Súper Resumen Álgebra Moderna

Tomás Ricardo Basile Álvarez
316617194

6 de enero de 2021

1. Grupos y Morfismos

Grupo: Es un conjunto G con una operación binaria asociativa, cerrada, con neutro y con inversos.
Se dice **abeliano** si la operación es conmutativa.

- **Ej 1, Enteros módulo n:** $\mathbb{Z}_n$ son las clases de congruencia $\bar{a} = \{a + kn | k \in \mathbb{Z}\}$ con la suma $\bar{a} + \bar{b} = \overline{a + b}$ (abeliano y orden n)
- **Ej 2: Enteros multiplicativos:** $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$ con la multiplicación $\bar{a}\bar{b} = \overline{ab}$ (abeliano y orden $\phi(n)$)
- **Ej 3 Matrices invertibles:** $GL_n(\mathbb{R})$: Conjunto de matrices de $n \times n$ invertibles con entradas en $\mathbb{R}$. con el producto. (No abeliano)

1.0.1. Propiedades Básicas

- El neutro y el inverso son únicos
- $(a^{-1})^{-1} = a \quad , \quad (ab)^{-1} = b^{-1}a^{-1}$
- Dados, $a, b \in G$, existe! $x, y \in G$ tal que $ax = b$ y que $ya = b$
- Si $au = bu \;\; \Rightarrow \;\; a = b$. Si $va = vb \;\Rightarrow\; a = b$

Notación: Definimos $a^0 := e$, $a^n := a \cdot (a^{n-1})$, $a^{-n} := (a^n)^{-1}$

Generado: El generado por $a, b \in G$ es $\langle a, b \rangle =$ todos los elementos de la forma $a^k b^j$.

Orden: El orden de $x \in G$ es el mínimo entero positivo n tal que $x^n = 1$
Si $|x| = n$, entonces $x^m = x^q$ sii $m \equiv q \;\; mod(n)$. Lo que implica que x sólo se anula al subirlo a potencias múltiplos de n.

Subgrupo: $H \leq G$ es un subgrupo si $H \subset G$ y H es un grupo. Se puede probar que si $H \subset G$ es cerrado bajo producto y inversión, entonces es un subrupo.

1.0.2. Grupos Diédricos

Es el grupo:

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

Entonces:

$$D_{2n} = \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}$$

Se cumplen las propiedades:

- $sr^k = r^{n-k}s$

No es abeliano. r tiene orden n y s tiene orden 2.

1.0.3. Grupo Simétrico

El **grupo simétrico en** X es S_X el grupo formado por todas las biyecciones $\phi : X \to X$ con la operación de composición.
En particular, S_n son las biyecciones entre $X = \{1, \cdots, n\}$ y se ve que $|S_n| = n!$

Ciclo: Un ciclo $(a_1\ a_2\ \cdots\ a_k)$ con $a_i \in \{1, \cdots, n\}$ es un elemento de S_n que hace $a_i \to a_{i+1}$ y que $a_k \to a_1$.
Son el tipo de permutaciones más sencillas.
Dos ciclos son disjuntos si no comparten ningún elemento.
Dos ciclos disjuntos conmutan, pero en general no es abeliano

Órbita: La órbita de un $p \in \{1, \cdots, n\}$ bajo α son todos los elementos
$O_p = \{p, \alpha(p), \alpha^2(p), \cdots\}$

Teorema: Toda permutación se expresa como composición de ciclos disjuntos.

1.0.4. Grupo Matricial

Es el grupo $GL_n(k)$ de todas las matrices de orden $n \times n$ invertibles con entradas en k, donde k es un campo.
No es conmutativo en general.

El conjunto SL_n es el subgrupo de matrices con determinante 1.

1.0.5. Grupo quaternones

El grupo es:

$$Q_8 = \{E, -E, I, -I, J, -J, K, -K\}$$

Con las operaciones $I^2 = J^2 = K^2 = -E$, $IJ = K, JK = I, KI = J$, $JI = -K, KJ = -I, IK = -J$

1.0.6. Morfismos

Tablas de Cayley de G: Es una tabla con todos los productos entre elementos de G. Contiene toda la información del grupo

Morfismo: Sean $(G, \star), (H, *)$ grupos. Un morfismo de G a H es una función $\phi : G \to H$ con:

$$\phi(x \star y) = \phi(x) * \phi(y)$$

Se llama **isomorfismo** si $\phi : G \to H$ es un morfismo biyectivo. Entonces G, H son isomorfos y se pone $G \simeq H$.
Si $\phi : G \to H$ es un isomorfismo, entonces la inversa $\phi^{-1} : H \to G$ es un isomorfismo.

Teorema:

a) Si $f : G \to H, g : H \to K$ son morfismos, entonces gf es un morfismo

b) Si $f : G \to H$ es un morfismo, entonces $f(e_G) = e_H$

c) Si $a \in G$, entonces $f(a^{-1}) = f(a)^{-1}$

c) Si $n \in \mathbb{Z}$, entonces $f(a^n) = f(a)^n$

2. Teoremas de Isomorfismos

Subgrupos: Un subgrupo $H \leq G$ es un subconjunto de G que es además un grupo.
Para probar que $H \leq G$ hay que probar que $\emptyset \neq H \subset G$ y que H es cerrado bajo producto y bajo inversos. Si G es finito, es suficiente con probar lo de cerrado bajo productos.

