Repaso.

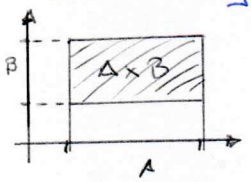
Introducción

$A \times B = \{(a,b) \mid a \in A \text{ y } b \in B\}$

Relación

Cualquier subconjunto de $A \times B$ es una relación de A en B

Si $A = B$, decimos que la relación es en A



R - relación

$R \subseteq A \times B$

Relación de equivalencia
- → simétrica
- → reflexiva
- → transitiva

} En algún sentido, los objetos son iguales.

{(Ana, José), (María, Juan), (Sofía, Pablo)} = R «está casado»

↳ «Qué no es lo mismo pero es igual».

Def. - Relación de equivalencia -

Sea R una relación en A, se tiene que R es una relación de equivalencia si:

- R es reflexiva: $(a,a) \in R$ para cada $a \in A$
- R es simétrica: si $(a,b) \in R$, entonces $(b,a) \in R$.
- R es transitiva: si $(a,b) \in R$ y $(b,c) \in R$, entonces $(a,c) \in R$

Notación

$(a,b) \in R$ se nota también $a \, R \, b$.

Ejemplos:

- $(=)$ es una relación de equivalencia.
  - → $a = a$
  - → $a = b \Rightarrow b = a$
  - → $a = b$ y $b = c \Rightarrow a = c$
- Sea $\mathcal{T}$ el conjunto de los triángulos, la relación $T_1 \overset{\text{semejante}}{\sim} T_2$
- $a \sim b$ si y solo si $a - b$ es par

Transitiva

1) $a \sim b$
2) $b \sim c$
3) $a - b$ es par
4) $b - c$ es par
5) $a - b + b - c$ es par
6) $a - c$ es par

Ejercicio. : Calculamos $\bigcap_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in \mathbb{R}^+} [-1, \alpha[= [-1, 0[$

$\subseteq$

1. Sea $x \in \bigcap_{\alpha \in I} A_\alpha$
2. Para todo $\alpha \in I$, se tiene que $x \in A_\alpha$
3. En particular, tomando $\alpha = 0$, $x \in A_\alpha$
4. $x \in [-1, 0[$
5. $\bigcap_{\alpha \in I} A_\alpha \subseteq [-1, 0[$

$\supseteq$

6. -

Estructuras Algebraicas -

Horario → 11:15 lunes, miércoles, viernes. (todos los días)

→ Sala de espera (la clase se abre para el ingreso desde 11:10 - 11.15 h)

→ La clase termina 13.00 h

Material (Materia) → Estructuras algebraicas.

Estructura algebraica → organización

⇕

Estructura computacional

Formato de la clase

→ 5 horas teóricas 1 hora ejercicios. (lunes)

→ 6 horas aproximadamente totales

Contenidos

→ Conjuntos, Relaciones

→ ~~Relaciones~~, Funciones

(20%) I Introducción → Enteros

(65%) II Grupos →

(15%) III Anillos

Noción de conjuntos

→ Unión $A \cup B$

→ Intersección $A \cap B$

→ Diferencia simétrica $A \Delta B$

→ Diferencia

$\bigcup_{i \in I} A_i$

$\bigcap_{i \in I} A_i$

conjuntos de índices

Bibliografía.

→ Topics in álgebra - Herstein

~~Martes~~.

Miércoles, 2 de junio de 2021

Sistema de calificación

- Pruebas o exámenes 70% (no avisadas)
- Participación, 30% (deberes para la casa, laboratorio.

Formato de demostración

- Teorema

Demostración (Reducción al absurdo)

1.- Conclusión 1. Razón 1

2.- Conclusión 2 Razón 2

Ejercicio.

Sea $I = \mathbb{R}^+$ y $A_\alpha = [-1, \alpha[$, $\alpha \in I$. Calcular $\bigcup_{\alpha \in I} A_\alpha$ y probar la afirmación.

Cálculo:

1.- Calculamos $\bigcup_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} [-1, \alpha[= \bigcup_{\alpha \in \mathbb{R}^+} [-1, \alpha[$ Reemplazamos las hipótesis

2.- $\bigcup_{\alpha \in \mathbb{R}^+} [-1, \alpha[= [-1, +\infty[$ Unión de conjuntos

Demostración

"$\subseteq$"

1. $x \in \bigcup_{\alpha \in I} A_\alpha$	Hipótesis
2. Existe $\alpha \in I$ tal que $x \in A_\alpha$	(1) y def. de unión
3. $x \in [-1, \alpha[$	(2) y def de A_α
4.. $x \in [-1, +\infty[$	$[-1, \alpha[\subseteq [-1, +\infty[$, (3) y (4)
5. $\bigcup_{\alpha \in I} A_\alpha \subseteq [-1, +\infty[$	(1-5) y definición de contenencia

"$\supseteq$"

6. $x \in [-1, +\infty[$	Hipótesis
7. Existe $n \in \mathbb{N}$ tal que $n > x$	(6) y prop. arquimediana.
8. $-1 \leq x < n$	(6) y (7)
9 $x \in [-1, n[$	(8) y def de intervalo.
10. $n \in \mathbb{R}^+$	(9) y $\mathbb{N} \subseteq \mathbb{R}^+$
11. Existe $\alpha_n \in I$ tal que $x \in A_{\alpha_n}$	(10) y (9)
12 $x \in \bigcup_{\alpha \in I} A_\alpha$	(11) y definición de unión

Deber. Haces lo mismo con $\bigcap_{\alpha \in I} A_\alpha$

Ejemplo 2. $\mathcal{A}$ es el conjunto de puntos del plano, $O \in \mathcal{A}$.
Definimos la relación «$\sim$» como $P \sim Q$ si y solo si $OP = OQ$

Ejercicio: Probar que «$\sim$» es una relación de equivalencia.

- Demostración

Reflexiva.
1. $OP = OP$ identidad
2. $P \sim P$ 1 y def

Simétrica
3. $OP \sim OQ$ Hip
4. $OP = OQ$ 3 y (def $\sim$)
5. $OQ = OP$ 4
6. $Q \sim P$ 5 y def

Transitiva.
7. $OP \sim OQ$ Hipótesis
8. $OQ \sim OT$ Hipótesis
9. $OP = OQ$ 7 y def
10. $OQ = OT$ 8 y def
11. $OP = OT$ 9 y 10
12. $P \sim T$ 11 y def

Ejemplo: Estar en la misma familia. A = personas
Ejemplo: Se comunica con: A = personas. (Goteras)
Ejemplo: Está en el mismo punto (se está escondiendo)

Clases de equivalencia.
Definición: Sea A un conjunto y $\sim$ una relación de equivalencia; $a \in A$, se define la clase de a

$$cl(a) = \{x \in A \mid x \sim a\}$$

Ejemplos.
1) A es cualquier conjunto, a
$cl(a) = \{x \in A \mid x = a\}$
$= \{a\}$

2) $A = \mathbb{Z}$,
$cl(2) = \{x \in A \mid x - 2 = par\}$ x pares
$\mathcal{C}(2) = \{x \in A \mid x - 1 = par\}$ x impares

3) $A = \mathcal{A}$ conjunto de puntos en el plano, $O \in \mathcal{A}$
$cl(P) : \{Q \in A \mid OP = OQ\}$ ⇔
→ círculo de radio P y centro O

4) A = personas, «$\sim$» está en la misma familia.
$a \in A$
$cl(a) = \{x \in A \mid x$ está en la misma familia que $a\}$
(familia, hermanos, padres) familia de ruben

5) A = personas, «$\sim$» se relaciona con
$a \in A$
$cl(a) = \{x \in A \mid x$ se comunica con $a\}$
↑ caso (ministros, asesores.

6 A = espacio tridimensional.
$cl(A) = \{x \in A \mid x$ está en la misma posición que $a\}$

7) A = goteras, «$\sim$» tienen canales en común
$cl(a) = \{x \in A \mid$

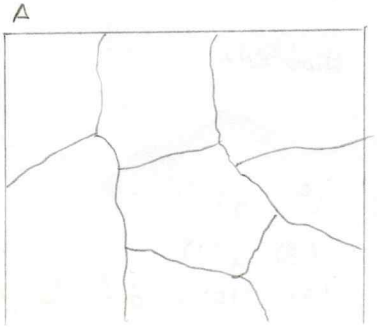
Teorema. 1.
Sea $\mathcal{C}$ el conjunto de las clases de equivalencia en A, entonces

1) $$\bigcup_{C \in \mathcal{C}} C = A$$

2) Las clases de equivalencia son dos a dos disjuntas
$C_1 \cap C_2 = \emptyset$ ó $C_1 \cap C_2 = C_1$

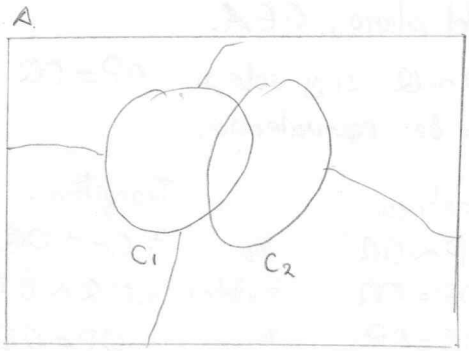
para todo $C_1, C_2 \in \mathcal{C}$.

Sí, son clases de equivalencia



(El dibujo va a ser mejorado en el futuro)

No, no son clases de equivalencia



Demostración del teorema 1

"$\subseteq$"

1. $x \in \bigcup_{C \in \mathcal{C}} C$ — Hipótesis
2. Existe $C \in \mathcal{C}$ tal que $x \in C$ — 1 y def de $\cup$
3. $C \subseteq A$
4. $x \in A$

"$\supseteq$"

1. $x \in A$ — Hipótesis
2. $x \in el(x)$ — 1 y definición $el(x)$
3. $el(x) \in \mathcal{C}$ — definición $\mathcal{C}$
4. existe $C \in \mathcal{C}$, tal que $x \in C$ — (2-3)
6. $x \in \bigcup_{C \in \mathcal{C}} C$ — 4 y definición de $\cup$

Lunes, 7 de junio de 2021

Teorema. Sea $\mathcal{C}$ una clase de subconjuntos de A tales que.

i) $\bigcup_{C \in \mathcal{C}} C = A$

ii) Los elementos de $\mathcal{C}$ son dos a dos disjuntos

Entonces existe una relación de equivalencia en A tal que $\mathcal{C}$ es el conjunto de las clases de equivalencia de A para dicha relación

1. $a \sim b$ si y solo si existe $C \in \mathcal{C}$ tal que $a, b \in C$

P.D. $a \sim b$ es una relación de equivalencia.

Reflexiva

2. $a \in A$ — Hipótesis
3. Existe $C \in \mathcal{C}$ tal que $a \in C$ — Hipótesis y def de unión (1) y (3)
4. $a \sim a$.

Simétrica

5. $a \sim b$ — Hipótesis

P.D $b \sim a$

6. Existe $C \in \mathcal{C}$ tal que $a, b \in C$ — (5) y (1)
7. $b \sim a$

Transitiva

8) $a \sim b$ y $b \sim c$ — Hipótesis

P.D $a \sim c$

9) Existe $C \in \mathcal{C}$ tal que $a, b \in C$ y — (8) y (1)
10) existe $D \in \mathcal{C}$ tal que $b, c \in D$ — (8) y (1)
11) $b \in C \cap D$ — (9) y (10) y def de intersección

12. $C \cap D \neq \emptyset$ (11) y def de $\emptyset$

13. $C = D$ (12) y (ii)

14. Existe $c \in \mathcal{C}$ tal que $a, b, c \in C$.

15 $a \sim c$

Práctica. Goteras.

Miércoles 9 de Junio de 2021.

Funciones.

Definición 1. Sean A y B conjuntos. Una función f de A en B, es un subconjunto de $A \times B$ con la propiedad de que si $(a,b) \in f$ y $(a,b') \in f$, entonces $b = b'$.

Definición 2. Sean A y B conjuntos, una función de A en B es una regla que a cada $x \in A$, le asocia un único elemento de B, y de B.

Ejemplos 1.

$$f = \{(1,a), (2,b)\}, \quad A = \{1,2\}, \quad B = \{a,b\}$$

Notación: Gracias a la unicidad de la definición, podemos escribir $a = f(1)$.

Notamos por $a = f(1)$ es lo mismo que $(1,a) \in f$.

Ejemplo 2.

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a,b) \longmapsto f((a,b)) = a + b$$

→ se llama operación binaria.

Ejercicio. ¿Cuáles de las siguientes relaciones, son funciones?

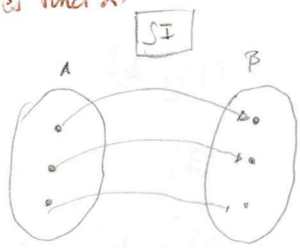
a) Padre de (si es función) b) Cónyuge de (si es función) c) Hijo de: (no es función)

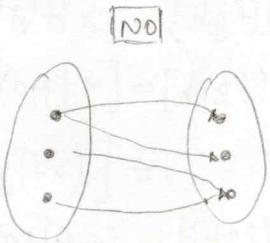
A = conjunto de personas contemporaneas

$f : A \to A$ donde f es la función

$f(\text{Caín}) = \text{Adán}$

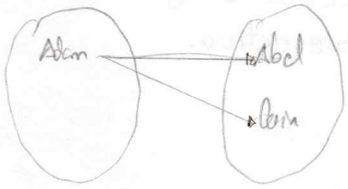
$f(\text{Abel}) = \text{Adán}$





$g : A \to A$ con g = hijo de.

$g(\text{Adán}) \leftarrow$ no es una función



Normalmente la notación es la de la derecha.

$$y = f(x)$$

Notación a la izquierda de funciones

También se puede escribir

$$x \, f \quad \text{en lugar de} \quad f(x)$$

→ Se invierte la posición de los signos

Composición de funciones

$f : A \to B$, $g : B \to C$

$$g \circ f : A \to C$$
$$x \longmapsto g(f(x))$$

En notación a la izquierda, se tiene que

$$x \, f \cdot g = (x \, f) \cdot g$$

Ejemplo 4.

Sea S un conjunto y $\sim$ una relación de equivalencia en S.

$f: S \to \mathcal{C}$ } si es función
$a \mapsto cl(a)$

$f: \mathcal{C} \to S$ } No es función, está mal definida.
$cl(a) \mapsto a$

→ $cl(\text{Aguinaga}) = cl(\text{Kavieres}) =$ equipo de fútbol
→ $f(\text{Equipo de fultbol})$

$f: A \to A$, $g: A \to A$ $\quad A = \{1,2,3\}$

f	g	fg ?
$1f = 2$	$1g = 1$	gf = ?
$2f = 3$	$2g = 3$	
$3f = 1$	$3g = 2$	

Composiciones.

fg	gf
$1fg = 3$	$1gf = 2$
$2fg = 2$	$2gf = 1$
$3fg = 1$	$3gf = 3$

Definición. - Igualdad de funciones -

Sean $f: S \to T$ y $g: S \to U$ dos funciones, entonces f y g son iguales si y solamente si para todo $x \in S$,

$xf = xg$.

