# Relacion de resultados teoricos para examen

## Algebra II

*Doble Grado en Matemáticas e Informática*

**Universidad de Granada**

**María Gallego Siles**

Junio 2025

# Índice

# 1. Tema1

Define el concepto de subgrupo normal de un grupo. Demuestra el Tercer Teorema de isomorfía para grupos.

# 2. Subgrupos normales

**Definición 1** (Subgrupos normales)**.** *Sea $G$ un grupo y $H < G$, diremos que $H$ es un subgrupo normal de $G$, denotado por $H \lhd G$, si las clases laterales de cada elemento coinciden, es decir, si:*

$$xH = Hx \qquad \forall x \in G$$

*En cuyo caso, tendremos que $G/ {}_H\sim \ = G/ \sim_H$, y notaremos a este conjunto como $G/H$, al que llamaremos conjunto de las clases laterales de $H$ en $G$.*

**Teorema 1** (Tercer Teorema de Isomorfía para grupos, o del doble cociente)**.** *Sea $G$ un grupo, $N \lhd G$, entonces existe una biyemathcalión entre los subgrupos de $G$ que contienen a $N$ y los subgrupos de $G/N$, dada por $H \longmapsto H/N$.*

*Además, $H \lhd G \iff H/N \lhd G/N$. En este caso:*

$$\frac{G/N}{H/N} \cong G/H$$

*Demostración.* Si consideramos la proyemathcalión al cociente $p : G \to G/N$ dada por $p(x) = xN$ para todo $x \in G$, consideramos las aplicaciones imagen directa e imagen inversa por $p$, dadas por:

$$\begin{gathered} p_* : \mathcal{P}(G) \to \mathcal{P}(G/N) \\ p^* : \mathcal{P}(G/N) \to \mathcal{P}(G) \\ p_*(H) = \{p(h) \mid h \in H\} \subseteq G/N \\ p^*(J) = \{x \in G \mid p(x) \in J\} \subseteq G \end{gathered}$$

Que podemos restringirlas en dominio y codominio a los conjuntos:

$$\begin{gathered} \mathcal{A} = \{H < G \mid N \subseteq H\} \\ \mathcal{B} = \{J < G/N\} \end{gathered}$$

Obteniendo aplicaciones (que nombramos igual ya que nos olvidamos de las otras):

$$\begin{gathered} p_* : \mathcal{A} \to \mathcal{B} \\ p^* : \mathcal{B} \to \mathcal{A} \end{gathered}$$

Veamos que estas aplicaciones están bien definidas (es decir, que podemos poner $\mathcal{B}$ como codominio de $p_*$ y $\mathcal{A}$ como codominio de $p^*$):

- Para $p_*$, hemos de observar primero que si cogemos $H \in \mathcal{A}$, entonces tendremos por el Corolario **??** que $N \lhd H$. En segundo lugar, ya vimos en la Proposición **??** que si $H < G$ entonces $p_*(H) < G/N$, por lo que la aplicación $p_*$ está bien definida. Vemos lo que pasa cuando la aplicamos a un elemento de $\mathcal{A}$:

$$p_*(H) = \{p(h) \mid h \in H\} = \{hN \mid h \in H\} = H/N < G/N$$

- Para $p^*$, vimos también en la Proposición **??** que si $J < G/N$ (es decir, $J \in \mathcal{B}$), entonces $p^*(J) < G$. Veamos que $N \subseteq p^*(J)$. Para ello, vemos que:

$$p(n) = nN = N \in J \qquad \forall n \in N$$

  Donde $N \in J$ por ser $N$ el elemento neutro para el grupo $G/N$ y ser $J < G/N$. En conclusión, $n \in p^*(J)$ $\forall n \in N$, y concluimos que $p^*$ está bien definida.

Veamos ahora qué sucede con la composición de las aplicaciones:

- Por una parte, dado $J \in \mathcal{B}$:

$$(p_* \circ p^*)(J) = p_*(\{x \in G \mid p(x) \in J\}) \stackrel{*}{=} J$$

  Donde en $(*)$ hemos aplicado que $p$ es sobreyectiva, por lo que si tenemos $yN \in J$, existirá un $x \in G$ de forma que $p(x) = yN$, luego todos los valores de $J$ se alcanzan.

- Dado $H \in \mathcal{A}$, veamos si $H = (p^* \circ p_*)(H)$:

  $\subseteq$) Sea $h \in H$, tenemos que:

$$\{h\} = p^*(\{p(h)\}) = p^*(p_*(\{h\})) \subseteq p^*(p_*(H))$$

  $\supseteq$) Sea $x \in p^*(p_*(H))$, entonces:

$$xN = p(x) \in p_*(H) = H/N = \{hN \mid h \in H\}$$

  Por lo que $x \in H$.

Concluimos que $(p_*)^{-1} = p^*$, por lo que $p_*$ es biyectiva y $\mathcal{A}$ es biyectivo con $\mathcal{B}$.

Veamos ahora que:

$$H \lhd G \Longleftrightarrow H/N \lhd G/N$$

$\Longrightarrow$) Sean $xN \in G/N$, $hN \in H/N$:

$$xNhN(xN)^{-1} = xNhNx^{-1}N \stackrel{*}{=} xhx^{-1}N \stackrel{(**)}{\in} H/N$$

Donde en $(*)$ hemos aplicado la definición del producto en el cociente y en $(**)$ hemos aplicado que $H \lhd G$, con lo que $xhx^{-1} \in H$.

$\Longleftarrow$) Ahora, sean $x \in G$ y $h \in H$:

$$xhx^{-1}N = xNhN(xN)^{-1} \in H/N$$

De donde concluimos que $xhx^{-1} \in H$, con lo que $H \lhd G$.