Núcleo: El núcleo de un morfismo $f : G \to H$ se define como:
$K_f = \{a \in G \mid f(a) = e_H\}$.
Y es un subgrupo de G.

Imagen: La imagen de un morfismo $f : G \to H$ es el conjunto:
$Im(f) = \{f(a) \in H \mid a \in G\}$
Y es un subgrupo de H.

Subgrupo Cíclico generado: Si $a \in G$, entonces el subgrupo generado por a es $\langle a \rangle =$ potencias de a.
Decimos que G es **cíclico** si existe $a \in G$ tal que $G = \langle a \rangle$

Orden: El orden de G es $|G|$
El orden de $a \in G$ es $|\langle a \rangle|$ que es igual a el mínimo $n \in \mathbb{N}$ tal que $a^n = e$

Generado: Si $S \subset G$ con G un grupo. El **subgrupo generado por** S es el mínimo subgrupo que contiene a S
Palabra: Si $X = \{a_1, \cdots, a_n\}$, una palabra en X es una expresión $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ donde $\alpha_i = \pm 1$ y $x_i \in X$ (se pueden repetir.)
El generado de X es igual al conjunto de todas las palabras de X

2.0.1. Teorema de Lagrange:

Clase Lateral Izquierda: Si $H \leq G$, una c.l.i de H es el conjunto:

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

es un conjunto y no necesariamente un grupo (a menos que $x \in H$)
Definimos una equivalencia en G como $a \sim_H b$ sii $a = bh$ (es decir $a \sim_H b$ sii $a \in bH$).
Se puede probar que es una relación de equivalencia y por tanto, las c.l.i separan a G en conjuntos disjuntos y que juntos forman todo G.

Teorema de Lagrange versión 1: Si G es un grupo finito y $H \leq G$, $\Rightarrow$ $|H| \mid |G|$

Corolario: Si $a \in G \Rightarrow |a| \mid G$
Si $|G| = p$ con p primo, entonces G es cíclico y todo $a \in G$ es de orden p.
Fermat: Si p es un primo. Entonces $\bar{a}^p = \bar{a}$ para todo $\bar{a} \in \mathbb{Z}_p$

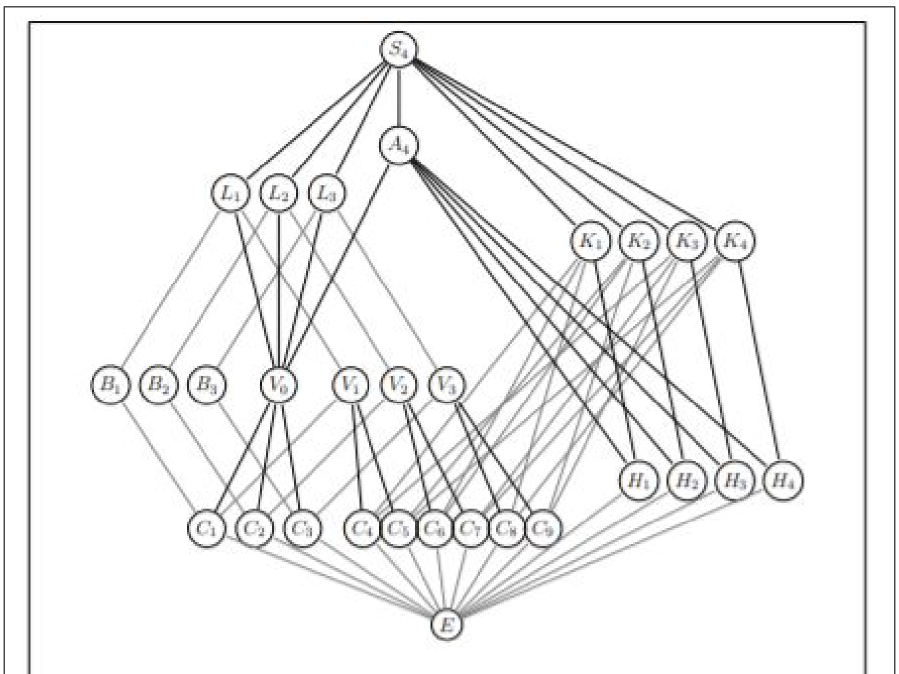
Teorema Sea G un grupo y $H \leq G$. Entonces, existe el mismo número de c.l.i y de c.l.d

Índice: Si $H \leq G$, el índice de H en G es $[G : H]$ igual al número de clases laterales

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

2.0.2. Retícula

La retícula (diagrama de Hasse) de un grupo G es una representación con todos sus subgrupos y las contenciones entre ellos.
Por ejemplo:



$L_i \cong D_{2(4)}$, $B_i \cong \mathbb{Z}_4$, $C_i \cong \mathbb{Z}_2$, $V_i \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $H_i \cong$, $K_i \cong S_3$

Vemos que si una parte de la retícula es igual a la terícula de otro grupo, entonces esa parte es isomorfa al otro grupo.