Ejemplos.

$f: \mathbb{R} \to \mathbb{R}$ $\quad x \mapsto x^2$

$g: \mathbb{R} \to [0, +\infty[$ $\quad x \mapsto x^2 - x + x$

¿ $f = g$?

Sí, pues para todo $x \in \mathbb{R}$, $xf = xg$.

Teorema.

$f(gh) = (fg)h$, donde $f: S \to T$, $g: T \to U$ y $h: U \to W$

Demostración

1.	$(f(gh)): S \to X$	Hipótesis
2.	$(fg)h: S \to X$	Hipótesis
P.D	$x[(fg)h] = x[f(gh)]$	
3.	$x[(fg)h] = [x(fg)]h$	(1) y def
4.	$= [(xf)g]h$	(3)
5.	$x[f(gh)] = (xf)(gh)$	(2) y def
6.	$= [(xf)g]h$	(5)
7.	$(fg)h = f(gh)$	(4) y (6)

Nota: De acuerdo al teorema anterior, la composición de funciones es asociativa.

Función inyectiva.

Sea $f: S \to T$

- $a \neq b$ entonces $f(a) \neq f(b)$
- Si $f(a) = f(b)$, entonces $a = b$.

Funciones sobreyectivas (simplemente sobre)

Sea $f: S \to T$, f es sobreyectiva si y solamente si para todo $t \in T$, existe $s \in S$ tal que $f(s) = t$.

Función biyectiva

Una función es biyectiva si y solamente si es inyectiva y sobreyectiva.

Teorema.

Si: $f: S \to T$ y $g: T \to U$ y fg es sobreyectiva si y solamente si f y g es sobe.

Demostración

1)	f, g sobre	Hipótesis
2)	$u \in U$	
P.D	existe $s \in S$ tal que $sfg = u$	
3)	existe $t \in T$ tal que $tg = u$	(1) y def de sobre
4)	existe $s \in S$ tal que $sf = t$	(1) y def de sobre
5)	$(sf)g = tg$	(4)
6)	$= u$	(3)

Teorema. El mismo teorema anterior con inyectividad, en lugar de sobreyectividad. (Deber)

Notación: La función identidad se la nota por Id.
Si queremos entatizar el conjunto o dominio, colocamos Id_A.

$$Id_A : A \longrightarrow A$$
$$x \longmapsto Id_A(x) = x.$$

Teorema. Sea f una función de $f: S \to T$, f es biyectiva si y solamente si existe $g: T \to S$ tal que $f \cdot g = Id_S$ y $g \cdot f = Id_T$.

Demostración

$\Rightarrow$)

1) f es biyectiva — Hipótesis
2) Para todo $t \in T$, existe único $s \in S$ tal que $sf = t$ — (1)
3) $g: T \to S$, $t \mapsto s$ — Nomenclatura
4) $(sf)g = tg$
5) $= s$
6) $fg = Id_S$ — Def y fórmulas 4, 5
7) $t(gf) = (tg)f$
8) $= sf$
9) $= t$
10) $gf = Id_T$ — Def igualdad líneas 7-9

$\Leftarrow$)

1) Existe $g: T \to S$ tal que $fg = Id_S$ y $gf = Id_T$

P.D Inyectividad.

2) Sean $s_1, s_2 \in S$ con $s_1 f = s_2 f$ — Hipótesis

P.D $s_1 = s_2$

3) $s_1(fg) = s_1$ — (1)
4) $s_2(fg) = s_2$ — (1)
5) $s_1(fg) = s_2(fg)$ — (1), (2)
6) $s_1 = s_2$ — (4) y (5)

P.D. Sobreyectividad.

7) $t \in T$, — Hipótesis

P.D Existe $s \in S$ tal que $sf = t$.

8) $tgf = t$ — (1) y (7)
9) $tg \in S$ — (1) y (8)
10) $s = tg$ — nomenclatura
11) $sf = t$ — (1) y (10)

Lunes, 14 de junio de 2021.

Enteros.

1. Principio de inducción
2. Principio de buena ordenación — (teorema)

Ejemplo: múltiplos de 5 mayores que 0.
$= \{5, 10, 15, 20, 25, \ldots\}$ el menor elemento es 5.

3. Algoritmo de la división (ó algoritmo de euclides) Si $a, b \in \mathbb{Z}$ y $b \neq 0$, existe $m, r \in \mathbb{Z}$ tal que

$$a = mb + r, \quad \text{con} \quad 0 \leq r < |b|$$

Ejemplo. $a=17$, $b=5$; así $m=3$ y $r=2$ $\Rightarrow$ $17 = 3\cdot 5 + 2 = 15+2 = 17$

$a=-17$, $b=5$; así $m=-4$ y $r=3$ $\Rightarrow$ $-17 = (-4)5+3 = -20+3 = -17$.

$a=17$, $b=-5$; así $m=-3$ y $r=2$ $\Rightarrow$ $17 = (-3)(-5)+2 = 15+2 = 17$

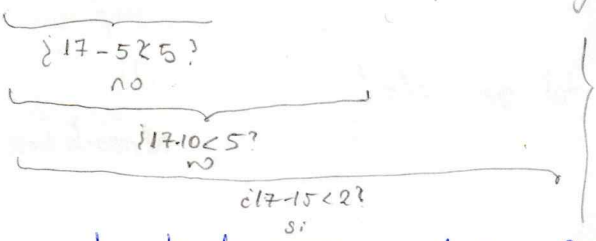
$a=-17$, $b=-5$; así $m=4$ y $r=3$ $\Rightarrow$ $-17 = (4)(-5)+3 = -20+3 = -17$.

Demostración (Idea)

multiplicamos el segmento hasta que la distancia sea menor que la longitud del segmento.

considaremos el caso
$a=5$ y $b=17$

$5 = a = (17)(0)+5$.



Definición -divide a-

Para $b\neq 0$, $b \mid a$ significa que b divide a a; es decir $a = kb$, donde k es algún entero. ("b es divisor de a")

Ejercicio:

Demostrar que si $a \mid 1$, entonces $a=-1$ o $a=1$.

(reducción al absurdo)

		Hipótesis
1)	$a \mid 1$	
2)	Existe $k\in\mathbb{Z}$ tal que $1 = ak$	(1) y def de divisor
3)	$a\neq 1$ y $a\neq -1$	(2)
4)	$a\neq 0$ y $k\neq 0$	(3)
5)	$\lvert a\rvert > 1$ $\lvert k\rvert > 1$	(3) y (4)
6)	$\lvert a\rvert\lvert k\rvert > 1$	(5)
7)	$\lvert ak\rvert > 1$	(6)
8)	$\lvert ak\rvert = 1$	(2)
9)	Contradicción.	(7) y (8).

Laboratorio con funciones biyectivas.

16 de junio de 2021.

Ejercicio. Si: $a \mid b$ y $b \mid a$, entonces $a = \pm b$.

Demostración:

		Hipótesis
1)	$a \mid b$ y $b \mid a$	(1) y def de $a \mid b$
2)	existen k y $k'\in\mathbb{Z}$ tales que $b = ka$ y $a = bk$	(2)
3)	$b = k(k'b)$	(3)
4)	$b = (kk')b$	(4)
5)	$kk' = 1$	(5)
6)	$kk' = \lvert kk'\rvert$	(6)
7)	$= \lvert k\rvert\lvert k'\rvert$	(7)
8)	$\lvert k\rvert = 1$; $\lvert k'\rvert = 1$	(8)
9)	$k = \pm 1$ y $k' = \pm 1$	(2) y (9)
10)	$a = \pm b$	

Ejercicio Si b es divisor de g y h, entonces b es divisor de $mg+nb$ para todo $m,n \in \mathbb{Z}$

1) $b \mid g$ y $b \mid h$	Hipótesis
P.D $b \mid (mg+nb)$	
2) Existen $k_1, k_2 \in \mathbb{Z}$ tal que $bk_1 = g$ y $bk_2 = h$	(1) y (def a|b)
3) Sea $m,n \in \mathbb{Z}$, entonces $mbk_1 = mg$ y $nbk_2 = nh$ $mg+nh = mbk_1 + nbk_2$	(2)
4) $b(mk_1+nk_2) = mg+nh$	(3)
5) $bk = mg+nh$ con $k = mk_1+nk_2$	(4) y nomenclatura
6) $b \mid mg+nh$.	

Definición - máximo común divisor -
El entero $c>0$ es un máximo común divisor si satisface las siguientes propiedades.
i) c es divisor de a y b.
ii) Si d es divisor de a y b, entonces $d \mid c$.

Teorema. Si existe el m.c.d entre a y b, entonces es único

Demostración (Por absurdo)

1) $c_1 = $ m.c.d. (a,b)	Hipótesis
2) $c_2 = $ m.c.d. (a,b)	Hipótesis
3) $c_1 \neq c_2$	Hipótesis - absurdo
4) c_1 es divisor de a,b	(2)(4) y (ii)
5) c_2 es divisor de a,b	(2),(4) y (ii)
6) $c_1 \mid c_2$	Teorema
7) $c_2 \mid c_1$	Hipótesis
8) $c_1 = \pm c_2$	(9) y (8)
9) $c_1>0$, $c_2>0$	(10) y (3).
10) $c_1 = c_2$	
11) Contradicción entre (3) y (10)	

Teorema. - Existencia del m.c.d -
Si $a,b \in \mathbb{Z}$, $ab \neq 0$, entonces existe el m.c.d. entre a y b. Además, existen $m_0, n_0 \in \mathbb{Z}$ tales que $c = m_0 a + n_0 b$. (Notación $c = (a,b)$, m.c.d (a,b))

Demostración

1. $m = \{ma+nb \mid m,n \in \mathbb{Z}\}$	Nomenclatura
1.5 $a \neq 0$ y $b \neq 0$	Hip
2.. Para $m=a$ y $n=b$ $aa+bb>0$	(1.5) y Teorema conocido
3.. m posee al menos un entero positivo	(1) y (3)
4.. $m^+ \{x \in m \mid x>0\}$	(3) y (4)
5.. $m^+ \neq \emptyset$	(5) y principio del buen orden
6. existe el menor elemento de m^+	(6) y nomenclatura.
7.. $c = \min\{m^+\}$	
8.. $c = m_0 a + n_0 b$ para algún $m_0, n_0 \in \mathbb{Z}$	(8) y (1)

P.D $c|x$ para todo $x \in m$

9) $x \in m$
10) $x = ma + nb$ para algún $n, m \in \mathbb{Z}$
11) $x = zc + r$, $0 \leq r < c$
12) $ma + nb = z(m_0 a + n_0 b) + r$
13) $r = (m - zm_0)a + b(m - zn_0)$
14) $r \in m$
15) $r = 0$
16) $ma + nb = z(m_0 a + n_0 b)$
17) $x = zc$
18) $c|x$

P.D $a, b \in m$.

19) $a = 1.a + 0b$
20) $a \in m$
21) $b = 0.a + 1.b$
22) $b \in m$.
23) $c|a$ y $c|b$

P.D.
24) $d|a$ y $d|b$
P.D $d|c$
25) $d|an_0 + bn_0$
26) $d|c$
27) $c = m.c.d.(a, b)$

Hipótesis
(a) y (1)
(10) y Algoritmo de eclides
(11) y (10) y 8
(12)
(13)
(11), def de c
(11) y (15)
(16) y notación.
(17) y notación

(1)
(19)
(1)
(21)
(**) (18)

Hipótesis

(24) y Teorema de la combinación lineal
(*) (25) y (def de c)
(26), (23) y def de m.c.d.

Ejercicio.
$A = \{2m + 5n \mid m, n \in \mathbb{Z}\}$. Pruebe que $A = \mathbb{Z}$

Demostración.
1) A contiene los pares
P.D A contiene los impares
2) $k \in \mathbb{Z}$
P.D $2k+1 \in A$
3) $2k+1 = 2(k-2) + 5$
4) $2k+1 \in A$.

Ejercicio. $A = \{m\,6 + n\,15 \mid m, n \in \mathbb{Z}$
¿$1 \in m$?
$1 \notin A$.
Demostración

1. $1 \in A$ Hipótesis
2. $1 = 6m + 15n$ para $n, m \in \mathbb{Z}$ (1) y def de A
3. $1 = 3(2m + 5n)$ para $n, m \in \mathbb{Z}$ (2)
4. 1 es múltiplo de 3 (3)
5. 1 no es múltiplo de 3 mul 3 = $\{0, \pm 3 \pm 6, \ldots\}$
6. Contradicción entre 5 y 6.

Definición - Primos relativos - a y b son primos relativos si y solo si $m.c.d.(a,b)=1$.

Teorema. Si a y b son primos relativos, entonces existen n_0 y $m_0 \in \mathbb{Z}$ tales que

$$m_0 a + n_0 b = 1.$$

Demostración

1. $H(a,3)=1$	Hipótesis.
2 Existen $n_0, m_0 \in \mathbb{Z}$ tales que $1=m_0a+n_0b$.	(1) y Teo. Existencia del m.cd

Definición - Números primos - Un número $p \in \mathbb{Z}$ es primo si y solo si sus únicos divisores son $\mp p$ y ± 1 y $p>0$.

Teorema. Si p es primo, entonces para todo $n \in \mathbb{N}$ $(p,n)=1$ ó $n=kp$

Demostración

1.) p es un primo	Hipótesis
2.) $n \in \mathbb{N}$	Hipótesis
3.) $(p,n)=1$ o $(p,n)=p$	(def de primo) y (m.c.d)
4.) $(p,n)=1$	(3)
5.) $(p,n)=p$	(3)
6.) $n=kp$	(def de m. c.d)
7.) $(p,n)=1$ o $n=kp$	(4)(6)

Teorema Si a es primo relativo a b y $a \mid bc$ entonces $a \mid c$.

Demostración

1) a primo relativo de b	Hipótes.
2) $(a,b)=1$	(1) y def primo
3) Existen $n_0, m_0 \in \mathbb{Z}$ tal que $m_0a+n_0b=1$	(2) y teorema
4) $a \mid bc$	Hipotesis.
5) $ak=bc$ para $k \in \mathbb{Z}$	(4) y def de divisor
6) $bcn_0=kan_0$	(5)
7) $m_0ac+n_0bc=c$	(3)
8) $m_0ac+kan_0=c$	(6) y (7)
9) $a(m_0c+kn_0)=c$	(8) ,
10) $a \mid c$	(9) y def

Teorema. Si p es primo y $p \mid b_1 b_2 \cdots b_n$ entonces $p \mid b_i$, para algún i.