Finalmente, en este caso veamos que $\frac{G/N}{H/N} \cong G/H$. Para ello, consideramos las proyemathcaliones $p_N : G \to G/N$ y $p_H : G \to G/H$. Como $N \subseteq H = \ker(p_H)$, sabemos por la Propiedad Universal del grupo cociente (Teorema **??**) que existe un único homomorfismo $\varphi : G/N \to G/H$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} G \arrow[r, "p_N"] \arrow[dr, "p_H"'] & G/N \arrow[d, dotted, "\varphi"] \\ & G/H \end{tikzcd}$$

Es decir, $\varphi$ cumplirá que:

$$\varphi \circ p_N = p_H$$

Si aplicamos ahora el Primer Teorema de Isomorfía sobre $\varphi$:

$$\frac{G/N}{\ker(\varphi)} \cong Im(\varphi)$$

Y basta observar que:

- Por ser $p_H$ sobreyectiva (es una proyemathcalión), $\varphi$ también será sobreyectiva, por lo que $Im(\varphi) = G/H$.
- Veamos que $\ker(\varphi) = H/N$:

  $\subseteq$) Sea $xN \in \ker(\varphi)$, entonces:

  $$H = \varphi(xN) = \varphi(p_N(x)) = p_H(x) = xH \Longrightarrow x \in H$$

  $\supseteq$) Sea $hN \in H/N$, entonces:

  $$\varphi(hN) = \varphi(p_N(h)) = p_H(h) = hH = H$$

  Por lo que $hN \in \ker(\varphi)$.

En definitiva, hemos probado que:

$$\frac{G/N}{H/N} \cong G/H$$

□

# 3. Tema2

Define los conceptos de serie de composición y de serie derivada de un grupo y da dos definiciones de grupo resoluble demostrando su equivalencia. Razona que $S_4$ es resoluble pero que $S_5$ no lo es.

**Definición 2** (Serie de composición)**.** *Una serie de $G$ se dice que es una serie de composición de $G$ si es una serie normal sin refinamientos normales propios. En una serie de composición, será usual referirnos a los factores como factores de composición, y a los índices como índices de composición.*

**Definición 3** (Serie derivada)**.** *La serie derivada de un grupo $G$ es la cadena de subgrupos normales:*

$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd \ldots$$

*Donde:*

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \qquad \forall k \in \mathbb{N}$$

*De esta forma, el subgrupo $G' = [G, G]$ recibe el nombre de subgrupo derivado de $G$, o primer derivado de $G$.*

**Definición 4.** *Un grupo $G$ se dice* <u>resoluble</u> *si existe un índice $k$ de forma que $G^{(k)} = \{1\}$. Es decir, la serie derivada de $G$ alcanza el $\{1\}$.*

**Caracterización 1.** *$G$ resoluble $\Leftrightarrow$ $G$ tiene una serie normal con factores abelianos.*

*Demostración.* $\Rightarrow$) Si $G$ es resoluble, la serie derivada será de la forma:

$$G = G^0 \rhd G' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Que es una serie normal con factores abelianos, ya que los factores son de la forma:

$$G^{(k-1)}/G^{(k)} = G^{(k-1)}/\left[G^{(k-1)}, G^{(k-1)}\right]$$

Ya que vimos que $[G^{(k-1)}, G^{(k-1)}$ es el grupo abelianizado de $G^{(k-1)}$ que es un grupo abeliano.

$\Leftarrow$) Consideramos una serie normal con factores abelianos:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Donde los grupos $G_k/G_{k+1}$ son abelianos, para todo $k \in \{0, \ldots, r-1\}$. Veamos que $G^{(k)} < G_k$, para todo $k \in \{1, \ldots, r\}$:

- <u>Para $k = 1$</u>: como el cociente $G/G_1$ es abeliano, tenemos que $G' = [G, G] < G_1$.

- Supuesto que $G^{(k)} < G_k$, veámoslo para $k+1$: Como tenemos por hipótesis que $G^{(k)} < G_k$, si consideramos el grupo derivado a ambos lados, tendremos que:
$$G^{(k+1)} = (G^{(k)})' < G'_k = [G_k, G_k]$$
Y finalmente, como el cociente $G_k/G_{k+1}$ es abeliano, deducimos que $G'_k = [G_k, G_k] < G_{k+1}$. En definitiva, tenemos $G^{(k+1)} < G_{k+1}$.

Una vez probado esto, en particular, tenemos que:
$$G^{(r)} < G_r = \{1\}$$
De donde deducimos que el $r-$ésimo grupo derivado de $G$ es trivial, con lo que $G$ es resoluble. $\square$

- $S_4$ es resoluble, ya que $S'_4 = [S_4, S_4] = A_4$ y en cuanto a la serie de $A_4$ se tiene que:
$$A'_4 = [A_4, A_4] = V$$
$$A''_4 = V' = [V, V] = \{1\}$$
Y la serie derivada es:
$$A_4 \rhd V \rhd \{1\}$$
Luego $A_4$ resoluble y por tanto $S_4$ tambien con serie derivada:
$$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

- $S_5$ es resoluble, ya que aplicando el Teorema de Abel tenemos que $S_5$ es simple, es decir, no tiene subgrupos normales propios luego:
$$S_5 \rhd 1$$

# 4. Tema3

Define, para un grupo G, los conceptos de G-conjunto X y de órbita y estabilizador de un elemento $x \in X$. Demuestra los resultados requeridos que conduzcan, en las condiciones oportunas, a la llamada fórmula de clases (—G— = —Z(G)— + . . .).

**Definición 5** (G-Conjunto)**.** *Sea $G$ un grupo y $X$ un conjunto no vacío, una acción de $G$ sobre $X$ es una aplicación:*

$$\begin{array}{rcl} ac\colon G\times X & \longrightarrow & X \\ (g,x) & \longmapsto & ac(g,x) \end{array}$$

*Que verifica:*

*i)* $ac(1,x) = x \quad \forall x \in X.$

*ii)* $ac(g, ac(h,x)) = ac(gh,x) \quad \forall x \in X, \quad \forall g,h \in G.$

*En dicho caso, diremos que $G$ actúa (o que opera) sobre $X$.*

*Si $G$ actúa sobre $X$, diremos que este conjunto $X$ es un $G-$conjunto a izquierda. A la aplicación $ac$ se le llama aplicación de la $G-$estructura.*