2.0.3. Grupos Cíclicos

Grupos Cíclicos: Si $H = \langle x \rangle$ y $n \in \mathbb{N}$. Entonces:

a) $|x| = n$ sii n es el menot natural tal que $x^n = e$.

b) $H \simeq \mathbb{Z}_n$. Y tenemos:

- $x^a = e$ sii $\bar{a} = \bar{0}$ en $\mathbb{Z}_n$

- $x^a = x^b$ sii $\bar{a} = \bar{b}$ en $\mathbb{Z}_n$

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

d) Si $|x| = \infty$, entonces $H \simeq \mathbb{Z}$ y se tiene que $x^a = x^b$ sii $a = b$

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

a) Si $x^n = x^m = e$. Entonces $x^d = e$

b) $x^m = e$ sii $|x| \mid m$

c) Si $|x| = \infty \Rightarrow |x^a| = \infty$

d) Si $|x| = n \Rightarrow |x^a| = \dfrac{n}{(n,a)}$

e) Si $|x| = st$, entonces $|x^s| = t$

Corolario: Si $H = \langle x \rangle$. Se cumple que:

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

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

c) Todo subgrupo de H es cíclico

d) $\langle x^a \rangle = \langle x^{(a,n)} \rangle$

Teorema de grupos cíclicos (regreso del T de Lagrange): Si $G = \langle x \rangle$ de orden n. Entonces para todo $d|n$ existe un único subgrupo $H \leq G$ tal que $|H| = d$. Además, $H = \langle x^{n/d} \rangle$

2.0.4. Subgrupos Normales

Primero vemos que si $\sigma = (a_1\ a_2\ \cdots\ a_k)$ y $\tau \in S_n$. Entonces:

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_k))$$

Y si $\sigma = \alpha_1\alpha_2\cdots\alpha_n$ con α_i la descomposición en ciclos. Tenemos que:

$$\tau\sigma\tau^{-1} = (\tau\alpha_1\tau^{-1})(\tau\alpha_2\tau^{-1})\cdots(\tau\alpha_n\tau^{-1})$$

Def (Grupo Normal): Sea G un grupo y $N \leq G$. Decimos que N es normal si $gNg^{-1} = N$ para todo $g \in G$. Lo anotamos como $N \trianglelefteq G$.

Lema: Sea G un grupo y $H \leq G$. Entonces es equivalente:

a) $H \trianglelefteq G$

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

c) $aHa^{-1} \subset H\ \ \ \forall a \in G$. Y de hecho $aHa^{-1} = H$

$\{e\}$ y G son siempre subgrupos de G.
Si G es abeliano, enotnces todo subrugpo es normal.
Si $[G:H]=2$, entonces H es normal en G.

Corolario: Si $G=\langle X\rangle$, y $H=\langle Y\rangle$ y $H\leq G$. Entonces $H\trianglelefteq G$ sii $xyx^{-1}\in H$ para todo $x\in X, y\in Y$
Corolario 2: Sea $H\leq G$. Si no existe $H'\leq G$ tal que $H'\simeq H$ con $H\neq H'$, entonces $H\trianglelefteq G$. Porque aHa^{-1} es siempre un grupo isomorfo a H y si no existe otro, entonces $aHa^{-1}=H$.

Centro: El centro de un grupo G es:

$$\{g\in G \mid gx=xg\ \forall x\in G\}$$

y se tiene que $Z(G)\trianglelefteq G$

Producto de Grupos
Def: Si $S,T\subset G$. Definimos:

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

Teorema: Sea G un grupo y $H,K\leq G$. Entonces:

$$|HK|=|H:H\cap K||K|$$
Si G es finito, tenemos que $|HK||H\cap K|=|H||K|$

Prop 15.6: Sean $N\trianglelefteq G, H\leq G$. Entonces $\langle N,H\rangle=NH=HN$
Lema: Sea G un grupo. $H,K\trianglelefteq G$. Si $H\cap K=\{e\}$, entonces $hk=kh$ para todo $h\in H$, $k\in K$
Teorema 15.10: Sea $H,K\trianglelefteq G$, entonces $HK\trianglelefteq G$ **Teorema:** Sea $H,K\trianglelefteq G$ con $H\cap K=\{e\}$, entonces $HK\simeq H\times K$

2.0.5. Grupos Cocientes

Lema: Si $H\leq G$ entonces los siguientes son equivalentes:

a) $H\trianglelefteq G$

b) La operación $aH\cdot bH=abH$ está bien definida.