Demostración (Por absurdo

1) p. primo	Hipótesis
2) $p \mid b_1 b_2 \cdots b_n$	Hipótesis
3) $p \nmid b_i$ para todo i	Hip
4) $p \mid b_1 (b_2 \cdot b_2 \cdots b_n)$	(2)
5) $p \mid b_2 (b_3 \cdots b_n)$	(4) y Teore.
6) $p \mid b_2 (b_3 \cdots b_n)$	(5) y (Asoci)
7) $p \mid b_3 \cdots b_n$	(6) y Teo
8) $p \mid b_n$	(7) y repet
9) contradicción (3,8)	(3) y (8)

Teorema - Teorema Fundamental de la aritmética -

Todo entero mayor o igual que 2 es producto de números primos. (Únicos)

Demostración (Inducción)

1) $n = 2$ Hipótesis
2) n es producto de primos
3) Enunciado verdadero para $k < n$
4) n es primo o n no es primo. Tercero excluido
5) n es primo Hip.
6) $n <$ producto de primos
7) n no es primo
8) $n = a \cdot b$ con $a, b \in \mathbb{Z}$ y $a, b < n$
9) $a = p_1 \cdot p_2 \cdots p_r$ con $p_1, p_2, \ldots, p_r$ - primos
10) $b = q_1 \cdot q_2 \cdots q_s$ con $q_1 \cdot q_2 \cdots q_s$ - primos
11) $n = (p_1 \cdots p_r)(q_{r+1} \cdots q_{r+s})$
12) n es producto de primos.

Demostración (Inducción)

13) $n = p_1 \cdots p_r$ y $n = q_1 \cdots q_s$ con $p_i \neq q_j$ para todo j Hipótesis
14) $n = p_1 (p_2 \cdots p_r)$
15) $n \mid p_1$ es entero
16) $p_1 \mid q_1 \cdots q_s$
17) $p_i \mid q_i$ para algún q_i
18) $q_i = 1 b p_1$
19) $k = 1$ y $p_1 = q_i$
20) Reordenamos q_j's de modo que q_i esté al principio
$n = q_1' q_2' \cdots q_s'$
con $q_i' = q_i$
21) $n / p_i = p_2 \cdot p_3 \cdots p_r$
22) $n / p_1 = n$
23) n / p_1 tiene descomposición única
24) $n / p_1 = q_2' q_3' \cdots q_r'$
25) $r = s$ y $p_i = q_j$
26) Contradicción (13, 25)

Lunes 21 de junio de 2021.

Teorema. Los números primos son infinitos.

Demostración: (Por absurdo)

1) Existe una cantidad finita de primos Hipótesis
2) $P = \{p_1, \ldots, p_n\}$, ordenados como $p_1 < p_2 < \cdots < p_n$ (1)
3) $N = p_1 p_2 p_3 \cdots p_n + 1$ Notación y (1)

4) N es primo o N no es primo.
5) N es primo
6) $N > p_i$, para todo $i \in \{1,\dots,n\}$
7) $N \notin P$
8) N no es primo
9) Contradicción (5, 8)
10) N no es primo
11) $N = q_1 q_2 \cdots q_n$ donde q_i son primos, posiblemente con repeticiones
12) $q_1 = p_j$ para algún j
13) $p_i \mid N$
14) $p_j \mid p_1 p_2 \cdots p_n$ para algún j
15) $p \mid 1$
16) $p = 1$ ó $p = -1$
17) $p \geq 2$
18) $p \neq 1$ y $p \neq -1$
19) Cont (18, 20)

Laboratorio.
Ejercicio 1: Algoritmo de euclides (sin división ni resto o módulo)
Ejercicio 2: Algoritmo para saber si es primo
Miércoles, 23 de junio de 2021.

Congruencias.

Definición: Sea $n > 0$, $n \in \mathbb{Z}$ $a \underset{n}{\sim} b$ si y solo si $n \mid a-b$

Así, «$\underset{n}{\sim}$» es una relación de equivalencia.

Demostración
Reflexiva P.D. $a \underset{n}{\sim} a$
1) $n \mid 0$
2) $n \mid a-a$
3) $a \sim a$

$0 = 1 \cdot 0$ y def $a \mid b$
1
2 y def $(\underset{n}{\sim})$

Simetria
4) $a \underset{n}{\sim} b$
5) $n \mid a-b$
6) Existe $k \in \mathbb{Z}$ tal que $nk = a-b$
7) $-nk = b-a$
8) $nk^* = b-a$ $\quad n^* \in \mathbb{Z}$
9) $n \mid b-a$
10) $b \underset{n}{\sim} a$

Hipótesis
4) y def de $\underset{n}{\sim}$
5) y def de $\mid$
6) y manipulación algebraica
7) y notación
8) y def de $\mid$
9) y def de $\underset{n}{\sim}$

Transitiva si $a \underset{n}{\sim} b$ y $b \underset{n}{\sim} c$ P.D $a \underset{n}{\sim} c$.
11) $a \underset{n}{\sim} b$, $b \underset{n}{\sim} c$
12) $n \mid a-b$ y $n \mid b-c$
13) $n \mid (a-b)+(b-c)$

Hipótesis
11) y def de $\underset{n}{\sim}$
12) y teorema

14) $n \mid a-c$ — 13) y manipulación algebraica

15) $a \sim_n c$ — 14) y def de $\sim_n$

Ejemplo si $n=2$, $a \sim_2 b \iff 2 \mid a-b$ (ie. $a-b$ es par)

¿Cuáles son las clases de equivalencia de $\sim_2$?

$\mathcal{C} = \{$ Pares, Impares $\}$

a) Notar que Pares $\cup$ Impares $= \mathbb{Z}$

b) Pares $\cap$ Impares $= \emptyset$

② Repito ① con $n=3$

$\mathcal{C}_3 = \{ el(0)$

$el(0) = \{3n \mid n \in \mathbb{Z}$

$= \{0, \pm 3, \pm 6, \pm 9, \ldots \}$

$el(1) =$ ~~[illegible]~~

$= \{-5, -2, 1, 4, \ldots \}$

$el(2) \{-1, 2, 5, 8$

Teorema. La relación $\sim_n$ define n clases de equivalencia

Demostración

1) $a \in \mathbb{Z}$ — Hipótesis

2) $a = kn + r$ para algún $k \in \mathbb{Z}$, $r \in \mathbb{Z}$ $0 \leq r < n$

3) $nk = a - r$

4) $n \mid a - r$

5) $a \sim_n r$

6) $r \in el(a)$

7) $el(r) = el(a)$

8) Hay a lo más, n clases de equivalencia

P.D. Hay exactamente n clases de equivalencia

Por absurdo

9) Supongamos que hay menos de n clases de equivalencia — (

10) $el(r) = el(r')$ con $0 \leq r < r' < n$ — 9 y prop de clases

11) $r' \in el(r)$ — 10 y def de clase

12) $r' \sim r$ — 11 y def $el(a)$

13) $n \mid r' - r$ — 12 y def $\sim_n$

14) $nj = r' - r$ — 13 y def $a \mid b$

15) $0 \leq r - r < n$ — 10

16) $0 < j < 1$ — 14, 15

17) No hay enteros entre 0 y 1

18) contradicción (16, 17)

Notación: Escribiremos $a = b \mod (n)$ en lugar de a

Se lee "a congruente con b módulo n"

Teorema. $a \equiv b \mod (n)$ y $c \equiv d \mod (n)$, $a + c \equiv b + d \mod n$.

Demostración

1) $a \equiv b \mod n$ y $c \equiv d \mod n$ — Hipótesis

2) $n \mid a-b$ y $n \mid c-d$ — 1) y def $\equiv$

3) $n \mid (a-b) + (c-d)$ — 2) y teorema

4) $n \mid (a+c) - (b+d)$ — 3) y asociativa

5) $a + c = b + d \mod n$ — 4) y def $\equiv$

Teorema. $a \equiv b \mod n$ y $c \equiv d \mod n$, $ac \equiv bd \mod n$, con $a - y$

Clase viernes 25 de junio.

Teorema. Si $ab = ac \mod n$ y a y n son primos relativos, entonces $b \equiv c \mod n$.

Demostración

1) $ab = cd \mod n$ — Hipótesis
2) $n \mid ab - ac$ — (1) y def $\equiv$
3) $n \mid a(b-c)$ — (2) y asociatividad
4) a y n primos relativos — Hipótesis
5) $n \mid b-c$ — (3), (4) y Teorema.

Notación.
En lugar de $\mathcal{C}(a)$, notamos $[a]$ } en congruencia modulo n {

Definición
$[a] + [b] = [a+b]$
$[a] * [b] = [a*b]$

Teorema. La definición anterior es correcta.
Demostración $c \in [a]$, $d \in [b]$, entonces $[c] + [d] = [a+b]$

1) $c \in [a]$ y $d \in [b]$ — Hipótesis
2) $c \equiv a \mod n$ $\quad d \equiv b \mod n$ — (1) y def de $[a]$
3) $c+d \equiv a+b \mod n$ — (2) y teorema anterior
4) $c+d \in [a+b]$ — (3) y def de $[a]$
5) $[a+b] = [c+d]$ — (4) y propiedades de clase
6) $[c]+[d] = [c+d] = [a+b] = [a]+[b]$

Análogamente se puede probar que $[a]*[b] = [a*b]$

Ejemplo

$[2] + [3]$ — Pares + impares. = Impares
$\|$ $\quad$ $\|$ $\quad$ $\|$
pares $\quad$ impares $\quad$ $[2] + [3] = [5]$
$\|$
$[80] + [33] = [113]$

Ejercicio.
Si $a \in \mathbb{Z}$, p primo. Sugerencia: Inducción
Probar que $a^p \equiv a \mod p$. Binomio de Newton
Demostración $(a \in \mathbb{N})$

1) $a = 1$ — Hipótesis
2) p - primo
P.O $1^p \equiv 1 \mod p$
3) $1^p = 1$
4) $1 \equiv 1 \mod p$ $\quad (p \mid 0)$
5) $1^1 \equiv 1 \mod p$
6) El resultado anterior es válido para todo $k \leq a$
7) $(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \binom{p}{3} a^{p-4} + \cdots + \binom{p}{p-1} a^1 + \binom{p}{0} a^0$
8) $\binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a^1 \equiv 0 \mod p$

9) $(a+1)^p \equiv a^{p+1} \mod p$

10) $a^p \equiv a \mod p$.

11) $(a+1)^p \equiv a+1 \mod p$

Teorema $i, j, k \in \mathbb{Z}$

1) $[i]+[j] = [j]+[i]$ } Conmutativas

2) $[i][j] = [j][i]$ }

3) $[i]+([j]+[k]) = ([i]+[j])+[k]$ } asociativa

4) $[i]*([j]*[k]) = ([i][j])[k]$ }

5) $[0]+[i] = [i]$

6) $[1][i] = [i]$

Demostración (3)

3) $\underbrace{[i]}_{\text{estructura gruesa}} + \underbrace{([j]+[k])}_{\text{estructura gruesa}} = [i]+[j+k]$

$= [i+(j+k)]$ estructura fina.

$= [(i+j)+k]$

$= [i+j]+[k]$

$= ([i]+[j])+[k]$

5) $[i]([j][k]) = [i]([jk])$ } Estructura gruesa.

$= [i(jk)]$

estructura fina (producto de números enteros)

$= [(ij)k]$

estructura fina (asociativa de los números enteros)

$= [ij][k]$ } Estructura gruesa

$= ([i][j])[k]$ }

Definición

Al conjunto de todas las clases

$\{[0], [1], \ldots, [n-1]\}$

más las dos operaciones «+» y «·», se denomina $\mathbb{Z}_n$ y a veces se denomina $(\mathbb{Z}_n, +, \cdot)$

Grupos

Lunes 28 de junio de 2021.

Definición Sea G un conjunto no vacío G es un grupo si en G se ha definido una operación binaria «·», que satisface las siguientes propiedades

1) $a \cdot b \in G$, para todo $a, b \in G$ (clausura)

2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in G$ (asociativa)

3) Existe un elemento e tal que $e \cdot a = a \cdot e = a$ (Existencia del inverso)

4) Para todo $a \in G$ existe $b \in G$ tal que $a \cdot b = b \cdot a = e$ (Inverso)

Si G es finito el grupo se conoce como grupo finito

Si G es infinito el grupo se conoce como grupo infinito

Notamos $(G, \cdot)$ para especificar la operación sobre el grupo.

- Si G es un grupo conmutativo, se conoce como grupo conmutativo o abeliano.

Ejemplos.

+ $(\mathbb{Z}, +)$ es un grupo.
- El $0 \in \mathbb{Z}$ es el elemento identidad
- $a \in \mathbb{Z}$ el inverso de a, es $-a$.

+ $(\mathbb{Z}, \cdot)$
- El neutro sería $1 \in \mathbb{Z}$
- No es grupo.

Ejercicio.

Averiguar si el conjunto de todas las funciones biyectivas de A en A, con A un conjunto arbitrario, no vacío, es grupo con la operación composición.

- Clausura

1) Sean $f, g : A \to A$ dos funciones biyectivas,
2) $f \circ g$ es biyectiva
3) $f \circ g \in G$

- Asociativo

4) $f \circ (g \circ c) = (f \circ g) \circ c$

- Existencia del inverso

5) $f : A \to A$ una función biyectiva
6) Consideremos $Id : A \to A$. la identidad es biyectiva
7) $f \circ Id = Id \circ f = f$

- Inverso

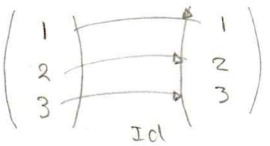
8) $f : A \to A$ una función biyectiva
9) Existe $f^{-1} : A \to A$ una función biyectiva
10) $f \circ f^{-1} = f^{-1} \circ f = Id$

Respuesta: sí es un grupo por los teoremas vistos anteriormente.

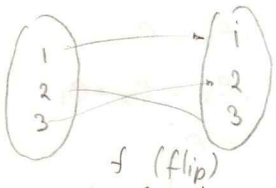
A este grupo lo llamamos $S_A = (S_A, \circ)$

Si $A = \{1, 2, \dots, n\}$ S_A se nota por S_n.

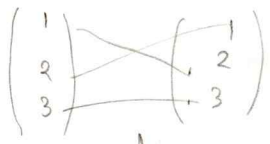
Encontrar $S_3 = \{Id$



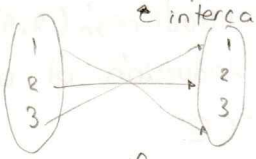
Id



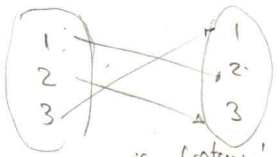
f (flip)
e intercambio



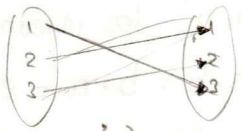
h



g



r (rotación



s)
rotación al contrario

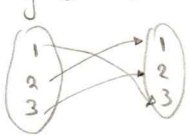
S_3 no es conmutativo pues la composición de funciones no es conmutativa.

$S_3 = \{Id, f, g, h, r, s\}$

Ejercicio: Probar que S_3 no es ableliana.

