Álgebra Moderna

Tomás Ricardo Basile Álvarez
316617194

14 de enero de 2021

Operación Binaria: Una operación binaria $*$ en G es una función $* : G \times G \to G$.
Es **Asociativa** si $a * (b * c) = (a * b) * c$
Es **Conmutativa** si $a * b = b * a$.
Es **Cerrada** en $H \subset G$ si para todo $a, b \in H$ se tiene que $a * b \in H$.

Definición 0.1. Un **Grupo** es un par ordenado $(G, *)$ con $*$ una operación binaria (cerrada) que cumple:

1. Es asociativa
2. Existe un **neutro**: un elemento $e \in G$ tal que $a * e = e * a = a \ \ \forall a \in G$
3. Todo elemento tiene un **inverso**: Para todo $a \in G$ existe un $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1}a = G$

Abeliano: El grupo es abeliano si la operación es conmutativa.

Ejemplo 0.1. Lo **Enteros Modulo n** $\mathbb{Z}_n$.
Se define una relación en $\mathbb{Z}$ como:

$$a \equiv b \text{ sii } n|(a-b)$$

que es una relación de equivalencia en $\mathbb{Z}$.

Para cada $a \in \mathbb{Z}$ denotamos por $\overline{a}$ a la clase de equivalencia de a módulo n (todos los números con el mismo residuo que a al dividir entre n) y se observa que:

$$\overline{a} = \{a + kn \ : \ k \in \mathbb{Z}\}$$

Se puede probar que existen exactamente n clases de equivalencia módulo n **Enteros Módulo n:** Se denota como $\mathbb{Z}_n$ o como $\mathbb{Z}/n\mathbb{Z}$ y es el conjunto de todas las clases de equivalencia módulo n (es decir, el conjunto $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$ donde se define la suma y el producto como:

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Se puede probar que $(\mathbb{Z}_n, +)$ es un grupo siempre y cuando $(\mathbb{Z}_n, \cdot)$ es un grupo solamente para n primo.

0.1. Propiedades Básicas

Definición de Grupo: Un grupo es un par ordenado $(G, *)$ donde G es un conjunto y $*$ es una operación binaria que cumple:

- $a1)*$ es asociativa.
- $a2)$ Existe un objeto neutro $e \in G$ tal que $a * e = e * a = a$
- $a3)$ Todo elemento tiene un inverso. Para todo $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1}a = e$

Decimos que es abeliano se $*$ conmuta.

Un ejemplo son las matrices de dimensión $n \times n$ invertibles (con determinante distinto de 0). Se denota como $GL_n(\mathbb{R})$ que es un conjunto no abeliano.

Propiedades Básicas:

- $a)$ El elemento Neutro es único.
- $b)$ Para cada $a \in G$, el inverso a^{-1} es único.
- $c)$ $(a^{-1})^{-1} = a \quad \forall a \in G$
- $d)$ $(a * b)^{-1} = b^{-1} * a^{-1}$
- $e)$ Para cualesquiera $a_1, a_2, ..., a_n \in G$, el valor de $a_1 a_2 \cdots a_n$ es independiente del orden de los paréntesis.

Definición de la notación:

- Sea $a \in G$, definimos a^n de la siguiente manera:
  - $a^0 := e$
  - $a^1 := a$
  - $a^n := a \cdot (a^{n-1})$ para todo $n \in \mathbb{N}$ mayor que 1.
  - $a^{-n} := (a^n)^{-1}$ para todo $n \geq 0$
- $a \cdot b$ se expresará sencillamente como ab.

- A menos que se denote como + en algunos casos y en este caso definimos productos en vez de potencias.
  - $0a := e$
  - $1a := a$
  - $na := a \cdot ((n-1)a)$ para todo $n \in \mathbb{N}$ mayor que 1.
  - $(-n)a := -(na)$ para todo $n \geq 0$

.

Sea G un grupo y $a, b \in G$. Entonces, se cumplen los siguientes enunciados:

- (a) Existe un único $x \in G$ tal que $ax = b$
- (b) Existe un único $y \in G$ tal que $ya = b$
- (c) Si $au = bu$ para algún $u \in G$, entonces $a = b$
- (d) si $va = vb$ para algún $v \in G$, entonces $a = b$

0.2. Grupos Diédricos:

Sea $n \in \mathbb{N}$ mayor o igual a 3. Denotamos como D_{2n} al conjunto de simetrías del $n-$gono regular. Recordemos que una simetría es una transformación rígida del $n-$gono en sí mismo.

En general, para cualquier $n \geq 3$, existen existen exactamente $2n$ simetrías para un $n-$gono. Para demostrarlo, notamos que:
Por cada vértice i existen dos simetrías que mandan el vértice 0 al vértice i: una rotación y una reflexión. Si es una rotación, entonces manda 1 al vértice $i+1$ y si es una reflexión, lo manda al vértice $i-1$. Una vez que sabemos a dónde manda al 0 y al 1, por la rigidez de la transformación, ya sabremos a dónde manda a todos los demás puntos. Existen exactamente n reflexiones y n rotaciones.

Propiedades: Sea $n \geq 3$. Dibujamos un n-gono centrado en el origen y numeramos los vértices del 0 al $n-1$ en sentido antihorario de tal forma que el vértice 0 se encuentra en el eje x. Denotamos por r a una rotación en $2\pi/n$ y como s una reflexión sobre la línea de simetría x. Entonces se cumple:

(a) $1, r, r^2, ..., r^{n-1}$ son rotaciones distintas dos a dos y $r^n = 1$, donde 1 es la simetría identidad.

(b) $s^2 = 1$.

(c) sr^k es la reflexión sobre la línea de simetría l' que resulta de rotar un ángulo de $\pi(n-k)/n$ al eje x.

(d) $r^k s$ es la reflexión sobre la línea de simetría l' que resulta de rotar un ángulo de $\pi k/n$ al eje x.

(e) $sr^k = r^{n-k}s$.

(f) $s \neq r^k$ para todo $k \in \mathbb{Z}$.

(g) Si i, j son dos enteros tales que $0 \leq i < j \leq n-1$ entonces $sr^i \neq sr^j$.

(h) $D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}$

Corolario: D_{2n} es un grupo bajo la composición de simetrías.

Genera: Decimos que $S \subset G$ genera a G si todo elemento de G se ve como un producto de potencias de elementos de S.
En este caso, se puede ver que $D_{2n} = \langle r, s \rangle$

Notamos que los enunciados a, b, e nos dan toda la información sobre el grupo D_{2n}. En efecto, se nota que:

$$r^n = 1, s^2 = 1, rs = sr^{-1}$$

Cuando sucede que tenemos un grupo de generadores S de un grupo G tal que conocemos ciertas igualdades $P_1, P_2, ..., P_s$ que nos dan toda la información del grupo, decimos que estas relaciones son las relaciones generadoras y escribimos:

$$G = \langle S | P_1, ..., P_s \rangle$$

En el caso del grupo dihédrico, tenemos que:

$$D_{2n} = \langle s, r \ \ | s^2 = 1, r^n = 1, sr^{-1} = rs \rangle$$

0.3. Grupos y Morfismos

Sea X un conjunto no vacío. Una permutación es una función biyectiva $X \to X$. Este es un grupo con la operación de composición y se denotra por S_X.

Definición:

a) Denotamos como S_X al conjunto de todas las permutaciones de X

b) Sea $X = \{1, ..., n\}$. En este caso se denota $X := I_n$, $S_n := S_X$ y diremos que S_n es el grupo simétrico de grado n

Observación: $|S_n| = n!$.

Definición: Sea $n \geq 2, \alpha \in S_n, s \in I_n$.

a) α deja fijo a s Si $\alpha(s) = s$

b) α mueve a s si $\alpha(s) \neq s$

Ciclo: Un ciclo es una función que permuta de manera cíclica a una sucesión finita de enteros $\{a_1, a_2, ...a_k\} \subset \{1, ..., n\}$. Es decir, una función $f : \{1, .., n\} \to \{1, ..., n\}$ tal que:

$$a_i \to a_{i+1} \quad \forall i \in \{1, ..., k-1\}$$

y que deja fijos a los demás elementos. El ciclo se denota por $(a_1 a_2 \cdots a_k)$ y se llama k-ciclo o ciclo de orden k.

Ejemplo:

a) $(123) \in S_3$ es la función que manda el 1 al 2, el 2 al 3 y el 3 al 1.

b) $(12) \in S_3$ es la función que manda el 1 al 2, el 2 al 1 y deja el 3 fijo.

c) $(2) \in S_6$ deja a todos los elementos fijos.

e) S_3 tiene exactamente dos 3-ciclos. A saber, $(123), (132)$

Definición: Sea $\alpha, \beta \in S_n$. Decimos que α, β son **disjuntas** si el conjunto de elementos que mueve α es disjunto al que mueve β.

Proposición: Para $n \geq 2$ se cumple lo siguientes:

a) Sea $\alpha \in S_n$. Si $\alpha(s) \neq s$, entonces $\alpha^k(s) \neq \alpha^{k-1}(s) \quad \forall k \neq 0$.

b) Sean α, β disjuntas, entonces $\alpha\beta = \beta\alpha$

Dem: a) Lo probamos por contradicción. Como α es biyectiva, entonces tiene inversa, calculamos la inversa $k-1$-ésima de ambos lados: $\alpha^k(s) = \alpha^{k-1}(s) \;\Rightarrow\; \alpha(s) = s$!
Esto quiere decir que si α mueve a x, entonces todas las potencias de α mueven a x

b) Sea $x \in I_n$. Si α mueve a x, entonces por (a), α mueve a $\alpha(s)$ y entonces β no mueve a x y tampoco a $\alpha(x)$. Por tanto, $(\alpha \circ \beta)(x) = \alpha(x)$ y $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \alpha(x)$
Si β mueve a x, se prueba similarmente pero al revés.
Si, ni α ni β mueve a x, entonces $\alpha(\beta(x)) = x = \beta(\alpha(x))$.

Simbología: Una permutación se puede denotar por dos renglones uno arriba del otro. En el de arriba se escribe I_n y en el de abajo se escribe a dónde va cada punto de I_n.

órbita: La órbita de $x \in I_n$ bajo α es el conjunto $O_x = \{\alpha^k(x) \quad | k \in \mathbb{N}\}$

Notamos que para los puntos fijos, la órbita de x es $\{x\}$.

Teorema de órbitas: Para $n \geq 2, \alpha \in S_n$, se cumple:

a) Sea $\sim$ la relación definida en I_n como $s \sim s'$ sii $s' = \alpha^k(s)$ para algún $k \in \mathbb{Z}$. Entonces, $\sim$ es una **relación de equivalencia**.

b) Sea $x \in I_n$ y sea O_x su órbita bajo α. Entonces, la familia de conjuntos $\{O_x\}_{x \in I_n}$ es una partición de I_n.

c) $\{O_x\}_{x\in I_n}$ es la partición dada por la relación de equivalencia $\sim$ en I_n.

d) Sean $a_1, ..., a_n \in I_n$ tales que $\{O_{a_i}\}_{i=1}^n$ es una partición de I_n con $O_{a_i} \neq O_{a_j}$. Para cada a_i consideramos el ciclo:

$$\sigma_i = (a_i\ \alpha(a_i)\ \alpha^2(a_i) \cdots \alpha^{k_i}(a_i))$$

Donde k_i es la longitud de la órbita O_{a_i}. Entonces, $\sigma_1, ..., \sigma_m$ es una familia de ciclos disjuntos con $\alpha = \sigma_1 \cdots \sigma_m$

Dem:

a)
- Sea $x \in I_n$, entonces $x = \alpha^0(x)$ y por tanto $x \sim x$.
- Sean $x, y \in I_n$ con $x \sim y$. Entonces existe $k \in \mathbb{Z}$ con $x = \alpha^k(y)$ y por tanto $y = \alpha^{-k}(x)$. Por lo que $y \sim x$.
- Sea $x, y, z \in I_n$ tales que $x \sim y \sim z$. Entonces $x = \alpha^k(y)$, $y = \alpha^l(z)$. Por tanto, $x = \alpha^{k+l}(z)$ y entonces $x \sim z$.

b) Vemos que la familia es una partición:

- $O_x \neq \emptyset$ porque $x \in I_n$ ya que $x = \alpha^0(x)$
- Sea $a \in O_x \cap O_y$. Entonces, $a = \alpha^k(x) = \alpha^l(y)$. Luego, $x = \alpha^{l-k}(y)$, $y = \alpha^{k-l}(x)$. Entonces,

$$\begin{aligned} O_x &= \{z \in I_n \,|z = \alpha^m \alpha^{l-k}(y) \quad \text{para un } m \in \mathbb{Z}\} \\ &= \{z \in I_n \,|y = \alpha^m(x) \text{ para un } m \in \mathbb{Z}\} = O_y \end{aligned}$$

- Finalmente, la familia cubre todo I_n porque para toda x podemos considerar O_x

c) Se sigue de la definición.

d) Para $a_1, ..., a_m$ escogemos un representante de cada clase de equivalencia. Luego, los ciclos $\sigma_1, ..., \sigma_m$ son disjuntos. Finalmente, $\alpha = \sigma_1 \cdots \sigma_m$. Esto porque para $x \in I_n$, por construcción $x \in O_{a_i}$ para un único a_i. Entonces, $\sigma_i(x) = \alpha(x)$ y $\sigma_j(x) = x \ \ \forall j \neq i$. Por lo tanto $\sigma_1 \cdots \sigma_m(x) = \sigma_i(x) = \alpha(x)$ y listo.

0.3.1. Algoritmo Para la Descomposición de Ciclos

Sea $n \geq 3$ y sea $\alpha \in S_n$. Los pasos son:

1. Calculamos la órbita de 1. Paramos hasta que se repita el 1. $O_1 = \{1, \alpha(1), \alpha^2(1), ..., \alpha^{k_1-1}(1)\}$
2. Definimos el ciclo $\sigma_1 := (1\ \alpha(1)\ \alpha(2)\ \cdots\ \alpha^{k_1-1}(1))$
3. Tomamos un elemento que sobre de I_n y calculamos su órbita.

4. Con eso le definimos su ciclo.

5. Seguimos hasta haber tomado todos los ciclos posibles.

Y con eso se encuentra la factorización en ciclos disjuntos.

Composición con la descomposición de ciclos: Si tenemos que $\alpha = (123)(45)$ y que $\beta = (234)(156)$, entonces:

$$\alpha\beta = (123)(45)(234)(156)$$

Sin embargo, esto no está descompuesto en ciclos. Hay que hacer el procedimiento de antes y calcular la órita de cada elemento. Calculando por ejemplo $\alpha\beta(1) = (123)(45)(234)(151)\ \ (1) = (123)(45)(234)\ \ (1) = (123)(45)\ \ (1) = (123)\ \ (1) = 2$

0.4. Grupos Matriciales y Cuaternios

Campo: Un campo es un conjunto K junto con dos operaciones binarias: una suma $+$ y un producto $\cdot$, tales que:
$(K, +)$ es un grupo abeliano.
$(K/\{0\}, \cdot)$ es un grupo abeliano.
$a \cdot (b + c) = a \cdot b + a \cdot c$

General Lineal: Dado un campo K, denotamos por $GL_n(K)$ al conjunto de matrices $n \times n$ con entradas en K y det diferente de 0.
Todas las propiedades del determinante para matrices reales aplican aquí también.

Lema: Sea $(G, \cdot)$ un grupo. Si S es un subconjunto no vacío de elementos con:

$$s_1 \cdot s_2 \in S \ \ \forall s_1, s_2 \in S \text{ y}$$
$$s^{-1} \in S \ \forall s \in S$$

Entonces S es un grupo.

Grupo de los Cuaternios:
Es el grupo formado por:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Cumplen las siguientes operaciones:

$$I^2 = J^2 = K^2 - E$$
$$IJ = K, JK = I, KI = J$$
$$KI = -K, KJ = -I, IK = -J$$

0.5. Morfismos

Tabla de Cayley: Sea G un grupo. Una tabla de Cayley de G es una tabla de multiplicar del grupo G en la que se ponene todos los productos.
Proposición: En cada columna y cada rengón de una tabla de Cayley de G no existen elementos repetidos.

Si dos conjuntos tienen la misma tabla, podemos pensar que en realidad son el mismo conjunto pero con diferentes nombres. Se puede ver por ejemplo que la tabla de S_3 es igual a la de D_6.

Definición (Morfismo): Sean $(G, \star)$ y $(H, \Diamond)$ dos grupos. Una función $\phi : G \to H$ tal que:

$$\phi(x \star y) = \phi(x) \Diamond \phi(y) \quad \forall x, y \in G$$

Esta función recibe el nombre de Morfismos.

Lema: Sean $(G, \star), (H, \Diamond)$ grupos y sea $\phi : G \to H$ un morfismo que además es biyectivo. Entonces, la función inversa $\phi^{-1} : H \to G$ es un morfismo de grupos.

Isomorfismo: Un morfismo que es biyectivo recibe el nombre de isomorfismo. Si $\phi : G \to H$ sea un isomorfismo, entonces denotamos que $G \cong H$ y G, H son isomorfos.
Si dos grupos son isomorfos, básicamente son el mismo grupo pero con distintos nombres.

Ejemplo:

- $f : \mathbb{Z} \to \mathbb{Z}_n$ definido por $f(a) = \overline{a}$ es un morfismo ya que:

$$f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b)$$

- La función $g : \mathbb{Z}_2 \to \mathbb{Z}_4$ es un morfismo (cosa que se puede probar alv)
- Para todo grupo G, la identidad $I : G \to G$ es un isomorfismo.
- La función exp: $(\mathbb{R}, +) \to (R^+, \cdot)$ es un isomorfismo de grupos, con inversa ln

Proposición: Sean $f : (G, \star) \to (H, \Diamond)$ y $g : (H, \Diamond) \to (K, *)$. Entonces, gf es un morfismo.

Teorema: Sea $\phi : (G, \star) \to (H, \Diamond)$ un morfismo. Entonces, se cumple:

- $f(e) = e'$ donde e, e' son los neutros de G, H
- Si $a \in G$, entonces $f(a^{-1}) = f(a)^{-1}$
- Si $a \in G, n \in \mathbb{Z}$, entonces $f(a^n) = f(a)^n$

1. Teoremas de Isomorfismos

1.1. Subgrupos

$H \subset G$ es un subgrupo de G si H es un grupo en sí mismo con la operación heredada de G.

Proposición: $H \subset G$ es un grupo si satisface:

- $xy \in H \ \ \forall x, y \in H$
- $\forall x \in H \ , \ x^{-1} \in H$

Todo grupo G tiene a los subgrupos $\{e\}, G$. Si tiene un subgrupo diferente a estos, decimos que es un subgrupo no trivial.