Con ello si N es normal, podemos crear un grupo de clases lateras.
Recordamos que G/N es el conjunto de todas las clases laterales de N en G.
Teorema: Sea $N\trianglelefteq G$. Denotamos como G/N al conjunto de clases laterales de N. Se cumple:

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

b) $\pi: G\to G/N$, $a\to aN$ es un morfismo sobreyectivo

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

d) Si $G = \langle a \rangle \ \Rightarrow \ \ G/N = \langle aN \rangle$

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

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

2.0.6. Teoremas de Isomorfismo

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

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

b) $Ker(f) := \{a \in G \mid f(a) = e'\}$

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

1er Teorema de Isomorfismos: Sea $f : G \to H$ un morfismo de grupos. Enntonces:

$$Ker(f) \trianglelefteq G \quad , \quad G/Ker(f) \simeq Im(f)$$

- $Aut(G) := \{\alpha : G \to G \mid \alpha \text{ es isomorfismo }\}$
- $Inn(G) = \{\alpha : G \to G \mid \exists a \in G \text{ con } \alpha(x) = axa^{-1} \ \}$

Se tiene que $Inn(G) \trianglelefteq Aut(G)$

Segundo Teorema de Isomorfismos (Teorema del diamante):
Sea G un grupo y $H, K \leq G$ con $K \trianglelefteq G$. Entonces HK es un subgrupo con:

$$K \trianglelefteq HK \ \ , \ \ H \cap K \trianglelefteq H$$
$$HK/K \simeq H/(H \cap K)$$

Lema: Sean $K \leq H_1 \leq G$ con $K \trianglelefteq G$. Entones:

a) $H_1/K \leq G/K$

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

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

- ϕ es biyectivo
- $\phi(H) \leq \phi(H')$ sii $H \leq H'$

Es decir, hay una correspondencia biyectiva entre subgrupos H que contienen a un subgrupo normal K de G. Con los subgrupos de G/K.
Hay tantos subgrupos de G/K como grupos H que están entre K y G.

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

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

3. Acciones de Grupos

Descomposición en ciclos ajenos:
Si $\alpha \in S_n$, entonces se puede escribir como:

$$\alpha = \sigma_1 \sigma_2 \cdots \sigma_k$$

Con σ_i ciclos ajenos y con $|\sigma_i| \leq |\sigma_{i+1}|$
Entonces, la **estructura cíclica** de α son los números:

$$(|\sigma_1|, |\sigma_2|, \cdots, |\sigma_k|)$$

Lema: Dos permutaciones $\alpha, \beta \in S_n$ tienen la misma estructura cíclica sii existe $\gamma \in S_n$ tal que $\alpha = \gamma\beta\gamma^{-1}$

Conjugados: En general, decimos que dos elementos $x, y \in G$ son conjugados si existe $z \in G$ tal que $x = zyz^{-1}$

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 subgrupo de S_n.

Acción de Grupo: Sea G un grupo y X un conjunto no vacío. Una función $G \times X \to X$ se llama acción de G en X. $(a, x) \to a \cdot x$. Si satisface:

a) $e \cdot x = x \quad \forall x \in X$

b) $a \cdot (b \cdot x) = (ab) \cdot x$

Ejemplos:

a) Sea $\alpha \in S_n$, $G = \langle \alpha \rangle$, $X = \{1, \cdots, n\}$. La función $G \times X \to X$ dada por $\alpha^k \cdot x = \alpha^k(x)$ es una acción en G (permutar elementos)

b) Sea $H \leq G$. La función $H \times G \to G$ dada por $h \cdot g = hg$ es una acción de H en G. (multiplicar elementos)

- 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 (conjugar elementos)

d) Sea G un grupo y S el conjunto de subgrupos de G. Entonces la función $G \times S \to S$ definida como $a \cdot H = aHa^{-1}$ es una acción de grupo (conjugar subgrupos)

Lema: Si G es un grupo y X n $G-$conjunto (conjunto sobre el que actúa G), entonces:

a) Si $a \cdot x = a \cdot y \quad \Rightarrow \quad x = y$

b) $a \cdot x = b \cdot y \quad$ sii $(b^{-1}a) \cdot x = y$

Teorema: Sea G un grupo y X un $G-$conjunto. Para cada $g \in G$ consideramos la correspondencia $\phi_g : X \to X$ dada por $x \to g \cdot x$. Se cumple:

a) ϕ_a es biyectiva para todo $a \in G$. Es decir $\phi_a \in S_X$

b) $\phi : G \to S_x$ dado por $a \to \phi_a$ es un morfismo de grupos.

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

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

0) **Relación de Equivalencia en X:** Decimos que $x, y \in X$ están relacionados, $x \sim y$ si existe un $g \in G$ tal que $x = g \cdot y$

a) La **orbita de** x

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

Es un subconjunto de X y puede tener diferentes tamanos dependiendo de x.
Dada la relación de equivalencia, O_x es la clase de equivalencia de x.
Así que todos los O_x para $x \in X$ forman una partición disjunta de X.

b) El **estabilizador de** x es el conjunto

$$S(x) = \{g \in G \mid g \cdot x = x\} \subset G$$

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

c) El **subconjunto fijo** es

$$X_f = \{x \in X \mid O_x = \{x\}\}.$$

Es decir, las x que no son movidas por nadie. Es un subconjunto de X.