Consideremos $f, g \in S_3$, tenemos que

$f \circ g$ y $g \circ f$



Así

$f \circ g = r$ y $g \circ f = s$

por lo tanto

$f \circ g = r \neq s = g \circ f$

Miércoles, 30 de junio de 2021

Teorema. Sea G un grupo, entonces

i) El elemento identidad es único

ii) El inverso es único

iii) $(a^{-1})^{-1} = a$

iv) $(ab)^{-1} = b^{-1}a^{-1}$

Demostración

i) Reducción al absurdo

1) La identidad no es única — Hipótesis

2) e_1, e_2 elementos identidad con $e_1 \neq e_2$ — Hipótesis

4) $a \cdot e_1 = e_1 \cdot a = a$ — Para todo $a \in G$ — Def grupo, def identidad

5) $a \cdot e_2 = e_2 \cdot a = a$ — Para todo $a \in G$ — Def grupo, def identidad

6) $e_2' e_1 = e_2$ — (4) con $a = e_2$

7) $e_1 e_2 = e_1$ — (5) con $a = e_1$

8) $e_1' e_2 = e_2 = e_1$ — La identidad conmuta

9) $e_1 = e_2$ — (6), (7) y (8)

10) Contradicción (2,9) — (1) y (9)

ii) (Reducción al absurdo)

1) $a \in G$ — H

2) El inverso de a no es único — H

3) b, b' los inversos de a con $b = b'$ — (2)

4) $a \cdot b = b \cdot a = e$ — Prop del inverso

5) $a \cdot b' = b' \cdot a = e$ — Propiedad del inverso

6) $(b'a)\,b = b'(a\,b)$ — (4) y (5)

7) $e\,b = b'\,e$ — Asociativa

8) $b = b'$ — (4), (5) y (6)

9) Contradicción (3,8)

iii) Demostración

1) $a \in G$ — H

2) $a^{-1} \in G$ — H y prop del inverso

3) $a^{-1}a = a^{-1} \cdot a = e$ — prop del inverso

4) $a = (a^{-1})^{-1}$ — 3 y teo (ii)

iv) Demostración

1) $(a \cdot b)(b^{-1}a^{-1}) = a(b \cdot b^{-1})a^{-1}$ — Asociativa

2) $= a \cdot a^{-1}$ — def de inverso

3) $= e$ — def de inverso

4) $(b^{-1}a^{-1}) = (ab)^{-1}$ — teo (ii)

Definición

$a^0 = e$, $a^1 = a$, $a^n = a\,a^{n-1}$ $a^{-n} = (a^n)^{-1}$ § definición recursiva

Queda definido a^n, para todo $n \in \mathbb{Z}$

Teorema

Viernes, 2 de julio de 2021

Teorema. Sea G un grupo y $a \in G$, además $m, n \in \mathbb{Z}$

i) Para todo $m \in \mathbb{Z}$, se tiene que $a a^m = a^m \cdot a$

ii) $a^m \cdot a^n = a^{m+n}$

iii) $(a^m)^n = a^{m \cdot n}$

Demostración

i)

1) $a \in G$ — Hipótesis
2) $m > 0$ — Hipótesis
3) $a \cdot a = a \cdot a$ — Identidad
4) $a^1 a = a^1 \cdot a$ — Def a^m, (3)
5) El teorema es cierto para enteras positivas menores que m — Hipótesis
6) $a^1 \cdot a^m = a \cdot (a \cdot a^{m-1})$ — Def a^m
7) $= a \cdot (a^{m-1} a)$ — (5)
8) $= (a \cdot a^{m-1}) \cdot a$ — Asociatividad
9) $= a^m \cdot a$ — Def a^m
10) $m = 0$ — Hipótesis
11) $a^0 a = ea$
12) $= ae$
13) $= a a^0$
14) $m < 0$
15) $-m > 0$
16) $n = -m$
17) $a a^m = a \cdot a^{-n}$
$= a \cdot (a^{-1})^n$

Ejercicio

Si $a^2 \cdot b^2 = (a \cdot b)^2$, entonces G es abeliano

Demostración

1) $a, b \in G$ — H
2) $(ab)^2 = (a \cdot b) \cdot (a \cdot b)$ — Def a^n
3) $a^2 \cdot b^2 = a \cdot a \cdot b \cdot b$ — Def a^n
4) $a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$ — H
5) $b \cdot a = a \cdot b$ — 4 y $a \cdot a^{-1} = e$

Ejercicio. Sea G un grupo tal que $(a\cdot b)^i = a^i b^i$ para tres enteros consecutivos i, y para todo $a, b \in G$. Probar que G es abeliano.

Demostración

1) $a, b \in H$
2) $(a\cdot b)^i = a^i b^i$
3) $(a\cdot b)^{i+1} = a^{i+1} b^{i+1}$
4) $(a\cdot b)^{i+2} = a^{i+2} b^{i+2}$
5) $(a\cdot b)^{i+2} = (a\cdot b)^{i+1}(a\cdot b)$
6) $= a^{i+1} b^{i+1} (a\cdot b)$
7) $a^{i+2} b^{i+2} = a^{i+1} b^{i+1} a b$
8) $a^{i+1} a\, b^{i+1} b = a^{i+1} b^{i+1} a b$
9) $a b^{i+1} = b^{i+1} a$
10) $(a\cdot b)^i (a\cdot b) = a^i a\, b^i b$
11) $b^i a = a b^i$
12) $b\, b^i a = a\cdot b\cdot b^i$
13) $b\, a b^i = a\, b\, b^i$
14) $ba = ab$

Ejercicio Si G es un grupo finito, probar que existe $n \in \mathbb{N}$ tal que $a^n = e$ para todo $a \in G$

Demostración

1) $a \in G$, $a \neq e$ — Hipótesis
2) G finito — Hipótesis
3) la lista $a, a^2, a^3, \ldots$ solo tiene un número finito de elementos distintos — (2)
4) $a^i = a^j$ para ciertos i, j con $i < j$ — (3)
5) $a^{-i} a^i = a^j a^{-i}$ — (4)
6) $= a^{j-i}$ — Prop $a^0 = e$
   $= e$ — 1-6.
7) Existe $N \in \mathbb{N}$ tal que $a^N = e$

Lunes 5 de julio de 2021

Si G es un grupo de orden par, entonces existe $a \in G$, tal que $a^2 = e$, con $a = e$

Demostración (Absurdo) $x^2 = e \Rightarrow x\,x = e \Rightarrow x = x^{-1} \Rightarrow$

0) No existe $x \neq e$ tal que
1) G es un grupo par — Hipótesis
2) $a \in G$ y $a \neq e$
3) Hacemos una lista de elementos del grupo

$\{e, b_1, b_1^{-1}, b_2, b_2^{-1}, \ldots, b_s, b_s^{-1}\}$

4) $k = 2s+1$
5) k es impar
6) El orden de G es impar
7) Contradicción (1, 6)

Ejercicio

- Todo grupo de orden 2 es abeliano
- Todo grupo de orden 3 es abeliano

a)

Demostración

1) G un grupo de orden 2 — Hipótesis
2) Los elementos del grupo satisfacen que e, a y $e \neq a$ — Hipótesis
3) $ae = ea$
4) $ee = ee$
5) $a \cdot a = a \cdot a$

b)

6) Grupo de orden 3
7) Enlistamos todos los elementos de G como $\{e\ a\ a^{-1}\}$

¿Qué es una ecuación?

$2x - 3 = 0$

8) $ea = ae$ } obvio.
9) $ea^{-1} = a^{-1}e$ } obvio.
* 10) $aa^{-1} = a^{-1}a = e$ } Muy obvio
11) $aa = aa$ } Muy obvio
12) $a^{-1}a^{-1} = a^{-1}a^{-1}$ } Muy obvio

Teorema - Ley cancelativa-

Sean $a, b \in G$ Las ecuaciones $ax = b$ y $ya = b$, tienen solución única y además

En particular

i) $au = aw$ entonces $u = w$ (cancelativa a la izquierda)

2) $ua = wa$ entonces $u = w$ (cancelativa por la derecha)

Demostración

1) Sean $a, b \in G$
2) $a(a^{-1}b) = (aa^{-1})b$
3) $= eb$
4) $= b$
5) Existe $x = a^{-1}b$ tal que $ax = b$
6) La ecuación $ax = b$ tiene solución

Unicidad (Absurdo)

7) Sean x_1 y $x_2 \in G$ $x_1 \neq x_2$ soluciones de la ecuación
8) $ax_1 = b$
9) $ax_2 = b$
10) $x_1 = a^{-1}b$
11) $x_2 = a^{-1}b$
12) $x_1 = x_2$
13) Contradicción (7, 12)

Demostración (Parte 2)

1) $au = aw$
2) $a^{-1}(au) = a^{-1}(aw)$
3) $(a^{-1}a)u = (a^{-1}a)w$
4) $u = w$.

Miércoles, 7 de julio de 2021

Grupos cíclicos.

Definición: Sea G el conjunto

$$G = \{a^0, a^1, a^2, \ldots, a^{n-1}\} \qquad a^0 = e$$

donde a es un símbolo

[Esta es una definición formal]

Se define formalmente el grupo cíclico g de orden n como $(G, \cdot)$, donde «$\cdot$» se define como

$$a^i \cdot a^j = \begin{cases} a^{i+j} & \text{si} \quad 0 \le i+j \le n-1 \\ a^{i+j-n} & \text{si} \quad i+j \ge n \end{cases}$$

Ejercicio
Probar que la definición anterior es correcta.

Demostración

1) $a^i, a^j \in G$ con $0 \le i-j \le n-1$
2) $i+j \le n-1$
3) $a^i \cdot a^j = a^{i+j}$ $\quad i+j \le n-1$
4) $a^{i+1} \in G$
5) $i+j \ge n$
6) $a^{i+j} = a^{i+j-n}$
7) $i+j-n \le n$
8) $a^i \cdot a^j \in G$

Identidad

1) $a^k \in G$
2) $a^0 a^k = a^{0+k}$
3) $\quad = a^k$
4) Existe $e \in G$ tal que $ea^k = a^k e = a^k$

Inverso

1) $a^k \in G$ con $0 \le k \le n-1$
2) $a^k a^{n-k} = a^{k+n-k}$
3) $\quad = a^n$
4) $\quad = a^0$

El grupo U_p, con p-primo ¿Es grupo $(\mathbb{Z}_n, \cdot)$?

$(\mathbb{R}, \cdot)$ no es un grupo; $\quad U_p = \{1, 2, \ldots, p-1\}$

$(\mathbb{R} - \{0\}, \cdot)$ sí es grupo $\quad (U_p, \cdot)$ multiplicación módulo p.

Demostración

1) $a \cdot b \in U_p$
P.D $a \cdot b \in U_p$
P.D $a \cdot b \neq 0$ (Por absurdo)
2) $a \cdot b = 0$ — Hipótesis
3) $a^{-1}(ab) = a^{-1}0$ — 2), Asociativa
4) $b = 0$ — 1), 4)
5) $b \in U_p$
6) $b \notin U_p$
7) Contradicción (5), (6)

Demostración (Asociativa)
- Caso particular de J_p donde J_p es asociativa.

9 de julio de 2021

Subgrupo.

Sea G un grupo y $H \subseteq G$, H es un grupo de G si y solo si H es un grupo con respecto a la operación de G.

Ejemplos

1) $G = \mathbb{Z}$ los pares son un grupo de $\mathbb{Z}$
2) $G = \mathbb{Z}$ los impares no son un grupo de $\mathbb{Z}$
3) $G = \{a^0, \dots, a^6, a^7\}$ $H = \{0^0, a^4\}$
4) $G = S_3$
   $H = \{Id, S_3\}$ Sí es un grupo y por lo tanto, subgrupo.
5) $G = S_3$ $H = \{Id, F, G\}$ No es subgrupo pues no es grupo (falla la clausura)

Teorema.

Si $H \subseteq H$ y G es un grupo, entonces H es un subgrupo en G si y solo si
i) H verifica la clausura
ii) Si $a \in H$, entonces $a^{-1} \in H$.

Demostración
$\Rightarrow$ Directa
$\Leftarrow$ i) H verifica la clausura
2) Si $a \in H$, entonces $a^{-1} \in H$
P.D H es grupo
3) $aa^{-1} = id = a^{-1}a$
4) $a\,id = a(aa^{-1}) = a = id\,a = (aa^{-1})a$

Asociativa
1) $a, b, c \in H$
P.D $(ab)c = a(bc)$
2. $a, b, c \in G$
3) $a(bc) = (ab)c$

Identidad
1. $a \in H$
2. $a^{-1} \in H$
3. $aa^{-1} \in H$
4. $aa^{-1} = e$
5. $e \in H$

Hipótesis
$H \in G$
(3) y G grupo.
H
(ii) 1
(i) ; (1, 2

Teorema. (finito)
Si $H \subseteq G$ (finito) y G es un grupo, entonces H es un subgrupo de G si y solo si H verifica la clausura.

Demostración
$\Rightarrow$ Directa
$\Leftarrow$ i) H verifica la clausura
2) $a, b, c \in H$
3) $a, b, c \in G$
4) $a(bc) = (ab)c$
5) Existe $n \in \mathbb{N}$ tal que $H = \{x_0, \dots, x_{n-1}\}$
6) Sea $a \in H$
7) Existe $k \in \{1, \dots n\}$ $a^k = e$.
8) $ae = ea = a$.
9) $a \in H$
   PD $a^{-1} \in H$

1) $a \in H$ — Hip
2) G es finito — Hip
3) H es finito — $H \subseteq G$ (3)
4) La lista $a_1, a_2, \ldots$ solo tiene elementos de H — (3) H es finito
5) La lista contiene repeticiones — (4), (3)
6) $a^i = a^j$ para algún i, j. con $i < j$ — (6)
7) $a^i a^{-i} = a^j a^{-i}$ — (7), teo $a^{q+i} = a^i a^i$
8) $e = a^{j-i}$ — (6),
9) $j - i > 1$ — (9)
10) $j - i - 1 > 0$ — (10) y teo $a^{p+q} = a^p a^q$
11) $a^{j-i-1} a = a^{j-i} = e$ — (11) unicidad
12) $a^{j-i-1} = a^{-1}$ — (8) y (9)
13) a^{j-i-1} está en la lista
14) $a^{j-i-1} \in H$

Ejercicio
Sea $H_6 = \mathbb{Z}_6$ y $H_9 = \mathbb{Z}_9$. $H_6 \cap H_9$?

H_6, múltiplos de 6 y H_9, múltiplos de 9. $H_6 \cap H_9$ multiplos de 6 y 9.