Proposición (Criterio para subgrupos): Se $H \subset G$ con G un grupo, entonces se cumplen los siguientes enunciados:

- H es un subgrupo de G sii $H \neq \emptyset$ y $xy^{-1} \in H \ \ \forall x, y \in H$
- En caso de ser H finito, H es subgrupo de G sii $xy \in H \ \ \forall x, y \in H$

Ejemplos:

a) Sea $f : G \to H$ un morfismo de grupos

a1) $G_1 = \{a \in G \,|f(a) = e_H\}$ es un subgrupo de G
Se llama **Núcleo de** f

a2) $H_1 = \{h \in H | h = f(a)$ para una $a \in G\}$ es un subgrupo de H.
Recibe el nombre de **Imagen de** f

Teorema: Sea G un grupo, entonces la intersección de cualquier familia de subgrupos de G es un subgrupo de G.

Def.: Sea G un grupo y $a \in G$. El **Subgrupo cíclico generado por** a denotado por $\langle a \rangle$, es el conjunto de potencias de a, el conjunto $\langle a \rangle = \{a^k \,|k \in \mathbb{Z}|\}$.
Claramente este conjunto es un subgrupo de G.
Decimos que G es cíclico si $G = \langle a \rangle$ para alguna $a \in G$

Def. (Orden): Sea G un grupo y $a \in G$.

a) El **orden de** G es el cardinal $|G|$

b) El **orden de** a es el cardinal $|\langle a \rangle|$

Def. Subgrupo Generado por un conjunto: Sea $S \subset G$ un conjunto no vacío. El subgrupo generado por S es el grupo:

$$\langle S \rangle := \bigcap_{K \in F} K \quad \text{, donde } F := \{H \leq G \,|S \subset H\}$$

Corolario: Si $S \subset G$ es un conjunto, entonces $\langle S \rangle$ es el subgrupo más chico que contiene a S.

Sea $X \subset G$ finito. Si $X = \{a_1, ..., a_n\}$, denotamos:

$$\langle a_1, ..., a_n \rangle := \langle X \rangle$$

Def. (palabra): Sea $X \subset G$ no vacío. Una palabra en X es un elemento $w \in G$ de la forma:

$$w = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$$

Donde $x_i \in X, \alpha_i = \pm 1$ y k es la longitud de la palabra. (los x_i se pueden repetir las veces que sea).

Teorema: Sea $X \subset G$. Entonces:

a) Si $X = \emptyset$, entonces $\langle X \rangle = \{e\}$

b) Si $X \neq 0$, entonces $\langle X \rangle$ es el conjunto de todas las palabras de X.

Ejemplo 8.17:
Encuentra todos los subgrupos de $(\mathbb{Z}, +)$:
Para cada $m \in \mathbb{Z}$, tenemos el grupo $\langle m \rangle = \{n \cdot m | n \in \mathbb{Z}\}$. Afirmamos que estos son todos los subgrupos que hay. Sea H un subgrupo de $\mathbb{Z}$. Por el principio del buen orden, existe el menor entero positivo $m \in H$. Claramente $\langle m \rangle \subset H$. Veamos que dado $p \in H$, existen $q \in \mathbb{Z}, 0 \leq r < m$ tales que $p = qm + r$. Observa que $r = p - qm \in /H$. Lo que implica que $r = 0$ debido a que $0 \leq r < m$ y m es el menot entero positivo en H. Por tanto, todos los elementos son de la forma $p = qm \in \langle m \rangle$. Entonces $H = \langle H \rangle$.

1.2. Teorema de Lagrange

Se observa que todos los subgrupos de grupos que hemos analizado tienen una cantidad de elementos que dividen a la cantidad de elementos del grupo.

Coset Izquierdo: Dado $H \leq G$, le definimos el coset izquierdo dado por x con

$$xH = \{xh | h \in H\}$$

Este coset no es un grupo ni nada (solamente si $x \in H$), es un conjunto.

Proposición: Sean G un grupo y $H \leq G$. Entonces e cumple:

a) Sea $\sim_H$ la relación definida en G como $a \sim_H b$ sii $a = bh$ para alguna $h \in H$. Entonces, $\sim_H$ es una relación de equivalencia.

b) Sean $x \in G$ y sea $xH = \{xh | h \in H\}$. Entonces, la familia de conjuntos $\{xH\}_{x \in G}$ es una partición disjunta de G.

c) $\{xH\}_{x \in G}$ es la partición dada por $\sim_H$ en G.

Dem:

a) Veamos que $\sim_H$ es de equivalencia.

- Sea $x \in G$. Entonces $x = xe$. Por tanto $x \sim_H x$ porque $e \in H$.
- Sean $x, y \in G$ tales que $x \sim_H y$. Entonces, existe una $h \in H$ tal que $x = yh$. Luego, $y = xh^{-1}$ con $h^{-1} \in H$, por lo que $y \sim_H$.
- Sea $x, y, z \in G$ tales que $x \sim_H y \sim_H z$. Entonces, existen $h, h' \in H$ tales que $x = yh$, $y = zh'$. Por tanto, $x = zh'h$ con $hh' \in H$. Por lo que $x \sim_H z$

b) Verificamos que es una familia.
$xH \neq \emptyset$ para todo $x \in G$ ya que $x = xe \in xH$.
Digamos que se intersectan xH y yH. Entonces, supongamos que $a \in xH \cap yH$. Por definición, existen $h, h; \in H$ tales que $a = xh = yh'$. Luego, tenemos que $x = yh'h^{-1}$ y $y = xhh'^{-1}$. Entonces, $xH \subset yH \subset xH$ y por tanto $xH = yH$.
Luego, estos conjuntos juntos forman todo G porque todo x está en algún xH.

c) Por la def.

Nota: Los incisos a) y b) son equivalentes, porque sabemos que la relación de equivalencia impone una partición.

Lema: Sea G un grupo y sea $H \leq G$ y $x \in G$. Entonces $|xH| = |H|$.

Dem: La funión $\alpha(h) = xh$ es biyectiva.

Corolario: Teorema de Lagrange: Si G es un grupo finito y $H \leq G$. Entonces $|H|$ divide a $|G|$.

Dem: Podemos partir G en grupos de equivalencia de H. Por el lema, todos estos conjuntos tienen la misma cantidad de elementos $|H|$.

Corolario: Sean $G, a \in G$. Entonces el orden de a divide a $|G|$.

Corolario: Si G es un grupo con $|G|$ = primo. Entonces G es un grupo cíclico y todo elemento no neutro de G es de orden p.

Teorema de Fermat: Si p es un enetro primo positivo, entonces $\overline{a}^p = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_p$.

Dem: $\mathbb{Z}_p - \{0\}$ es un grupo de $p-1$ elementos bajo el producto. Luego, todo $\overline{a} \in \mathbb{Z}_p$ tiene un orden que divide a $p-1$. Por tanto, $\overline{a}^{p-1} = \overline{1}$

1.2.1. Parte 2

Empezamos con un ejemplo de $D_{2(4)}$

mos que todos los subgrupos propios no nulos de $D_{2(4)}$ son

$$\begin{aligned} \langle r \rangle &= \{1, r, r^2, r^3\} = \langle r^3 \rangle, & \langle sr \rangle &= \{1, sr\}, \\ \langle r^2 \rangle &= \{1, r^2\}, & \langle sr^2 \rangle &= \{1, sr^2\}, \\ \langle r^2, s \rangle &= \{1, r^2, s, sr^2\} = \langle r^2, sr^2 \rangle = \langle sr^2, s \rangle, & \langle s \rangle &= \{1, s\}, \\ \langle r^2, sr^3 \rangle &= \{1, r^2, sr^3, sr\} = \langle r^2, sr \rangle = \langle sr, sr^3 \rangle, & \langle sr^3 \rangle &= \{1, sr^3\}. \end{aligned}$$

Notemos que tenemos las particiones $D_{2(4)} = \langle r^2 \rangle \cup \langle r^2 \rangle s \cup \langle r^2 \rangle r \cup \langle r^2 \rangle sr$, $D_{2(4)} = \langle r \rangle \cup \langle r \rangle s$ y $D_{2(4)} = \langle r^2, s \rangle \cup \langle r^2, s \rangle r$, y además que

$$\begin{aligned} \langle r \rangle s &= \langle r \rangle sr^3 = \langle r \rangle sr^2 = \langle r \rangle sr \\ \langle r^2 \rangle s &= \langle r^2 \rangle sr^2 \\ \langle r^2, s \rangle r &= \langle r^2, s \rangle r^3 = \langle r^2, s \rangle sr = \langle r^2, s \rangle sr^3. \end{aligned}$$

En particular vale la pena observar que

$$s \langle r^2, s \rangle = \{s, sr^2, 1, r^2\} = \langle r^2, s \rangle s,$$

pero que

$$s \langle 1, sr \rangle = \{s, r\} \neq \{s, r^3\} = \langle 1, sr \rangle s$$

Con lo que observamos que xH no siempre es igual a Hx. Pero que en cualquier caso se forman particiones de G en conjuntos de misma cardinalidad.
La cantidad de cosets izquierdos es igual a la de cosets derechos pero no son necesariamente iguales estos conjuntos.

Definición: Sea G un grupo, $H \leq G$ y $x \in G$. Definimos:

a) El conjunto xH se llama clase lateral izquierda de H asociada a x.

b) El conjunto Hx es la clase lateral derecha de H asociada a x.

Hemos probado ya que la cantidad de grupos izquierdos es igual a la de grupos derechos (pero lo probamos para grupos finitos).

Para un caso más general, definimos una función $\phi : D \to I$ (con D los cosets derechos e I los izquierdos).
Definimos que $\phi(Hx) = x^{-1}H$.

- **Bien definida:** Hay que probar que si $Hx = Hy \Rightarrow \phi(Hx) = \phi(Hy)$. Para ello vemos que como $x \in Hx = Hy$, tenemos que $x = h'y$. Entonces:
  $a \in x^{-1}H \Leftrightarrow a = x^{-1}h$ p.a $h \in H \Leftrightarrow a = y^{-1}h'^{-1} \Leftrightarrow a \in y^{-1}H$ Por tanto, $\phi(Hx) = x^{-1}H = y^{-1}H = \phi(Hy)$
- **Biyectiva:** Vemos que si $\phi(Hx) = \phi(Hy)$, entonces $x^{-1}H = y^{-1}H$. Por lo que $x^{-1} = y^{-1}h$.
  Entonces, $e = xx^{-1} = y^{-1}hx \Rightarrow y = yx^{-1}x = yy^{-1}hx = hx$.
  Por lo tanto $y \in Hx$ y así, $Hy = Hx$. Con lo que probamos que es inyectiva.
  Vemos que es supra pues $zH = \phi(Hz^{-1})$.

Def. Sea G un grupo y sea $H \leq G$. EL índice de H en G, denotado por $[G : H]$ es la cantidad de clases laterales.

Teorema de Lagrange: Sea G un grupo finito y $H \leq G$. Entonces $[G : H] = |G|/|H|$.

Es válido el recíproco?? Es decir, dado un grupo finito G, para todo divisor d de $|G|$ existe un grupo de d elementos?
NO.

Teorema: Sea p un primo mayor que 2 y sea G un grupo de orden $2p$. Entonces $G \sim \mathbb{Z}_{2p}$ o $G \sim D_{2(p)}$

Dem: Digamos que G no es isomorfo a $\mathbb{Z}_{2p}$, entonces no existen elementos de orden $2p$. Por lo que el orden de los elementos de G puede ser $1, 2, p$.

Vemos que existe un $x \in G$ de orden p. En efecto, si suponemos lo contrario, todos los elementos de G serían de orden 2. Pero esto implica que G es abeliano y podemos construir el grupo $\{e, a, b, ab\}$ que contradice el teorema de Lagrange. Por lo tanto, existe al menos un elemento de orden p.

Sea $a \in G$ de orden p. Denotamos por $H = \langle a \rangle = \{e, a, a^2, ..., a^{p-1}\}$.

Vemos que si $x \in G$ y $x \notin H$, entonces $x^2 = e$. Notamos que $[G : H] = 2$ por lagrange. Entonces, tenemos la partición $G = H \cup xH$. Supongamos que $x \in G - H$ tiene orden p. Entonces, por una tarea, tenemos que $x^2 \in H$. Por loo tanto:

$$x = xx^p = x^{p+1} = x^{2(\frac{p+1}{2})} \in H$$

Lo cual contradice que $x \in G - H$. Por lo que todo $x \in G - H$ es de orden 2.
Escogemos $b \in G - H$. Como tenemos la partición $G = H \cup bH$, podemos concluir que:

$$G = \{e, a, a^2, ..., a^{p-1}, ba, ba^2, ..., ba^{p-1}\}$$

Notamos también que $ba \notin H$ por lo que $(ba)^2 = e$. De modo que $(ba) = (ba)^{-1} = a^{-1}b^{-1} = a^{-1}b$. Con lo que hemos probado que:

$$G = \langle a, b | a^p = e = b^2, ba = a^{-1}b \rangle$$

Con esto y algunos resultados de las tareas, tenemos todos los grupos de orden primo (son isomorfos a $\mathbb{Z}_p$), de orden $2p$ (son isomorfos a $\mathbb{Z}_p$ o a $D_{2(p)}$

1.3. Retícula de Subgrupos (Cíclicos)

Digamos que tenemos una familia $\{H_i\}_{i\in I}$ de subgrupos de G. Entonces, le podemos definir un **Ínfimo** dado por $\bigcap_{i\in I} H_i$ (el subgrupo más grande contenido en todas las H) y un supremo $\langle \bigcup_{i\in I} H_i \rangle$ (el grupo más chico que contiene a todas las H).
A una familia con ínfimo y supremo se le conoce como una retícula.

Rícula de un Cíclico

Propiedades: Sea $H = \langle x \rangle$ y $n \in \mathbb{N}$. Entonces:

a) $|x| = n$ sii, n es el menor natural positivo tal que $x^n = e$ y en tal caso, $\langle x \rangle \{e, x, x^2, ..., x^{n-1}\}$

b) Si $|x| = n$, entonces $(H, \cdot) \simeq (\mathbb{Z}_n, +)$. En particular:

b1) $x^a = e$ sii $\overline{a} = \overline{0}$ en $\mathbb{Z}_n$

b2) $x^a = x^b$ sii $\overline{a} = \overline{b}$ en $\mathbb{Z}_n$

c) $|x| = \infty$ sii $x^n \neq e$ para todo $k \neq 0$

d) Si $|x| = \infty$, entonces $(H, \cdot) \simeq (\mathbb{Z}, +)$. En particular:

d1) $x^a = e$ sii $a = 0$

d2) $x^a = x^b$ sii $a = b$

Proposición: Sea G un grupo, $x \in G$, $m, n \in \mathbb{Z}$ y $d = (m, n)$.

a) Si $x^n = x^m = e$, entonces $x^d = e$

b) $x^m = e$ sii $|x|$ divide a m

Dem: a) Sabemos que $d = \lambda m + \mu n$ y es la mínima combinación de este tipo. Luego, $x^d = x^{\lambda m + \mu n} = (x^m)^\lambda (x^n)^\mu = e$
b) Suponemos que $x^m = e$. Sabemos que $s = |x|$ es el mínimo entero tal que $x^s = e$. Entonces, por (a) tenemos que $x^d = e$ con $d = (|x|, m)$. Pero por la minimalidad de $|x|$ se sigue que $d = |x|$ y por tanto, $|x|$ divide a m.

Sea G un grupo cíclico, $x \in G$, $a \in \mathbb{Z} - \{0\}$. Se cumplen los siguientes enunciados:

a) Si $|x| = \infty$, entonces $|x^a| = \infty$

b) Si $|x| = n < \infty$, entonces $|x^a| = \dfrac{n}{(n, a)}$

c) Si $|x| = st < \infty$, entonces $|x|^s = t$

Dem: a) Por contradicción. Si $|x^a| = m$, entonces $x^{am} = e$, pero entonces $|x| < \infty$

b) Sean $d = (n, a)$ y $k = \frac{n}{d}$. Notamos que $x^d, x^{2d}, x^{3d}, ..., x^{kd} = e$ son todos distintos debido a que $|x| = n$. Por tanto, tenemos que $|x| = n$. Así que $|x^d| = k$. Veamos que $\langle x^a \rangle = \langle x^d \rangle$. Como $d|a$, se sigue que $x^a \in \langle x^d \rangle$. Pero como $d = (a, n)$, sabemos que $d = \lambda a + \mu n$. De modo que:
$x^d = x^{\lambda a + \mu n} = x^{\lambda a} x^{\mu n} = x^{\lambda a} \in \langle x^a \rangle$
Por tanto, $\langle x^d \rangle = \langle x^a \rangle$. Y entonces $|x^a| = |x^d| = k = \dfrac{n}{(a, n)}$

c) Se sigue de b

Corolario: Sea $H = \langle x \rangle$. Se cumple lo siguiente:

a) Sea $|x| = \infty$. Entonces $H = \langle x^a \rangle$ sii $a = \pm 1$

b) Sea $|x| = n < \infty$. Entonces, $H = \langle x^a \rangle$ sii $(a, n) = 1$

c) Todo subgrupo de H es cíclico

d) Sea $|x| = n < \infty$. Entonces, $\langle x^a \rangle = \langle x^{(a,n)} \rangle$

e) $\langle x^a, x^b) \rangle = \langle x^{(a,b)} \rangle$ y $\langle x^a \rangle \cap \langle x^b \rangle = \langle x^{[a,b]} \rangle$

Dem: a) Se puede ver que $\langle x \rangle = \langle x^{-1} \rangle$. Además, $x \notin \langle x^a \rangle$ para todo $a \neq \pm 1$.

b) Se sigue de la parte b del teorema anterior ($\langle x^a \rangle$ tiene $n/(n, a)$ elementos. Por lo que es igual a todo H (tiene n elementos) sii $(n, a) = 1$

c) Sea $K \leq H$. Por el principiio de buen orden, existe un mínimo k tal que $x^k \in K$. Por el algoritmo de división se puede probar que $K = \langle x^k \rangle$

d) Se probó en la dem de la parte b del teorema pasado.

e)Medio Larga pero obvia (notas clase 11)

Teorema Fundamental de Grupos Cíclicos: Sea $G = \langle x \rangle$ un grupo de orden n. Entonces, para todo d divisor de n existe un único grupo $H \leq G$ de orden d. Más aún, el grupo es $H = \langle x^{n/d} \rangle$.

Dem: Sea d un divisor de $|G|$. Por la proposición anterior b), sabemos que $|x^{n/d}| = \frac{n}{(n, n/d)} = \dfrac{n}{n/d} = d$. Y entonces existe el grupo $\langle x^{n/d} \rangle$ de orden d
Nos queda probar que es único. Es decir, si $H \leq G$ tiene orden d, entonces $H = \langle x^{n/d} \rangle$.