**Definición 6** (Órbita)**.** *Sea $G$ un grupo y $X$ un $G-$conjunto, definimos en $X$ una relación de equivalencia $\sim$ (se comprueba a continuación) dada por:*

$$y \sim x \iff \exists g \in G \mid y = {}^g x$$

*La clase de equivalencia de cada $x \in X$ se llama <u>órbita de $x$</u>, denotada por:*

$$Orb(x) = \{y \in X \mid \exists g \in G \text{ con } y = {}^g x\}$$

*Como estamos considerando una acción, será equivalente escribir:*

$$Orb(x) = \{y \in X \mid \exists g \in G \text{ con } {}^g y = x\}$$

*Tenemos de esta forma que el conjunto cociente $X/\sim$ es el conjunto formado por las órbitas de todos los elementos de $X$:*

$$X/\sim\, = \{Orb(x) \mid x \in X\}$$

**Definición 7** (Estabilizador)**.** *Sea $G$ un grupo y $X$ un $G-$conjunto, definimos el grupo de estabilizadores de $x \in X$ en $G$ como:*

$$Stab_G(x) = \{g \in G \mid {}^g x = x\}$$

*También se le llama grupo de isotropía.*

### 4.0.1. Fórmula de clases

**Definición 8** (Centralizador)**.** *Sea $G$ un grupo y $S \subseteq G$, llamamos centralizador de $S$ en $G$ al conjunto:*

$$C_G(S) = \{x \in G \mid xs = sx \quad \forall s \in S\}$$

**Definición 9** (Normalizador)**.** *Sea $G$ un grupo y $S \subseteq G$, llamamos normalizador de $S$ en $G$ al conjunto:*

$$N_G(S) = \{x \in G \mid xS = Sx\}$$

Considerando la acción por conjugación, :

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = ghg^{-1}\} = \{ghg^{-1} \mid g \in G\} = Cl_G(h) \qquad \forall h \in G$$

De esta forma, llamaremos a la órbita de $h$ por la acción por conjugación la clase de conjugación de $h$ en $G$.

$$Stab_G(h) = \{g \in G \mid {}^g h = ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = C_G(h)$$

El estabilizador de $h$ en $G$ coincide con el centralizador de $h$ en $G$, y como la órbita de $h$ coincidía con la clase de conjugación de $h$ en $G$, tenemos que:

$$|Cl_G(h)| = |Orb(h)| = [G : Stab_G(h)] = [G : C_G(h)] \qquad \forall h \in G$$

Y en el caso de que $G$ sea finito:

$$|Cl_G(h)||C_G(h)| = |G|$$

Para los puntos fijos:

$$Fix(X) = \{h \in G \mid ghg^{-1} = {}^g h = h \quad \forall g \in G\} = \{h \in G \mid gh = hg \quad \forall g \in G\} = Z(G)$$

Podemos particularizar la fórmula anteriormente obtenida:

$$|X| = |Fix(X)| + \sum_{y \in \Gamma} [G : Stab_G(y)]$$

Para la acción por conjugación, obteniendo la **fórmula de clases**:

$$|G| = |Z(G)| + \sum_{y \in \Gamma} [G : C_G(y)]$$

Donde podemos pensar en $\Gamma$ en el conjunto formado por los representantes de las órbitas con más de un elemento.

Esta última podemos generalizarla para cualquier subgrupo $H \lhd G$, obteniendo la **fórmula de clases general**:

$$|H| = |H \cap Z(G)| + \sum_{y \in \Gamma} [G : C_G(y)]$$

## 5. Tema4

Demuestra el Teorema de Cauchy (Si G es un grupo finito y p es un primo que divide a —G—, entonces G tiene un elemento de orden p). Concluye que, si G es finito, entonces G es un p-grupo si y sólo si su orden es una potencia de p.

**Teorema 2** (de Cauchy)**.** *Si $G$ es un grupo finito y $p$ es un primo que divide a $|G|$, entonces $G$ tiene un elemento de orden $p$, y por tanto tendrá un $p-$subgrupo de orden $p$.*

*Demostración.* Si consideramos:

$$X = \{(a_1, a_2, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = 1\}$$

Si $|G| = n$, entonces $|X| = n^{p-1}$, ya que elegimos libremente las $p-1$ primeras coordenadas (variación con repetición):

$$a_1, a_2, \dots, a_{p-1} \in G \quad \text{arbitrarios}$$

Y la última viene condicionada:

$$a_p = (a_1, a_2, \dots, a_{p-1})^{-1}$$

Sea $\sigma = (1\ 2\ \dots\ p) \in S_p$, consideramos $H = \langle\sigma\rangle = \{1, \sigma, \dots, \sigma^{p-1}\} \subseteq S_p$. Consideramos también la acción $ac : H \times X \to X$ dada por (compruébese que es una acción):

$$ac(\sigma^k, (a_1, a_2, \dots, a_p)) = \left(a_{\sigma^k(1)}, a_{\sigma^k(2)}, \dots, a_{\sigma^k(p)}\right) \qquad \forall (a_1, \dots, a_p) \in X, \forall \sigma^k \in H$$

Tenemos que:

$$|Orb(z)| = [H : Stab_H(z)] = \frac{|H|}{|Stab_H(z)|} \qquad \forall z \in X$$

De donde tenemos que $|Orb(a_1, \dots, a_p)|$ es un divisor de $|H|$, $\forall (a_1, \dots, a_p) \in X$. En dicho caso, $|Orb(a_1, \dots, a_p)| \in \{1, p\}$, por ser $|H| = p$. Por tanto, las órbitas de un elemento serán unitarias o bien tendrán cardinal $p$.

Por tanto, sean $r$ el número de órbitas con un elemento y $s$ el número de órbitas con $p$ elementos, entonces ($|\Gamma| = s$):

$$n^{p-1} = |X| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)| = r + \sum_{y \in \Gamma} p = r + sp$$

Veamos ahora cómo son los elementos de $Orb(a_1, \dots, a_p)$:

$$\begin{aligned} Orb(a_1, \dots, a_p) &= \left\{{}^{\sigma^k}(a_1, \dots, a_p) \mid k \in \{0, \dots, p-1\}\right\} \\ &= \{(a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots, (a_p, a_1, \dots, a_{p-1})\} \end{aligned}$$

Por tanto, la órbita será unitaria si y solo si $a_1 = a_2 = \ldots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geq 1$), como $Orb(1, 1, \ldots, 1)$. Busquemos más: por hipótesis, $p \mid n$ y además $r = n^{p-1} - sp$, de donde $p \mid r$, por lo que $r \geq 2$ (ya que lo divide un primo).