$H_6 = \{ \pm 6, \pm 12, \pm 18 \}$

$H_9 = \{ 0, \pm 9, \pm 18, \pm 27 \}$

$H_6 \cap H_9$ = múltiplos de 18
$= \{ 0, \pm 18, \pm 36, \pm 54 \} = \{ n \mid \text{múltiplos de } 18 \}$

$H_6 \cap H_9$ sí es grupo

Teorema. Sea I un conjunto de índices, G grupo y H_i subgrupos para todo $i \in I$

$$\bigcap_{i \in I} H_i$$

es un subgrupo de G

Demostración
P.D. H es subgrupo
Clausura
1) $a, b \in H$
P.D $ab \in H$
2) Para todo $i \in I$ $ab \in H_i$
3) $ab \in H_i$ para todo $i \in I$
4) $ab \in \bigcap_{i \in I} H_i$

Inverso
5) $a \in H$
P.D $a^{-1} \in H$
6) $\forall i \in I$ $a \in H_i$
7) Existe $a^{-1} \in H_i$ para todo $i \in I$
8) $a^{-1} \in \bigcap_{i \in I} H_i$

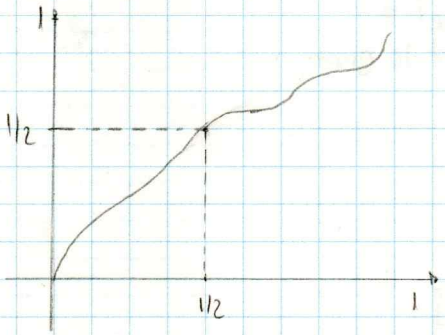
Ejercicio $G = \{ f : [0,1] \to [0,1]$, tal que f es biyectiva? $\}$ $H_{1/2} = \{ f \in G : f(1/2) = 1/2 \}$
Probar que $H_{1/2}$ es un grupo de G

Demostración
P.D H es un subgrupo

1) Sean $f, g \in H_{1/2}$
2) $f(1/2) = 1/2$
3) $g(1/2) = 1/2$
4) $f(g(1/2)) = 1/2$
5) $fg \in H_{1/2}$

Inverso
5) $f \in H_{1/2}$
6) $f(1/2) = 1/2$
P.D Si g es la inversa de f, entonces $g \in H_{1/2}$ $g(1/2) = 1/2$
7) $g(f(1/2)) = g(1/2)$
8) $Id(1/2) = g(1/2)$
9) $1/2 = g(1/2)$
10) $g(1/2) \in H_{1/2}$

Representación gráfica



Hacer lo mismo $H_{1/4}$, $H_{1/8}$. Pruebe que $H_{2^n} : \bigcap H_{1/2^n}$

Demostración

1) Sean $f, g \in \bigcap_{n \in \mathbb{N}} H_{1/2^n}$
2) $f(1/2^n) = 1/2^n$ para todo $n \in \mathbb{N}$
2) $g(1/2^n) = 1/2^n$ para todo $n \in \mathbb{N}$
3) $f(g(1/2^n)) = f(1/2^n)$
$= 1/2^n$
4) $f(g(1/2^n)) = 1/2^n$
5) $f \cdot g \in H_{1/2^n}$

Inverso
1) $f \in H_{1/2}$
2) Si g es la inversa de

Lunes 12 de julio de 2021

Definición Sean G un grupo y $a \in G$ y el conjunto $H = \{a^0 = e, a, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \dots\}$, es un subgrupo de G y se llama un grupo cíclico de G

Notación: $(a) = H$

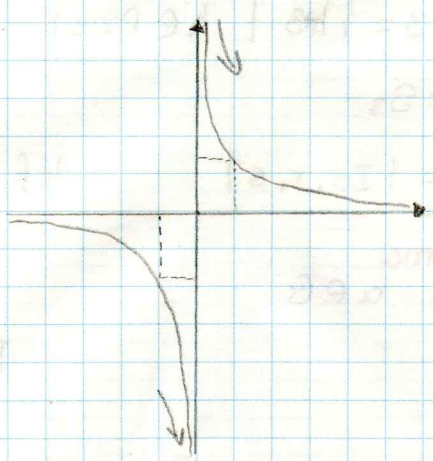
Observación Todo grupo tiene subgrupos cíclicos

Ejemplo $G = (\mathbb{Z}, +)$ y $3 \in G$ $(3) = \{0, 3^{\pm}, 9^{\pm}, \dots\}$

$G = (S_3, \circ)$ $a = f \in G$

$(r) = \{Id, r^{\pm 1}, r^{\pm 2}, r^{\pm 3}, \dots\}$ $(Id) = \{Id\}$

$= \{Id, r, s\}$



$\langle f \rangle = \{ Id, f \}$

Definición Sea G un grupo y H un subgrupo.
Para $a, b \in G$, definimos $a \equiv b \bmod H$ si y solo si $ab^{-1} \in H$.

Teorema La relación $a \equiv b \bmod H$ es una relación de equivalencia.

Demostración
Reflexiva
1) $a \in G$
2) $a^{-1} \in G$
3) $aa^{-1} = e \in G$
4) $a \equiv a \bmod H$

Simétrica
1) $a \equiv b \bmod H$
2) $ab^{-1} \in H$
3) $(ab^{-1})^{-1} \in H$
4) $ba^{-1} \in H$
5) $b \equiv a \bmod H$

Hip
def $\equiv$
def de grupo

Transitiva

1) $a \equiv b \bmod H$
2) $b \equiv c \bmod H$
3) $ab^{-1} \in H$
4) $bc^{-1} \in H$
5) $ab^{-1}bc^{-1} = ac^{-1} \in H$
6) $a \equiv c \bmod H$

Hip
def

Observación Puesto que $a \equiv b \bmod H$ es una relación de equivalencia, esta relación induce las clases de equivalencia. Aquí también usamos la misma notación

$$[a] = \{ x \in G \mid a \equiv x \bmod H \}$$

Definición (Clase lateral derecha)
Sea G un grupo y H un subgrupo de G y $a \in G$, definimos

$$Ha = \{ ha \mid h \in H \}.$$

Ha se llama clase lateral derecha.

Ejemplos.

- $G = \mathbb{Z}$ y $(a = 2)$ $H =$ pares.

  $H3 = \{ h3 \mid h \in \text{Pares} \}$ $\quad h = 2k$ $\quad 2k+3 =$ impares

- $G = S_3$

  $H = \{ Id, r, s \}$ $\quad Hf = Idf = f$ $\quad rf = h$ $\quad sf = g$ $\quad Hf = \{ f, g, h \}$

Teorema
Sea $a \in G$

$$[a] = Ha$$

Teorema: Sea G un grupo y H un subgrupo de G, entonces

$$[a] = Ha = \{x \in G \mid a \equiv x \bmod H\}$$

Demostración

($\subseteq$)

1) $x \in [a]$ — Hip
2) $a \equiv x \bmod H$ — Def $[a]$ y 1
3) $ax^{-1} \in H$ — 2 def $\equiv$
4) $h = ax^{-1} \in H$ — Nomencla
5) $hx = a$ — 4 y teo $aa^{-1} = e$
6) $x = h^{-1}a$ — 5 y teo $aa^{-1} = e$
7) $h^{-1} \in H$ — 4 y H subgrupo de G
8) $x \in Ha$ — 7 y def de Ha

($\supseteq$)

1) $x \in Ha$ — Hip
2) $x = ha$ con $h \in H$ — 1 y Def
3) $xa^{-1} = h$ — 2 y $aa^{-1} = e$ y $ae = a$
4) $xa^{-1} \in H$ — 3 y 2
5) $x \equiv a^{-1} \bmod H$ — 4 y def de $\equiv$
6) $x \in [a]$ — 5 y def de $[a]$

Ejemplo

Sea $G = S_3$, $H = \{Id, f\}$ $K = \{Id, r, s\}$

Encontrar todas las clases con respecto a H y K

$$Ha = \{ha \mid h \in H\} = Id = [a] = \{x \in G \mid a \equiv Id \bmod H\} = a\,id^{-1} \in H = aId = \{Id, f\}$$

y

$$af^{-1} \in H = \{f\}.$$

- H: $a \in G$

$Hg = \{Idg, fg\} = \{g, s\}$
$Hh = \{Idh, fh\} = \{h, r\}$
$Hid = H$
$Hf = \{f, Id\}$
$Hr = \{Idr, fr\} = \{r, h\}$
$Hs = \{Ids, fs\} = \{s, g\}$

- K: $a \in G$

$KId = K$
$Kf = \{Idf, rf, sf\} = \{f, g, h\}$
$Kg = \{Idg, rg, sg\} = \{g, h, f\}$
$Kh = \{Idh, rh, sh\} = \{h, f, g\}$
$Kr = \{Idr, rr, rs\} = \{r, s, Id\}$
$Ks = \{Ids, rs, ss\} = \{s, Id, r\}$

$1-3,\ 2-2,\ 3-1$

Teorema.

Sea G un grupo y H un subgrupo de G, entonces, existe una función biyectiva entre las clases laterales derechas.

Demostración

1) G es grupo y H es un subgrupo — Hipótesis
2) $a, b \in G$
3) $f: Ha \longrightarrow Hb$, $ha \longrightarrow f(ha) = hb$
4) $1-1$
5) $x, y \in Ha$ $\quad f(x) = f(y)$
6) $x = h_1a$ con $h_1 \in H$ y $y = h_2a$ con $h_2 \in H$
7) $f(h_1a) = f(h_2a)$
8) $h_1b = h_2b$
9) $h_1 = h_2$
10) $h_1a = h_2a$
11) $x = y$

Sobre

13) $y \in Hb$

P.D Existe $x \in Ha$ $f(x) = y$

14) $y = hb$ con $h \in H$

15) $x = ha$

16 $f(ha) = hb$

17) $f(x) = y$

18) f es sobre

$rf = g$

$fr = h$

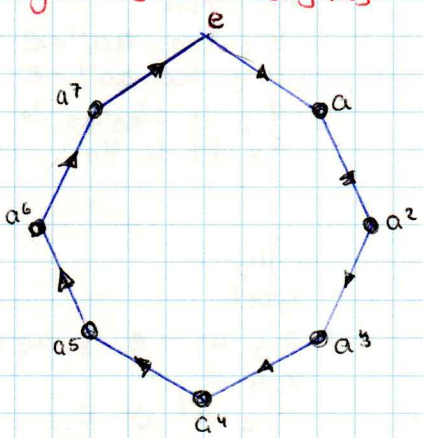
$sf = h$

$fs = g$

Visualización de grupos y subgrupos

1) Diagramas de Caylay

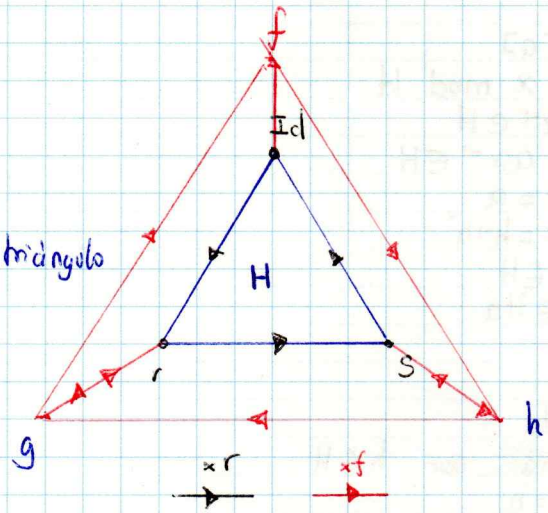
Grupo cíclico



S_3

H corresponde al triángulo interno

Hf corresponde al triángulo externo



El número de flechas que entran, es igual a las que salen

Clase 16 de julio de 2021

Tablas de multiplicar

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\} = \{0, 1, 2, 3\}$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

S_3 convención, primero la fila

	Id	r	s	f	g	h
Id	Id	r	s	f	g	h
r	r	s	Id	g	h	f
s	s	Id	r	h	f	g
f	f	h	g	Id	s	r
g	g	f	h	r	Id	s
h	h	g	f	s	r	Id

clase lateral Hf

azul = subgrupo

Repaso: G - grupo finito

o(G): orden del grupo

Definición: Sea G un grupo, $a \in G$ y n el menor entero positivo tal que $a^n = e$ si tal n existe a este n se le llama el orden de a, y se lo nota por

$$o(a)$$

Ejemplos.

$o(f) = 2$,

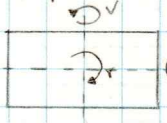
$o(r) = 3$

G - grupo

- ¿Cual es el orden de a?
- ¿Cual es el orden de (a)?

} respuesta $o(a)$, $o(o(a)) = o(a)$

Grupo de KLEIN



Simetrías de un rectángulo no cuadrado

$r = 180°$

$h = 180°$

$v = 180°$

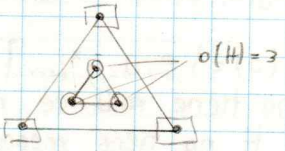
	Id	r	h	v
Id	Id	r	h	v
r	r	Id	v	h
h	h	v	Id	r
v	v	h	r	Id

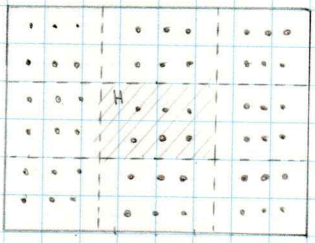
Clase 19 de julio de 2021

Teorema (Teorema de Lagrange)
Si G es un grupo finito y H un subgrupo de G entonces $o(H) \mid o(G)$

Ejemplos y visualización

Si $G = S_3$ y $H = \{Id, r, s\}$ $\quad o(G) = 6$ y $o(H) = 3$





3 | 6

Demostración del teorema

1) G - grupo finito
2) $o(G) = n$
3) H - subgrupo finito
4) $o(H) \leq k \leq n$
5) Hay una biyección entre clases laterales de equivalencia
6) $\bigcup Ha = G$ y $\bigcap Ha \cap Hb = \varnothing$ cuando $a \neq b$
7) $n = pk$ con p el número de clases
8) $k \mid n$
9) $o(H) \mid o(G)$

Hipótesis
↓
Hipótesis
(2) y (3)

(5) y (6)

Definición Sea G un grupo y H un subgrupo de G (G no necesariamente finito)
El número de clases laterales derechas con respecto a H se llama el índice de H en G y se lo nota por $i_G(H)$

Calcular: $i_G(H)$

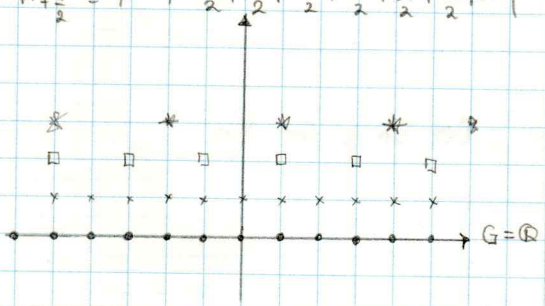
a) $G = S_3$ $\quad H = \{Id, r, s\}$ $\quad i_G(H) = 2$
b) $G = S_3$ $\quad H = \{Id, f\}$ $\quad i_G(H) = 3$
c) $G = \mathbb{Z}$ $\quad H = \text{Pares}$ $\quad i_G(H) = 2$
d) $G = (\mathbb{Q}, +)$ $\quad H = \mathbb{Z}$ $\quad i_G(H) = +\infty$

$H_{+\frac{1}{3}} = \{-2/3, 1/3, 4/3, 7/3, 10/3, \dots\}$

$H_{+\frac{1}{2}} = \{\dots, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}, \dots\}$

$H_{+\frac{1}{2}} \cap H_{+\frac{1}{3}} = \varnothing$

En general, hay infinitas clases laterales derechas



Teorema:
Si $a \in G$ y G es finito, entonces $a^{o(G)} = e$

Clase miércoles 21 de julio

Teorema
Si G es finito y $a \in G$, entonces $o(a) \mid o(G)$

Demostración

1) $n = o(a)$ es decir n es el menor entero positivo tal que $a^n = e$ — Notación

P.D. $n \mid o(G)$

Estrategia: Encontrar un subgrupo de H de G que tenga n elementos

2) $H = (a) = \{e, a, a^2, \ldots\}$ P.D. H tiene n elementos — Hip 1

3) H no tiene más de n elementos

P.D. H no tiene menos de n elementos

Por absurdo

4) H tiene m elementos, con $m < n$

5) Existen repeticiones en la lista $e, a^2, \ldots, a^{n-1}$

6) $a^i = a^j$ con $i \leq m$ y $m < j \leq n-1$

7) $a^{-i}a^i = a^i a^j$

8) $e = a^{j-i}$

9) $j - i > 0$ y $j - i \leq n-1 < n$

10) Existe un entero positivo menor que n tal que $a^k = e$

11) Contradicción (1, 10)

Demostración (Teorema clase pasada)

1) $o(a) \mid o(G)$

2) $o(a)\, m = o(G)$

3) $a^{o(G)} = a^{o(a)m}$

4) $= (a^{o(a)})^m$

5) $= (e)^m$

6) $= e$

Función de Euler (φ)

- $\varphi(1)$
- $\varphi(n)$ = número de primos relativos que son menores que n

Ejemplo

$\varphi(15) = 8$ $\{1, 2, 4, 7, 8, 11, 13, 14\}$

$\varphi(8) = 4$ $\{1, 3, 5, 7\}$

Teorema.

