^n}/K) = \begin{cases} |C_{p^n}/K| & \text{si } H \subseteq K \\ 0 & \text{si } H \not\subseteq K \end{cases}$$

Ahora la marca induce la siguiente inclusión:

$$\begin{aligned} \varphi : B_p(C_{p^n}) &\rightarrow \mathbb{Z}_p^{n+1} \\ X &\mapsto (\varphi_{H_0}(X), \dots, \varphi_{H_n}(X)) \end{aligned}$$

Por lo anterior, podemos ver a $B_p(G)$ como el subanillo de \mathbb{Z}_p^{n+1} , generado por las columnas de la siguiente matriz (conocida como la tabla de marcas de C_{p^n})

$$\begin{pmatrix} p^n & p^{n-1} & \dots & p & 1 \\ 0 & p^{n-1} & \dots & p & 1 \\ 0 & 0 & \dots & p & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & p & 1 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in M_{(n+1)}(\mathbb{Z}_p)$$

en donde la i -ésima columna esta dada por:

$$\varphi_{H_j}(C_{p^n}/H_{i-1}) = \begin{cases} p^{n-i+1} & \text{si } j \leq i-1 \\ 0 & \text{en otro caso} \end{cases}$$

para $j = 0, \dots, n$.

Lema 5.1. Sean P y K dos grupos finitos tales que P es un p -grupo para algún $p \in \mathbb{Z}$ primo y K de orden coprimo a p . Si $G = P \times K$ entonces:

$$B_p(G) \cong \prod_{H \in \mathcal{C}(K)} B_p(P)$$

Demostración. La prueba se basa en el Teorema 3.1 de [5], y el lector la puede encontrar en el Lema 5.1 de [1]. ■

Recordemos:

1. Si G_1, G_2 son grupos finitos tales que $|G_1|, |G_2|$ son primos relativos, entonces todo subgrupo de $G_1 \times G_2$ es de la forma $H_1 \times H_2$ con $H_1 \leq G_1, H_2 \leq G_2$.

2. Si G es un grupo nilpotente finito, entonces G es producto de sus subgrupos de Sylow.

Teorema 5.2. (El anillo de Burnside para grupos nilpotentes finitos.) Sea G un grupo nilpotente finito de orden $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con $p_i \in \mathbb{Z}$ primo y $\alpha_i \in \mathbb{N}$ para cada $i = 1, \dots, r$. Sea P_i el p_i -subgrupo de Sylow de G . Entonces:

$$B_{p_i}(G) \cong (B_{p_i}(P_i))^{\prod_{j \neq i} |\mathcal{C}(P_j)|}$$

Demostración. Consideremos $p_i \neq p_j$ si $i \neq j$, entonces por 1. de la nota anterior anterior $|\mathcal{C}(\prod_{j \neq i} P_j)| = \prod_{j \neq i} |\mathcal{C}(P_j)|$, por 2. de la nota anterior tenemos que $G \cong \prod_{j=1}^r P_j$. Sea $i \in \{1, \dots, r\}$ por el Lema anterior tenemos que:

$$\begin{aligned} B_{p_i}(G) &\cong (B_{p_i}(P_i))^{|\mathcal{C}(\prod_{j \neq i} P_j)|} \\ &= (B_{p_i}(P_i))^{\prod_{j \neq i} |\mathcal{C}(P_j)|}. \end{aligned}$$

■

Corolario 5.3. Con la notación del teorema anterior, si cada P_i es cíclico de orden $p_i^{\alpha_i}$ para $i = 1, \dots, r$. Entonces $(B_{p_i}(G) \cong B_{p_i}(P_i))^{\prod_{j \neq i} (\alpha_j + 1)}$ para cada $i = 1, \dots, r$.

Demostración. Observemos que $|\mathcal{C}(P_j)| = \alpha_j + 1$ para cada $j \in \{1, \dots, r\}$. El resultado es inmediato de el Teorema anterior. ■

Ejemplos. Sean $p, q \in \mathbb{Z}$ primos distintos y sea $G = P \times Q$ con P cíclico de orden p y Q cíclico de orden q^2

1. Del ejemplo para C_{p^n} tenemos:

$$\mathcal{C}(P) = \{H_0 = \{e\}, H_1 = P\}$$

una base para $B_p(P)$ es $a_0 = \frac{P}{\{e\}}$ y $a_1 = \frac{P}{P}$, es decir $B_p(P) = \mathbb{Z}_p a_0 \oplus \mathbb{Z}_p a_1$.

$$\begin{aligned} \varphi : B_p(P) &\rightarrow \mathbb{Z}_p^2 \\ a_0 &\mapsto (p, 0) \\ a_1 &\mapsto (1, 1) \end{aligned}$$

Así $B_p(P) \subseteq \mathbb{Z}_p^2$ está generada por las columnas de su tabla de marcas:

$$\begin{pmatrix} p & 1 \\ 0 & 1 \end{pmatrix}.$$

2. $\mathcal{C}(Q) = \{K_0 = \{e\}, K_1, K_2 = Q\}$ donde $K_1 \leq Q$ es de orden q .