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

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

Descomposición en Órbitas: Sea G un grupo que actúa sobre X. Y digamos que X se descompone como $X = O_{x_1} \cup \cdots \cup O_{x_k} \cup O_{k+1} \cup \cdots \cup O_{x_m}$ en órbitas.
Donde $x_1, \cdots x_k \notin X_f$ y $x_{k+1}, \cdots, x_m \in X_f$. Entonces:

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

3.0.1. Casos particulares

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

  - **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:
  $$O_x = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$
  Recibe el nombre de **clase de conjugación de** x
  - **Estabilizador:** El estabilizador de un $x \in X$ es:
  $$S(x) := N(x) = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\}$$
  Recibe el nombre de **centralizador de** x y son los elementos que conmutan con x.
  - **Conjunto Fijo:** Es el conjunto:
  $$X_f = \{x \in X \mid g \cdot x = x \; \forall g \in G\} = G_f - \{x \in G \mid gxg^{-1} = x \; \forall g \in G\}$$
  Son los elementos de x que conmutan con todo. Recibe el nombre de **Centro de** G.
  - **Teorema Órbita-Estabilizador:**
  $$|O_x| = \frac{|G|}{N(x)}$$
  Ecuación de Clase:
  $$|G| = |Z(G)| + \sum_{i=1}^{m} |O_{x_i}|$$

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

  - **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:
  $$O_A = \{g \cdot A \mid g \in G\} = \{gAg^{-1} \mid g \in G\}$$
  Recibe el nombre de **clase de conjugación de** A
  - **Estabilizador:** El estabilizador de $A \in S$ es:
  $$S(A) := N(A) = \{g \in G \mid g \cdot A = A\} = \{g \in G \mid gAg^{-1} = A\}$$
  Recibe el nombre de **normalizador de** A y son los elementos $g \in G$ para los cuales la c.l.i gA es igual a la derecha Ag.
  - **Conjunto Fijo:** Es el conjunto:

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

Son los grupos normales. Juntos forman el conjunto de todos los grupos normales de G.

- **Teorema Órbita Estabilizador**

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

- **Ecuación de Clases:**

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

La suma corre sólo en los grupos A_i no normales.

- **Permutaciones**:
  Digamos que $G = \langle \alpha \rangle$ con $\alpha \in S_n$ y $X = \{1, 2, \cdots, n\}$. La función $G \times X \to X$ definida como $\alpha^k \cdot x = \alpha^k(x)$ es una acción

  - **Relación de Equivalencia:** $\alpha^k \sim \alpha^j$ sii $\alpha = \gamma\alpha^j\gamma^{-1}$ para un $\gamma \in G$
  - **Órbita:** La órbita de un $p \in X$ es:

$$O_{\alpha^k} = \{\alpha^k \cdot x \mid \alpha^k \in G\} = \{\alpha^k(x) \mid \alpha^k \in G\}$$

  - **Estabilizador:**

$$S(p) = \{\alpha^k \in G \mid \alpha^k \cdot x = x\} = \{\alpha^k \in G \ ; \mid \alpha^k(x) = x\}$$

Teorema de Cauchy: Si G es un grupo finito y p un primo que divide a $|G|$, entonces G tiene un elemento de orden p y por tanto, un subgrupo de orden p.

3.0.2. Contar órbitas

Sea X un $G-$conjunto.
Digamos que el número de órbitas de X es k.

Definimos un nuevo conjunto:

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

Es decir, son los elementos de X fijados por la acción.

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

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

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.

6

Finalmente, por el Lema de Frobenius podemos concluir que

$$
\begin{aligned}
k &= \sum_{g\in G} \frac{|F(g)|}{|G|} \\
&= \frac{1}{|G|}\left(\sum_{g\in G} |F(g)|\right) \\
&= \left(\frac{1}{24}\right)\left(3^2 8 + 3^3 6 + 3^4 3 + 3^3 6 + 3^6\right) \\
&= \frac{1368}{24} = 57.
\end{aligned}
$$

□

The sides of a square are to be colored by either red or blue. How many different arrangements are there if