Si n es un entero positivo, entonces (y a es primo relativo con n)

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Demostración:

1) U_n tiene $\varphi(n)$ elementos. (los números primos menores que n) Def U_n y def φ_n

2) $a^{\varphi(n)} = e$ con e, elemento identidad de U_n

3) $a^{\varphi(n)} = 1 \bmod n$.

Teorema (Teorema de Fermat)

Si p es primo, entonces $a^p \equiv a \bmod p$. (con a un entero)

Demostración

1) $\varphi(p) = p - 1$

2) $a^{\varphi(p)} \equiv 1 \bmod p$

3) $a^{p-1} \equiv 1 \bmod p$

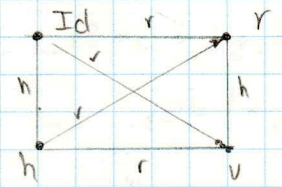
4) $a \equiv a \bmod p$

5) $a^p \equiv a \bmod p$

Teorema:
Si G es un grupo finito y el orden de G $o(G)=p$ con p primo. G es cíclico

Ejercicios
1) Hacer un diagrama de Caylay para el grupo de Klein
2) Hallar la tapla de multiplicar de U_{12}
3) Hacer diagrama de Caylas de U_{12}.

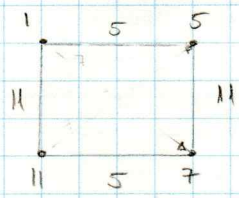
1)



2) Tabla U_{12}

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

3) Diagrama de U_{12}



Clase, 23 de julio de 2021

Demostración (Teorema anterior)
1) G es un grupo finito
2) $o(G)=p$ p primo
3) H un subgrupo de G con $H \neq (e)$
4) $o(H) \mid o(G)$
5) $o(H) \nmid p$
6) $o(H)=p$

10) $o(H)=p$
11) $H \subseteq G$
12) $H=G$
13) $a \in G$, con $a \neq e$
14) (a) es subgrupo de G
15) $(a)=G$
16) G es cíclico

Definición:
Si H y K son subgrupos de G,

$$HK=\{hk \mid h \in H \text{ y } k \in K\}$$

Ejemplo $G=\mathbb{Z}$ H pares
K múltiplos de 3

$HK = \{hk : h \in$ Para $k \in$ Múltiplos de $3\}$

$h = 2i \quad i \in \mathbb{Z} \quad$ y $\quad k = 3j$ con $j \in \mathbb{Z}$

$hk = h + k = 2i + 3j$

Tomando

$2i_1 + 3j_1 + 2i_2 + 3j_2$

$\Rightarrow 2(i_1 + i_2) + 3(j_1 + j_2) \in HK$ * clausura.

⑥ $G = S_3$

$H = \{Id, f\}$

$K = \{Id, g\}$

$HK = \{Id, g, f, s\}$

$KH = \{Id, f, g, r\}$

} No son subgrupos

$G = S_3$

$H = \{Id, f\}$

$K = \{Id, r, s\}$

$HK = \{hk : h \in H, k \in K\}$

$= \{Id, r, s, f, h, g\} = G = S_3$

$KH = \{Id, f, r, g, s, h\} = S_3$

Teorema.
Sea G un grupo y H y K subgrupos de G, entonces $HK = KH$ si y solo si HK es un subgrupo de G

Demostración:

($\Rightarrow$)

1) G es grupo, H y K son subgrupos
2) $HK = KH$

P.D. HK es un subgrupo

P.D. H verifica la clausura y si $a \in H$, $a^{-1} \in H$

3) Sean $a, b \in HK \quad a = h_1k_1 \quad b = h_2k_2$
2) $a = h_1k_1 \quad b = h_2k_2$
3) $ab = (h_1k_1)(h_2k_2)$
4) $= h_1(k_1h_2)k_2$
5) $k_1h_1 \in KH$
6) $k_1h_1 = h_2k_3$
7) $ab = h_1h_3k_3k_2$
8) $ab \in HK$

($\Leftarrow$)

14) HK es subgrupo de G

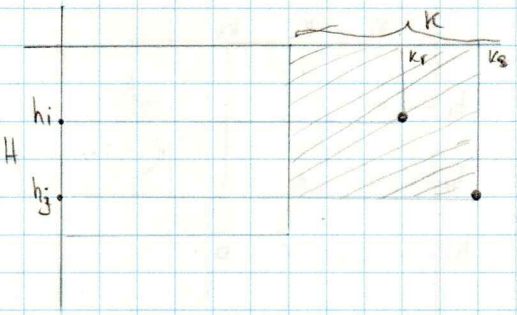
($\subseteq$)

15) $x \in HK$
16) $x^{-1} \in HK$
17) $x^{-1} = hk$
18) $x = (x^{-1})^{-1}$
19) $x = (hk)^{-1}$
20) $= k^{-1}h^{-1}$
21) $x \in KH$

"$\supseteq$" (Similar)

Teorema: Sea G un grupo finito, H, K subgrupo de G finitos y $H \cap K = (e)$

Entonces $o(HK) = o(H) \cap o(K)$



Demostración: (Por el absurdo)

1) $h_i, h_j \in H$ $\quad h_i \neq h_j$
2) $k_r k_s \in K$ $\quad k_r \neq k_s$
3) $h_i k_r = h_j k_s$
4) $k_r = h_i^{-1} h_j k_s$
5) $k_r k_s^{-1} = h_i^{-1} h_j$
6) $k_r k_s^{-1} = e$
7) $k_r = k_s$

Clase, lunes 26 de julio

12, H subgrupo de G de orden 3 $\quad o(HK) = o(H)\,o(K) = 3.4 = 12.$
K subgrupo de G de orden 4

y $H \cap K = \{e\}$, calcular $o(HK)$

Solución
1) $H \cap K = (e)$ $\quad$ Concluimos que $HK = G \quad (HK \subseteq G)$
2) H s.g. $o(H) = 3$
3) K s.g $o(K) = 4$
4) $o(HK) = o(H)\,o(K)$
5) $= 3.4$
6) $= 12.$

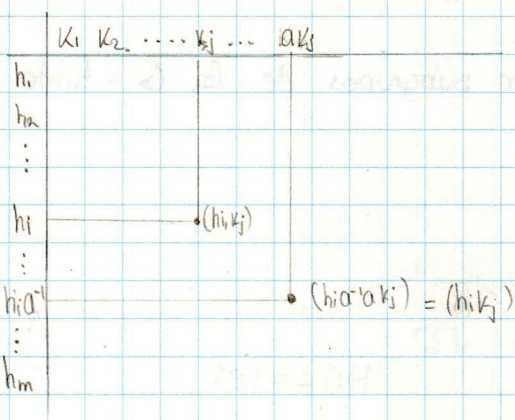
Teorema. Si H y K son subgrupos de G y $H \cap K = \{e, a\}$, con $a \neq e$, entonces $o(HK) = o(H)\,o(K)/2$

Pregunta: Si G es un grupo finito. ¿Cuántas repeticiones hay en una fila de la tabla? ¿Cuántas repeticiones hay en una columna de la tabla?

Respuesta: No hay repeticiones
1) Hay repeticiones
2) Existen $a, b, c \in G$ tal que $ab = ac \quad b \neq c$
3) $a^{-1}ab = a^{-1}ac$
4) $b = c$
5) Contradicción (2,4)

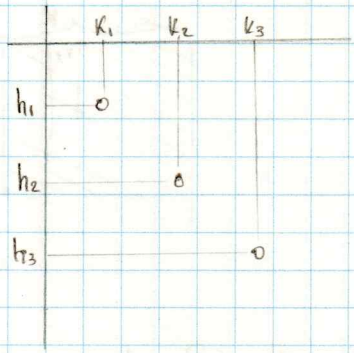
Demostración
P.D. Hay al menos dos repeticiones en la tabla HK

1) $h \in H$ y $k \in K$ $\quad$ Hipótesis
2) $hk \in HK$ $\quad$ 1 y def de HK
3) $ha^{-1} \in H$ $\quad$ 1. Hip $a \in H$
4) $ak \in K$ $\quad$ 2. Hip $a \in K$
5) $(ha^{-1})(ak) \in HK$
6) $h \neq ha^{-1}$
7) $k = ak$
8) Hay al menos dos repeticiones en HK.



Demostración (Por absurdo) Segunda parte

9) Hay más de dos repeticiones
10) Hay mínimo tres repeticiones
11) $h_1, h_2, h_3 \in H$ y $k_1, k_2, k_3 \in H$ dos a dos dijuntos
12) $h_1k_1 = h_2k_2 = h_3k_3$
13) $h_1k_1 = h_2k_2$
14) $k_1k_2^{-1} = h^{-1}h_2$
15) $k_1k_2^{-1} \in K$
16) $h_1^{-1}h_2 \in H$
17) $k_1k_2^{-1} \in K \cap H$
18) $h_1^{-1}h_2 \in K \cap H$
19) $k_1k_2^{-1} = e$ o $k_1k_2^{-1} = a$
20) $k_1k_2^{-1} = e$
21) $k_1 = k_2$
22) Contradicción (21, 11)
23) $k_1k_2^{-1} = a$
24) $k_1 = ak_2$
25) $k_3k_2^{-1} = a$
26) $k_3 = ak_2$
27) $k_1 = k_3$
28) Contradicción (27, 11)
29) $O(HK) = O(H)O(K)/2$



Teorema

Sea G un grupo, H, K subgrupos de G finitos $O(HK) = \frac{O(H)O(K)}{O(H \cap K)}$

Demostración:

Similar a la anterior.

Ejercicio

Sea G un grupo de orden 30, ~~y H un subgrupo de G~~, probar ~~que~~ si G tiene un ~~subgrupo de orden 10~~

Probar que si G tiene un subgrupo de orden 10 y orden 6 y la intersección de los subgrupos de orden 2, entonces el producto de las subgrupos es todo G

Solución

1) $O(H \cap K) = 2$
2) $O(H) = 10$ finito
3) $O(K) = 6$ finito
4) G es un grupo
5) $O(HK) = O(H)O(K)/O(H \cap K) = (10 \cdot 6)/2 = 60/2 = 30$
6) $HK \subseteq G$
7) $O(G) = 30$
8) $HK = G$

Clase miércoles, 28 de julio de 20

Teorema.

Si H, K son subgrupos de G, G - finito y $O(H) > \sqrt{O(G)}$ y $O(K) > \sqrt{O(G)}$, entonces $H \cap K \neq (e)$

Ejemplo:

1) $G = S_3$ 2)

$H = \{Id, f\} < \sqrt{6}$
$K = \{Id, G\} \sqrt{6}$

$H \cap K = \{e\}$

Demostración

1) $HK \subseteq G$
2) $o(G) \geq o(HK)$
3) $\geq \frac{o(H)\,o(K)}{o(H\cap K)}$
4) $\geq \frac{\sqrt{o(G)}\,\sqrt{o(G)}}{o(H\cap K)}$
5) $\geq \frac{o(G)}{o(H\cap K)}$
6) $1 \geq \frac{1}{o(H\cap K)}$
7) $o(H\cap K) \geq 1$
8) $H\cap K \neq (e)$

Teorema:
Si G es un grupo finito de orden pq, con p y q primos y $p>q$. Entonces G tiene a lo más un grupo de orden p.

Ejemplo:
$G = S_3$ — S_3 tiene exactamente un grupo de orden 3
$o(G) = 2\ \ 3$
"p" "q"

Demostración (Por absurdo)

1.	G es un grupo $o(G) = p\cdot q$, p, q primos, $p>q$	Hipótesis
2)	Existen dos grupos H, K,	Hipótesis
3)	$o(G) < p^2$	(1)
4)	$\sqrt{o(G)} < p$	(3)
5)	$\sqrt{o(G)} < o(H)$	(2), (4)
6)	$\sqrt{o(K)} < o(K)$	(2), (4)
7)	$H\cap K \neq (e)$	Teorema anterior (5), 6)
8)	$H\cap K$ subgrupo de H	Teorema, intersección de subgrupos
9)	H solo tiene subgrupos triviales $(e), H$	o(H) es primo, H tiene solo subgrupos triv
10)	$H\cap K = H$	(8) y (9)
11)	$K = H$	(10) y (2)
12)	Contradicción (2, 11)	

Clases laterales izquierdas
Similar a clases laterales derechas, pero cambiando el orden

$\underbrace{Ha}_{\text{clase lateral derecha}}$ $\underbrace{aH}_{\text{clase lateral izquierda}}$

$G = (\mathbb{Z}, +)$

$H+1 = \text{impares} = 1+H$ impares

$G = S_3$

$H = \{Id, r, s\}$

$Hf = \{f, g\ h\}$
$fH = \{f, h, g\}$
$\Big\} Hf = fH$

$G = S_3$
$H = \{Id, f\}$

$Hr = \{r, h\}$
$rH = \{r, g\}$

Teorema:
Existe una biyección entre las clases laterales derechas y el conjunto de clases laterales izquierdas.