Para ello, se tiene que $H = \langle x^m \rangle$ para algún m (subgrupo de cíclico es cíclico). Además, tenemos que $H = \langle x^{(m,n)} \rangle$ por el corolario d). Pero entonces:

$$d = |H| = |x^{(m,n)}| = \frac{n}{(m,n)}$$

Por tanto, $(m,n) = n/d$. Y así que $H = \langle x^{(m,n)} \rangle = \langle x^{n/d} \rangle$

Def. Diagrama de Hasse: Si se tiene una retícula de subgrupos de G, un diagrama de Hasse consiste en vértices v_H para cada $H \leq G$ y de líneas que indican contención. (El neutro va hasta abajo)
Para construir un diagrama, se siguen los siguientes pasos:

a) Dibujamos $\langle e \rangle$ hasta abajo.

b) Dibujamos más arriba a todos los subgrupos cuyo único subgrupos sea $\langle e \rangle$

c) Seguimos subiendo.

Ejemplo:
Encuentra todos los subgrupos de $\mathbb{Z}_{45}$, da un generador para cada uno y describe las contenciones entre ellos.

Primero vamos a enlistar los subgrupos cíclicos de $\mathbb{Z}_{45}$, es decir, los que están generados por un solo elemento.
Antes de empezar, notamos que podemos parar de escribir el conjunto cuando llegamos a $\overline{0}$, porque a partir de ahí se empiezan a repetir los elementos.
Por esto, notamos que si $m \in \{1, ..., 45\}$, entonces, $\langle \overline{m} \rangle$ serán todos los múltiplos de m y como dijimos antes, la cadena de múltiplos se empezará a repetir cuando lleguemos a $\overline{0}$, es decir, cuando alcancemos un múltiplo de 45.
El primer múltiplo de 45 que alcanzaremos se dará cuando nos encontremos en el mínimo común múltiplo de m y 45 (que denotamos por $[m, 45]$)
Por lo que la cantidad de elementos de $\langle \overline{m} \rangle$ (denotada por $|\langle \overline{m} \rangle|$) es igual a la cantidad de múltiplos de m que hay hasta llegar a $[m, 45]$, es decir, es igual a $\frac{[m,45]}{m}$.
Pero si $(m, 45)$ denota al máximo común divisor de m y 45, sabemos que se tiene la relación : $(m, 45)[m, 45] = 45 \cdot m$, y por lo tanto, $\frac{[m,45]}{m} = \frac{45}{(45,m)}$.
Juntando esto, tenemos que la cantidad de elementos $|\langle \overline{m} \rangle| = \frac{[m,45]}{m} = \frac{45}{(45,m)}$

Por otro lado, probaremos que se cumple que $\langle \overline{m} \rangle = \langle \overline{(45,m)} \rangle$.
Primero vemos que estos dos conjuntos tienen la misma cantidad de elementos, pues $\langle \overline{m} \rangle$ tiene $\frac{45}{(45,m)}$ elementos.

Mientras que $\langle\overline{(45,m)}\rangle$ tiene $\dfrac{45}{(45,(45,m))}$ elementos. Pero como $(45,m)$ divide a 45 por definición, entonces el máximo común divisor entre 45 y $(45,m)$ es $(45,m)$ por lo que $(45,(45,m)) = (45,m)$ y la cantidad de elementos de $\langle\overline{(45,m)}\rangle$ es entonces sencillamente $\dfrac{45}{(45,m)}$.

Ahora, sea $km \in \langle\overline{m}\rangle$ (con $k \in \mathbb{Z}$). Y como $(45,m)$ divide a m, podemos encontrar un entero i tal que $m = (45,m)i$. Por tanto, $km = k(45,m)i$, lo cual es un elemento de $\langle\overline{(45,m)}\rangle$ porque es un múltiplo de $(45,m)$.
Entonces, $\langle\overline{m}\rangle \subset \langle\overline{(45,m)}\rangle$. Y como probamos que tienen la misma cantidad de elementos, estos conjuntos son necesariamente iguales.

Luego, si tenemos un $m \in \{1,2,...,45\}$, ya sabremos que $\langle\overline{m}\rangle = \langle\overline{(45,m)}\rangle$ y nos podemos ahorrar el trabajo de calcular $\langle\overline{m}\rangle$ si es que ya calculamos $\langle\overline{(45,m)}\rangle$

Con esto, notamos en particular que si un elemento m es coprimo con 45, entonces $(45,m) = 1$ y se tiene que $\langle\overline{m}\rangle = \langle\overline{1}\rangle = \mathbb{Z}_{45}$

Usaremos esta proposición para calcular varios generados a la vez. Para esto, agruparemos a los cíclicos en todos los que tienen el mismo MCD con 45.

- $\langle\overline{0}\rangle = \{\overline{0}\}$
- **Los coprimos con 45:** (todos estos generados son iguales a $\mathbb{Z}_{45}$ por lo mencionado antes) $\langle\overline{1}\rangle = \langle\overline{2}\rangle = \langle\overline{4}\rangle = \langle\overline{7}\rangle = \langle\overline{8}\rangle = \langle\overline{11}\rangle = \langle\overline{13}\rangle = \langle\overline{14}\rangle = \langle\overline{16}\rangle = \langle\overline{17}\rangle = \langle\overline{19}\rangle = \langle\overline{23}\rangle = \langle\overline{26}\rangle = \langle\overline{28}\rangle = \langle\overline{29}\rangle = \langle\overline{31}\rangle = \langle\overline{32}\rangle = \langle\overline{34}\rangle = \langle\overline{37}\rangle = \langle\overline{38}\rangle = \langle\overline{41}\rangle = \langle\overline{43}\rangle = \langle\overline{44}\rangle = \mathbb{Z}_{45}$
- m **tal que (m,45) = 3:** cualquiera de estos $\langle\overline{m}\rangle$ son iguales a $\langle\overline{(m,45)}\rangle = \langle\overline{3}\rangle$ por lo mencionado antes, entonces: $\langle\overline{3}\rangle = \langle\overline{6}\rangle = \langle\overline{12}\rangle = \langle\overline{21}\rangle = \langle\overline{24}\rangle = \langle\overline{33}\rangle = \langle\overline{39}\rangle = \langle\overline{42}\rangle$ $= \{\overline{3},\overline{6},\overline{9},\overline{12},...,\overline{45} = \overline{0}\}$
- **m tal que (m,45) = 5:** $\langle\overline{5}\rangle = \langle\overline{10}\rangle = \langle\overline{20}\rangle = \langle\overline{25}\rangle = \langle\overline{35}\rangle = \langle\overline{40}\rangle = \{\overline{5},\overline{10},\overline{15},...,\overline{45} = \overline{0}\}$
- **m tal que (m,45) = 9:** $\langle\overline{9}\rangle = \langle\overline{18}\rangle = \langle\overline{27}\rangle = \langle\overline{36}\rangle$ $= \{\overline{9},\overline{18},\overline{27},...,\overline{35},\overline{45} = \overline{0}\}$
- **m tal que (m,45) = 15:** $\langle\overline{15}\rangle = \langle\overline{30}\rangle$ $= \{\overline{15},\overline{30},\overline{45} = \overline{0}\}$

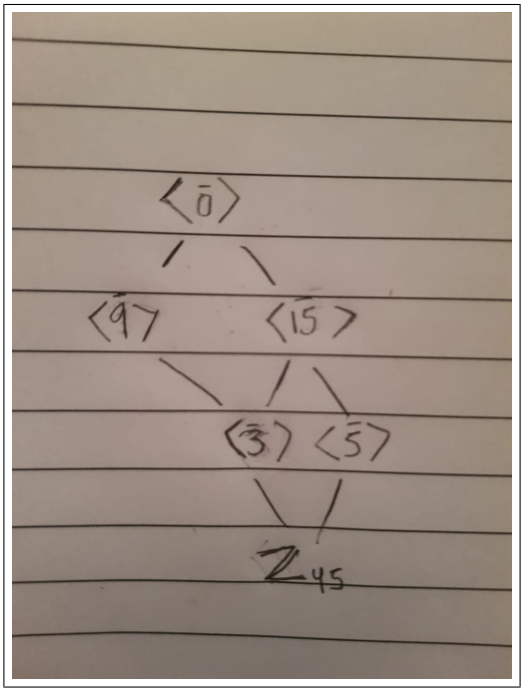
Luego, los únicos subgrupos propios cíclicos de $\mathbb{Z}_{45}$ son $\mathbb{Z}_{45}, \langle\overline{3}\rangle, \langle\overline{5}\rangle, \langle\overline{9}\rangle, \langle\overline{15}\rangle$.

Pero además, resulta que todos los subgrupos de $\mathbb{Z}_{45}$ son cíclicos. Para probar esto, digamos que $H \leq \mathbb{Z}_{45}$ es un subgrupo.

Por el principio del buen orden, hay un entero mínimo $\overline{m} \in H$. Y sea ahora $\overline{p} \in H$. Probaremos que $\overline{p} \in \langle \overline{m} \rangle$.

Por el algoritmo de la división, existe $q \in \mathbb{Z}$ y $0 \leq r < m$ tal que $p = qm + r$. Enotnces, $r = p - qm$, pero como $\overline{m} \in H$, entonces $\overline{qm} \in H$ y por tanto $p - qm \in H$. Lo que implica que $\overline{r}$ es un elemento de H, pero $0 \leq r < m$ y el entero más chiquito en H era m, por lo que se debe de tener que $r = 0$. Por lo tanto, $p = qm \in \langle \overline{m} \rangle$ y así, todos los elementos de H son generados por m y $H = \langle \overline{m} \rangle$.

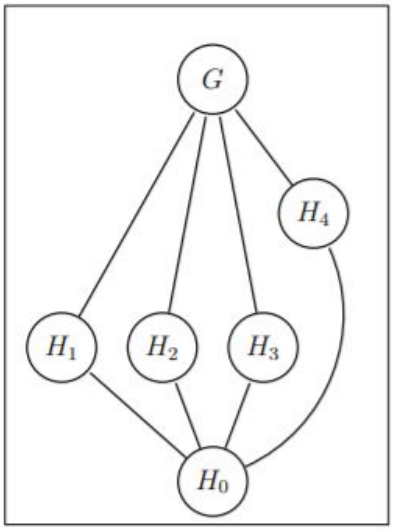
Entonces, los grupos cíclicos que encontramos arriba son en realidad todos los que tiene $\mathbb{Z}_{45}$
Y además, las contenciones que tienen se pueden ver fácilmente y se resumen en el siguiente diagrama (en el que una línea indica que el grupo de arriba está contenido en el de abajo)



1.4. La retícula parte 2

Veremos estrategias para construir el diagrama de Hasse para cualquier grupo finito (no necesariamente cíclico).

(b) Dibuja el diagrama de S_3.



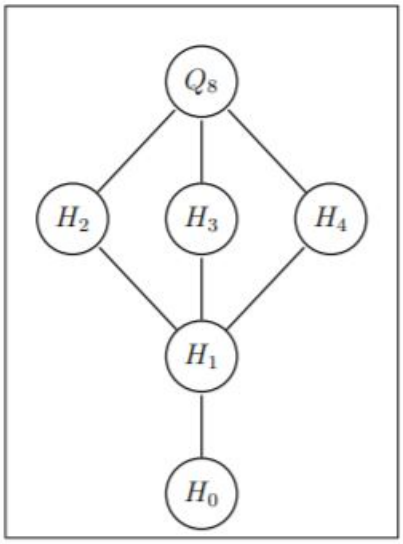
Solución. Por 8.17 ya conocemos todos los subgrupos: S_3, $H_1 := \langle(1\ \ 2)\rangle$, $H_2 := \langle(1\ \ 3)\rangle$, $H_3 := \langle(3\ \ 2)\rangle$, $H_4 := \langle(1\ \ 2\ \ 3)\rangle$ y $H_0 = \{(1)\}$. Notemos que H_1, H_2 y H_3 son subgrupos de orden 2 y H_4 es un subgrupo de orden 3. Así que, por el teorema de Lagrange sabemos que H_1, H_2, H_3 y H_4 no pueden ser subgrupos entre sí. Con esta información ya nos damos una idea de la forma del diagrama. Finalmente, para no perder la intuición de que

$$|H_4| > |H_1| = |H_2| = |H_3|,$$

dibujamos a H_3 ligeramente más arriba que H_1, H_2 y H_3. □

En el diagrama anterior pusimos los subgrupos a nivel diferente dependiendo del tamaño. Por lo general seguiremos utilizando esta convención sin necesidad de mencionarlo.

(c) Encuentra el diagrama de Q_8.



Solución. En 9.1(a) vimos que todos los subgrupos de Q_8 son: $H_0 = \{1\}$, $H_1 = \langle i\rangle$, $H_2 = \langle j\rangle$, $H_3 = \langle k\rangle$, $H_4 = \langle k\rangle$ y Q_8. Además, sabemos que:

- $|H_1| = 2$;
- $|H_2| = |H_3| = |H_4| = 4$;
- $H_1 = H_2 \cap H_3 \cap H_4$; y
- H_2, H_3 y H_4 no se contienen entre sí.

Con esta información sólo nos queda dibujar el diagrama. □

Es momento de hacer una pausa en el trabajo de hoy. Los ejemplos hasta ahora parecen muy sencillos de hacer, pero hay que recordar que nos estamos apoyando en el trabajo de clases pasadas. Veamos cómo podemos proceder con un grupo que no tenemos tan estudiado.

Parte 3

Empezamos con un ejemplo. El **Grupo de Pauli:**
Consideramos al grupo $G_1 := \langle X, Y, Z\rangle \leq GL_2(\mathbb{Z}_2)$, donde:

$$X \begin{pmatrix} 0 & 1 \\ 1 & \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Observamos primero que X, Y, Z son de orden 2. Y vemos la siguiente relación al multiplicarlos entre sí:

$$XY = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = iZ, \quad YZ = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = iX, \qquad ZX = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iY,$$
$$YX = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = -iZ, \; ZY = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -iX, \; XZ = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -iY.$$

Con lo que llevamos podemos concluir que $G_1 = \{\pm E, \pm iE, \pm X, \pm Y, \pm Z, \pm iX, \pm iY, \pm iZ\}$

Por lo que tenemos que son 16 elementos.
Primero encontramos los grupos cíclicos, que son $H_1 = \langle X\rangle, H_2 = \langle Y\rangle, H_3 = \langle Z\rangle$ que son de orden 2 y $H_1' = \langle -X\rangle, H_2' = \langle -Y\rangle, H_3' = \langle -Z\rangle, S = \langle -E\rangle$.
En los cíclicos de orden 4 tenemos uno ssimilares a los de Q_8, que son: $K_0 = \langle iE\rangle, K_1 = \langle iX\rangle = \{E, iX, -E, -iX\}$, $K_2 = \langle iY\rangle$, $K_3 = \langle iZ\rangle$.

Ahora hay que buscar todos los grupos que se pueden generar por dos elementos. Los de orden 4 van a ser isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$, por lo que tienen que ser generados por dos elementos de orden 2 que conmutan.
Estos son: $V_1 = \langle -E, X\rangle$, $V_2 = \langle -E, Y\rangle, V_3 = \langle -E, Z\rangle$.

Luego siguen los de orden 8 generados por dos elementos. Notamos que un grupo así debe de ser generado por almentos un elementos de orden 4 en este caso. Como los únicos elementos de orden 4 son $\pm iX, \pm iY, \pm iZ$, es fácil concluir que el grupo de orden 8 es Q_8

Supongamos ahora que H sólo tiene un generador de orden 4. Nuestras opciones para tal generador de orden 4 son: iX, iY, iZ, iE (no consideramos $-iX, -iY, -iZ, -iE$ porque generan lo mismo). Si el generador es iX, entonces el segundo generador no puede ser $-E$ debido a que $-E \in \langle iX \rangle$. Por lo tanto, por método de eliminación nuestras únicas opciones son $\pm X$,$\pm Y$ o $\pm Z$. Dado que $-E \in \langle iX \rangle$, podemos reducir estas opciones a X, Y o Z.

En caso de ser X el segundo generador de H, tenemos

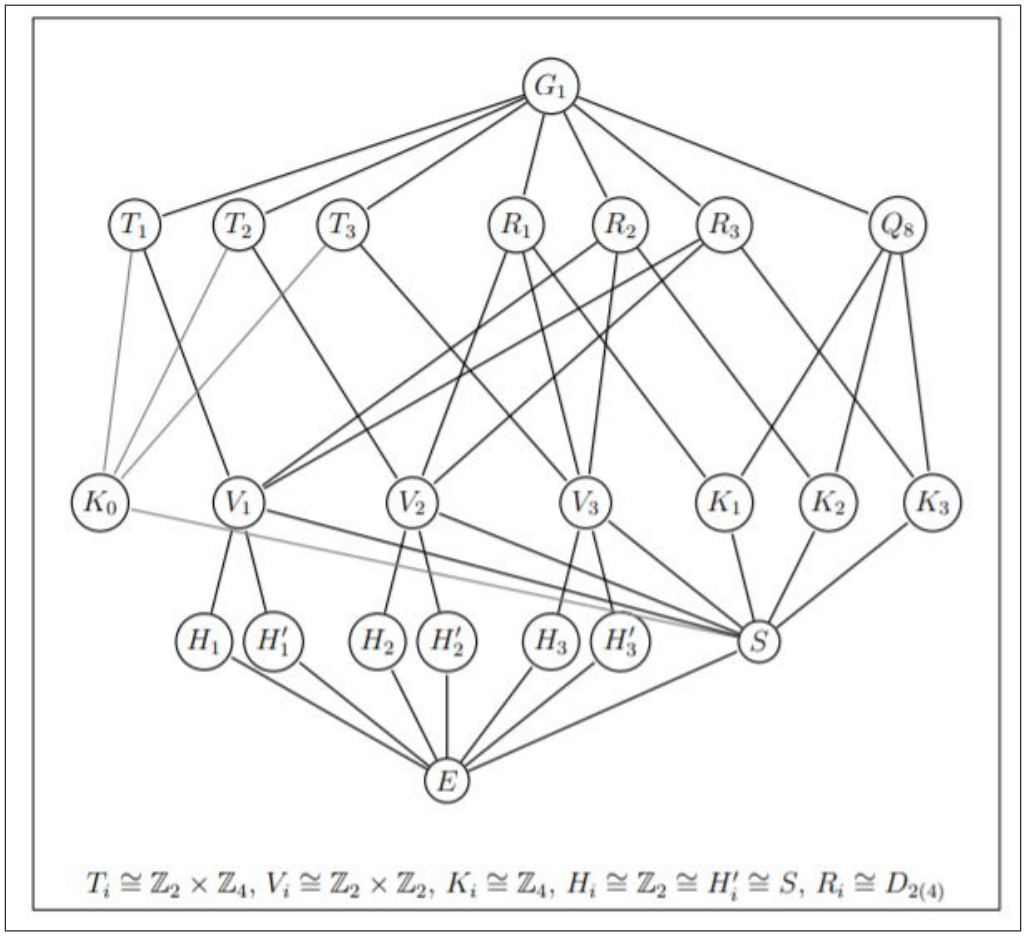
$$T_1 := \langle X, iX \rangle = \{\pm E, \pm iX, \pm X, \pm iE\}.$$

(Observa además que, como X y iX conmutan, entonces $T_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$). Nota que $T_1 = \langle K_0 \cup V_1 \rangle$. De manera similar obtenemos los subgrupos $T_2 := \langle Y, iY \rangle = \langle K_0 \cup V_2 \rangle$ y $T_3 := \langle Z, iZ \rangle = \langle K_0 \cup V_3 \rangle$.