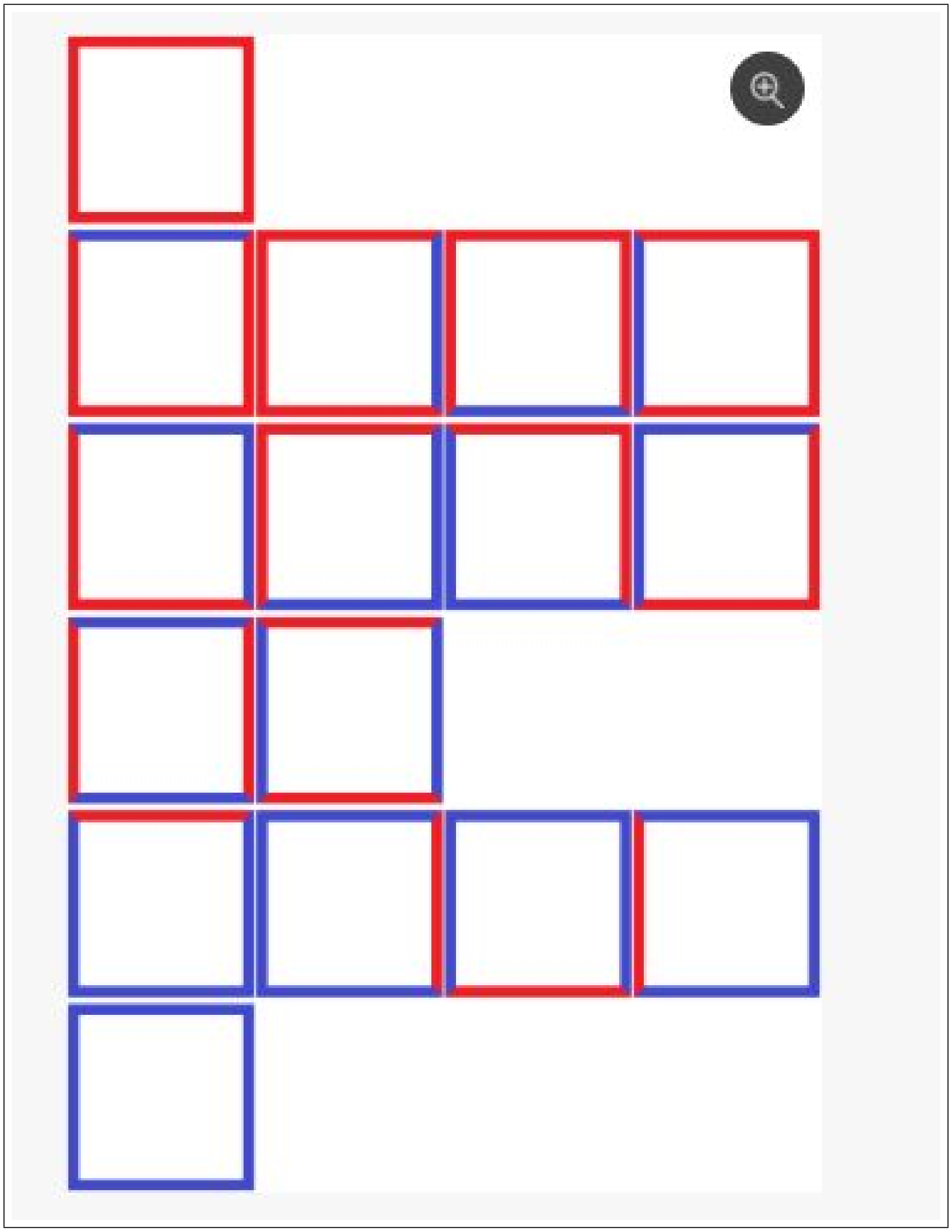
1. a coloring that can be obtained from another by rotation is considered **different**, or
2. a coloring that can be obtained from another by rotation is considered **identical**?

For the first problem, this is simple. Since symmetry is not taken into account, we can simply use usual counting methods. Each side has two possible choices, and all of these are independent, so we can multiply everything: $2^4 = 16$ for four sides.

The second problem is much harder since we need to be careful not to double-count things that can be obtained by rotation. We can try a case by case analysis:

- All red is one. All blue is also one.
- One red (and the rest blue) has four possibilities, all of them able to be obtained from each other by rotation. Thus there is only one unique coloring here.
- One blue (and the rest red) also has only one unique coloring.
- Among two reds and two blues, there are two possible ways. Either the reds are adjacent to each other, in which there are four colorings but all of them identical, or they aren't, in which there are just two and also identical. This case gives us two unique colorings.

In total, there are $1 + 1 + 1 + 1 + 2 = 6$ such colorings:



However, we can apply Burnside's lemma to this.

The group G is made up of four elements: "rotate by 0°," "rotate by 90°," "rotate by 180°," and "rotate by 270°" (all clockwise). (This group is also known as the cyclic group of order 4, or C_4). The set X contains all $2^4 = 16$ colorings if we assume rotations are distinct (as in the first problem). Now, we need to count the number of fixed points:

- "Rotate by 0°" is the identity transformation. This clearly doesn't change any of the 16 colorings; there are 16 fixed points.
- To determine the fixed points of "rotate by 90°," we can inspect the sides. The top side will become the right side; if they are of different colors, clearly the coloring isn't a fixed point (since the right sides will be different). For example, if the top side is red and the right side is blue, after rotating, we have the right side to become red; since the right side has different colors before and after transformation, this is not a fixed point. Likewise, the right side and the bottom side must have the same color. The same goes with the bottom and left, and left and top. In other words, all sides must have the same color. There are only two such colorings, all red or all blue, and thus 2 fixed points.
- "Rotate by 270°" has a similar argument as above; we also get 2 fixed points here.
- "Rotate by 180°" is a little more complex. The top and bottom sides must be the same color, and so must the left and right sides, but otherwise there's not much else. Indeed, we can give colors independently: one color for the top and bottom, and another (may be identical) for the left and right sides, giving $2^2 = 4$ fixed points.

In total, we have $16 + 2 + 2 + 4 = 24$ fixed points, over 4 group elements. By Burnside's lemma, the number of orbits, and thus the number of distinct colorings including rotation, is $\frac{24}{4} = 6$. This matches our case-by-case work. □

The sides of a square are to be colored by n colors (each side has one color, but a color may color many sides). How many different arrangements are there if two arrangements that can be obtained from each other by rotation are identical?

We can use Burnside's lemma here to avoid casework entirely. We already identified all four elements above:

- "rotate by 0°" fixes all n^4 elements,
- "rotate by 90°" and "rotate by 270°" fix n elements each, and
- "rotate by 180°" fixes n^2 elements.