Idea de la Demostración
$\mathcal{I}$ = conjunto de clases laterales izquierdas
$\mathcal{D}$ = conjunto de clases laterales derechas

$f: J \longrightarrow D$ Probar que f es biyectiva.
$aH \longmapsto Ha^{-1}$

Clase - viernes 30 de julio de 2021

Subgrupos normales

Sea G un grupo y N un subgrupo de G. N es un subgrupo normal de G si y solo si para todo $g \in G$ y para todo $n \in N$ $gng^{-1} \in N$

N es un subgrupo normal de G si y solo si $gNg^{-1} \subseteq N$

Demostración "$\supseteq$"

1) N sgn de G	Hipótesis
2) $n \in N$ y $g \in G$	Hipótesis
3) $g^{-1}ng \in N$	(1)(2)
4) $g(g^{-1}ng)g^{-1} \in gNg^{-1}$	(3), (2) y (1)
5) $(gg^{-1})n(gg^{-1}) \in gNg^{-1}$	(4), asociatividad
6) $n \in gNg^{-1}$	(5) prop de inverso e identidad

Teorema. N sg de G, N sgn de G si y solo si toda clase lateral izquierda de N es una clase lateral derecha (con respecto a N)

Demostración $\Rightarrow$

1) N es sgn de G	Hipótesis
2) $g \in G$	Hipótesis
3) $N = gNg^{-1}$	Teorema anterior y (1) y (2)
4) $Ng = (gNg^{-1})g$	def de Ng
5) $Ng = (gN)(g^{-1}g)$	(4) y prop asociativa
6) $Ng = gN$	(5), inverso e identidad

($\Leftarrow$)

(7) X clase lateral izquierda		Hipótesis
(8) $X = Ng$	para algún $g \in G$	Hipótesis
(9) $X = g'N$	para algún $g' \in G$	Hipótesis
(10) $g \in gN$		Prop. verdadera
(11) $g \in Ng$		Prop verdadera
(12) $g \in Ng'$		(8), (9) y (10)
(13) $Ng = Ng'$		(11) y (12)
(14) $gN = Ng$		

Teorema $HH = H$ donde H sg de G.

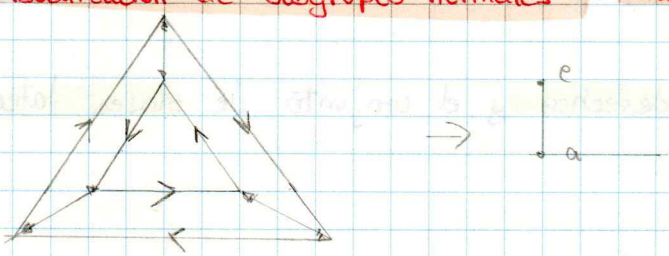
Teorema Si N sgn de G, entonces $NaNb = Nab$

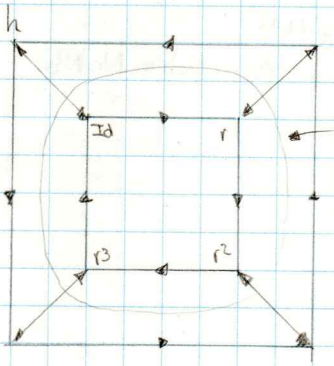
Demostración

1) N sgn de G
2) $a, b \in G$
3) $NaNb = (aN)(Nb)$
$= aNb$
$= (Na)b$
$= Nab$

Clase • lunes 2 de agosto de 2021

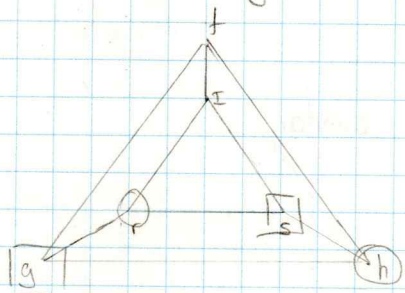
Visualización de subgrupos normales - Diagramas de Cayley





Nh otra clase lateral derecha

¿Qué no es un grupo normal?



H

Ruptura de la continuidad

$N = \{Id, r, s\}$ sgn de G

$Nf = \{f, g, h\}$

$H = \{Id, f\}$, $\overset{\circ}{Hr} = \{r, h\}$, $\overset{\square}{Hs} = \{s, g\}$

	Id	f	g	h	r	s
Id	Id	f	g	h	r	s
f	f	Id	s	r	h	g
g	g	r	Id	s	f	h
h	h	s	r	Id	g	f
r	r	g	h	f	s	Id
s	s	h	f	g	Id	r

Teorema. Sea G un grupo y N un sgn de G, entonces G/N es un grupo con respecto a la operación multiplicación en subconjuntos de un grupo $[AB = \{ab \mid a \in A \text{ y } b \in B\}$

Definición G/N es el conjunto de clases laterales derechas de G en N

Clase · miércoles 4 de agosto de 2021

Teorema: Sea G un grupo y N un subgrupo normal, entonces G/N es un grupo con la operación de producto de subgrupos de un grupo $[AB = \{ab \mid a \in A \text{ y } b \in B\}$ $A, B \subseteq G]$

Demostración: (se lee G partido por N)

Clausura.

1) $X, Y \in G/N$ P.D. $XY \in G/N$
2) $Ng_1 = X$ con $g_1 \in G$
3) $Ng_2 = Y$ con $g_2 \in G$
4) $XY = Ng_1 Ng_2$
5) $= Ng_1g_2$
6) $g_1g_2 \in G$
7) $Ng_1g_2 \in G/N$
8) $XY \in G/N$

Hip.
(1) y def G/N
(2) y def G/N
(2) (3) y (4)
(4) y teorema $N_aN_b = N_{ab}$
(2), (3) y clausura en G
(5), (6) y def G/N
(7) y (4)

Asociatividad

9) $X, Y, Z \in G/N$ P.D. $X(YZ) = (XY)Z$
10) $X = Ng_1$, $Y = Ng_2$, $Z = Ng_3$ con g_1, g_2 y $g_3 \in G$

Hip
(9) y def G/N

11) $X(YZ) = Ng_1(Ng_2 Ng_3)$ (9) y (10)
12) $= Ng_1(Ng_2 g_3)$ (11) y teo $Nab = NaNb$
13) $= Ng_1(g_2 g_3)$ (12)
14) $= N(g_1 g_2)g_3$ (13)
15) $= Ng_1 g_2 Ng_3$ (14)
16) $= (Ng_1 Ng_2)Ng_3$ (15)
17) $= (XY)Z$

Identidad

20) $X \in G/N$ P.D. $NX = XN = X$
21) $X = Ng$
22) $NX = N Ng = Ne\, Ng$
23) $= Neg$
24) $= Ng$
25) $= X$
26) $XN = X$ similar

Inverso

27) $X \in G/N$ P.D. Existe $Y \in G/N$ tq $XY = N$
28) $X = Ng$, $g \in G$
29) $Y = Ng^{-1}$
30) $XY = Ng\, Ng^{-1}$
31) $= Ngg^{-1}$
32) $= Ne$
33) $= N$
34) $YX = N$ similar

Ejercicio Verificar el teorema anterior con $G = \mathbb{Z}$ y N pares.

$(G,+)$ grupo G/N = clases laterales derechas de los pares

$G/N = \{N, N+1\}$
pares impares

	N	$N+1$
N	N	$N+1$
$N+1$	$N+1$	N

Ejercicio
Si G es un grupo y H es un subgrupo de índice 2 de G, pruebe que H es un subgrupo normal de G

Demostración
1) G grupo Hip
2) H sg de G Hip
3) $i_G(H) = 2$ Hip
P.D H sgn de G
4) Número de clases laterales derechas es 2 (3)
5) $D = \{H, Xf\}$, $X \neq H$ (4)
6) $I = \{H, Yf\}$, $Y \neq H$ teo biyección entre clases laterales
7) $X = H^c$ (5) y clases disjuntas
8) $Y = H^c$ (6) y clases disjuntos
9) $X = Y$ (7), (8)
10) Toda clase lateral derecha es clase lateral izquierda (5), (6) y (9)
11) H es subgrupo normal de G (10) y teorema sgn

• Clase • viernes 6 de agosto de 2021

Ejercicio. H es subgrupo de G y para todo $a, b \in G$, existe $c \in G$ tal que $HaHb = Hc$ entonces es subgrupo normal de G.

Demostración.
P. D. $gHg^{-1} \subseteq H$
1) $g \in G$
2) $HgHg^{-1} = Hc$ para algún $c \in G$.
3) $e = ege g^{-1}$ y $e \in H$
4) $e \in HgHg^{-1}$
5) $e \in Hc$
6) $Hc = He = H$
7) $HgHg^{-1} = H$
8) $x \in gHg^{-1}$
9) $x = ghg^{-1}$ para algún $h \in H$
10) $g = eg$
11) $x = egh g^{-1}$
12) $x \in HgHg^{-1}$
13) $x \in H$
14) $gHg^{-1} \subseteq H$
15) H es subgrupo normal de G.

Teorema. Si G es finito y N un subgrupo normal, entonces $o(G/N) = o(G)/o(N)$.

Demostración
1) G - finito
2) N sgn.
3) $o(G) =$ # clases laterales derechas $\cdot\ o(N)$
4) $o(G) = o(G/N) \cdot o(N)$
5) $o(G/N) = o(G)/o(N)$.

Ejercicio. Si N es un subgrupo normal de G y H es un subgrupo de G, entonces NH es subgrupo de G

Demostración P.D $NH = HN$.
1) $x \in NH$ P.D $x \in HN$
2) $x = nk$ $n \in N$ y $h \in H$
3) $x \in Nh$
4) $Nh = hN$
5) $x \in hN$
6) $x = hn'$
7) $x = HN$
8) $NH \subseteq HN$.
9) $y \in HN$
10) $y = hn_1$ para algún $h_1 \in H$ y $n_1 \in N$
11) $y \in h_1 N$
12) $y \in Nh_1$
13) $y = n'' h_1$
14) $y \in NH$
15) $HN \subseteq NH$
16) $NH = HN$

Ejercicio. Probar que la intersección de dos subgrupos normales de G es un subgrupo normal de G

Demostración
1) N, H sgn normales de G. Hipótesis
2) $N \cap H$ sg de G
3) $g \in G$ y $x \in N \cap H$
P.D $gxg^{-1} \in N \cap H$
4) $x \in N$ y $x \in H$
5) $gxg^{-1} \in N$ y $gxg^{-1} \in H$

6) $gxg^{-1} \in N \cap H$
7) $H \cap N$ es un subgrupo normal.

Ejercicio. Todo subgrupo de un grupo abeliano es normal

Demostración
1) G un grupo abeliano y $H \subseteq G$ un subgrupo de G
P.D. H es normal.
2) Sea $g \in G$. y $h \in H$
P.D $ghg^{-1} \in H$
3) $ghg^{-1} = gg^{-1}h$
4) $= eh$
5) $= h$
6) $ghg^{-1} \in H$.

Ejercicio Si N y H son sgn de G. Probar que NH es subgrupo normal de G.

Demostración
1) G un grupo y N, H sgn de G.
2) NM es subgrupo de G
P.D. NH es normal
3) Sea $x \in NH$
4) $x = nm$ para algún $n \in N$ y $m \in H$
5) $gxg^{-1} = gnmg^{-1}$
6) $= gnemg^{-1}$
7) $= gng^{-1}gmg^{-1}$
8) $= n'm'$
9) $\in NH$

Ejercicio (Grupo cíclico de orden n se llama C_n) (Grupo de Klein IV) (Da simetrías del cuadrado)
Si un cierto subgrupo cíclico T de G es normal en G, entonces todo subgrupo de T es sg normal de G.

Demostración.
1) G un grupo, T sg cn (subgrupo cíclico normal) y $H \subseteq T$ subgrupo normal.
2) $T = \{e, a, a^{\pm 2}, a^{\pm 3}, \dots\}$

Demostración
1) T sgn cíclico de G — Hipótesis
2) H sg de T — Hip
3) $T = (a)$ con $a \in G$ — (1),(2) y def de grupo cíclico
4) H es sg cíclico — Teorema: Todo sg de un sg cíclico es cíclico
5) $H = (a^k)$
P.D. H sgn de G $ghg^{-1} \in H$ $h \in H$.
$\underbrace{\quad}_{r \text{ veces}}$ $g(a^k)^r g^{-1}$ con r entero
6) $g(a^k)^r g^{-1} = g a^k \cdots a^k g^{-1}$ — def b^m
7) $= g a^k g^{-1} g a^k g^{-1} g a^k g^{-1} \cdots g a^k g^{-1}$ — $g^{-1}g = e$
8) $= (gaag^{-1})(gaag^{-1}) \cdots (gaag^{-1}) = (gaag^{-1})^r$ — (7) y def b^m y asociativ
9) $= \underbrace{(ga^s g^{-1})^k}_{\in T}$ — similar (6-8)
10) $g(a^s)^r g^{-1} \in T$ — (9) y (1)
11) $ga^s g^{-1} = a^s$ para algún s
12) $(a^s)^k = (a^k)^s \in T$
13) $(a^k)^s \in H$
14) $ghg^{-1} \in H$

Anillos → anillo

Definición

Sea R un conjunto no vacío, si en R están definidas dos operaciones notadas por «$+$» y «$\cdot$» que satisfacen las siguientes propiedades

1) $a+b \in R$, para todo $a, b \in R$
2) $a+b = b+a$
3) $a+(b+c) = (a+b)+c$
4) Existe 0 tal que para todo $a \in R$ $a+0 = a$
5) Para todo $a \in R$, existe $b \in R$ tal que $a+b = 0$

Propiedades de grupo abeliano

6) $a.b \in R$
7) $(a.b).c = a.(b.c)$
8) $a.(b+c) = a.b + a.c$
8.b) $(a+b).c = a.c + b.c$

Propiedades de semigrupo. Combinada. (prop. distributiva)

Nota: si $a.b = b.a$, el anillo se llama anillo conmutativo.

Ejercicio.

Dar ejemplos de anillos.