En caso de ser Y (o Z) el segundo generador de H tenemos

$$R_1 := \langle Y, iX \rangle = \{\pm E, \pm Y, \pm Z, \pm iX\}.$$

(Observa que $Y \cdot iX = (iX)^{-1} \cdot Y$, con esto se puede concluir que $R_1 \cong D_{2(4)}$). Observa que $R_1 = \langle V_2 \cup V_3 \cup K_1 \rangle$. De manera similar obtenemos los subgrupos $R_2 = \langle V_1 \cup V_3 \cup K_2 \rangle$ y $R_3 = \langle V_2 \cup V_1 \cup K_3 \rangle$. Con esto hemos terminado de calcular todos los subgrupos de G_1. ¿Cómo ha quedado tu retícula?



1.5. Subgrupos Normales

Definición (Normal): Sea G un grupo y sea $N \leq G$. Decimos que N es un subgrupo normal si $gNg^{-1} = N$ para todo $g \in G$. Usaremos la notación $N \trianglelefteq G$.

Lema: Sea G un grupo y $H \leq G$. Los siguientes enunciados son equivalentes:

a) $H \trianglelefteq G$

b) $aH = Ha \ \ \forall a \in G$

c) $aHa^{-1} \subset H \ \ \forall a \in G$

Corolario: Sea $G = \langle X \rangle$ y $H \leq G$. Entonces, $H \trianglelefteq G$ sii $xHx^{-1} \subset H \ \ \forall x \in X$. Más aún, si $H = \langle Y \rangle$, entonces $H \trianglelefteq G$ sii $xyx^{-1} \in H \ \forall x \in X, y \in Y$

Ejemplo: Consideramos al grupo diédrico $D_{2(n)}$. Y definimos $H = \langle r \rangle$. Vemos que es un subgrupo normal de $D_{2(n)}$. Por el corolario anterior, basta probar que $rrr^{-1} \in H$ y que $srs^{-1} \in H$.

Corolario: Sea G un grupo y $H \leq G$. Si no existe $H' \leq G$ tal que $H' \simeq H$ y $H \neq H'$, entonces $H \trianglelefteq G$.

Esto se puede ver porque gHg^{-1} es también un subgrupo de G con $|H|$ elementos. Pero si H es el único grupo con esta característica, entonces $H = gHg^{-1}$.

Teorema: Sea G un grupo y $H \leq G$. Si $[G : H] = 2$, entonces $H \trianglelefteq G$.

Definición: Sean S, T subconjuntos no vacíos de un grupo G. Definimos su producto como:

$$ST := \{st \,|s \in S, t \in T\}$$

Cumple las siguientes características:

a) $S(TU) = (ST)U$

b) Si $S \leq G$, entonces $T \subset ST$ (porque $e \in S$).

c) En caso de que $T \leq G$, tenemos que $e \in T$, por lo que $S \subset ST$.

d) Si $S \leq G$, $T \leq G$, no necesariamente se sigue que $ST \leq G$.

Teorema: SEa G un grupo (no necesariamente finito) y $H, K \leq G$. Entonces, $|HK| = [H : H \cap K]|K|$.
En particular, si G es finito, entonces:

$$|HK||H \cap K| = |H||K|$$

Dem: Sea $x, y \in HK$. Diremos que $x \sim y$ sii existe $k \in K$ tal que $x = yk$. Se puede ver que es una relación de equivalencia.
Vemos que las clases de equivalencia son:

$$O_x := \{xk|k \in K\} = xK \text{ con } x \in HK.$$

Por lo tanto existen $x_1, ..., x_s \in HK$ tales que $HK = x_1K \cup x_2K \cup ... \cup x_sK$ es una partición. Por lo que $|HK| = s|K|$.
Solamente hay que probar que $s = [H : H \cap K]$. (notas clase 15).

Proposición: Sean $N \trianglelefteq G$, $H \leq G$. Entonces $\langle N, H\rangle = NH = HN$.

Como $N, H \leq \langle N, H\rangle$, entonces $NH \subset \langle N, H\rangle$. Para la contención opuesta basta mostrar que NH es un subgrupo que contiene a N, H por la propiedad de supremo de $\langle N, H\rangle$. Sea $x, y \in NH$ con la forma n_1h_1, n_2h_2.
Entonces su producto es:

$$(n_1h_1)(n_2h_2) = n_1h_1n_2h_1^{-1}h_1h_2 = n_1n'h_1h_2$$

Porque N es normal. Por tanto, el producto en NH es cerrado. Por otro lado, $(n_1h_1)^{-1} = h_1^{-1}n_1^{-1} = (h_1^{-1}n_1^{-1}h_1)h_1^{-1} = n^*h_1^{-1}$. Por lo que los inversos son cerrados en NH.

Ejemplo: Por ejemplo, en S_4, V_0 es un subgrupo normal de 4 elementos. Y H_i es uno de tres elementos. Como su intersección es vacía, entonces $|HV_0| = |H||V_0|$ y por tanto su producto es de 12 elementos. Y como V_0 es normal, este producto es un subgrupo. Por lo que debe de ser $A_4 = V_0H_i$

Lema: Sea G un grupo, $H \trianglelefteq G, K \trianglelefteq G$. Si $H \cap K = \{e\}$, entonces $hk = kh$ para todo h, k.
Dem: Consideramos $x = hkh^{-1}k^{-1}$. Como H y K son normales, entonces $hkh^{-1} \in K, kh^{-1}k^{-1} \in H$. Por tanto, $x \in H, K$ y entonces $x = e \;\Rightarrow\; hkh^{-1}k^{-1} = e \;\Rightarrow\; hk = kh$.

Teorema: Sea $H \trianglelefteq G, K \trianglelefteq G$ tales que $H \cap K = \{e\}$, entonces $HK \simeq H \times K$.
Dem: Consideramos la función $(h, k) \to hk$. Vemos que es un morfismo:

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1) \cdot \phi(h_2, k_2)$$

Queda probar que ϕ es biyectiva. Claramente es supra. Suponemos que $\phi(hk) = e$, entonces $hk = e$, $h = k^{-1}$. Pero como los grupos no se intersectan no trivialmente, entonces $h = k = e$. Por lo que $hk = e$.

Ejemplo: Sean $m, n \in \mathbb{Z}$ con $(m, n) = 1$, entonces $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n$

1.5.1. Grupos Cociente

Proposición: Sea G un grupo y $N \trianglelefteq G$, entonces:

a) $aN \cdot (bN \cdot cN) = (aN \cdot bN) \cdot cN$

b) $aN \cdot N = N \cdot aN = aN$

c) $(aN)(a^{-1}N) = (aNa^{-1})N = N \cdot N = N$

Entonces, al multiplicar clases laterales se cumple asociatividad, neutro e inverso. Sin embargo, antes de concluir que las clases laterales forman un grupo, necesitamos ver que la operación entre $aN \cdot bN$ es cerrada y bien definida. La normalidad nos permite probar que dos clases laterales (izquierdas) de N dan como resultado una clase lateral (izquierda). Esto porque:

$$aN \cdot bN = aNb \cdot N = a(Nb)N = a(bN)N = ab(NN) = abN$$

Entonces, si N es normal, el grupo de clases laterales sí es un grupo.

Lema: Los siguientes enunciados son equivalentes para un subgrupo $H \leq G$:

- $H \trianglelefteq G$

- la operación binaria $aH \cdot bH = abH$ está bien definida.

Dem: Supongamos que $aH = a'H$ y que $bH = b'H$. Recordemos que $xH = yH$ sii $y^{-1}x \in H$.
Vemos que $abH = a'b'H$ porque:

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}(a^{-1}a')b' = b^{-1}(a^{-1}a')bb^{-1}b' \in (b^{-1}Hb)H = H$$

Regreso: Basta probar que $a^{-1}ha \in H$. Notamos que $hH = H$. Entonces, $haH = hH \cdot aH = H \cdot aH = aH$

Teorema: Sea $N \trianglelefteq G$. Denotamos como G/N al conjunto de clases laterales de N. Se cumple que:

a) G/N es un grupo con la operación $aN \cdot bN = abN$

b) La función $\pi : G \to G/N$, con $\pi(a) = aN$ es un morfismo de grupos sobreyectivo.

c) Si G es abeliano, entonces G/N es abeliano.

d) Si G es cíclico igual a $\langle a \rangle$, entonces $G/N = \langle aN \rangle$

e) Si G es finito, entonces $|G/N| = |G|/|N|$

f) $N = \{a \in G | \pi(a) = N\}$

Dem:

a) Ya se probó

b) $\pi(ab) = abN = aN \cdot bN = \pi(a)\pi(b)$ y claramente es sobreyectivo.

c) Vemos que $aN \cdot bN = (ab)N = (ba)N = bN \cdot aN$

d) Como para todo $b \in G$, $b = a^k$. Entonces, $bN = a^kN = (aN)^k$

e Por teorema de Lagrange.

1.6. Teoremas de Isomorfismos

Def: Sea $f : G \to H$ un morfismo de grupos:

a) **imagen**:

$$\text{Im(f)} := \{a \in H \mid \exists\, a \in G \,|f(a) = x\}$$

b) **Núcleo**

$$Ker(f) := \{a \in G \,|f(a) = e_H\}$$

Se puede probar que el núcleo es siempre un subgrupo normal de G. E incluso, usando el punto f del teorema anterior se puede concluir que un subgrupo N de G es normal sii es el núcleo de un morfismo con dominio G.

Entonces, probar que un grupo es normal se puede resolver fácilmente al encontrar un morfismo del cual dicho subgrupo es el kernel.

Por ejemplo, dado el conjunto de simetrías del icosaedro y H el conjunto de simetrías que preservan orientación, se puede ver que $H \trianglelefteq G$ usando el morfismo que a cada simetría le da el determinante de su matriz. Las simetrías que preservan orientación tienen determinante 1 y por tanto son el núcleo.

Teorema: Sea $f : G \to H$ un morfismo. Entonces f es inyectiva sii $Ker(f) = \{e\}$ con e el neutro de G.

Primer Teorema de Isomorfismos:

Sea $f : G \to H$ un morfismos de grupos. Entonces, $Ker(f) \trianglelefteq G$ y $G/Ker(f) \simeq Im(f)$.

Dem: Sea K el kernel de f y sea $\overline{f} : G/K \to Im(f)$ dado por $\overline{f}(aK) = f(a)$.
Vemos que $\overline{f}$ está bien definida, para ello notamos que:

$$aK = bK \;\Leftrightarrow\; b^{-1}a \in K \;\Leftrightarrow\; f(b^{-1}a) = e' \;\Leftrightarrow\; f(b)^{-1}f(a) = e' \;\leftrightarrow\; f(a) = f(b)$$

Por lo que $\overline{f}$ está bien definida y es inyectiva.
Vemos que es un morfismo pues:

$$\overline{f}(aKbK) = \overline{f}(abK) = f(ab) = f(a)f(b) = f(aK)f(bK)$$

Y es claro que $\overline{f}$ es sobreyectiva. Por lo que es un isomorfismo y entonces $G/K \simeq Im(f)$

Ejemplo

- Sean $N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2$. Preuba que $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ y que $(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2)$

  COnsideramos la función $f : G_1 \times G_2 \to G_1/N_1 \times G_2/N_2$, $(a_1, a_2) \to (a_1N, a_2N)$

  Vemos que f es un morfismo suprayectivo y que su kernel es $K(f) = N_1 \times N_2$. Por lo que el primer teorema de isomorfismos nos da lo que queremos.

- Sea G un grupo. Definimos $Aut(G) = \{\alpha : G \to G$ tal que α es un isomorfismo $\}$, que es un grupo. Y consideramos el subgrupo $Inn(G) = \{\alpha : G \to G \mid \exists a \in G\ , \alpha(x) = axa^{-1} \forall x \in G\}$.
  Podemos probar que $G/Z(G) \simeq Inn(G)$

  Dem: Consideramos la función $f : G \to Inn(G)\ , a \to \alpha_a$. Donde $\alpha_a(x) = axa^{-1}$.
  Es un morfismo sobreyectivo. Ahora observamos que:

$$a \in Ker(f) \ \Leftrightarrow\ \alpha_a(x) = x\ \forall x \in G\ \Leftrightarrow\ axa^{-1} = x\ \forall x \in G\ \Leftrightarrow\ ax = xa\ \forall a \in G$$

  Por lo que el $Ker(f) = Z(G)$.

Nota: Dado $f : G \to H$ un morfismo. Podemos considerar 3 morfismos más. Tenemos la proyección $\pi : G \to G/K$ dada por $a \to aK$. La inclusión $i : Im(f) \to H$ dada por $x \to x$ y el morfismo $\overline{f} : G/K \to Im(f)\ ,\ \overline{f}(aK) = f(a)$.
Notamos que $f = i\overline{f}\pi$.

Ejemplo: Existen exactamente dos morfimsos de $D_{2(3)}$ en $\mathbb{Z}_6$.
Dem: Sabemos que $Ker(f) \trianglelefteq D_{2(3)}$. Pero $D_{2(3)}$ solo tiene los grupos normales $\{1\}, \langle r\rangle, D_{2(3)}$. Entonces, tenemos tres casos:

1) Que $Ker(f) = D_{2(3)}$ en cuyo caso f es la función 0.

2. Que $Ker(f) = \langle r\rangle$. En cuyo caso $Im(f) \simeq D_{2(3)}/\langle r\rangle$. Este grupo es de orden 2. Por lo que $Im(f) \simeq \mathbb{Z}_2$. Pero $\mathbb{Z}_6$ tiene un único subgrupo de orden 2, el $\langle 3\rangle$. Por lo tnato, la función debe de estar definida por $f(r) = 0, f(s) = 3$.

3. Sea $Ker(f) = \{1\}$. En este caso f debería ser inyectiva. Pero eso implicaría que f es un isomorfismo, lo que es imposible.

Ley Modular: Sea H, K, M subgrupos de G tales que $H \leq M$. Entonces, $H(K \cap M) = (HK) \cap M$.

Segundo Teorema de Isomorfismo:

Sea G un grupo y $H, K \leq G$ con $K \trianglelefteq G$. Entonces, HK es un subgrupo tal que $K \trianglelefteq HK, H \cap K \trianglelefteq H, HK/K \simeq H/(H \cap K)$

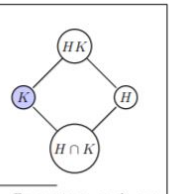
Demostración. Recordemos que, por 15.6, tenemos que $HK = \langle H \cup K\rangle$. Además, como $K \trianglelefteq G$, es sencillo mostrar que $K \trianglelefteq HK$ (ver 17.15(a)), por lo que podemos considerar el grupo cociente HK/K. Utilizaremos el primer teorema de isomorfismo para probar el resto. ¿Puedes proponer cómo sigue la prueba?

Consideramos la función $f : H \to HK/K$, $h \mapsto hK$. Se puede mostrar con argumentos sencillos que f es un morfismo de grupos sobreyectivo. Además,

$$h \in \operatorname{Ker}(f) \ \Leftrightarrow\ hK = K\ \Leftrightarrow\ h \in H \cap K.$$

Por lo tanto, del primer teorema de isomorfismo, tenemos que $H \cap K \trianglelefteq H$ y $H/H \cap K \cong HK/K$. □

Observación 17.12. Como podrás adivinar, el nombre de *teorema diamante* viene del diagrama adjunto. La manera adecuada de pensar este teorema es, primero, visualizar el diagrama de Hasse de un grupo; segundo, localizar un rombo, o diamante, donde alguno de los vértices laterales corresponda a un subgrupo normal; y tercero; hecho esto podemos concluir que el cociente del vértice superior, con el vértice del subgrupo normal, es isomorfo al cociente del otro vértice lateral con el vértice inferior.



En ocaciones es de ayuda remarcar en el diagrama los subgrupos normales que cono-

Lema: Sea $K \leq H_1 \leq G$ con $K \trianglelefteq G$. Entonces:

a) H_1/K es un subgrupo de G/K

b) Dado $K \leq H_2 \leq G$, tenemos que $H_1 \subset H_2$ sii $(H_1/K) \subset (H_2/K)$

O sea, para cada subgrupo H de G, tenemos un subgrupo H/K de G/K.

Teorema de Correspondencia: Sea $K \trianglelefteq G$. Consideramos los conjuntos $X := \{H \leq G | K \leq H\}$, $Y := \{\mathbb{H} \leq G/K\}$ y la correspondencia $\phi : X \to Y$ definida por $\phi(H) = H/K$. Entonces:

a) ϕ es biyectiva

b) ϕ presertva el orden. Es decir, $\phi(H) \leq \phi(H')$ sii $H \leq H'$

c) $\phi(H) \trianglelefteq \phi(H')$ sii $H \trianglelefteq H'$

d) $\phi(H' \cap H)\phi(H') \cap \phi(H)$

e $\phi(\langle H \cap H' \rangle) = \langle \phi(H) \cap \phi(H') \rangle$

Tercer teorema de Isomorfismos:
Sean $K \trianglelefteq H \trianglelefteq G$. Entonces $(H/K) \trianglelefteq (G/K)$ y :

$$(G/K)/(H/K) \simeq G/K$$

Metacíclico: Diremos que G es metacíclico si existe un grupo normal N tal que N y G/N son cíclicos.

Teorema 18.10: Sea G metacíclico, entonces todo subgrupo y todo cociente de G es metacíclico.

2. Acciones de Grupos

2.1. Teorema de Cayley y Clases de Conjugación

Recordemos que todo elemento $\alpha \in S_n$ se puede escribir como una descomposición en cliclos ajenos dos a dos $\alpha = \sigma_1\sigma_2 \cdots \sigma_k$. Donde los ordenaremos como $|\sigma_i| \leq |\sigma_{i+1}|$.

Le decimos **Estructura cíclica** a la sucesión de números naturales $(|\sigma_1|, |\sigma_2|, ..., |\sigma_k|)$ con esta descomposición.
La estructura cícilica está bien definida.

Lema: Sean $\alpha, \beta \in S_n$. Entonces α, β tienen la misma estructura cíclica sii existe $\gamma \in S_n$ tal que $\alpha = \gamma\beta\gamma^{-1}$.