En conclusión, $\exists a \in G \setminus \{1\}$ de forma que $Orb(a, a, \ldots a)$ es unitaria, de donde $a^p = 1$, por lo que $O(a) = p$.

Finalmente, sea $x \in \langle a \rangle \setminus \{1\}$, tenemos entonces que $1 \neq O(x) \mid p$, por lo que $O(x) = p$ y tenemos que todo elemento del subgrupo $\langle a \rangle$ es de orden $p$. En definitiva, $\langle a \rangle$ es un $p-$subgrupo de $G$ de orden $p$. $\square$

**Corolario 1.** *Sea $G$ un grupo finito y $p$ un número primo:*

$$G \text{ es un } p\text{-grupo} \iff \exists n \in \mathbb{N} \text{ con } |G| = p^n$$

*Demostración.* Veamos la doble implicación.

$\Longleftarrow$) Si $|G| = p^n$ para cierto $n \in \mathbb{N}$, entonces tendremos que $O(x)|p^n$ para todo $x \in G$, de donde $O(x) = p^k$ para cierto $k \in \mathbb{N}$, luego $G$ es un $p-$grupo.

$\Longrightarrow$) Suponemos que $q$ es un primo que divide al orden de $|G|$, luego por el Teorema de Cauchy debe existir $x \in G$ de forma que $O(x) = q$. En dicho caso, como $G$ es un $p-$grupo, $q = p^r$ para cierto $r \in \mathbb{N}$, de donde ($q$ y $p$ son primos) $r = 1$ y $q = p$.

De esta forma, el único primo que divide a $|G|$ es $p$, luego $|G| = p^n$, para algún $n \in \mathbb{N}$. $\square$

## 6. Tema5

Demuestra el Teorema de Burnside (el centro de un p-grupo finito es no trivial) y concluye, como consecuencia, que todo grupo de orden $p^2$ es abeliano. Clasifica entonces, salvo isomorfismo, todos los grupos de órdenes 4, 9 y 841.

**Teorema 3** (de Burnside)**.** *Si $G$ es un $p-$grupo finito no trivial, entonces $|Z(G)| \geq p$, y en particular, $|Z(G)| \neq \{1\}$.*

*Demostración.* Distinguimos casos:

- Si $G$ es abeliano, $Z(G) = G$ y tenemos que $|Z(G)| = |G| = p^n$ para cierto $n \in \mathbb{N}$, por lo que $|Z(G)| \geq p$. En particular, $Z(G) = G$ no es trivial.

- Si $G$ es no abeliano, entonces $Z(G) < G$ y por la fórmula anterior de clases:
$$p^n = |G| = |Z(G)| + \sum_{h \in \Gamma} [G : C_G(h)]$$
Como $G$ es finito, $[G : C_G(h)]$ divide a $|G| = p^n$ para cualquier $h \in \Gamma$ y para cierto $n \in \mathbb{N}$. Es decir:
$$[G : C_G(h)] = p^k \qquad \text{para algún } k \in \mathbb{N}, \quad \forall h \in \Gamma$$
En ningún caso puede ser $k = 0$, ya que diríamos que $C_G(h) = G$ y:
$$C_G(h) = \{g \in G \mid gh = hg\}$$
De donde $h \in Z(G)$, por lo que $h$ no estaría en $\Gamma \subseteq G \setminus Z(G)$.

  En dicho caso, $p \mid [G : C_G(h)]$ para todo $h \in \Gamma$, $p \mid |Z(G)|$ (despejar $|Z(G)|$ de la anterior igualdad), de donde $|Z(G)| \geq p$.

□

**Corolario 2.** *Si $|G| = p^2$ entonces $G$ es abeliano*

*Demostración.* Sabemos que $Z(G) < G$ luego $|Z(G)|||G|$ entonces tenemos tres posibilidades:

- $|Z(G)| = 1$ pero ya hemos visto que no podía ser por Burnside.

- $|Z(G)| = p$ entonces:
$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$
Pero un grupo de orden $p$ es cíclico, y si $G/Z(G)$ es cíclico, entonces $G$ es abeliano. Pero si $G$ es abeliano, entonces $Z(G) = G$ lo cual contradice que $|Z(G)| = p < p^2$.

- $|Z(G)| = p^2 = |G|$ que es la unica posibilidad que nos queda.

Luego para $|G| = p^2$ se tiene que $G = Z(G)$ y por tanto $G$ es abeliano. $\square$

Ahora procederemos a la clasificacion. Tenemos que:

- Si $|G| = 4 = 2^2$
- Si $|G| = 9 = 3^2$
- Si $|G| = 841 = 29^2$

Luego tebemos que dado G se tiene $|G| = p^2$ para algun p primo. Por el Corolario de Burnside tenemos que G es un grupo abeliano finito. Luego podremos clasificarlos de la siguiente manera:

- Para saber los grupos abelianos finitos de orden $4 = 2^2$, calculamos cada una de las particiones de 2:

$$2 \longrightarrow G \cong C_4$$
$$1, 1 \longrightarrow G \cong C_2 \oplus C_2$$

- Para saber los grupos abelianos finitos de orden $9 = 3^2$, calculamos cada una de las particiones de 2:

$$2 \longrightarrow G \cong C_9$$
$$1, 1 \longrightarrow G \cong C_3 \oplus C_3$$

- Para saber los grupos abelianos finitos de orden $841 = 29^2$, calculamos cada una de las particiones de 2:

$$2 \longrightarrow G \cong C_{841}$$
$$1, 1 \longrightarrow G \cong C_{29} \oplus C_{29}$$

# 7. Tema6

(Teoremas de Sylow) Demuestra que, si G es un grupo finito, para cualquier potencia de un primo p que divida al orden del grupo existe un subgrupo cuyo orden es esa potencia de p. Define entonces el concepto de p-subgrupo de Sylow de un grupo finito G y concluye la existencia de p-subgrupos de Sylow de G.