In total, that's $n^4 + n^2 + 2n$ elements, and dividing this by the number of transformations 4 gives the desired number of distinct colorings, $\frac{n^4+n^2+2n}{4}$.

This allows us to compute, for example, that the number of distinct colorings with 2016 colors is 4129545225456 by simply plugging into the formula. We can technically do case work, but it will be messy. □

The sides of a rectangle (that is not a square) are to be colored by either red or blue. How many possible colorings are there, if two colorings that can be obtained from each other by **rotation and/or reflection** are considered identical?

The group in question is the dihedral group of order 2, also known as D_2, which has these four elements:

- identity transformation
- rotate by 180°
- reflect along the short side
- reflect along the long side.

We now use Burnside's lemma again:

- Identity transformation fixes $2^4 = 16$ elements. No restrictions on sides.
- Rotating by 180° fixes $2^2 = 4$ elements. Long sides must match, and so must short sides.
- Reflecting along the short side fixes $2^3 = 8$ elements. Short sides must match, but the two long sides may not match.
- Reflecting along the long side fixes $2^3 = 8$ elements. Long sides must match, but the two short sides may not match.

That gives a total of $\frac{1}{4} \cdot (16 + 4 + 8 + 8) = 9$ orbits. □

Six indistinguishable balls are to be distributed into three indistinguishable boxes. How many ways are there to do this?

At first, this doesn't look like a Burnside's lemma problem. However, we can still solve it with Burnside's lemma anyway.

The relevant group is the permutation group on three elements, also known as S_3, which has these elements:

- Don't move the boxes.
- Swap the first and the second boxes.
- Swap the first and the third boxes.
- Swap the second and the third boxes.
- Make the first box to be the second and push the others in circular fashion.
- Make the first box to be the third and push the others in circular fashion.

Or alternatively, represented as permutations,

- $(1,2,3)$ stays as $(1,2,3)$;
- $(1,2,3)$ becomes $(2,1,3)$;
- $(1,2,3)$ becomes $(3,2,1)$;
- $(1,2,3)$ becomes $(1,3,2)$;
- $(1,2,3)$ becomes $(2,3,1)$;
- $(1,2,3)$ becomes $(3,1,2)$.

This time we can simplify our work a bit:

- The identity permutation fixes all possible configurations.
- The three permutations which swap two boxes fix configurations in which the contents of the two swapped boxes are equal.
- The two permutations which rotate the boxes fix configurations in which the contents of all boxes are equal.

The problem, now, is to compute how many possible configurations fall in each possibility.

The case of identity permutation is the hardest one. We can imagine that the boxes are now distinguishable (since we are no longer to move them around, we might as well name them first, second, and third box). This problem of putting 6 indistinguishable balls in 3 distinguishable boxes can be solved using the stars and bars technique, which tells us that there are $\binom{8}{2} = 28$ configurations.

The second, where two boxes are swapped, is easier because we can just do a simple case work. The contents of the two swapped boxes must be either 0, 1, 2, or 3 balls each, and the content of the remaining box follows (6, 4, 2, or 0 balls respectively). There are 4 configurations here for each pair of swapped boxes.

The third, where boxes are rotated, is the simplest: since all of them have the same number of balls, all of them must necessarily have 2 balls. There is exactly one configuration in this case.

Adding everything up, we obtain $\frac{1}{6} \cdot (28+4+4+4+1+1) = 7$ orbits; that is, there are 7 ways to put them. We can verify this with casework:

$$6+0+0,\ 5+1+0,\ 4+2+0,\ 4+1+1,\ 3+3+0,\ 3+2+1,\ 2+2+2$$

are all of them. □

Teorema de Cayley Extendido: Sea G un grupo, $H \leq G$ con $m = [G:H]$. Enotnces existe un morfismo de grupos $\phi : G \to S_m$ que cumple:

- $Ker(\phi) = \bigcap_{g\in G} gHg^{-1}$
- $Ker(\phi) \leq H$
- Si $K \trianglelefteq G$ y $K \leq H \quad \Rightarrow \quad K \leq Ker(\phi)$
- $H \trianglelefteq G$ sii $Ker(\phi) = H$

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.

4. Teoremas de Sylow

Def: Sea G un grupo. Decimos que es un p-grupo si para toda $g \in G$ existe $m \in \mathbb{Z}$ tal que el orden de g es p^m

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

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

Teorema: Si G es un p-grupo finito, entonce $Z(G) \neq \{e\}$
Corolario: Si G es un p-grupo finito, entonces existe un $x \in G$ de orden p tal que $xy = yx$ para todo $y \in G$.

Teorema 24.7: Si G es un grupo de orden p^2, entonces $G \simeq \mathbb{Z}_{p^2}$ o $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$
Con otros teoremas parecidos, podemos llegar a las clasificaciones:

$\|G\|$	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

Donde:

$$H_p := \{a, b, c \mid a^p = b^p = c^p = e \ , \ cac^{-1} = ab^{-1} \ , \ ab = ba \ , \ bc = cb\}$$
$$E_p = \{(x, y) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \mid x \in \langle p \rangle\}$$

4.0.1. Teoremas de Sylow

Teorema: Sea G un grupo finito. Si p es un primo y $p^k \mid |G|$, entonces G tiene un subgrupo de orden p^k.

