Teoremas previos

- Si $a \in G$, b es inverso por izquierda y b' por derecha entonces $b = b'$.
  (G no necesariamente grupo sino que alcanza con que cumpla la asociatividad y tener neutro).

  Observaciones:

  No necesariamente si es inverso por izquierda es inverso por derecha

Grupos

$< G,*, e_G >$ es un grupo si cumple:

1) Cierre $\forall a, b \in G,\ a * b \in G$ y es único
2) Asociativa: $\forall a, b, c \in G,\ a * (b * c) = (a * b) * c$
3) Neutro: Existe y es único algún elemento $e_G \in G / e_G * a = a * e_G = a \ \ \forall a \in G$
4) Opuesto al inverso: $\forall a \in G,\ \exists a' \in G / a * a' = a' * a = e_G$

Propiedades:

1) El e_G es único
2) El inverso de g es único
3) $(a * b)^{-1} = b^{-1}a^{-1}\ \forall a, b \in G$
4) Cancelativas:
   a) $x * g = x * h \Leftrightarrow g = h$
   b) $g * x = h * x \Leftrightarrow g = h$
5) $(a^n)^{-1} = (a^{-1})^n \ \ \forall a \in G$

Grupo abeliano

Un grupo $(G,*, e_G)$ es abeliano si $a * b = b * a\ \forall a, b \in G$

Propiedades:

1) $(a * b)^{-1} = a^{-1} * b^{-1}\ \forall a, b \in G \Leftrightarrow G$ abeliano
2) $(a * b)^n = a^n * b^n\ \forall a, b \in G \Leftrightarrow G$ abeliano
3) Si G es un grupo con 4 elementos, es abeliano
4) Si G es abeliano $\sigma(a) = n$ y $\sigma(b) = m \Rightarrow \sigma(ab) = mcm(n, m)$
   (si no es abeliano esto es falso)

Tabla de Cayley

En los casilleros se coloca el resultado de $a * b$

1) Se cumple el SUDOKU
2) En cada fila y en cada columna aparecen todos los elementos de G
3) Si la tabla es simétrica (en la diagonal de esquina superior derecha a la esquina inferior izquierda) G es abeliano
4) Para llenar la tabla mirar los inversos

Enteros módulo n

Son los $Z_n = \{\overline{1}, \overline{2}, \overline{3}, ... \overline{n}\}$

Invertibles módulo n

Los invertibles módulo n son un grupo abeliano con el producto:

$$U_n = \{[x] : mcd(x, n) = 1\}$$

<u>Propiedades:</u>

1) $a \in U_n \Rightarrow \sigma(a)$ divide a $|U_n| = \varphi(n)$ (Por Teorema de Lagrange)

Subgrupo

Sea $(G, *, e_G)$ un grupo, $H < G$, $(H, *, e_G)$ es un subgrupo de $(G, *, e_G)$ si:

1) $H \subset G,\ H \neq \theta$
2) El neutro de G pertenece a H
3) $\forall a, b \in H,\ a * b \in H$
4) $\forall a \in H,\ a^{-1} \in G$ y $a^{-1} \in H$

<u>Observaciones</u>:

1) $(H, *, e_G)$ es un grupo en sí mismo
2) Si G es un grupo finito $\Rightarrow$ no es necesario chequear la (4)

Intersección de grupos

Sea $(G,*,e_G)$ un grupo, H_1 y H_2 son subgrupos de G

1) $H_1 \cap H_2 < G$
2) $H_1 \cap H_2 < H_1$
3) $H_1 \cap H_2 < H_2$

Propiedades:

1) $mcd(|H|, |K|) = 1 \Rightarrow H \cap K = \{e\}$

Orden de un grupo

Es la cantidad de elementos que hay en el grupo.
Ejemplos:

1) $|Z_n| = n$
2) $|S_n| = n!$
3) $|U_n| = \varphi(n)$ (Por definición de φ)
4) $\sigma(e_G) = 1$

Propiedades:

1) $\sigma(ab) = \sigma(ba)\ \forall a, b \in G$
2) Si $a \in G$ y $\sigma(a) = 1 \Rightarrow a = e_G$
3) Si G finito y $a \in G \Rightarrow \sigma(a)$ divide a $|G|$
4) Si el orden de G es p **primo** todos los elementos no triviales tienen orden p. En particular, es **cíclico**
5) Si G es finito y $g \in G \Rightarrow g^{|G|} = e_G$ (Esto generaliza el **Teorema de Euler**)
6) Si $a^n = e_G \Rightarrow \sigma(a)$ divide a n
7) Si $a^n \neq e_G \Rightarrow \sigma(a)$ no divide a n

Notas:

1) Si G finito, todo elemento suyo tiene orden finito
2) Un ejemplo de grupo de orden infinito donde todos sus elementos salvo el neutro tienen orden infinito es $(Z,+)$
3) Un grupo de orden infinito donde todos los elementos tienen orden finito es $Z_2 x Z_2$