**Teorema 4.** *Sea $G$ un grupo finito con $|G| = n$ y sea $p$ un número primo, entonces para toda potencia $p^k$ que divida a $n$, existe un subgrupo $H < G$ con orden $|H| = p^k$.*

*Demostración.* Por inducción sobre $k$:

- Si $k = 1$: tenemos el Teorema de Cauchy.
- Primera hipótesis de inducción: el resultado es cierto para todo $l < k$: si $p^l$ divide a $|G|$, entonces $\exists H < G$ con $|H| = p^l$.
  Veamos qué ocurre con $k$, es decir, si $|G| = p^k r = n$ para cierto $r \in \mathbb{N}$.

  Por inducción sobre $r$:

  - Si $r = 1$: tomamos $H = G$.
  - Segunda hipótesis de inducción: si $r > 1$, suponemos el resultado cierto para todo grupo de orden divisible por $p^k$ que sea de la forma $p^k m$ con $m < r$, es decir, $\exists H < G$ con $|H| = p^k$, veamos qué ocurre con $G$:

    Para ello, distinguimos casos:

    - Si existe $K < G$, $K \neq G$ de forma que $p \nmid [G : K]$. En dicho caso: $|G| = [G : K]|K|$ y $p^k \mid |G|$, entonces $p^k$ dividirá a $|K|$. Usando la Segunda Hipótesis de inducción, tendremos $H < K < G$ de forma que $|H| = p^k$.
    - Si para cualquier $K < G$, $K \neq G$ se tiene que $p \mid [G : K]$, entonces usando la fórmula de las clases:

      $$|Z(G)| = G - \sum_{h \in \Gamma} [G : C_G(h)]$$

      Y como $p$ divide a todos los $[G : C_G(h)]$, concluimos que $p \mid |Z(G)|$. Por el Teorema de Cauchy, podemos encontrar $K < Z(G)$ de forma que $|K| = p$.
      Por ser $K \subseteq Z(G)$, entonces $K \lhd G$ y podemos considerar el conjunto cociente $G/K$, con orden:

      $$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{p}$$

      De donde $p^{k-1} \mid |G/K|$.

Por la Primera Hipótesis de inducción, existe otro $L < G/K$ con $|L| = p^{k-1}$. Por el Tercer Teorema de Isomorfía, sabemos que $\exists K \lhd H < G$ de forma que:

$$L = H/K$$

De donde:

$$|H| = |H/K||K| = p^{k-1}p = p^k$$

$\square$

**Definición 10** ($p-$subgrupos de Sylow)**.** *Si $G$ es un grupo finito y $p$ un número primo que divide a $|G|$, un $p-$subgrupo de Sylow de $G$ es un $p-$subgrupo de $G$ cuyo orden es la máxima potencia de $p$ que divide a $|G|$.*

*Es decir, si $|G| = p^k m$ con $(p, m) = 1$ y $p$ primo, un $p-$subgrupo $H < G$ es de Sylow si $|H| = p^k$.*

**Corolario 3** (Primer Teorema de Sylow)**.** *Para todo grupo finito $G$ y todo divisor primo $p$ de su orden, existe al menos un $p-$subgrupo de Sylow.*

*Demostración.* Es evidente a partir del Teorema 4. $\square$

## 8. Tema 7: Teoremas de Sylow

Demuestra que todo $p$-subgrupo de un grupo finito $G$ (con $|G| = p^k m$ y $mcd(p, m) = 1$) está contenido en un $p$-subgrupo de Sylow, y que el número $n_p$ de $p$-subgrupos de Sylow de $G$ satisface:

- $n_p \mid m$
- $n_p \equiv 1 \pmod p$

**Teorema 5** (Segundo Teorema de Sylow)**.** *Sea $G$ un grupo finito, $p$ un número primo, supongamos que $|G| = p^k m$ con $(p, m) = 1$ y $n_p$ denota el número de $p-$subgrupos de Sylow de $G$, entonces:*

*i)* *Todo $p-$subgrupo de $G$ está contenido (como subgrupo) en un $p-$subgrupo de Sylow de $G$.*

*ii)* *Cualesquiera dos $p-$subgrupos de Sylow de $G$ son conjugados.*

*iii)* *$n_p \mid m$ y $n_p \equiv 1 \mod p$.*

*Demostración.* Demostramos cada apartado:

*i)* Si llamamos $S = Syl_p(G) = \{P \mid P \text{ es un } p-\text{subgrupo de Sylow de } G\}$, consideramos la acción por conjugación $G \times S \to S$ dada por:

$$ac(g, P) = {}^gP = gPg^{-1} \in S$$

Que estará bien definida, ya que el orden del conjugado de un elemento coincide con el orden del propio elemento, por lo que $ac(g, P)$ seguirá siendo un $p-$subgrupo de Sylow, para cualquier $P \in S$ y $g \in G$. Sea $P_1 \in S$, estudiemos su órbita y su estabilizador:

$$Orb(P_1) = \{gP_1g^{-1} \mid g \in G\}$$
$$Stab_G(P_1) = \{g \in G \mid gP_1g^{-1} = P_1\} = N_G(P_1)$$