Def: Sea G un grupo y $x, y \in G$. Decimos que son conjugados si existe una $z \in G$ con $x = zyz^{-1}$.

Teorema de Cayley: Todo grupo G es isomorfo a un subgrupo de S_G. En particular, si $|G| = n$, entonces G es isomorfo a un un subgrupo de S_n.

Dem: Consideramos para $a \in G$ a la función $\tau_a(x) = ax$.
Se puede ver que es una biyección, por lo que $\tau_a \in S_G$. Cabe notar además que $\tau_{ab} = \tau_a\tau_b$.
Entonces consideramos la correspondencia $\phi : G \to S_G$ como $a \to \tau_a$. esta función está bien definida y es un homomorfismo, por lo que $G \simeq Im(\phi)$.

Lema: Sea G un grupo. Se cumplen los siguientes enunciados:

a) Sea $\sim$ la relación definida en G como $a \sim b$ sii existe $g \in G$ tal que $a = gbg^{-1}$.

b) Sean $a \in G$ y $O_a = \{xax^{-1} \ | x \in G\}$. Entonces la familia $\{O_a\}_{a\in G}$ es una partición de G.

c) La partición del inciso anteror es la inducida por $\sim$.

d) $|O_a| = 1$ sii $a \in Z(G)$

e) Su $x \in O_a$, entonces $|x| = |a|$

Lema: Sea G un grupo y S el conjunto de todos los subgrupos de G. Entonces, se cumplen los siguientes enunciados:

a) Sea $\approx$ la relación definida en S como $A \approx B$ sii existe $g \in G$ tal que $A = gBg^{-1}$. Entonces $\approx$ es una relación de equivalencia.

b) Sean $A \in S$, $O_A = \{xAx^{-1} | x \in G\}$, llamado **clase de conjugación** de A. Entonces $\{O_A\}_{A\in S}$ es una partición de S.

c) La familia $\{O_A\}_{A\in S}$ es la partición inducida $\approx$.

d) $|O_A| = 1$ sii $A \trianglelefteq G$

e) Si $B \in O_A$ para algún $A \leq G$, entonces $B \cong A$.

3. Grupos de Frobenius

Ejemplo: Considera el grupo diédrico:

$$D_{2(5)} = \langle r, s | r^5 = s^2 = e, rs = sr^{-1} \rangle$$

Definimos a F_5 como el grupo de automorfismos de $D_{2(5)}$.

- **Orden de F_5:** Sea $f : D_{2(5)} \to D_{2(5)}$ un isomorfismo. Observamos que $f(s)$ tiene orden 2 y que $f(r)$ tiene orden 5. Sabemos que los elementos de orden 2 son s, sr, sr^2, sr^3, sr^4 y los de orden 5 son r, r^2, r^3, r^4. Por lo tanto, $f(s)$ pertenece al primer grupo y $f(r)$ pertenece al segundo.
  Por tanto, el isomorfismo debe de hacer $r \to r^i$ y $s \to sr^j$. Con $i = \{1, 2, 3, 4\}, j = \{0, 1, 2, 3, 4\}$
  Y la imagen de cualquier otro elemento queda determinada con $f(s), f(r)$. Por lo que con escoger estos dos números queda totalmente determinado el automorfismo.
  Por lo que hay 20 automorfismos.

- **Elementos y relaciones generadores de F_5:** Los elementos de F_5 son las funciones $g_{i,j}$ definidas como $g_{i,j}(r) = r^i, g_{i,j}(s) = st^j$. Con i del 1 al 4 y j del 0 al 4. Notamos que $g_{1,0}$ es el neutro de F_5.
  Consideramos ahora en particular los isomorfismos $\rho := g_{2,0}$, $\sigma := g_{1,1}$.
  Es decir, están definidas por:

  $$\rho(r) = r^2 \ , \ \rho(s) = s \qquad \sigma(r) = r \ , \ \sigma(s) = sr$$

  Veamos el orden de estos elementos.
  Vemos que $\rho^2(r) = r^4, \rho^3(r) = r^8 = r^3 \ , \ \rho^4(r) = r^6 = r$ Y también tenemos que $\rho^k(s) = s \ \ \forall s$.
  Por lo tanto, $\rho^2 = g_{4,0} \ , \ \rho^3 = g_{3,0} \ , \ \rho^4 = g_{1,0}$. Y así, $|\rho| = 4$.

  Vemos que $\sigma^2(s) = sr^2 \ , \ \sigma^3(s) = sr^3 \ , \ \sigma^4(s) = sr^4 \ , \ \sigma^5(s) = sr^5 = s$. Y $\sigma^k(r) = r \ \ \forall k$.
  Por lo tanto, $\sigma^2 = g_{1,2} \ , \ \sigma^3 = g_{1,3} \ , \ \sigma^4 = g_{1,4} \ , \ \sigma^5 = g_{1,0}$. Así que $|\sigma| = 5$

  Por otro lado, se puede ver que $\rho\sigma = \sigma^2\rho$.

  Entonces, podemos afirmar que:

  $$F_5 = \langle \rho, \sigma | \rho^4 = \sigma^5 = e \ , \ \rho\sigma = \sigma^2\rho \rangle$$

Diagrama de Hasse de las clases de Conjugación de F_5

- **Subgrupos cícilicos:** Los cíclicos son $\langle\sigma\rangle$ de orden 5. $\langle\rho\rangle$ de orden 4 y $\langle\rho^2\rangle$ que es de orden 2.
  Luego, como $\rho\sigma = \sigma^2\rho$, se puede probar que $\langle\sigma\rangle$ es un subgrupo normal y que todos los demás elementos de F_5 son conjugados a ρ o a ρ^2. Por lo tanto, estos son todos los vértices que necesitamos.

- **Encontrar el vértice asociado al supremo de cada pareja de vértices que tenemos:**
  Enocntramos el generado de un par de vértices conocidos. Por ejemplo, $\langle\langle\sigma\rangle \cup \langle\rho^2\rangle\rangle = \langle\sigma, \rho^2\rangle$. Luego, $\langle\sigma, \rho\rangle = F_5$, $\langle\rho, \rho^2\rangle = \langle\rho\rangle$.

- **Asegurarnos que no existan vértices intermedios**
  Tenemos vértices H y K tales que $H \leq K$. El objetivo es demostrar que no existen grupos intermedios A tales que $H \leq A \leq K$.
  En efecto, se tiene que $[K : H] = [K : A][A : H]$ siempre que $H \leq A \leq K$. De modo que si $[K : H]$ es primo , no puede existir un grupo intermedio, y este es el caso de todos nuestro vértices.

- **Repetir los pasos 2 y 3 hasta obtener todo** F_5 Ya.

Contar el número de clases de Conjugación de un subgrupo.

Sea G un grupo, $A \leq G$ y O_A la clase de conjugación de A. Es decir, $O_A = \{gAg^{-1} \mid g \in G\}$.
La acción de conjugar el subgrupo A es una permutación de O_A. En efecto, la acción de conjugar por un elemento $g \in G$, la podemos describir como una función $\phi_g : O_A \to O_A$, $H \to gHg^{-1}$. Se puede ver que ϕ_g es biyectiva, por lo que para todo $g \in G$, tenemos una permutación $\phi_g \in S_{O_A}$.

Lema: Sean G un grupo y $A \leq G$. Consideremos la correspondencia $\phi : G \to S_{O_A}$, $g \to \phi_g$. Donde ϕ_g es la permutación definida como $\phi_g(H) = gHg^{-1}$. Se cumple:

a) ϕ es un morfismo de grupos.

b) Para cada $K \in O_A$, definimos el **normalizador de** K como:

$$N(K) := \{g \in G | \phi_g \text{ deja fijo a } K\} = \{g \in G | gKg^{-1} = K\}$$

El cual es unsubgrupo tal que $K \trianglelefteq N(K)$

c) Si $A = \langle x\rangle$, entonces $N(a) := N(A) = \{g \in G | gx = xg\}$, por ello, $N(A)$ recibe el nombre de **centralizador de** x

d) Si $A \trianglelefteq B \leq G$, entonces $B \subset N(A)$

e) $Ker(\phi) = \cap_{K \in O_A} N(K)$

.

Teorema: Sea G un grupo. Se cumplen los siguientes enunciados:

a) El número de conjugados de $x \in G$ es igual a $[G : N(x)]$, es decir:

$$|\{a \in G | a = gxg^{-1}, g \in G\}| = [G : N(x)]$$

b) El número de conjugados de $H \leq G$ es igual a $[G : N(H)]$, es decir:

$$|\{K \leq G | K = gHg^{-1}, g \in G\}| = [G : N(H)]$$

Dem

a) Sea $N := N(x)$. Para probarlo, mostramos una biyección entre el conjunto $X := \{a \in G \ | a = gxg^{-1}, g \in G\}$ y las clases laterales de N. Consideramos la correspondencia $f : X \to \{xN | x \in G\}$ por $axa^{-1} \to aN$.
Observamos que:

$$axa^{-1} = bxb^{-1} \Leftrightarrow (b^{-1}a)x(b^{-1}a)^{-1} = x \Leftrightarrow b^{-1}a \in N \Leftrightarrow aN = bN$$

Por lo tanto, f está bien definida y es inyectiva. Además, f es claramente suprayectiva.

3.0.1. La ecuación de Clase:

Sea G un grupo finito:

a) Si $G = O_{a_1} \cup \cdots \cup O_{a_s} \cup O_{a_s+1} \cup \cdots \cup O_{a_k}$ es la partición inducida por la relación de conjugación, entonces:

$$|G| = \sum_{i=1}^{k} |O_{a_i}| = |Z(G)| + \sum_{i=1}^{s} |O_{a_i}|$$

Donde $a_1, ..., a_s \notin Z(G)$ y $a_{s+1}, ..., a_k \in Z(G)$.

b) Sea $\mathcal{S}$ el conjunto de los subgrupos de G, $\mathcal{N}$ el conjunto de los subgrupos normales de G y $\mathcal{S} = O_{A_1} \cup \cdots \cup O_{A_t} \cup O_{A_{t+1}} \cup \cdots \cup O_{A_r}$ es la partición inducida por la relación de conjugación, entonces:

$$|\mathcal{S}| = \sum_{i=1}^{r} |O_{A_i}| = |\mathcal{N}| + \sum_{i=1}^{t} |O_{A_i}|$$

Donde $A_1, ..., A_t \notin \mathcal{N}$, $A_{t+1}, \cdots A_r \in \mathcal{N}$

Probamos ya que éstas son particiones de sus conjuntos correspondientes. Y además que $|O_a| = 1$ si y sólo si $a \in Z(G)$ y que $|O_K| = 1$ si y sólo si $K \in \mathcal{N}$

3.0.2. Teorema de Cauchy

Teorema: Sea G un grupo finito y p un entero primo que divide a $|G|$. Entonces, G tiene un elemento de orden p.

Dem: Supongamos que G es abeliano de orden $|G| = pn$. Probamos por inducción fuerte sobre n que G tiene un elemento de orden p.
Para los casos $n = 1, 2$, ya sabemos que existe un elemento de orden p (10.8 y 10.13). Supongamos que $n > 3$. Observamos que, en caso de encontrar un elemento x con $|x| = pm$, tenemos que $|x^m| = p$ (clase 11). Ahora, supongamos que no encontramos ningún elemento de orden p.
Entonces escogemos un elemento $x \in G - \{e\}$ y consideramos el grupo cociente G/X, donde $X = \langle x \rangle$. Del teorema de Lagrange se sigue que $p||G/X|$.
Así que por hipótesis de inducción, existe $yX \in G/X$ de orden p. Sea $Y = \langle y \rangle$. Por el segundo teorema de isomorfismo.

3.1. Acciones de Grupo

Definición: Sea G un grupo y X un conjunto no vacío. Una función $G \times X \to X \ \ (a, x) \to a \cdot x$, recibe el nombre de **acción de** G si satisface:

A1 $e \cdot x = x \quad \forall x \in X$

A2 $a \cdot (b \cdot x) = (ab) \cdot x \quad \forall x \in X, \forall a, b \in G$

Ejemplos:

a) Sean $\alpha \in S_n, G = \langle \alpha \rangle$ y $X = \{1, 2, 3, ..., n\}$. La función $G \times X \to X$ definida como $\alpha^k \cdot x = \alpha^k(x)$ es una acción de G. La usamos para estudiar permutaciones

b) Sean $H \leq G$. La función $H \times G \to G$ definida como $h \cdot g = hg$ es una acción de H en G. La usamos para estudiar clases laterales.

c) Sea G un grupo . La función $G \times G \to G$ definida por $a \cdot b = aba^{-1}$ es una acción de G en G. La usamos para estudiar las clases de conjugación en G

d) Sea G un grupo y $\mathcal{S}$ el conjunto de subgrupos de G. Entonces la función $G \times \mathcal{S} \to \mathcal{S}$ definida como $a \cdot H = aHa^{-1}$, es decir la acción de conjugar, es una acción de G en $\mathcal{S}$. Utilizamos esta acción para estudiar las clases de conjugación.

e) Sea X un conjunto no vacío y $G \subset S_X$. Entonces, la función $G \times X \to X$ definida como $g \cdot x = g(x)$ es una acción de G en X.

f) Sea $H \leq G$, y $X = \{gH | g \in G\}$. La función $G \times X \to X$ definida por $g \cdot (aH) = (ga)H$ es una acción de G en X.

g) Sea $H \leq G$ y $X = \{gHg^{-1} | g \in G\}$. La función $G \times X \to X$ definida como $g \cdot (aHa^{-1}) = (ga)H(ga)^{-1}$ es una acción de G en X.

Lema: Sean G un grupo, X un G-conjunto, $x, y \in X$ y $a, b \in G$. Se cumple:

a) Si $a \cdot x = a \cdot y$, entonces $x = y$

b) $a \cdot x = b \cdot y$ si y sólo si $(b^{-1}a) \cdot x = y$.

Teorema: Sean G un grupo y X un $G-$conjunto. Para cada $g \in G$ consideramos la correspondencia $\phi_g : X \to X$, $x \to g \cdot x$. Se cumplen los siguientes enunciados:

a) ϕ_a es biyectiva para todo $a \in G$. En particular, $\phi_a \in S_X$

b) La correspondencia $\phi : G \to S_X$, $a \to \phi_a$ es un morfismo de grupos.

c) $Ker(\phi) = \{a \in G | a \cdot x = x \forall x \in X\}$

Teorema Cayley Extendido: Sean G un grupo y $H \leq G$ con $m = [G : H]$. Entonces, existe un morfismo de grupos $\phi : G \to S_m$ que cumple los siguientes enunciados:

a) $Ker(\phi) = \bigcap_{g \in G} gHg^{-1}$

b) $Ker(\phi) \leq H$

c) Si $K \trianglelefteq G$ y $K \leq H$, entonces $K \leq Ker(\phi)$

d) $H \trianglelefteq G$ si y sólo si $Ker(\phi) = H$

Corolario: Sean G un grupo finito y p el menor primo dividiendo a $|G|$. Entonces todo $H \leq G$ con $[G : H] = p$ es un subgrupo normal de G.

Lema: Sean G un grupo y X un $G-$conjunto. Consideramos la relación $\sim$ en X, definida como $x \sim y$ si y sólo si existe $g \in G$ tal que $x = g \cdot y$. Se cumple:

a) La relación $\sim$ es de equivalencia

b) La relación $\sim$ induce una particuón $X = \bigcup U_{x \in X} O_x$ donde:

$$O_x := \{g \cdot x \, | g \in G\}$$

c) Dado $x \in X$, $S(x) := \{g \in G \, | g \cdot x = x\}$ es un subgrupo de G

d) $|O_x| = [G : S(x)]$ para todo $x \in X$.

Definición: Sea G un grupo, X un G conjunto y $x \in X$:

a) O_x recibe el nombre de **órbita de** x, también se le denota como $G \cdot x$

b) La partición $\bigcup_{x \in X} O_x$ se llama **descomposición en órbitas de** X

c) $S(x)$ recibe el nombre de **estabilizador de** x

d) $X_f = \{x \in X \mid O_x = \{x\}\}$ rebie el nombre de **subconjunto fijo.**

Teorema (Descomposición en órbitas): Sea G un grupo, X un $G-$conjunto finito y $X = O_{x_1} \cup \cdots \cup O_{x_k} \cup O_{x_k+1} \cup \cdots \cup O_{x_m}$ la descomposición en órbitas, donde $x_1, ..., x_k \notin X_f$ y $x_{k+1}, \cdots x_m \in X_f$. Entonces:

$$|X| = \sum_{i=1}^{m} [G : S(x_i)] = |X_f| + \sum_{i=1}^{k} [G : S(x_i)]$$

.

3.2. Acciones de Grupos (Zaldivar)

Definición: Sea G un grupo y X un conjunto no vacío. Una función $G \times X \to X \ \ (a, x) \to a \cdot x$, recibe el nombre de **acción de** G si satisface:

A1 $e \cdot x = x \quad \forall x \in X$

A2 $a \cdot (b \cdot x) = (ab) \cdot x \quad \forall x \in X, \forall a, b \in G$

Ejemplos:

a) Sean $\alpha \in S_n, G = \langle \alpha \rangle$ y $X = \{1, 2, 3, ..., n\}$. La función $G \times X \to X$ definida como $\alpha^k \cdot x = \alpha^k(x)$ es una acción de G. La usamos para estudiar permutaciones

b) Sean $H \leq G$. La función $H \times G \to G$ definida como $h \cdot g = hg$ es una acción de H en G. La usamos para estudiar clases laterales.

c) Sea G un grupo . La función $G \times G \to G$ definida por $a \cdot b = aba^{-1}$ es una acción de G en G. La usamos para estudiar las clases de conjugación en G

d) Sea G un grupo y $\mathcal{S}$ el conjunto de subgrupos de G. Entonces la función $G \times \mathcal{S} \to \mathcal{S}$ definida como $a \cdot H = aHa^{-1}$, es decir la acción de conjugar, es una acción de G en $\mathcal{S}$. Utilizamos esta acción para estudiar las clases de conjugación.

e) Sea X un conjunto no vacío y $G \subset S_X$. Entonces, la función $G \times X \to X$ definida como $g \cdot x = g(x)$ es una acción de G en X.

f) Sea $H \leq G$, y $X = \{gH | g \in G\}$. La función $G \times X \to X$ definida por $g \cdot (aH) = (ga)H$ es una acción de G en X.

g) Sea $H \leq G$ y $X = \{gHg^{-1} | g \in G\}$. La función $G \times X \to X$ definida como $g \cdot (aHa^{-1}) = (ga)H(ga)^{-1}$ es una acción de G en X.