Potencia de elementos de un grupo

Sea $(G,*,e_G)$ un grupo y sea $a \in G$:

$a^0 = e_G$ Por definición.
$a^1 = a$
$a^2 = a * a$
$a^n = a * .... * a$ (n veces)

$a^{-1} =$ inverso de a en $(G,*,e_G)$
$a^{-n} = (a^{-1}) * (a^{-1}) * (a^{-1}) * .... * (a^{-1})$ (n veces)

Orden de un elemento de G

Sea $(G,*,e_G)$ un grupo, $a \in G$:

1) Se $\exists n \in N / a^n = e_G$ Se llama $\sigma(a)$ al mínimo natural que lo cumple
2) Si no existe $n \in N$ tal que $a^n = e_G$ $\sigma(a) = \infty$

Propiedades:

Sea G un grupo:

1) $a^n = e_G \Leftrightarrow \sigma(a)$ divide a n $\forall a \in G$ y $n \in N$
2) $\sigma(x * y) = \sigma(y * x)$ $\forall x, y \in G$

Teorema de Lagrange

(H) G es un grupo finito y $H < G$ $\Rightarrow$ **(T)** $|H|$ divide a $|G|$

Corolarios:

1) Todo grupo de orden **primo** es cíclico
2) Para todo grupo G finito, $\forall a \in G$ $\sigma(a)$ divide a $|G|$
3) Para todo grupo G finito, $\forall a \in G$ $a^{|G|} = e_G$

Subgrupo generado

Dado $(G, *, e_G)$ un grupo y $a \in G$:

- El conjunto $< a >= \{a^n \ tal \ que \ n \in Z\}$ se llama subgrupo de G generado por a $< a > \ \leq \ G$
- $< a >$ es un grupo

Propiedades:

1) $< a >$ es un subgrupo de G que contiene a a
2) $< a >$ es el menor de los subgrupos de G que contiene a a

Teorema

(H) Si $\sigma(a)$ es finito y $\sigma(a) = m_o \ \Rightarrow$

(T) El conjunto $H = \{e_G, a, a^2, ..., a^{m_o - 1}\}$ es el subgrupo generado por a, $H = \ < a >$ y $|< a >| = \sigma(a)$

Grupo cíclico

Un grupo G lo es si:

1) $|G|$ es finito
2) $G =< a >$ para algún $a \in G$
3) $|G| = |< a >| = \sigma(a)$

Propiedades:

1) Si G es cíclico $\Rightarrow$ todo subgrupo de G también lo es
2) Si G solo tiene subgrupos triviales $(H = \{e_G\} \ \wedge \ H = G) \ \Rightarrow \ G$ es cíclico, finito y $|G|$ es **primo**
3) Todo grupo de orden **primo** es cíclico
4) Si G es cíclico $\Rightarrow$ es abeliano
   Es falso que si G es abeliano $\Rightarrow$ es cíclico

Clases en el grupo

Dado $(G,*,e_G)$ un grupo. $H \leq G$ $a \in G$ fijo. Se llama "Coclase" de a con respecto al subgrupo H al conjunto:

$$\text{“} a * H \text{"} = \{g \in G \,/\, g = a * h \text{ para algún } h \in H\}$$

<u>Observaciones</u>:

$a \in H$ pues $e_G \in H$ y $a = a * e_G$

Teorema

(H) H finito ⇒ **(T)** Toda coclase tiene igual cantidad de elementos que H

Teorema

(H) $(G,*,e_G)$ un grupo cualquiera y $H \leq G$

(T) Sean $a * H$ y $b * H$ dos coclases cualquiera respecto de H, se cumple:

- O bien son disjuntas
- O bien coinciden

Relación

Sean $a, b \in G$ decimos que $a \sim b$ cuando $a * H = b * H$

Esta es una **relación de equivalencia**

- Reflexiva
- Simétrica
- Transitiva

Homomorfismo de grupos (morfismo)

$f: G_1 \to G_2$ se llama homomorfismo de grupos si:

1) $f: G_1 \to G_2$ con $(G, *, e_{G_1})$ y $\left(G_2,\ x, e_{G_2}\right)$ grupos
2) $\forall a, b \in G_1\ f(a * b) = f(a)\, x\, f(b)$

Morfismo trivial

$f: G \to G'$ lo es si $f(a) = e_{G'}\ \forall a \in G$ ($Ker(f) = G$)

Núcleo de f

$$Ker(f) = \{a \in G \,/\, f(a) = e_{G'}\}$$

Propiedades

f es homomorfismo $f: G \to G'$

1) $Ker(f)$ es subgrupo de G
2) $f(e_G) = e_{G'}$
3) $\forall a \in G\ f(a^{-1}) = [f(a)]^{-1}$
4) $\forall a \in G\ f(a^n) = [f(a)]^n\quad \forall n \in Z$
5) $\forall a \in G$, si $\sigma(a)$ es finito $\Rightarrow$ $\sigma(f(a))$ divide a $\sigma(a)$
6) $|Ker(f)|$ divide a $|G|$