Tenemos:

$$|Orb(P_1)| = [G : N_G(P_1)]$$
$$P_1 < N_G(P_1) < G$$
$$[G : P_1] = [G : N_G(P_1)][N_G(P_1) : P_1]$$

Por lo que $|Orb(P_1)|$ divide a $[G : P_1] = m$. En definitiva:

$$(|Orb(P_1)|, p) = 1$$

Ahora, veamos que todo $p-$subgrupo está contenido en un $p-$subgrupo de Sylow. Para ello, sea $H$ un $p-$subgrupo de $G$, consideramos la acción sobre la órbita de $P_1 \in S$, $H \times Orb(P_1) \to Orb(P_1)$, dada por:

$$ac(h, P) = {}^hP = hPh^{-1} \in Orb(P_1)$$

Tendremos:

$$Stab_H(P) = \{h \in H \mid hPh^{-1} = P\} = H \cap N_G(P) < H$$

Además, también tendremos que $H \cap N_G(P) < P$, ya que si $H$ es un $p-$subgrupo de $N_G(P)$, entonces $H < P$. En definitiva:

$$Stab_H(P) = H \cap N_G(P) < H \cap P < H \cap N_G(P)$$

De donde tenemos que $H \cap N_G(P) = H \cap P$. Usando la fórmula de la órbita:

$$|Orb(P_1)| = \sum_P [H : Stab_H(P)] = \sum_P [H : H \cap P]$$

De donde cada sumando divide a $|H|$ con $H$ un $p-$subgrupo de $P$, por lo que $|H|$ es una potencia de $p$. Sin embargo, como $p \nmid |Orb(P_1)|$ (su máximo común divisor era 1), ha de existir un grupo $P \in Orb(P_1)$ (notemos que $P$ es un $p-$subgrupo de Sylow. De hecho, $P$ es un conjugado de $P_1$) de forma que:

$$[H : H \cap P] = 1$$

Por lo que $H \cap P = H$ y $H < P$.

*ii)* Veamos ahora que cualesquiera dos $p-$subgrupos de Sylow de $G$ son conjugados. Para ello, sean $P_1, P_2$ dos $p-$subgrupos de Sylow de $G$, antes vimos (el lema) que si $H = P_2 < G$, entonces $H$ está contenido en un subgrupo de Sylow, por lo que $\exists P$, un $p-$subgrupo de Sylow, conjugado de $P_1$ (por *i)*) de forma que $P_2 < P$, pero $|P| = |P_2|$, luego $P_2 = P$.

*iii)* Veamos ahora que $n_p \mid m$ y que $n_p \equiv 1 \mod p$.

En el apartado *ii)* hemos visto que $Orb(P_1) = S$, luego:

$$n_p = |S| = |Orb(P_1)| = [G : N_G(P_1)]$$

Por lo que $n_p \mid m$.

Si en el apartado *i)* tomamos $H = P_1$ (el de la demostración anterior):

$$n_p = |Orb(P_1)| = \sum_P [P_1 : P_1 \cap P]$$

Por lo que $[P_1 : P_1 \cap P] = 1$ y los demás eran múltiplos de $p$, deducimos que $n_p \equiv 1 \mod p$.

□

# 9. Tema8

Prueba que todos los grupos de orden $2p$, siendo $p$ un primo impar, y también todos los de orden $pq$, siendo $p$, $q$ primos con $p > q$ y $q \nmid (p-1)$, son producto semidirecto.

Clasifica los grupos de estos órdenes y concluye entonces con la clasificación de todos los grupos de órdenes 6, 10, 14, 15, 161 y 1994.

Aplicaremos el siguiente teeorema para demostrar que los grupos de orden $2p$ y $pq$ son producto semidirecto:

**Teorema 6.** *Sea $G$ un grupo y $K, H < G$ con $K \lhd G$, $KH = G$ y $K \cap H = \{1\}$, sea $\theta : H \to Aut(K)$ un homomorfismo que nos da la acción $ac : H \times K \to K$ por conjugación:*

$$\theta(h)(k) = hkh^{-1} \qquad \forall h \in H, \forall k \in K$$

*Entonces, $K \rtimes_\theta H \cong G$.*

- Para $|G| = 2p$ con $p$ primo impar tenemos que como $p||G|$ entonces aplicando el Teorema 4 tendremos que existe $H < G$ tal que $|H| = p$. Considerando el Segundo Teorema de Sylow veamos cuanto vale $n_p$:

$$\left.\begin{array}{r} n_p \mid 2 \\ n_p \equiv 1 \mod p \end{array}\right\} \Longrightarrow n_p \in \{1, 2\}$$

  - Si $n_p = 2$ entonces $2 \equiv 1 \mod p \Leftrightarrow 2 = \mathbb{Z}p + 1$. Luego tendriamos que solo se cumple para $p = 1$. Entonces $|P| = 1 \Rightarrow |G| = 2$. Entonces $G \cong C_2 \cong C_2$ x {e} siendo e el elemento neutro.
  - Si $n_p = 1$ entonces existe un único $p$-subgrupo de Sylow P de orden $|P| = p$ que es normal en G, es decir, $P \lhd G$. Y podemos considerar su cociente de manera que:

$$|K| = [G : P] = \frac{|G|}{|P|} = 2$$

    Veamos que se verifican las condiciones del Teorema:

    - $P, K < G$ con $P \lhd G$.
    - $PK = G$ ya que $|PK| = |G|$
    - $P \cap K = \{1\}$, veamoslo:
      Sea $x \in P \cap K$ entonces:

$$\left.\begin{array}{r} o(x) \mid |P| = p \\ o(x) \mid |K| = 2 \end{array}\right\} \Longrightarrow o(x) \in \{1, 2\}$$

      Si $|P| \neq 2$ entonces $o(x) = 1$ con lo que $x = 1$. Y habremos demostrado que $P \cap K = \{1\}$.

Si $|P| = 2 = p$ pero por hipotesis p es un primo impar luego este caso queda descartado y por tanto tenemos que G se escribe como producto semidirecto:

$$G = P \rtimes_\theta K$$

donde $\theta$ es una acción dada por $\theta : P \to Aut(K)$.