Corolario (1er Teorema de Sylow): Sea G un grupo de orden $p^k m$, donde p no divide a m. Entonces, G tiene un subgrupo de orden p^k .

Def Subgrupo de Sylow: 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.

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

Def: Definimos:

$$Syl_p(G) := \{ \text{ el conjunto de todos los } p \text{ subgrupos de } G\}$$

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

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

Tercer Teorema de Sylow:
Sea G un grupo de orden $p^k m$, donde p es un primo que no divide a m. Se cumplen los siguientes enunciados:

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

b) n_p divide a m

c) $n_p \equiv 1 \quad (mod\ p)$

4.0.2. Producto Semidirecto

teorema: Sean $H_1, \cdots, H_k \leq G$. Los siguientes enunciados son equivalentes:

a) $G \simeq H_1 \times \cdots \times H_k$

b) Para todo $g \in G$, existe un único $(h_1, \cdots, h_k) \in H_1 \times \cdots \times H_k$ tal que $g = h_1 \cdots h_k$ y $H_i \trianglelefteq G$

c) $G = H_i \cdots H_k$, $H_i \cap (\Pi_{i \neq j} H_j) = \{e\}$. Y $h_i h_j = h_j = h_i$ para $h_i \in H_i$, $h_j \in H_j$

Prop 29.3: Sea G un grupo. $H \trianglelefteq G$ y $K \leq G$ tales que$KH = G$ y $H \cap K = \{e\}$. Consideramos el morfismo $\sigma : K \to Aut(H)$, $k \to \sigma_k$. Se cumple lo siguiente:

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

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

es un grupo que denotamos $H \times_\sigma K$

b) $G \simeq H \times_\sigma K$

Producto Interno Semidirecto: Sea G un grupo y $H, K \leq G$. Decimos que G es el producto interno semidirecto de H, K si $G = HK$, $H \cap K = \{e\}$ y $H \trianglelefteq G$. En tal caso, escribimos $G = H \rtimes K$
Pero conste que G no es isomorfo a $H \times K$

Teorema: Sean H, K grupos. Consideramos un morfismo de grupos $\phi : K \to Aut(H)$, $k \to \phi_k$. Se cumple:

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

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

es un grupo que denotamos $H \rtimes_\phi K$

b) Los conjuntos $H_0 := H \times \{e_K\}$ y $K_0 := \{e_H\} \times K$ son subgrupos de $H \rtimes_\phi K$ tales que $H \rtimes_\phi K = H_0 \rtimes K_0$

Con ello, se puede llegar a los siguientes isomorfismos:

$\|G\|$	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

Donde:

$$H_p := \{a, b, c \mid a^p = b^p = c^p = e\ ,\ cac^{-1} = ab^{-1}\ ,\ ab = ba\ ,\ bc = cb\}$$
$$E_p = \{(x, y) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \mid x \in \langle p \rangle\}$$
$$F_n \text{ es el grupo de automorfismos de } D_{2n}$$
$$Q_{4n} = \langle x, y | x^{2n} = y^4 = 1\ ,\ x^n = y^2\ ,\ y^{-1}xy = x^{-1}\}$$

5. Teorema Fundamental de Grupos Abelianos Finitos

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

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

b) $P_i \trianglelefteq G$

c) $G \simeq P_1 \times P_2 \times \cdots \times P_k$

Denotamos por C_q al grupo cíclico de orden q.

Prop 32.4: Sea G un p-grupo abeliano 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 $G \simeq C_{p^{a_1}} \times \cdots \times C_{p^{a_r}}$

Lema: $(m, n) = 1$ sii $C_{mn} = C_m \times C_n$

Prop: 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 $G \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$

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

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 $(p, p, p\cdot, p)$. $|G_p| = p^r$ y G^p es de tipo $(p^{a_1 - 1}, \cdots, p^{a_r - 1})$

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

Componente de Torsión de G: Sea G un grupo abeliano. El subgrupo:

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

En caso de que $\tau G = \{e\}$, decimos que G es libre de torsión.

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

Rango: Sea G un grupo, su rango es:

$$ran(G) = \text{mín}\{|X| \ : \ \langle X \rangle = G\}$$

Si es finito, decimos que G es **finitamente generado**.

Teorema fundamental de grupo abelianos finitamente generados
Sea G un grupo abeliano finitamente generado. Entonces:

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

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

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

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

6. Series Normales

Serie subnormal: Si G es un grupo, una serie subnormal es una cadena:

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

Donde $G_{i+1} \trianglelefteq G_i$
Se llama **serie normal** si $G_i \trianglelefteq G$ para todo i.
Factor de la Serie: El iésimo factor de la serie es el grupo cociente $Q_i := G_{i-1}/G_i$

Simple: Un grupo G es simple si $\{e\}$ y G son los únicos normales.

Serie de Composición: Es una serie subnormal en la que todos los factores son grupos simples.

Teorema de 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 los mismos factores (quizá en otro orden)

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

6.0.1. Grupo alternante:

Definimos A_n como el grupo de todas las permutaciones de S_n que son pares.

Teorema: A_n es simple para todo $n \geq 5$.