Si $b_0 = \frac{Q}{K_0}$, $b_1 = \frac{Q}{K_1}$ y $b_2 = \frac{Q}{K_2}$, entonces $B_q(Q) = \mathbb{Z}_q b_0 \oplus \mathbb{Z}_q b_1 \oplus \mathbb{Z}_q b_2$.

$$\begin{aligned} \varphi : B_q(Q) &\rightarrow \mathbb{Z}_q^3 \\ b_0 &\mapsto (q^2, 0, 0) \\ b_1 &\mapsto (q, q, 0) \\ b_2 &\mapsto (1, 1, 1) \end{aligned}$$

Así $B_q(Q) \subseteq \mathbb{Z}_q^3$ está generada por las columnas de su tabla de marcas:

$$\begin{pmatrix} q^2 & q & 1 \\ 0 & q & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

3. $\mathcal{C}(G) = \mathcal{C}(P \times Q) = \{H_0 \times K_0, H_0 \times K_1, H_0 \times K_2, H_1 \times K_0, H_1 \times K_1, H_1 \times K_2\}$

Si $c_0 = \frac{G}{H_0 \times K_0}$, $c_1 = \frac{G}{H_0 \times K_1}$, $c_2 = \frac{G}{H_0 \times K_2}$, $c_3 = \frac{G}{H_1 \times K_0}$, $c_4 = \frac{G}{H_1 \times K_1}$, $c_5 = \frac{G}{H_1 \times K_2}$, entonces:

$$\begin{aligned} \varphi : B_q(G) &= \bigoplus_{i=0}^5 \mathbb{Z}_q c_i \rightarrow \mathbb{Z}_q^6 \\ c_0 &\mapsto (pq^2, 0, 0, 0, 0, 0) \\ c_1 &\mapsto (pq, pq, 0, 0, 0, 0) \\ c_2 &\mapsto (p, p, p, 0, 0, 0) \\ c_3 &\mapsto (q^2, 0, 0, q^2, 0, 0) \\ c_4 &\mapsto (q, q, 0, q, q, 0) \\ c_5 &\mapsto (1, 1, 1, 1, 1, 1) \end{aligned}$$

Así $B_q(G) \subseteq \mathbb{Z}_q^6$ está generada por las columnas de su tabla de marcas:

$$\begin{pmatrix} pq^2 & pq & p & q^2 & q & 1 \\ 0 & pq & p & 0 & q & 1 \\ 0 & 0 & p & 0 & 0 & 1 \\ 0 & 0 & 0 & q^2 & q & 1 \\ 0 & 0 & 0 & 0 & q & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

como $p \in \mathbb{Z}_q$ es unidad tenemos que p es invertible. Así, aplicando operaciones elementales en columnas tenemos que es equivalente a la matriz:

$$\begin{pmatrix} q^2 & q & 1 & 0 & 0 & 0 \\ 0 & q & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & q^2 & q & 1 \\ 0 & 0 & 0 & 0 & q & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Notemos que $B_q(G) \cong B_q(Q)^{|\mathcal{C}(P)|} = (B_q(Q))^2$.

4. $\mathcal{C}(G) = \mathcal{C}(P \times Q) = \{H_0 \times K_0, H_1 \times K_0, H_0 \times K_1, H_1 \times K_1, H_0 \times K_2, H_1 \times K_2\}$

Si $d_0 = \frac{G}{H_0 \times K_0}$, $d_1 = \frac{G}{H_1 \times K_0}$, $d_2 = \frac{G}{H_0 \times K_1}$, $d_3 = \frac{G}{H_1 \times K_1}$, $d_4 = \frac{G}{H_0 \times K_2}$, $d_5 = \frac{G}{H_1 \times K_2}$, entonces:

$$\begin{aligned} \varphi : B_p(G) &= \bigoplus_{i=0}^5 \mathbb{Z}_p d_i \rightarrow \mathbb{Z}_p^6 \\ d_0 &\mapsto (pq^2, 0, 0, 0, 0, 0) \\ d_1 &\mapsto (q^2, q^2, 0, 0, 0, 0) \\ d_2 &\mapsto (pq, 0, pq, 0, 0, 0) \\ d_3 &\mapsto (q, q, q, q, 0, 0) \\ d_4 &\mapsto (p, 0, p, 0, p, 0) \\ d_5 &\mapsto (1, 1, 1, 1, 1, 1) \end{aligned}$$

Así $B_p(G) \subseteq \mathbb{Z}_p^6$ está generada por las columnas de su tabla de marcas:

$$\begin{pmatrix} pq^2 & q^2 & pq & q & p & 1 \\ 0 & q^2 & 0 & q & 0 & 1 \\ 0 & 0 & pq & q & p & 1 \\ 0 & 0 & 0 & q & 0 & 1 \\ 0 & 0 & 0 & 0 & p & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

como $q \in \mathbb{Z}_p$ es unidad tenemos que q es invertible. Así, aplicando operaciones elementales en columnas tenemos que es equivalente a la matriz:

$$\begin{pmatrix} p & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & p & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & p & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Notemos que $B_p(G) \cong B_p(P)^{|C(Q)|} = (B_p(P))^3$.

Bibliografía

- [1] D. Villa-Hernández, *Zeta function of the Burnside ring for cyclic groups*, Int. J. Algebra, **5** (26) (2011), 1255-1266.
- [2] J. Rotman, *Advanced Modern Algebra*. Prentice Hall, 2002.
- [3] J. Rotman, *An Introduction to the Theory of Groups*. Springer, 1995 .
- [4] S. Bouc, *Burnside rings*, Handbook of Algebra, Vol 2, North Holland, Amsterdam, (2000), 739-804.
- [5] W. Kimmerle, F. Luca and G. Raggi-Cardenas, *Irreducible components and isomorphisms of the Burnside ring*, J. Group Theory, **11**(6) (2008), 831-844.