3.2.1. Lema 22.4

Sea G un grupo, X un G grupo, $x, y \in X$ y $a, b \in G$. Se cumple:

a) Si $a \cdot x = a \cdot y$ entonces $x = y$

b) $a \cdot x = b \cdot y$ si y sólo si $(b^{-1}a) \cdot x = y$

3.2.2. Definiciones Generales:

Dado un grupo G que actúa sobre un conjunto X, podemos definir lo siguiente:

- **Relación de Equivalencia en X:** Decimos que $x, y \in X$ están relacionados, $x \sim y$ si existe un $g \in G$ tal que $x = gy$
- **Órbita de un $x \in X$:** La órbita de $x \in X$ es el conjunto:

$$O_x = G \cdot x = \{g \cdot x | g \in G\} \subset X$$

  Es un subconjunto de X y puede tener diferentes tamanos dependiendo de quíen sea x.
  Dada la relación de equivalencia del item pasado, O_x es la clase de equivalencia de x.
  Así que Todos los O_x para $x \in X$ forman una partición de X en clases de equivalencia disjuntas.

- **Estabilizador de un $x \in X$**: El estabilizador de $x \in X$ se define como:

$$S(x) = \{g \in G | gx = x\} \leq G$$

  Son los elementos de G que dejan fijo a dicho x. Son un subgrupo de G.

- **Subconjunto Fijo:** El subconjunto fijo de X es:

$$X_f = \{x \in X | O_x = \{x\}\} = \{x \in X | g \cdot x = x \ \ \forall g \in G\} \subset X$$

  Es el conjunto de elementos de X que no se mueven sin importar el elemento del grupo que actúe sobre ellos. Es un subconjunto de X.

Teoremas importantes:

- **Teorema de Cayley Extendido:** Sea G un grupo y $H \leq G$ con $m = [G : H]$. Entonces existe un morfismo de grupos $\phi : G \to S_m$ que cumple con los siguientes enunciados:

  a) $Ker(\phi) = \bigcap_{g \in G} \ gHg^{-1}$

  b) $Ker(\phi) \leq H$

  c) Si $K \trianglelefteq G$ y $K \leq H$, entonces $K \leq Ker(\phi)$

d) $H \trianglelefteq G$ si y sólo si $Ker(\phi) = H$

- **Teorema de Órbita - Estabilizador** El teorema dice que para todo $x \in X$ se cumple:

$$|O_x| = [G : S(x)] = \frac{|G|}{|S(x)|}$$

Dem: Encontramos una función Biyectiva entre O_x y $\mathcal{X} = \{gS(x) \mid g \in S(x)\}$.
Sea $f : O_x \to \mathcal{X}$ la correspondencia definida como $g \cdot x \to gS(x)$. Entonces, observamos que:
$a \cdot x = b \cdot x \implies (b^{-1}a) \cdot x = \cdot x \iff b^{-1}a \in S(x) \iff aS = bS$
Por lo que f es inyectiva. La suprayectividad queda clara. Por lo que f es biyectiva.

- **Descomposición en órbitas**: Sean G un grupo que actúa en X. Y digamos que X se descompone como $X = O_{x_1} \cap \cdots \cap O_{x_k} \cap O_{k+1} \cap \cdots \cap O_{x_m}$ la descomposición en órbitas. Donde $x_1, \cdots x_k \notin X_f$ y $x_{k+1}, \cdots, x_m \in X_f$. Entonces:

$$|X| = \sum_{i=1}^{m} [G : S(x_i)] = |X_f| + \sum_{i=1}^{k} [G : S(x_i)]$$

Dem: Como las O forman una partición de X, tenemos que:

$$|X| = |O_{x_1} \cup \cdots \cup O_{x_m}| = \sum_{i=1}^{m} |O_{x_i}| = \sum_{i=1}^{m} [G : S(x_i)] = |X_f| + \sum_{i=1}^{k} [G : S(x_i)]$$

Casos Particulares:

- **Elementos Conjugados:**
Digamos que G actúa sobre si mismo por conjugación como: $g \cdot k = gkg^{-1}$. Entonces tenemos lo siguiente:

  - **Relación de Equivalencia:** $g \sim h$ sii $g = khk^{-1}$ para algún $k \in G$
  - **Órbita:** La órbita de un elemento $x \in G$ es:

$$O_x = \{g \cdot x | g \in G\} = \{gxg^{-1} | g \in G\}$$

    Recibe el nombre de **clase de conjugación de** x
  - **Estabilizador:** El estabilizador de un $x \in X$ es:

$$S(x) := N(x) = \{g \in G | g \cdot x = x\} = \{g \in G | gxg^{-1} = x\}$$

    Recibe el nombre de **centralizador de** x y son los elementos que conmutan con x.
  - **Conjunto fijo:** Es el conjunto:

$$X_f = \{x \in X | g \cdot x = x \ \ \forall g \in G\} = G_f = \{x \in G | gxg^{-1} = x \ \ \forall g \in G\}$$

Son los elementos $x \in G$ que conmutan con todo. Recibe el nombre de **Centro de** G

- **Teorema Órbita-Estabilizador:**

$$|O_x| = \frac{|G|}{N(x)}$$

- **Ecuación de Clases:**

$$|G| = |Z(G)| + \sum_{i=1}^{m} |O_{x_i}|$$

Donde la suma corre solamente en los elementos x_i tales que no están en el centro.

- **Conjuntos Conjugados:**
Digamos que G actúa sobre S (el conjunto de subgrupos de G) como: $g \cdot A = gAg^{-1}$. Entonces tenemos lo siguiente:

  - **Relación de Equivalencia:** $A \sim B$ sii $A = kBk^{-1}$ para algún $k \in G$
  - **Órbita:** La órbita de un elemento $A \in S$ es:

$$O_A = \{g \cdot A | g \in G\} = \{gAg^{-1} | g \in G\}$$

Recibe el nombre de **clase de conjugación de** A

  - **Estabilizador:** El estabilizador de un $A \in S$ es:

$$S(A) := N(A) = \{g \in G | g \cdot A = A\} = \{g \in G | gAg^{-1} = A\}$$

Recibe el nombre de **normalizador de** A y son los elementos $g \in G$ para los cuales la clase lateral izquierda de gA es la clase lateral derecha Ag.

  - **Conjunto fijo:** Es el conjunto:

$$S_f = \{A \in S | g \cdot A = A \ \ \forall g \in G\} = \{A \in S | gAg^{-1} = A \ \ \forall g \in G\}$$

Son los grupos normales. Juntos forman el conjunto $\mathcal{N}$ de grupos normales de G.

  - **Teorema Órbita-Estabilizador:**

$$|O_A| = \frac{|G|}{N(A)}$$

  - **Ecuación de Clases:**

$$|G| = |N(G)| + \sum_{i=1}^{m} |O_{A_i}|$$

Donde la suma corre solamente en los subgrupos A_i tales que no son normales

  - **Teorema:**

$$A \trianglelefteq B \leq G \quad \Rightarrow \quad B \subset N(A)$$

Pues sí.

3.2.3. Teoremas 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, un subgrupo de orden p

3.3. Contar Órbitas

Digamos que X es un G conjunto. Hemos probado que $|O_x| = |G|/|S(x)|$, entonces $|S(x)| = |G|/|O_x|$. Por lo cual, $|S(a)| = |S(x)|$ pata todo $a \in O_x$. Con esto podemos concluir que:

$$\sum_{a\in O_x} |S(a)| = \sum_{a\in O_x} \frac{|G|}{|O_x|} = |O_x|\frac{|G|}{|O_x|} = |G|$$

Que se satisface para cualquier órbita. Entonces, si consideramos la descomposición en orbitas $X = O_{x_1} \cup \cdots \cup O_{x_k}$ tenemos:

$$\sum_{a\in X} |S(a)| = \sum_{i=1}^{k} \left(\sum_{a\in O_{x_i}} |S(a)| \right) = \sum_{i=1}^{k} |G| = k|G|$$

con k el número de órbitas. Por lo que:

$$k = \sum_{a\in X} \frac{|S(a)|}{|G|}$$

Sin embargo, esta formulita puede ser medio complicada. Por lo que definimos un nuevo conjunto:

$$S(a) = \{g \in G \mid g \cdot a = a\}$$
$$F(g) = \{a \in X \mid g \cdot a = a\}$$

Entonces, ahora consideramos todos los pares ordenados de la forma:

$$T := \{(g, a) \in G \times X \mid g \cdot a = a\}$$

Y tenemos lo siguientes:

- Para cada $a_0 \in X, S(a_0) \times \{a_0\} = \{(g, a_0) \in G \times X | g_0 \cdot a = a\} \subset T$
- Para cada $g_0 \in G$, $g_0 \times F(g_0) = \{(g_0, a) \in G \times X \mid g_0 \cdot a = a\} \subset T$
- $T = \bigcup_{a\in X} S(a) \times \{a\} = \bigcup_{g\in G}\{g\} \times F(g)$

Por lo tanto, tenemos que:

$$\sum_{a\in X} |S(a)| = |\bigcup_{a\in X} S(a) \times \{a\}| = |T| = |\bigcup_{g\in G}\{g\} \times F(g)| = \sum_{g\in G} |F(g)|$$

Leam de Burnside Frobenius: Sea G un grupo finito y X un $G-$conjunto finito. Si k es el número de orbitas en las que se descompone X, entonces:

$$k = \sum_{g \in G} \frac{|F(g)|}{|G|}$$

Ejemplo 23.4. ¿Cuántas maneras *esencialmente* diferentes hay de pintar un cubo con tres colores distintos de tal manera que cada cara del cubo se pinte de un solo color?

Solución. Nos enfrentamos a un problema de conteo. Consideremos el conjunto X de todas las posibles maneras en que se puede pintar el cubo. Los elementos de X los podemos visualizar como sucesiones finitas de la forma

$$(a, b, c, d, e, f),$$

donde cada entrada representa una cara del cubo (la primer entrada es la que da al norte, la segunda da al este, la tercera al sur, la cuarta al oeste, la quita hacia arriba y la sexta hacia abajo) y cada letra a, b, c, d, e, f representa el color del que está pintado. Como tenemos tres colores a escoger y el cubo tiene seis caras, tenemos que $|X| = 3^6$. Aquí el problema es cómo distinguir si dos de estas maneras son iguales al rotar el cubo. Por ejemplo, si ρ es la rotación que manda la cara norte a la cara este, tenemos que $\rho(a, b, c, d, e, f) = (d, a, b, c, e, f)$. Por lo tanto, la manera de pintar (a, b, c, d, e, f) es *esencialmente* igual a la manera (d, a, b, c, e, f). ¿Cómo resolver esto?

Sea G el grupo de rotaciones del cubo. Notemos que X es un G-conjunto de tal manera que dos maneras de pintar el cubo son esencialmente iguales si y sólo si pertenecen a la misma órbita. Por lo tanto, **el número de órbitas es igual al número de maneras esencialmente diferentes de pintar el cubo**.

Sólo nos queda hacer las cuentas necesarias. Para ello, observamos que G consta de 24 elementos. A saber, G consta de:

(a) ocho rotaciones (de ángulo $2\pi/3$ o $4\pi/3$) que tienen como eje de rotación una diagonal entre vértices opuestos;

(b) seis rotaciones (de ángulo π) que tienen como eje de rotación el punto medio de aristas opuestas;

(c) tres rotaciones (de ángulo π) que tienen como eje de rotación el punto medio de caras opuestas;

(d) seis rotaciones (de ángulo $\pi/2$ o $3\pi/2$) que tienen como eje de rotación el punto medio de caras opuestas; y

(e) la rotación nula, es decir el objeto neutro de G.

Recordemos que los elementos de X son de la forma

$$(\text{norte}, \text{este}, \text{sur}, \text{oeste}, \text{arriba}, \text{abajo}).$$

Notamos que:

(a') Las rotaciones de (a) dejan fijos a los elementos de X de la forma (x, y, y, x, x, y),(x, x, y, y, x, y), (x, x, y, y, y, x) o (x, y, y, x, y, x). Por lo tanto, las rotaciones de (a) permiten dos elecciones de color. En conclusión hay 3^2 elementos de X fijos por cada una de estas rotaciones.

(b') De manera similar, las rotaciones de (b) permiten 3 elecciones de color. En conclusión hay 3^3 elementos de X fijos por cada una de estas rotaciones.

(c') Las rotaciones de (c) permiten 4 elecciones de color. En conclusión hay 3^4 elementos de X fijos por cada una de estas rotaciones.

(d') Las rotaciones de (d) permiten 3 elecciones de color. En conclusión hay 3^3 elementos de X fijos por cada una de estas rotaciones.

(e') Finalmente, el neutro deja fijo a todo elemento de X. Por lo tanto, hay 3^6 elementos fijos para el neutro.

(b) seis rotaciones (de ángulo π) que tienen como eje de rotación el punto medio de aristas opuestas;

(c) tres rotaciones (de ángulo π) que tienen como eje de rotación el punto medio de caras opuestas;

(d) seis rotaciones (de ángulo $\pi/2$ o $3\pi/2$) que tienen como eje de rotación el punto medio de caras opuestas; y

(e) la rotación nula, es decir el objeto neutro de G.

Recordemos que los elementos de X son de la forma

$$(\text{norte}, \text{este}, \text{sur}, \text{oeste}, \text{arriba}, \text{abajo}).$$

Notamos que:

(a') Las rotaciones de (a) dejan fijos a los elementos de X de la forma (x, y, y, x, x, y),(x, x, y, y, x, y), (x, x, y, y, y, x) o (x, y, y, x, y, x). Por lo tanto, las rotaciones de (a) permiten dos elecciones de color. En conclusión hay 3^2 elementos de X fijos por cada una de estas rotaciones.

(b') De manera similar, las rotaciones de (b) permiten 3 elecciones de color. En conclusión hay 3^3 elementos de X fijos por cada una de estas rotaciones.

(c') Las rotaciones de (c) permiten 4 elecciones de color. En conclusión hay 3^4 elementos de X fijos por cada una de estas rotaciones.

(d') Las rotaciones de (d) permiten 3 elecciones de color. En conclusión hay 3^3 elementos de X fijos por cada una de estas rotaciones.

(e') Finalmente, el neutro deja fijo a todo elemento de X. Por lo tanto, hay 3^6 elementos fijos para el neutro.

4. Teoremas de Sylow

P-Grupos

4.0.1. p-Grupos

Decimos que G es un p-grupo si para toda $g \in G$ existe una $m \in \mathbb{Z}$ tal que el orden de g es p^m.
Un grupo de orden p^k siempre es un p-grupo.

Teorema:
Sean G un grupo y $K \trianglelefteq G$. Entonces, G es un p-grupo si y sólo si K y N/N son p-grupos.

Lema: Sea G un grupo finito. Entonces, G es un p-grupo si y sólo si $|G| = p^m$.

Dem: El teorema de Cauchy contradice que haya otros factors primos de $|G|$.

Teorema: Si G es un p-gtupo finito, entonces $Z(G) \neq \{e\}$

Corolario: SiG es un p-grupo finito, entonces existe $x \in G$ de orden p tal que $xy = yx \ \ \forall y \in G$.

Teorema: Si G es un grupo de orden p^2 entonces $G \simeq \mathbb{Z}_{p^2}$ o $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

Teorema Sea G de orden 2^3. entonces:

a) SiG es abeliano, entonces G es isomorfo a $\mathbb{Z}_{2^3}, \mathbb{Z}_{2^2} \times \mathbb{Z}_2$ o $\mathbb{Z}_2^3$

b) Si G no es abeliano, entonces G es isomorfo a $D_{2(4)}$ o a Q_8

$\|G\|$	G abeliano	G no abeliano
2	$\mathbb{Z}_2$	-
3	$\mathbb{Z}_3$	-
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	-
5	$\mathbb{Z}_5$	-
6	$\mathbb{Z}_6$	$D_{2(3)}$
7	$\mathbb{Z}_7$	-
8	$\mathbb{Z}_{2^3}$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2$, $\mathbb{Z}_2^3$	$D_{2(4)}$, Q_8
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	-
$2p$	$\mathbb{Z}_{2p}$	$D_{2(p)}$
pq	$\mathbb{Z}_{pq}$	-
p^2	$\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$	-
p^3	$\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $\mathbb{Z}_p^3$	H_p, E_p

4.1. Primer Teorema de Sylow

Lema: Sea G un grupo **abeliano** finito. Si p es un primo y $p^k||G|$ entonces G tiene un subgrupo de orden p^k

Teorema de Sylow: Sea G un grupo finito. Si p es un primo y $p^k||G|$, entonces G tiene un subgrupo de orden p^k.
Dem:
Def. Sea G un grupo de orden $p^k m$, donde p no divide a m. Un p-subgrupo de Sylow de G es un subgrupo de orden p^k.

4.2. Segundo Teorema de Sylow

Sea G un grupo con $|G| = n$, donde $n = p_1^{a_i} \cdots p_k^{a^k}$ es la descomposición en primos de n. Estamos interesado en estudiar los subgrupos de G de orden p^b con b natural. Este tipo de subgrupos se llaman $p-$subgrupos de G. En la clase pasada probamos que para cada primo p_i, existe al menos un subgrupo H_i de orden $p_i^{a_i}$. Este tipo de subgrupos los llamaremos p_i-**subgrupos de Sylow**.

Comencemos considerando un grupo G finito de orden $p^k m$ tal que p no divide a m. Por el primero teorema de Sylow, sabemos que existe un subgrupo de Sylow. Es decir, un subgrupo P de G de orden p^k. Consideremos un subgrupo H de G de orden p^s.

Teorema: Sea G un grupo finito y p un primo divisor de $|G|$. Si P es un p-subgrupo de Sylow y H es un p-subgrupo de G, entonces existe $a \in G$ tal que $aHa^{-1} \leq P$.

Dem: Sea $X = \{gP | g \in G\}$. Sabemos que X es un $H-$conjunto bajo la acción $h \cdot (gP) := (hg)P$. Tenemos una partición $X = O_{x_1 P} \cup \cdots \cup O_{x_k P} \cup O_{x_{k+1} P} \cup \cdots \cup O_{x_m P}$ la cual la podemos escoger de manera que $x_1 P, ..., x_k P \notin X_f = \{gP \in X | hgP = gP \ \ \forall h \in H\}$. Entonces:

$$|X| = |X_f| + \sum_{i=1}^{k} [H : S(x_i P)]$$

Donde $S(xP) := \{h \in H \mid h \cdot xP = xP\}$.
Ahora notamos que $|X| = [G : P] = |G|/|P| = p^k m / p^k = m$,

Corolario (Segundo Teorema de Sylow): Sean G un grupo finito y p un primo que divide a $|G|$. Si P y P' son dos p-subgrupos de Sylow, entonces $a \in G$ tal que $P' = aPa^{-1}$

Definición: Sea G un grupo y p un primo que divide a $|G|$. Definimos el conjunto $Syl_p(G)$ como la familia de todos los p-subgrupos de Sylow.