- Para $|G| = pq$ con $p, q$ numeros primos con $q > p$ tenemos que como $q||G|$ entonces aplicando el Teorema 4 tendremos que existe $H < G$ tal que $|H| = q$. Considerando el Segundo Teorema de Sylow veamos cuanto vale $n_q$:

$$\left.\begin{array}{r} n_q \mid p \\ n_q \equiv 1 \pmod{q} \end{array}\right\} \Longrightarrow n_p \in \{1, p\}$$

  - Si $n_q = p$ entonces $p \equiv 1 \pmod{p} \Leftrightarrow p = \mathbb{Z}q + 1 \Leftrightarrow p - 1 = \mathbb{Z}q$. Como por hipotesis tenemos que $q > p$ luego la unica pobilidad es es que $p - 1 = 0 \Leftrightarrow p = 1$. Entonces existe un único $q$-subgrupo de Sylow Q de orden $|Q| = q$ que es normal en G, es decir, $Q \triangleleft G$. Y podemos considerar su cociente de manera que:

$$|P| = [G : Q] = \frac{|G|}{|Q|} = p$$

    Veamos que se verifican las condiciones del Teorema:

    - $P, Q < G$ con $Q \triangleleft G$.
    - $PQ = G$ ya que $|PQ| = |G|$
    - $P \cap Q = \{1\}$, veamoslo:
      Sea $x \in P \cap K$ entonces:

$$\left.\begin{array}{l} o(x) \mid |P| = p \\ o(x) \mid |Q| = q \end{array}\right\} \Longrightarrow o(x) = mcd(p, q) = 1$$

      Luego tendremos que $x = 1$ y por tanto $P \cap Q = \{1\}$ como queriamos. Podemos aplicar el Teorema y por tanto tenemos que G se escribe como producto semidirecto:

$$G = P \rtimes_\theta K$$

      donde $\theta$ es una acción dada por $\theta : P \to Aut(K)$.

Ahora procederemos a la clasificacion, en primer lugar vemos que, para los ordenes dados se tiene:

$$\begin{array}{ll} |G| = 6 = 2 \cdot 3 & |G| = 14 = 2 \cdot 7 \\ |G| = 15 = 3 \cdot 5 & |G| = 10 = 2 \cdot 5 \\ |G| = 161 = 7 \cdot 23 & |G| = 1994 = 2 \cdot 997 \end{array}$$

Para G con orden 6, 10,14 y 1994 estamos en el caso en el que $|G| = 2p$ y para G con orden 15 y 161 $|G| = pq$ con $p, q$ primos luego se tendra que:

$$\begin{array}{ll} \text{Si } |G| = 6 & \Rightarrow G \cong S_3 \text{ o } G \cong C_6 \\ \text{Si } |G| = 10 & \Rightarrow G \cong D_5 \text{ o } G \cong C_{10} \\ \text{Si } |G| = 14 & \Rightarrow G \cong D_7 \text{ o } G \cong C_{14} \\ \text{Si } |G| = 15 & \Rightarrow G \cong P \rtimes_\theta K \text{ o } G \cong C_{15} \\ \text{Si } |G| = 161 & \Rightarrow G \cong P \rtimes_\theta K \text{ o } G \cong C_{161} \\ \text{Si } |G| = 1994 & \Rightarrow G \cong P \rtimes_\theta K \text{ o } G \cong C_{1994} \end{array}$$

# 10. Tema9

Clasifica, salvo isomorfismo, todos los grupos de orden 8.

## 10.1. Grupos de orden 8

Sea $G$ un grupo de orden 8, no vamos a tener $p-$subgrupos de Sylow, porque el único es el total. Los grupos abelianos son:

$$C_2 \times C_2 \times C_2 \qquad C_2 \times C_4 \qquad C_8$$

### 10.1.1. No abelianos

Si $G$ es un grupo no abeliano de orden 8, entonces no existen elementos en $G$ de orden 8, ya que entonces $G$ sería cíclico, luego abeliano. Por tanto, los elementos de $G$ tendrán orden 2 o 4. Tampoco pueden ser todos de orden 2, puesto que $G$ también sería abeliano, por lo que $\exists a \in G$ de forma que $O(a) = 4$. Consideramos:

$$H = \langle a \rangle = \{1, a, a^2, a^3\}$$

Tenemos que $[G : H] = 2$, por lo que $H \lhd G$. Dado $b \in G \setminus H$, tendremos dos clases en el cociente:

$$G = H \cup Hb$$

De esta forma, podemos describir $G$ como:

$$G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

Si consideramos $b^2$, veamos en qué clase está. Supuesto que $b^2 \in Hb$, entonces:

- Puede ser que $b^2 = b \Longrightarrow b = 1$.
- Puede ser $b^2 = ab \Longrightarrow b = a$.
- Puede ser $b^2 = a^2b \Longrightarrow b = a^2$.
- Puede ser $b^2 = a^3b \Longrightarrow b = a^3$.

Todas imposibles, por lo que $b^2 \in H = \{1, a, a^2, a^3\}$, de donde:

- Si $b^2 = a$, entonces $O(b^2) = O(a) \Longrightarrow O(b) = 8$, imposible.
- Si $b^2 = a^3$, entonces $O(b^2) = O(a^3) = O(a)$, imposible.
- Si $b^2 = 1$, veamos que $ba = a^3b$. Como $H \lhd G$, tenemos que $bab^{-1} \in H$, pero como $O(b) = 2$, tenemos que $bab \in H$ y:

  $$O(bab) = O(a) = 4$$

  De donde $bab \in \{a, a^3\}$. Si $bab = a$, entonces $G$ es abeliano, imposible, por lo que:

  $$bab = a^3$$

Por lo que en este caso tenemos:

$$G = \langle a, b \mid a^4 = b^2 = 1, ba = a^3 b \rangle = D_4$$

- Si $b^2 = a^2$, vamos a probar la misma igualdad: $ba = a^3 b$. Para ello, como $H \lhd G$, tenemos que $bab^{-1} \in H$, pero como:

  $$O(bab^{-1}) = O(a) = 4$$

  Por lo que $bab^{-1} \in \{a, a^3\}$. Si $bab^{-1} = a$, entonces es abeliano, por lo que también tenemos $bab = a^3$. En este caso:

  $$G = \langle a, b \mid a^4 = 1, a^2 = b^2, ba = a^3 b \rangle = Q_2$$

De esta forma, los únicos grupos no abelianos de orden 8 son:

$$D_4 \qquad Q_2$$

# 11. Tema10

Prueba que todo grupo de orden 12 es un producto semidirecto y clasifica, salvo isomorfismo, todos los grupos de orden 12 identificándolos con productos semidirectos.