Teorema: Homomorfismos inyectivos

Un homomorfismo de grupos $f: G \to G'$ es inyectivo $\leftrightarrow$ $Ker(f) = \{e_G\}$

Corolarios:

1) $|G| = p$ primo, $f: G \to G'$ **homomorfismo** entonces:
   a) O bien f es trivial $(Ker(f) = G)$
   b) O bien f es inyectiva $(Ker(f) = \{e_G\})$
2) $f: G \to G'$ **homomorfismo**, $|G| = p$ **primo**, $|G| > |G'|$ $\Rightarrow$ f es trivial $(Ker(f) = G)$

Propiedades:

Si $f: G \to G'$ homomorfismo

1) Si $|G'|$ es finito y si $a \in G \,/\, \sigma(a)$ finito $\Rightarrow$ $\sigma(f(a))$ divide a $mcd(\sigma(a),\ |G'|)$
2) Si $|G|$ y $|G'|$ es finito y $mcd(|G|, |G'|) = 1$ $\Rightarrow$ su morfismo f es trivial $(Ker(f) = G)$

Ejemplos:

1) Una **Transformación Lineal** es un morfismo de grupos

Imágen de f

$$Im(f) = \{h \in G' \,/\, \exists\, g \in G,\ f(g) = h\}$$

Propiedades:

$f : G \to G'$ es homomorfismo de grupos

1) $Im(f)$ es subgrupo de G'
2) $|Im(f)|$ divide a $|G'|$
3) Si $g \in G \Rightarrow \sigma(f(g))$ divide a $mcd(|G|, Im(f))$

Afirmación:

Sean $(G, *, e_G)$ y $(G', \otimes, e_{G'})$ grupos.
$\forall a, b \in G$, $f : G \to G'$ homomorfismo:
La coclase de a coincide con la coclase de b $\Leftrightarrow$ $f(a) = f(b)$

Consecuencia:

\# coclases diferentes = $|Im(f)|$

Teorema de los órdenes para morfismos de grupos

(H) $f : G \to G'$ homomorfismo de grupos, $|G|$ es finito

(T) $|G| = |Ker(f)| \,.\, |Im(f)|$

Isomorfismos:

$f : G \to G'$ es un isomorfismo de grupos si es:

1) f un homomorfismo
2) f biyectiva

Notación: $G \simeq G'$

Isomorfos

2 grupos G y G' son "isomorfos" si existe algún isomorfismo $f : G \to G'$

Propiedades:

1) Si G y G' son isomorfos $\Rightarrow$ $|G| = |G'|$
2) Si G es cíclico $\Rightarrow$ $G \simeq Z$
3) Si G es cíclico y no es finito $\Rightarrow$ $G \simeq Z$
4) Si G es cíclico y $|G| = n$ $\Rightarrow$ $G \simeq Z_n$
5) Dado $x \in G$, $x = g^k$ $\Rightarrow$ $\varphi(x) = k$ y φ es un isomorfismo
6) Si f es un isomorfismo $\Rightarrow$ $\sigma(f(g))$ divide a $\sigma(g)$
7) Si $g_1 \neq g_2$ antes no triviales $\Rightarrow$ $g_1 g_2 = g_3$ con g_3 el otro orden de 2
8) G, H cíclicos:

   $G \simeq H \Leftrightarrow |G| = |H|$
9) $f : G \to G'$ es isomorfismo

   $\Leftrightarrow$ f morfismo, f inyectiva $(Ker(f) = \{e_G\})$

   $\Leftrightarrow$ f morfismo, f sobreyectiva $(Im(f) = G')$

Observaciones:

Si $f : G \to G'$ es biyectiva $\Rightarrow$ Existe otra función f^{-1} biyectiva tal que:

$f^{-1} : G' \to G$:

- $\forall a \in G : f^{-1}(f(a)) = a$
- $\forall x \in G' : f\left(f^{-1}(x)\right) = x$

Ejemplos:

1) Z_4 no es isomorfo con $Z_2 x Z_2$
2) G grupo tal que $|G| = 4$ $\Rightarrow$ $G \simeq Z_4$ o $G \simeq Z_2 x Z_2$

Proposición

Si $f : G \to G'$ es un isomorfismo $\Rightarrow$ $f^{-1} : G' \to G$ también lo es.

Propiedades:

Sea $f : G \to G'$ isomorfismo:

1) $\forall a \in G$, si $\sigma(a)$ es finito $\Rightarrow$ $\sigma(a) = \sigma(f(a))$
2) G es cíclico $\Leftrightarrow$ G' es cíclico
3) G es abeliano $\Leftrightarrow$ G' es abeliano