Observación: Sean G un grupo y p un primo que divide a $|G|$. Entonces:

a) El teorema de Sylow nos dice que $Syl_p(G) \neq \emptyset$

b) Sea $P \in Syl_p(G)$. El segundo teorema de SYlow nos dice que $Syl_p(G) = \{aPa^{-1} \mid a \in G\}$

Corolario: Sean G un grupo finito y p un primo que divide a $|G|$. Si H es un p-subgrupo de G, entonces existe $P \in Syl_p(G)$ tal que $H \leq P$.

Corolario: Sean G un grupo finito, p un primo que divide a $|G|$ y $P \in Syl_p(G)$. Entonces $P \trianglelefteq G$ si y sólo si $Syl_p(G) = \{P\}$

Teorema: Sean G un grupo finito, p un primo que divide a $|G|$ y $K \trianglelefteq G$. Se cumplen los siguientes enunciados:

a) Sea $H \leq K$. Entonces $H \in Syl_p(K)$ si y sólo si existe $P \in Syl_p(G)$ tal que $H = P \cap K$.

b) Sea $K \leq H \leq G$. Entonces $H/K \in Syl_p(G/K)$ si y sólo si existe $P \in Syl_p(G)$ tal que $H = PK$

4.3. Tercer Teorema de Sylow

Def 26.1: Sea G un grupo finito y p un primo tal que $p||G|$. Denotamos por n_p al número de p-subgrupos de Sylow. Es decir, $n_p = |Syl_p(G)|$.

Sea G un grupo finito y $P \int Syl_p(G)$. El segundo teorema de Sylow nos dice que $Syl_p(G)$ es el conjunto de subgrupos conjugados de P. Es decir, $Syl_p(G) = \{aPa^{-1} \mid a \in G\}$. Este conjunto ya lo sabemos contar. Tenemos que $|\{aPa^{-1} | a \in G\} = [G : N(P)]$ donde $N(P) = \{g \in G | gPg^{-1} = P\}$ es el estabilizador de P. Por lo tanto:

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

Sean $X = Syl_p(G)$ y $P \in X$. Observamos que P actúa en X con la conjugación:

$$a \cdot Q = aQa^{-1}$$

El teorema de descomposición de órbitas dice que $X = O_{Q_1} \cup \cdots O_{Q_k} \cup O_{Q_{k+1}} \cup \cdots \cup O_{Q_m}$. De manera que $x_1, ..., x_k \in X_f$ y $x_{k+1}, \cdots, x_m \in X_f$. Donde $X_f = \{Q \in X | aQa^{-1} = Q \ \ \forall a \in P\}$. Entonces:

$$n_p = |X| = \sum_{i=1}^{m} [P : S(Q_i)] = |X_f| + \sum_{i=1}^{k} [P : S(Q_i)]$$

Observa que $1 < [P : S(Q_i)]$ para todo $Q_i \notin X_f$. Por lo tanto:

$$n_p = |X_f| + ps$$

Para $s \in \mathbb{N}$

Teorema 26.4: (Tercer Teorema de SYlow). Sea G un grupo de orden $p^k m$, donde p es un primo que no divide a m. Se cumple lo siguiente:

a) $n_p = [G : N(P)]$ para cualquier $P \in Syl_p(G)$

b) n_p divide a m

c) $n_p \equiv 1 \pmod p$

4.4. Todos los grupos de orden 12

Primero definimos un grupo Q_{2n} que es una generalización de los quaterniones. Definimos el **grupo dicíclico de orden 2n**: Sea $n = 2m$

$$Q_{2n} = \langle a, b | a^n = e, ab = ba^{-1}, b^2 = a^m \rangle$$

Teorema (Todos los grupos de orden 12): Todo rupo de orden 12 es isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2, A_4, D_{2(6)}, Q_{2(6)}$

Dem: Sea G un grupo de orden $12 = 2^2 3$. Sea n_2 el número de 2-subgrupos, entonces $n_2|(12/2^2) \Rightarrow n_2|3$. Además, $n_2 \equiv 1 \pmod 2$. Por lo tanto, tenemos que $n_2 = 1, 3$

Por otro lado, n_3 divide a $12/3 = 4$. Y $n_3 \equiv 1 \pmod 3$. Entonces, nos queda que $n_3 = 1, 4$. Analizamos las opciones.

a) $n_2 = 3, n_3 = 4$:
Tenemos 4 3-subgrupos de Sylow. A saber, P_1, P_2, P_3, P_4. Observamos que estos grupos se intersectan solamente en el trivial (sino serían iguales). Entonces, tenemos que $|P_1 \cup P_2 \cup P_3 \cup P_4| = 12 - 4 = 8$.
Esto implica que G tiene 9 elementos de orden 1 o 3. Y tiene tres elementos x, y, z de otro orden. Entonces, como los 2-subgrupos de Sylow son de orden 4, se sigue que $\{e, x, y, z\}$ debe de ser el único 2-subgrupo de Sylow.

b) Sea $n_2 = 1, n_3 = 1$. Tenemos un único 2-subgrupo de Sylow normal P, y un único 3-subgrupo de Sylow normal Q. Entonces $G = PQ \simeq P \times Q$. Entonces, como $|P| = 4, P \simeq \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$. Por lo tanto, tenemos que $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

c) Sea $n_2 = 3, n_3 = 1$. Observamos

4.5. Producto Semidirecto

Hasta ahora, empezamos con un grupo G y descomponemos su orden en primos como $|G| = p_1^{a_1} \cdots p_k^{a_k}$. Y luego encontramos las cantidades de todos los p-subgrupos de Sylow. Sin embargo, no tenemos una estrategia clara para esa parte.

Teorema: Sean $H_1, ..., H_k$ subgrupos de G. Los siguientes enunciados son equivalentes:

- $G \simeq H_1 \times \cdots \times H_k$
- Para todo $g \in G$, existe un único $(h_1, ..., h_k) \in H_1 \times \cdots \times H_k$ tal que $g = h_1 \cdots h_k$ y $H_i \trianglelefteq G \ \forall i$
- $G = H_1 \cdots H_k$, $H_i \cap (\Pi_{j \neq i} H_j) = \{e\} \ \forall i$, y $h_i h_j = h_j h_i \ \forall h_i \in H_i$ y $\forall h_j \in H_j$

El caso en que todos los subgrupos de Sylow son todos normales, entonces se puede usar este teorema y encontrar el grupo isomorfo a G muy fácil.

Sin embargo, si no todos los n_i son 1, se complica la cosa.

Proposición 29.3 Sea G un grupo, $H \trianglelefteq G$ y $K \leq G$ tales que $KH = G$ y que $H \cap K\{e\}$. Consideramos el morfismo $\sigma : K \to Aut(H)$, $k \to \sigma_k$ con $\sigma_k(h) = khk^{-1}$. Entonces,se cumplen los siguientes enunciados:

- El conjunto $H \times K$ con la operación binaria:

$$(h_0, k_0) * (h_1, k_1) = (h_0 \cdot \sigma_{k_0}(h_1), k_0 \cdot k_1)$$

  Es un grupo que denotamos por $H \rtimes_\sigma K$

- $G \simeq \rtimes_\sigma K$

Producto interno semidirecto: Sea H un grupo y H, K subgrupos de G. Diremos que G es el **producto interno semidirecto de H y K** si $G = HK$, $H \cap K = \{e\}$ y $H \trianglelefteq G$. Lo escribimos como $G = H \rtimes K$

Teorema 29.7 Sean H, K grupos. Consideramos el morfismo de grupos $\phi : K \to Aut(H)$, $k \to \phi_k$. Se cumplen los siguientes enunciados:

a) El conjunto $H \times K$ con la operación binaria:

$$(h_0, k_0) * (h_1, k_1) = (h_0 \cdot \phi_{k_0}(h_1), k_0 \cdot k_1)$$

- Los conjuntos $H_0 = H \times \{e_K\}, K_0 = \{e_H\} \times K$ son subgrupos de $H \rtimes_\phi K$ tales que $H \rtimes_\phi K = H_0 \rtimes K_0$

Decir que $G \simeq P \rtimes Q$ quiere decir que G tiene los elementos de $P \times Q$ pero que no tiene la operación tal cual de $P \times Q$. Esto porque solamente P es normal pero Q no.

Def (Producto Semidirecto): Sean H, K grupos y $\phi : K \to Aut(H)$, $k \to \phi_k$, un morfismo de grupos. El **producto semidirecto entre H, K vía ϕ** denotado como $H \rtimes_\phi K$ es el grupo definido por el conjunto $H \times K$ con la operación binaria $(h_0, k_0) * (h_1, k_1) = (h_0 \cdot \phi_{k_0}(h_1), k_0 \cdot k_1)$

Lema: Sea $n \in \mathbb{N}$ mayor que 2. Entonces $Aut(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$

Donde $\mathbb{Z}_n^*$ indica todos los elementos de $\mathbb{Z}_n$ que son coprimos con n y es el grupo multiplicativo, por lo que son de orden n. Esto porque $Aut(\mathbb{Z}_n) = \{f_a | (a, n) = 1, a \in \{0, 1, ..., n-1\}\}$. Con $f_a(\overline{x}) = a\overline{x}$.

Lema 30.3: Sea p un primo mayor que 2. Entonces $Aut(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$.
Esto porque $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$ (se puede probar que tiene el mismo número de elementos y que es cíclico).

Teorema 30.5: Sean p, q primeos distintos tales que $p < q$. Se cumple lo siguiente:

- El único morfismo $\mathbb{Z}_q \to Aut(\mathbb{Z}_p)$
- Si $q \not\equiv 1 \ (mod\ p)$, el único morfismo $\mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ es el trivial.
- Si $q \equiv 1 \ (mod\ p)$, existe exactamente p morfismos $\mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ incluyendo al trivial. Más aún, dado un morfismo $\phi : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ no trivial, tenemos que $\phi_1, ..., \phi_{p-1}$ son todos los morfismos no triviales $\mathbb{Z}_p \to Aut(\mathbb{Z}_q)$, los cuales están definidos como $\phi_i(\bar{a}) = (\phi(\bar{a}))^i$

Se dice **producto semidirecto trivial** a $H \rtimes_{\phi_0} K$ cuando $\phi_0 : K \to Aut(H)$, $k \to Id_H$. Entonces:

Lema 30.7 Sean p, q primos distintos tales que $p < q$:

- El único producto semidirecto $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$ es el trivial.
- Si $q \not\equiv 1 \ \ (mod\ p)$, entonces el único producto semidirecto $\mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$ es el trivial.
- Si $q \equiv 1 \ (mod\ p)$, entonces existen productos semidirectos $\mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$ no triviales. Mas áun, los producto semidirectos no triviales son isomorfos.

Teorema 30.9: Sea G un grupo de orden pq, donde p, q son primos tales que $p < q$.

- Si $q \not\equiv 1 \ (mod\ p)$ entonces $G \equiv \mathbb{Z}_p \times \mathbb{Z}_q$
- Si $q \equiv 1 \ (mod\ p)$ entonces $G \equiv \mathbb{Z}_p \times \mathbb{Z}_q$, o $G \simeq \mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$.

Corolario 30.10: Sean p, q primos tales que $p < q$ y que $q \equiv 1 \ \ (mod\ p)$. Consideramos un grupo G isomorfo al producto semidirecto no trivial $G \simeq \mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$. Entonces, existen exactamente p elementos $r \in \{1, 2, ..., q-1\}$ tales que $r^p \equiv 1 \ (mod\ q)$. Más aún, para cada $m \in \{2, ..., q-1\}$ tal que $m^p \equiv 1 \ (mod\ q)$ existen $a, b \in G$ tales que:

$$G = \langle x, y | x^q = y^p = e, xy = yx^m \rangle$$

Teorema de Schur: Sea G un grupo. Si G admite un subgrupo normal abeliano K tal que $|K|$ y $|G/K|$ son primos relativos, entonces G admite un subgrupo de orden $|G/K|$. Más aún, en tal caso existe $H \leq G$ tal que $G = K \rtimes H$.

Teorema de Schur-Zassenhaus Sea G un grupo de orden kn con $(k, n) = 1$. Si G admite un subgrupo normal K de orden k, entonces existe $H \leq G$ de orden n de manera que $G = K \rtimes H$

$\lvert G\rvert$	G abeliano	G no abeliano	condiciones adicionales
2	$\mathbb{Z}_2$	-	
3	$\mathbb{Z}_3$	-	
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	-	
5	$\mathbb{Z}_5$	-	
6	$\mathbb{Z}_6$	$D_{2(3)}$	
7	$\mathbb{Z}_7$	-	
8	$\mathbb{Z}_{2^3}, \mathbb{Z}_{2^2} \times \mathbb{Z}_2, \mathbb{Z}_2^3$	$D_{2(4)}, Q_8$	
9	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	-	
10	$\mathbb{Z}_2 \times \mathbb{Z}_5$	$D_{2(5)}$	
11	$\mathbb{Z}_{11}$	-	
12	$\mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$A_4, D_{2(6)}, Q_{2(6)}$	
13	$\mathbb{Z}_{13}$	-	
14	$\mathbb{Z}_2 \times \mathbb{Z}_7$	$D_{2(7)}$	
15	$\mathbb{Z}_3 \times \mathbb{Z}_5$	-	
16	$\mathbb{Z}_{16}, \mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_2^2 \times \mathbb{Z}_4, \mathbb{Z}_2^4, \mathbb{Z}_4^2$	$D_{2(8)}, Q_{2(8)}, Q_8 \rtimes \mathbb{Z}_2, \mathbb{Z}_8 \rtimes_3 \mathbb{Z}_2, G_1, \mathbb{Z}_2^2 \rtimes \mathbb{Z}, \mathbb{Z}_4 \rtimes \mathbb{Z}_4, \mathbb{Z}_2 \times D_{2(4)}, \mathbb{Z}_2 \times Q_8$	
17	$\mathbb{Z}_{17}$	-	
18	$\mathbb{Z}_{18}$	$D_{2(9)}, \mathbb{Z}_3 \rtimes S_3, \mathbb{Z}_3 \rtimes \mathbb{Z}_6, \mathbb{Z}_3 \rtimes S_3$	
19	$\mathbb{Z}_{19}$	-	
20	$\mathbb{Z}_{20}, \mathbb{Z}_2 \times \mathbb{Z}_{10}$	$D_{2(10)}, F_5, Q_{2(10)}$	
21	$\mathbb{Z}_{21}$	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	
$2p$	$\mathbb{Z}_{2p}$	$D_{2(p)}$	
pq	$\mathbb{Z}_{pq}$	$\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$	$q \overset{p}{\equiv} 1$ p, q primos
pq	$\mathbb{Z}_{pq}$	-	$q \overset{p}{\not\equiv} 1$ p, q primos
p^2	$\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p$	-	p primo
p^3	$\mathbb{Z}_{p^3}, \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \mathbb{Z}_p^3$	H_p, E_p	p primo

5. T.F. Grupos Abelianos Finitos

5.1. p-Grupos Abelianos Finitos

Denotamos por $C = \langle x \rangle$ al grupo cíclico infinito. Y $C_n = \{e, x, x^2, \cdots, x^{n-1}\}$ al grupo cíclico de orden n.

Proposición 32.2: Sea G un grupo abeliano finito de orden n y $n = p_1^{a_1} \cdots p_k^{a_k}$ su descomposición en primos. Se cumple:

a) Existe un único $P_i \leq G$ de orden $p_i^{a_i}$

- $P_i \trianglelefteq G$
- $G \simeq P_1 \times P_2 \times \cdots \times P_k$

Dem: Por el teorema de Sylow 1, sabemos que existe P_1. Como G es abeliano, entonces P_i es normal en G y por tanto, es el único grupo de este orden. La parte c) se sigue de que la intersección de dos grupos es trivial y del producto y así.

Hecho lo anterior, sólo nos queda determinar todos los $p-$grupos finitos abelianos.

Proposición 32.4: Sea G un p-grupo abeliano finito de orden p^n. Entonces existen $a_1, \cdots, a_r \in \mathbb{N}$ tales que $a_1 \geq a_2 \geq \cdots \geq a_r \geq 1$, $n = a_1 + \cdots + a_r$ y $G \simeq C_{p^{a_1}} \times \cdots \times C_{p^{a_r}}$

Dem: Inducción.

Por ejemplo, si tenemos un grupo de orden p^5. Entonces, es isomorfo a uno de los siguientes (se consigue encontrando las formas de sumar 5):

- $C_p \times C_p \times C_p \times C_p \times C_p$
- $C_p \times C_p \times C_p \times C_{p^2}$
- $C_p \times C_{p^2} \times C_{p^2}$
- $C_p \times C_p \times C_{p^3}$
- $C_{p^2} \times C_{p^3}$
- $C_p \times C_{p^4}$
- C_{p^5}

5.2. Grupos Abelianos Finitos

En la clase pasada vimos que cada grupo abeliano de orden p^k se puede identificar con una sucesión de naturales $a_1 \geq a_2 \geq \cdots \geq a_s \geq 1$ tal que $k = a_1 + \cdots + a_s$. Y $G \simeq C_{p^{a_1}} \times \cdots C_{p^{a_s}}$

Lema 33.1: Sean m, n naturales. Entonces $(m, n) = 1$ sii $C_{mn} = C_m \times C_n$

Prop 33.5: Sea G un grupo abeliano finito. Entonces existe una sucesión finita de números naturales $n_1, \cdots, n_s$ donde n_i divide a n_j para $i > j$. Y $n = n_1 n_2 \cdots n_s$. Tal que $G \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$

Ejemplo 33.6. Sea $G = C_{3^2} \times C_{3^3} \times C_5 \times C_5 \times C_5 \times C_{7^4}$. Encuentra una sucesión finita de números naturales $n_1, \cdots, n_s$, donde n_i divide a n_j para todo $i > j$ y $|G| = n_1 n_2 \cdots n_s$, tal que $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$.