## 11.1. Grupos de orden 12

Sea $G$ un grupo de orden $|G| = 12 = 2^2 \cdot 3$.

Sabemos que grupos abelianos de orden 12 tenemos:

$$C_2 \times C_2 \times C_3 \cong C_2 \times C_6 \qquad C_4 \times C_3 \cong C_{12}$$

Supuesto que $G$ no es abeliano:

$$\left.\begin{array}{r} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Longrightarrow n_2 \in \{1,3\}$$

$$\left.\begin{array}{r} n_3 \mid 4 \\ n_3 \equiv 1 \mod 4 \end{array}\right\} \Longrightarrow n_3 \in \{1,4\}$$

- Supongamos que $n_4 = 3$ y $n_3 = 4$, entonces tendremos:

  $$\begin{array}{ll} P_1, P_2, P_3, P_4 \in Syl_3(G) & |P_i| = 3 \\ Q_1, Q_2, Q_3 \in Syl_2(G) & |Q_i| = 4 \end{array}$$

  Por lo que sacamos 8 elementos distintos de orden 3 y 9 elementos de orden 2 o 4, con lo que este caso es imposible.

- Si $n_2 = 1$ o $n_3 = 1$, tendremos en cualquier caso de la existencia de un $p-$subgrupo de Sylow ($p \in \{2,3\}$) $K \lhd G$. Si consideramos su complemento, $H < G$, tendremos que:
  $$G \cong K \rtimes_\theta H$$

  Si suponemos que $K \in Syl_3(G)$ y $H \in Syl_2(G)$ (en otro caso es análogo), tendremos entonces que $K \cong C_3$ y $|H| = 4$, por lo que $H \cong C_4$ o $H \cong C_2 \times C_2$

- Si $n_2 = 1 = n_3$, entonces tenemos dos subgrupos normales, con lo que:

  $$G \cong C_2 \times C_6 \quad \text{o} \quad G \cong C_{12}$$

  El primer caso si $H = C_2 \times C_2$ y el segundo si $H = C_4$, por lo que volvemos al caso abeliano.

- Si $n_3 = 1$ y $n_2 = 3$, tenemos entonces que:

  $$G \cong K \rtimes H \cong \left\{ \begin{array}{l} C_3 \rtimes C_4 \\ C_3 \rtimes C_2 \times C_2 \end{array}\right.$$

Y vendrá por una acción:

$$\theta : C_4 \to Aut(C_3)$$
$$\theta : C_2 \times C_2 \to Aut(C_3)$$

Alguno de ellos. sin embargo, como $Aut(C_3) \cong C_2 = \{1, x^{-1}\}$

- En $C_3 \rtimes C_4$ para la acción ${}^x y = x^{-1}$, tenemos que:

$$C_3 \rtimes C_4 = \langle x, y \mid x^3 = 1, y^4 = 1, yxy^{-1} = x^{-1} \rangle$$

- En $C_3 \rtimes (C_2 \times C_2)$, los automorfismos de la forma:

$$C_2 \times C_2 \to Aut(C_3)$$

Solo tenemos uno no trivial, que es ($y, x$ son los generadores):

$$\theta : C_2 \times C_2 \to Aut(C_3)$$
$$y \longmapsto \alpha$$
$$x \longmapsto 1$$

Tendremos que:

$$C_3 \rtimes_\theta (C_2 \times C_2) = \langle x, y, z \mid x^3 = 1, y^2 = z^2 = 1, yxy^{-1} = x^{-1}, zxz^{-1} = x, yzy^{-1} = zy \rangle$$

Que es isomorfo a $D_6 \cong D_3 \times C_2$, tomando $r = xy$ y $s = yz$

- En el caso $n_3 = 4$ y $n_2 = 1$, hay un ejercicio en la relación de $p-$grupos que decía que si un grupo de orden 12 tiene más de $3-$subgrupos de Sylow, entonces $G \cong A_4$. Para ello:

$$\phi : G \to Perm(Syl_3(G)) \cong S_4$$
$$G/\ker(\phi) \cong G \cong Im(\phi) \subseteq S_4$$

Por lo que $G < S_4$ con $|G| = 12$, luego ha de ser $G \cong A_4$. Tendremos ahora:

$$G \cong H \rtimes K \cong \begin{cases} C_4 \rtimes C_3 \\ (C_2 \times C_2) \rtimes C_3 \end{cases}$$

  - Si $C_4 \rtimes C_3$, tendremos que la única acción no trivial es:

$$\begin{array}{rcl} \theta \colon C_3 & \longrightarrow & \mathrm{Aut}(C_4) \cong C_2 \\ y & \longmapsto & y^{-1} \end{array}$$

Con orden 2. Sin embargo, como su orden ha de dividir a $|C_3| = 3$, el morfismo no divide a 3, luego no hay nada no trivial ahí: todos los automorfismos son triviales. En dicho caso, tenemos:

$$C_4 \rtimes C_3 = C_4 \times C_3 = C_{12}$$

- En el caso $(C_2 \times C_2) \rtimes C_3$, buscamos una acción $C_3 \to Aut(C_2 \times C_2) \cong S_3$, por lo que tendremos dos automorfismos no triviales de $C_2 \times C_2$ de orden 3.

$$\theta_1 : x \longmapsto \alpha$$

$$\alpha \begin{cases} y \longmapsto z \\ z \longmapsto yz \end{cases}$$

$$\theta_2 : x \longmapsto \alpha^2$$

$$\alpha^2 \begin{cases} y \longmapsto yz \\ z \longmapsto y \end{cases}$$

Que podemos pensarlo con:

$$(1,0),(0,1) \longmapsto (0,1),(1,1)$$

Por lo que:

$$\begin{aligned} &(C_2 \times C_2) \rtimes_{\theta_1} C_3 \\ &= \langle x, y, z \mid x^3 = 1, y^2 = z^2 = 1, xyx^{-1} = z, xzx^{-1} = zy, yz = zy \rangle \cong A_4 \end{aligned}$$

Este último isomorfismo no sale fácil. Ver que un grupo es $A_4$ suele verse siempre viendo que tiene más de un $3-$subgrupo de Sylow.