Solución. Ya tenemos expresado el grupo como el producto de sus subgrupos de Sylow. Para encontrar la expresión deseada podemos visualizar el procedimiento de la demostración anterior de la siguiente manera. Tenemos

$$\begin{aligned} G = & C_{3^3} \times C_{3^2} \\ & C_5 \times C_5 \times C_5 \\ & C_{7^4}. \end{aligned}$$

Llenando con factores triviales tenemos

$$\begin{aligned} G = & C_{3^3} \times C_{3^2} \times \{e\} \\ & C_5 \times C_5 \times C_5 \\ & C_{7^4} \times \{e\} \times \{e\}. \end{aligned}$$

Ahora, haciendo un reacomodo, que podríamos llamar *cambiar columnas por renglones*, obtenemos

$$\begin{aligned} G = & C_{3^3} \times C_5 \times C_{7^4} \\ & C_{3^2} \times C_5 \times \{e\} \\ & \{e\} \times C_5 \times \{e\}. \end{aligned}$$

Finalmente, agrupando por renglones y aplicando 33.2, podemos concluir que

$$G = (C_{3^3} \times C_5 \times C_{7^4}) \times (C_{3^2} \times C_5 \times \{e\}) \times (\{e\} \times C_5 \times \{e\}) = C_{3^3 \cdot 5 \cdot 7^4} \times C_{3^2 \cdot 5} \times C_5.$$

□

Def: Sea G un grupo abeliano finito y $n_1, \cdots, n_s$ una sucesión de naturales > 1 tales que n_i divide n_j para todo $i > j$. Diremos que G es de tipo $(n_1, \cdots, n_s)$ si $G \simeq C_{n1} \times \cdots \times C_{n_s}$

Prop 33.9: Sea p un primo y G un grupo abeliano finito. Se cumplen:

a) El conjunto $G_p = \{x \in G \mid |x| = 1, p\}$ es un subgrupo de G.

b) El conjunto $G^p]\{x^p | x \in G\}$ es un subgrupo de G.

c) Si G es un p-grupo de tipo $(p^{a_1}, \cdots, p^{a_r})$, entonces G_p es de tipo $(p, p, \cdots, p)$, $|G_p| = p^r$ y G^p es de tipo $(p^{a_1-1}, \cdots, p^{a_r-1})$

Prop 33.11 Sea G abeliano finito. Entonces existe una única sucesión finita de naturales $n_1, \cdots, n_k$ tal que G es de tipo $(n_1, \cdots, n_k)$

5.3. Grupos Abelianos Finitamente Generados

Def: Sea G un grupo abeliano, el grupo:

$$\tau G := \{x \in G \mid |x| < \infty\}$$

llamado, **componente de torsión** de G. es un subgrupo. En caso de que $G = \tau G$, diremos que G es un **grupo de torsión**. En caso de que $\tau G = \{e\}$, diremos que es un **grupo libre de torsión**.

Teorema 34.3: Sea G un grupo abeliano. Entonces, $G/\tau G$ es libre de torsión.

Lo que nos prueba que el estudio de G se puede partir en el estudio de τG (que es de torsión) y el $G/\tau G$ que es libre de torsión.

Rango de un grupo: Definimos el rango de G como:

$$rank(G) = \text{mín}\{|X| \mid \langle X \rangle = G\}$$

Es el número de elementos mínimos para generar a G.

Teorema Fundamental de GRupos abelianos finitamente generados:
Sea G un grupo finitamente generado. Entonces, se cumple:

a) $G \simeq (\tau G) \times (G/\tau G)$

b τG es un grupo abeliano finito de tipo $(n_1, \cdots, n_r)$

c) $G/\tau G \simeq \mathbb{Z}^s = \mathbb{Z} \times \cdots \times \mathbb{Z}$

d) $rank(G) = r + s$

Para grupos de rango finito no se cumple.

5.3.1. Grupos Divisibles

Sea G abeliano y $x \in G$.

- Decimos que x es **divisible** si para todo $n \in \mathbb{N}$ existe $y \in G$ tal que $y^n = x$
- Si todo elemento de G es divisible, decimos que G es **divisible**
- Para grupos aditivos, esto se ve como que x es divisible si para todo $n \in \mathbb{N}$ existe $y \in G$ tal que $ny = x$

Prop: Sea G un grupo abeliano. Si D es un subgrupo divisible de G, entonces existe un subgrupo $Y \leq G$ tal que $G = D \times Y$

Reducido: Sea G abeliano. Si G no tiene subgrupos divisibles, decimos que es reducido.

Teorema: Sea G abeliano:

a) Existe un subgrupo divisible maximal dG.

b) Existe un subgrupo reducido $R \leq G$ tal que $G = dG \times R$

Suma directa: Dado $\{A_i\}_{i \in I}$ una familia de grupos. Definimos $\otimes_{i \in I} A_i$ como el subgrupo con todas las I- adas $(x_i)_{i \in I} \in \Pi_{i \in I} A_i$ tales que casi todo x_i es el neutro.
Si $A_i = A$, entonces denotamos $\otimes A_i = A^{(I)}$

Teorema: Sea G abeliano.

a) Si G es libre de torsión, entonces $dG \simeq \mathbb{Q}^{(X)}$ para algún conjunto X

b) Si G es de torsión, entonces $dG \simeq \otimes_{p \in P} C_{p^\infty}^{X_p}$

c) En general, $dG = \mathbb{Q}^{(X)} \times \otimes_{p \in P} C_{p^\infty}^{X_p}$

6. Series Normales

6.1. Teorema de Jordan-Holder

Ya que descompusimos a los grupos abelianos, ahora intentaremos descomponer los grupos no abelianos.

Dado un grupo G podemos considerar los morfismos:

$$N \to_i G \to_p Q$$

Donde N es un subgrupo normal de G y Q es G/N.
$i : N \to G$ es la inclusión dada por $n \to_i n$
$p : G \to G/N$ es la proyección $g \to_p gN$

Si G es un grupo, se puede deducir información a partir de N y G/N. Pero puede ser que $N, G/N$ sean digíciles de estudiar, en ese caso, necesitamos la cadena:

$$\{e\} \trianglelefteq G_{k+1} \trianglelefteq G_k \trianglelefteq G_{k-1} \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$$

De esta manera, podemos deducir información de G_{k-1} a partir de G_k y de $Q_k := G_{k-1}/G_k$. Con esto podemos deducir información de G_{k-2} a través de G_{k-1} y de $Q_{k-1} := G_{k-2}/G_{k-1}$. Y así hasta llegar a G.

Def 35.1: Sea G un grupo, una **cadena subnormal** de subgrupos:

$$\{e\} \subset G_{k+1} \subset G_k \subset G_{k-1} \subset \cdots \subset G_2 \subset G_1 \subset G_0 = G$$

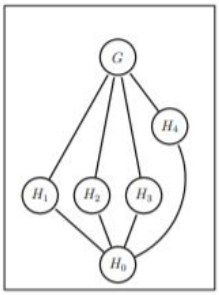
tal que $G_{k+1} \trianglelefteq G_i$.
Si $G_i \trianglelefteq G$ para todo i, se llama **serie normal**.
En cualquier caso, el cociente $Q_i := G_{i-1}/G_i$ es el i-**ésimo factor de la serie**

Intuitivamente puedes visualizar esta idea como que los grupos son torres que vamos construyendo con ladrillos, donde los ladrillos con los factores. Si nos ayudamos con un diagrama de la retícula de subgrupos, entonces podemos pensar a las series subnormales como los caminos que van del subgrupo trivial $\{e\}$ al grupo total G tales que cada vértice representa un subgrupo normal del vértice que sigue, y a las series normales como los caminos donde cada vértice representa un subgrupo normal de G.

Veamos algunos ejemplos.

Ejemplo 35.3.

(a)



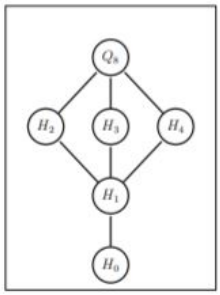
Comencemos considerando el grupo S_3. Recordemos que en 11.1.(b) describimos la retícula de subgrupos de este grupo. Observamos que el único subgrupo normal es $H_4 = \langle (1\,2\,3) \rangle$. Por lo tanto, la única serie subnormal de S_3 es

$$\{e\} \subseteq H_4 \subseteq G$$

y los factores de la serie son $Q_1 = G/H_4 \cong C_2$ y $Q_2 = H_4 \cong C_3$.
Cabe hacer notar que, para C_6 podemos construir dos series normales con los mismos factores. En efecto, considera

$$\{e\} \subseteq \langle x^2 \rangle \subseteq C_6 \text{ y } \{e\} \subseteq \langle x^3 \rangle \subseteq C_6.$$

(b) Consideremos el grupo de los cuaternios Q_8 (ver 12.1(c)). Recordemos que todos los subgrupos de Q_8 son normales. Por lo tanto, todas las cadenas que escojamos serán series normales. Más aún, notemos que existen tres series normales tales que todos los factores son isomorfos a C_2. En efecto, las series son

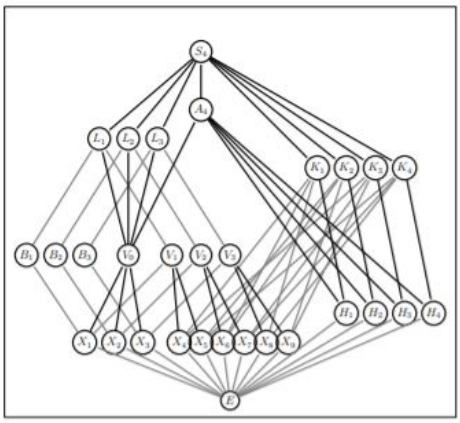


$$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq Q_8$$
$$\{e\} = H_0 \subseteq H_1 \subseteq H_3 \subseteq Q_8$$
$$\{e\} = H_0 \subseteq H_1 \subseteq H_4 \subseteq Q_8.$$

(c) Por último consideremos el grupo simétrico S_4 (ver clase 14). Notemos que los únicos subgrupos normales de S_4 son A_4 y V_0. Por lo tanto, las únicas series normales son

$$\{e\} \subseteq V_0 \subseteq S_4$$
$$\{e\} \subseteq A_4 \subseteq S_4$$
$$\{e\} \subseteq V_0 \subseteq A_4 \subseteq S_4.$$

En la primera tenemos los factores $S_4/V_0 \cong S_3$ y $V_0 \cong C_2^2$.



(d) En el inciso anterior mostramos que S_4 sólo tiene tres series normales. Sin embargo, no es difícil mostrar que tiene muchas series subnormales. Tantas que podemos mostrar tres series normales tales que sus factores son grupos cíclicos de orden primo. A saber, esas series son las siguientes

$$\{e\} \subseteq X_1 \subseteq V_0 \subseteq A_4 \subseteq S_4$$
$$\{e\} \subseteq X_2 \subseteq V_0 \subseteq A_4 \subseteq S_4$$
$$\{e\} \subseteq X_3 \subseteq V_0 \subseteq A_4 \subseteq S_4.$$

6.1.1. El teorema de Jordan Holder

Grupo Simple: Es un grupo G con únicos subgrupos normales $\{e\}$ y G

Serie de Composición: Sea G un grupo. Diremos que una serie subnormal:

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_2 \subset G_1 \subset G_0 = G$$

es una **serie de composición** si todo factor es un grupo simple. En tal caso n es la **longitud de la serie de composición**.

Teorema 35.8 Jordan Holder: Sea G un grupo que admite una serie de composición. Entonces, todas las series de composición de G tienen la misma longitud y mismos factores (tal vez en distinto orden)

Esto ha impulsado al programa Holder, un plan para encontrar todos los grupos finitos. Consiste en:

a) Probar que todos los grupos finitos admiten una serie de composición

b) Clasificar todos los grupos simples

c) Dado un grupo simple finito S y un grupo finito H. Encontrar todos los grupos G que admiten un subgrupo normal N isomorfo a H tal que G/N es isomorfo a S.

El paso b) se logró tras mucho trabajo y se llegó a que:

Teorema: Los grupos simples se pueden clasificar en 18 familias infinitas, más 26 grupos simples que no entran en las familias anteriores.

6.1.2. El grupo alternante:

El grupo alternante A_n se define como el subgrupo de S_n conformado por todas las permutaciones pares. Que son las que se expresan como el producto de un número par de transposiciones.

Prop: Si $|G| = 60$ y G tiene más de un 5- subgrupos de Sylow, entonces G es simple.

- Observamos que por el tercer teorema de Sylow eso implica que $n_5 = 6$.
  Suponemos que H es un subgrupo normal propio no trivial de G. Tenemos dos casos:
  - **Caso 1:** 5 divide a $|H|$. En este caso H contiene los 6 5-subgrupos de Sylow. Como no se intersectan, estos son 25 elementos. Por lo que $|H| = 30$. Sin embargo, para $|H| = 30$, tenemos que el número de 5-subgrupos de Sylow es un divisor de 15. Lo que contradice que H contiene 6 5-subgrupos de Sylow.
  - **Caso 2:** 5 no divide a $|H|$... contradicción.

Teorema: A_n es simple $\forall n \geq 5$.
Se puede demostrar por inducción.

6.2. Grupo Lineal Proyectivo

Def: Sea k un campo. Definimos el **grupo de matrices escalares de** $n \times n$ sobre k como $Z_n(k)$, como el grupo de las matrices $A \in SL_n(k)$ tales que $A = \lambda I_n$ donde $\lambda \in k$.
Definimos el **grupo especial lineal proyectivo de** $n \times n$ **sobre** k denotado como $PSL_n(k)$ como el grupo cociente $SL_n(k)/Z_n(k)$.

Estos grupos forman una familia de grupos simples.

Prop 37.7: Sea G un grupo finito con $|G| > 1$. Entonces, G admite una serie de composición.

6.3. Grupos Solubles

Grupo Soluble: Es un grupo que admite una serie de la forma:

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

Donde cada uno de los grupos es normal en el siguiente y los factores son abelianos.
Por el principio de buen orden, existe una serie de longitud mínima k y en tal caso diremos que G es **un grupo de longitud** k.

- Todos los grupos abelianos son solubles (se toma la serie trivial)
- Si G es un grupo no abeliano y simple, no es soluble (pues se toma la serie trivial y el factor es isomorfo a G).
  Los A_n con $n \geq 5$ son ejemplos de esto.

Definición:

- **Conmutador de** G es el subgrupo $G' = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$
- Definimos los siguientes subgrupos:
  - $G^{(0)} := G$
  - $G^{(1)}$ el **primer derivado de** G es el conmutador de G
  - $G^{(n)}$ es el **nésimo derivado de** G, el conmutador de $G^{(n-1)}$
- Observamos que la serie:

$$\cdots \subset G^{(n)} \subset G^{(n-1)} \subset \cdots \subset G^{(1)} \subset G^{(0)} = G$$

Si existe un $G^{(n)}$ que sea igual a $\{e\}$, la serie derivada muestra que G es soluble.

Teorema: G es soluble sii existe $n \geq 0$ tal que $G^{(n)} = \{e\}$

Teorema: Si G es un grupo soluble, entonces todo subgrupo y todo cociente de G es soluble

Teorema: Sean G un grupo y $K \trianglelefteq G$. Entonces, G es soluble sii $K, G/K$ son solubles.

Teorema: Las siguientes condiciones son equivalentes para un grupo finito G:

a) G es soluble

b) Los factores de composición de G son abelianos

c) $H' \neq H$ para todo $\{e\} \neq H \leq G$

Teorema:

- **Teorema de Burnside:** Si $|G| = p^a q^b$, con p, q primos, entonces G es soluble
- **Teorema de Frobenius:** Si n^2 no divide a $|G|$ para todo $n \neq 1$, entonces G es soluble
- **Teorema de Feit-Thompson:** Si$|G|$ es impar, entonces G es soluble
- **Teorema de Hall:** Si $|G| = nm$ con $(n, m) = 1$ y G es soluble, entonces se cumplen los siguientes enunciados:

  a) Existe un subgrupo H de orden n

  b) Todo subgrupo de orden n es conjugado a H

  c) Si $k|n$ y K es un subgrupo de orden k, entonces $K \leq xHx^{-1}$ para algún $x \in G$

6.4. Grupos Nilpotentes

En la clase pasada vimos que podemos encontrar una serie subnormal llamada **serie derivada** como:

$$\cdots \subset G^{(n)} \subset G^{(n-1)} \subset \cdots \subset G^{(1)} \subset G^{(0)} = G$$

De tal manera que G es **soluble** sii $G^{(n)} = \{e\}$ para algún $n \geq 0$.

Serie Central Descendente
Definimos los conmutadores superiores como:

a) $\Gamma_0(G) = G$

b) Para $n \geq 0$, $\Gamma_n(G) = \langle aba^{-1}b^{-1} \mid a \in \Gamma_{n-1}(G)\ , b \in G \rangle$

Con lo que se puede construir la **serie central descendente:**

$$\cdots \subset \Gamma_n(G) \subset \Gamma_{n-1}(G) \subset \cdots \subset \Gamma_1(G) \subset \Gamma_0(G) = G$$

Que resulta ser una serie normal con factores abelianos.

Centralizadores Superiores de G:
Definimos como:

a) $Z_0(G) = \{e\}$

- Para $n > 0$, $Z_n(G)$ es el único subgrupo normal que contiene a $Z_{n-1}(G)$ y satisface que:

$$Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$$

Donde $Z(H) = \{x \in H \mid xy = yx \ \ \forall y \in H\}$

Esto nos da la **serie central ascendente o inferior** definida como:

$$\{e\} = Z_0(G) \subset Z_1(G) \subset Z_2(G) \subset \cdots \subset Z_n(G) \subset Z_{n+1}(G) \subset \cdots$$

Que resulta ser una serie con factores abelianos.

Definición: Sea G un grupo:

a) Definimos $[a, b] := aba^{-1}b^{-1}$ para todo $a, b \in G$

b) $[H, K] = \langle [h, k] \mid h \in H \ , \ k \in K \rangle$

En particular notamos que $G' = [G, G] = \Gamma_1[G]$ y que $\Gamma_n(G) = [\Gamma_{n-1}(G), G]$

Lema: Sean $H, K \leq G$. Entonces:

a) $[H, K] = [K, H]$

b) Si $H \trianglelefteq G, K \trianglelefteq G \ \Rightarrow \ [H, K] \trianglelefteq G$

c) $H \trianglelefteq G$ sii $[H, G] \subset G$

d) $K \leq H \leq G \ , \ K \trianglelefteq G$. Entonces $H/K \subset Z(G/K)$ sii $[H, G] \leq K$

Teorema: Los siguientes enunciados son equivalentes para un grupo G y un entero $n \geq 0$

a) $\Gamma_n(G) = \{e\}$

b) $Z_n(G) = G$

c) Existe una serie normal:

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

Tal que $G_i/G_{i+1} \subset Z(G/G_{i+1})$

Nilpotente de Clase n: Sea G un grupo y $n \geq 0$. Diremos que G es nilpotente de clase n si satisface las condiciones del teorema anterior.

Teorema: Sea G nilpotente. Entonces, todo subgrupo y todo cociente de G es nilpotente.

Teorema: Sea G un grupo , $K \subset Z(G)$. Si G/K es nilpotente, entonces G es nilpotente.

Teorema: Sean $G_1, \cdots, G_n$ nilpotentes, entonces $G_1 \times \cdots \times G_n$ es nilpotente.

Teorema: Teorema de Burnside Wielandt. Sea G un grupo no trivial, los siguientes enunciados son equivalentes:

a) G es nilpotente

b) $N(H) \neq H$ para todo subgrupo propio $H \leq G$

c) Todo subgrupo maximal es normal en G

d) Todo subgrupo de Sylow de G es normal en G

e) G es isomorfo al producto de todos sus subgrupos de Sylow