(a) Infinito y abeliano Enteros. $(\mathbb{C}, +, \cdot)$; $(\mathbb{Z}, +, \cdot)$; (Polinomios coeficientes reales, $+, \cdot$)

(b) Infinito y no abeliano E. Matrices

(c) Finito abeliano $\mathbb{Z}_n$ con la suma y producto usual $(\mathbb{Z}_n, +, \cdot)$

El anillo de los cuaterniones

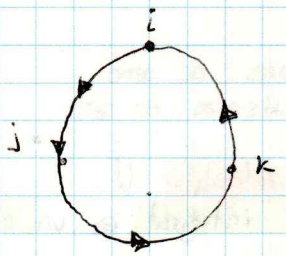
Clase. viernes 13 de agosto de 2021

$(\mathbb{C}, +, \cdot)$ es un anillo.
↳ tiene unidad (respecto a «$\cdot$»)
↳ es abeliano

Todo elemento z de $\mathbb{C} \setminus \{0\}$ tiene inversa si $z = a+bi$ con $a, b \in \mathbb{R}$

Los cuaterniones se generan por analogía con $\mathbb{C}$ añadiendo «unidades imaginarias» i, j, k.
Los cuaterniones se notan por $\mathbb{Q}$

$$\mathbb{Q} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$$



$i \cdot j = k$
$k \cdot j = j$
$i \cdot k = -j$
$j \cdot i = -k$

Si $x, y \in \mathbb{Q}$. $x+y = ?$ $x \cdot y \in ?$

Queremos que $(\mathbb{Q}, +, \cdot)$ sea un anillo.

$$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2) = (a_1+a_2) + (b_1+b_2) i + (c_1+c_2) j + (d_1+d_2) k$$

$$i \cdot i = j \cdot j = k \cdot k = -1$$

Calcular $x \cdot y$

$$\begin{aligned}(1+3j+k)(1-i) &= 1.1 - 1.i + 3j.1 - 3j.i + k.1 - k.i \\ &= 1 - i + 3j + 3k + k - j \\ &= 1 - i + 2j + 4k\end{aligned}$$

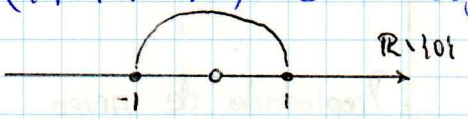
¿Cuál es el inverso de $x = a+bi+cj+dk$?

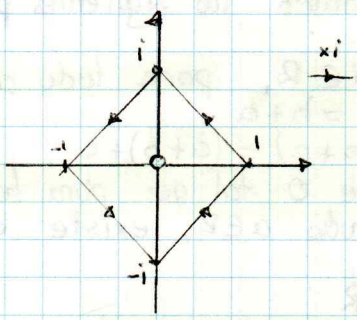
$$x \cdot x^{-1} = 1 \Rightarrow x^{-1} = \frac{1}{a+bi+cj+dk} = \frac{1}{a+bi+cj+dk} \cdot \frac{a-bi-cj-dk}{a-bi-cj-dk}$$

$= \frac{1}{a^2+b^2+c^2+d^2} \cdot (a-bi-cj-dk)$

$\{-1,1\} \subseteq \mathbb{R}$ ¿$(\{-1,1\},\cdot)$ qué estructura tiene? Es un subgrupo de $(\mathbb{R}\setminus\{0\},\cdot)$

$(\{i,-i,1,-1\},\cdot)$ es un subgrupo de $(\mathbb{C}\setminus\{0\},\cdot)$





$(\mathbb{Q},\cdot)$ grupo de los cuaterniones subgrupo de $(\mathbb{Q}\setminus\{0\},+)$

$\{1,-1,i,-i,j,-j,k,-k\}$

Dar un ejemplo de R tal que $(R\setminus\{0\},\cdot)$ es finito y es grupo finito y otro ejemplo de $(R\setminus\{0\})$ es finito pero no es grupo.

Respuesta ($R = J_7 \setminus \{0\}$, • multiplicación módulo 7)

	1	2	3	4	5	6
1						
2						
3	3	6	2	5	1	4
4						
5						
6						

Clase • martes 16 de agosto de 2021

Definición -divisor de cero-
Si R es un anillo, entonces $b \in R$ es un divisor de cero si $b \neq 0$, existe $c \in R$ con $c \neq 0$ tal que $bc = 0$

- En J_6 hay divisores de cero ejemplo el 2 es un divisor de cero.
- En J_5 NO hay divisores de cero

Definición -dominio integral-
Un dominio integral integral es un anillo conmutativo que no tiene divisores de cero

Ejemplos:
1) $J_7 = (J_7, +, \cdot)$ es un dominio integral
2) $(\mathbb{R}, +, \cdot)$
3) $(\geq, +, \cdot)$

Definición - Anillo con división-
Un anillo R es un anillo con división si $(R\setminus\{0\},\cdot)$ es un grupo.

Definición - Campo-
Un cuerpo o campo es un anillo con división conmutativo

Ejemplos:

Ejemplos

	(1)	(2)	(3)	(4)
$\mathbb{C}$	0	1	1	1
$\mathbb{R}$	0	1	1	1
$\mathbb{Q}$	0	0	0	0
$\mathbb{Z}_p$ con p primo	1	1	1	1

① Finito ③ Dominio integral
② Abeliano ④ Campo.

Teorema:
Sea R un anillo, entonces para todo $a \in R$
- $a \cdot 0 = 0 \cdot a = 0$
- $a(-b) = (-a)\cdot(b) = -(a.b)$
- $(-a)(-b) = ab$

Si adicionalmente R es un anillo con unidad
- $(-1)a = -a$
- $(-1)(-1) = 1$

Demostración:
Propiedad i)
1) $a \in R$
2) $a \cdot 0 = a(0+0)$
3) $= a0 + a0$
4) $a \cdot 0 = 0$.

Hipotesis
0 es el neutro
(2) y distributiva
(2), (3), unicidad del cero.

Propiedad ii)
1) $a, b \in R$
2) $a \cdot 0 = a(b+(-b))$
3) $= ab + a(-b)$
4) $a \cdot 0 = 0$
5) $ab + a(-b) = 0$
6) $-(ab) = a(-b)$

Hip
$0 = b + (-b)$
Distributiva
Parte i
(3), (4)
Unicidad del inverso.

Propiedad (iii)
1) $x, y \in R$
2) $(-x)(-y) = -(-xy)$
3) $= -(-xy)$
4) $= xy$

Propiedades (iv) y (v) son casi triviales luego de (ii) y (iii)

Ejercicio.
Implementar $\mathbb{Q}$ con las operaciones $+, \cdot, ^{-1}$
Clase • 18 de agosto de 2021

Teorema: Todo dominio integral finito es un campo

Demostración
1) D dominio integral
Idea: Analizar si una fila de la tabla de multiplicar absorbe o no elementos. PD. $D = E$

2) $a \in D$, $a \neq 0$
3) $E = \{ax_1, \ldots, ax_n\}$
P.D. No hay repeticiones $o(E) = n$.
Por reducción al absurdo

4) $ax_i = ax_j$ con $i \neq j$ — Hip

5) $ax_i + (-ax_j) = ax_j + (-ax_j) = 0$

6) $ax_i + a(-x_j) = 0$

7) $a(x_i + (-x_j)) = 0$

8) $x_i + (-x_j) = 0$

9) $-x_i = x_j$ — Unicidad del inverso

10) $-(-x_i) = -(-x_j)$

11) $x_i = x_j$

12) Contradicción (1, 11)

13) $E = D$ — $F \subseteq D$, $o(E) = o(D)$

14) $a = ax_j$

15) x_j es la unidad de a.

16) $y \in D$

17) $y \in E$

18) $y = ax_i$

19) $x_j y = x_j a x_i$

20) $= (x_j \cdot a) \cdot x_i$

21) $= a \cdot x_i$

22) $= y$

23) $x_j y = y$

24) x_j es la unidad de D

25) $x_j = 1$

P. D.

26) $b \in D$

27) $1 \in D = E$

28) $1 = ax_k$ para algún k

29) $x_k = a^{-1}$

30) Todo a tiene inverso

Ejercicio.
Probar que $\mathbb{Z}_p$ es un campo, cuando p es primo

Demostración

1) $\mathbb{Z}_p$ es finito

P. D $\mathbb{Z}_p$ es un dominio integral

Por absurdo

2) $a, b \in \mathbb{Z}_p$, $a \neq 0$, $b \neq 0$ y $ab = 0$

3) $ab \equiv 0 \mod p$

4) $p \mid ab$ — 3 y def $x \equiv y \mod p$

5) $p \mid a$ o $p \mid b$ — 4 y teo

6) $a \equiv 0 \mod p$, $b \equiv 0 \mod p$ — p primo y $a < p$, $b < p$

Ejercicio
Si para todo $x \in R$, $x^2 = x$, probar que R es conmutativo (anillo)

I Demostración

1) $a, b \in R$

2) $(a+b)^2 = (a+b)(a+b)$

3) $= (a+b)a + (a+b)b$

4) $= a^2 + ba + ab + b^2$

5) $= a + ba + ab + b$

6) $(a+b)^2 = (a+b)$

7) $a + b = a + ba + ab + b$

8) $0 = ba + ab$

9) $ba = -ab$

II

P.D $x = -x$

10) $(-x) = (-x)^2$
11) $= (-x)(-x)$
12) $= x \cdot x$
13) $= x^2$
14) $= x$
15) $-x = x$
16) $ab = ba$

Ideales

(Es el análogo de grupos normales para anillos)

Definición

Sea $\mathcal{U}$ un subconjunto de un anillo, entonces $\mathcal{U}$ es un ideal de R si satisface las siguientes propiedades

i) $\mathcal{U}$ es un subgrupo de R bajo la adición
ii) Para todo $u \in \mathcal{U}$ y para todo $r \in R$ $ur \in \mathcal{U}$ y $ru \in \mathcal{U}$

Ejemplos.

- $\mathcal{U} = \{0\}$, es un ideal del anillo $\mathbb{R}$
- $R = \mathbb{Z}$ $\mathcal{U}$ = Pares es un ideal de $\mathbb{Z}$

  i) $(\mathcal{U}, +)$ es un grupo

  ii) Para todo $n \in \mathcal{U}$ y para todo $m \in \mathbb{Z}$

  $$nm \in \mathcal{U} \quad y \quad mn \in \mathcal{U}$$

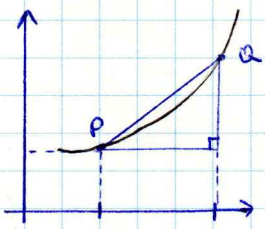
- R = polinomios

  $\mathcal{U} = \{(x^2+1)p(x) \mid p \text{ es polinomio}\}$

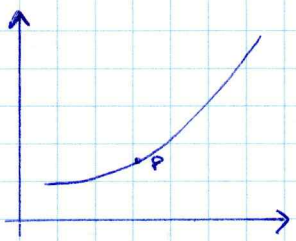
- (Del análisis no estándar)

Clase • viernes 20 de agosto de 2021

Newton



Leibniz



$f'(b) = \frac{dy}{dt}$ $\quad dx \in \mathbb{R}^+$

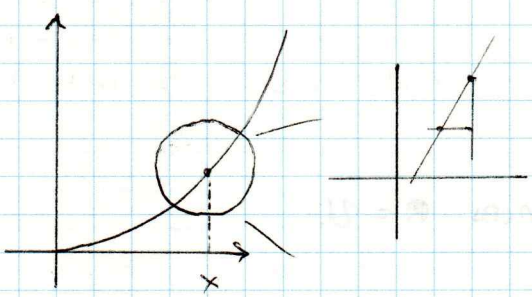
$\forall \varepsilon \in \mathbb{R}^+$

$f(x) = x^2$ $\quad 0 < dx < \varepsilon$

$f'(x) =$ Si hay infinitos

$(dx)^{-1} > u$
$\forall u \in \mathbb{R}$

Pregunta ¿Qué se piede?



$$\frac{f(x+dx) - f(x)}{dx} = \frac{(x+dx)^2 - (x)^2}{dx}$$

$$= \frac{x^2 + 2x\,dx + dx^2 - x^2}{dx}$$

$$= \frac{(2x + dx)\,dx}{dx} = 2x + dx = x$$

Pérdidas.
1) Completitud (Axioma del supremo)
2) Propiedad arquimediana
3) Se pierde la igualdad.

Los infinitesimales

I es un ideal en $\mathbb{R}^*$

$F = \{\mathbb{R}^* \mid F$ anillo de los finitos.
I es un ideal en en F

Definición:
Sea $\mathcal{U}$ un ideal de un anillo R, entonces

$$R/U = \{U \overset{def}{=} \{\underbrace{U + a}_{a+\mathcal{U}} \dashv$$

$$(a+\mathcal{U}) + (b+\mathcal{U}) = (a+b)+\mathcal{U}$$

$$(a+\mathcal{U})\cdot(b+\mathcal{U}) = a\cdot b + \mathcal{U}$$

Teorema:
La definición de multiplicación de clases es correcta si $a' \in a+\mathcal{U}$ y $b' \in b+\mathcal{U}$ entonces $(a+\mathcal{U})\cdot(b+\mathcal{U}) = ab+\mathcal{U}$.

Demostración
1) $a' \in a+\mathcal{U}$ y $b' \in b+\mathcal{U}$ Hipótesis
2) $a' = a + u_1$ con $u_1 \in \mathcal{U}$
3) $b' = b + u_2$
4) $(a'+\mathcal{U})(b'+\mathcal{U}) = (a+u_1+\mathcal{U})(b+u_2+\mathcal{U})$
5) $= (a+u_1)(b+u_2) + \mathcal{U}$
6) $= ab + au_2 + u_1 b + u_1 u_2 + \mathcal{U}$
7) $au_2, u_1 b, u_1 u_2 \in \mathcal{U}$
8) $au_2 + u_1 b + u_1 u_2 \in \mathcal{U}$
9) $ab + \mathcal{U}$
10) $(a'+\mathcal{U})\cdot(b'+\mathcal{U}) = ab + \mathcal{U}$

Teorema. $R/\mathcal{U}$ es un anillo.
Demostración
1 $R/\mathcal{U}$ es grupo conmutativo con la suma (Similar a teoría de grupos)

P.D. $R/\mathcal{U}$ satisface las propiedades de anillo con respecto a las otras propiedades

Asociativa
2) $X, Y, Z \in R/\mathcal{U}$
3) $X\cdot(Y\cdot Z) = (X\cdot Y)\cdot Z$
3) $X = a+\mathcal{U}$, $Y = b+\mathcal{U}$, $Z = c+\mathcal{U}$
4) $X\cdot(Y\cdot Z) = (a+U)((b+U)(c+U))$
5) $= (a+U)(bc+U)$
6) $= a(bc)+U$
7) $= (ab)c+U$
8) $= (ab+U)(c+U)$
9) $= ((a+U)(b+U))\cdot(c+U)$
10) $= (X\cdot Y)\cdot Z$

Ejercido
Probar que si $\mathcal{U}$ es un ideal de R, y $1 \in \mathcal{U}$, entonces $R = \mathcal{U}$.

19) $1 \in R$, r tiene unidad
20) $Ra = \{0\}$ v $Ra = R$
21) $a = 1 \cdot a$
22) $Ra \neq \{0\}$
23) $Ra = R$
24) $1 = ba$
25) b es el inverso
26) R es un campo

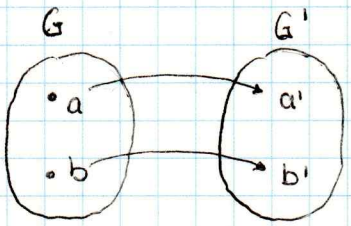
Homomorfismos

Se aplica a grupos y a anillos

Definición

Sea G un grupo, G' otro grupo, $\varphi : G \to G'$ se llama un homomorfismo para todo $a, b \in G$ se tiene que

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$



Ejemplo:

$\varphi : G \to G'$, G cualquier grupo
$x \mapsto$

$\varphi(a \cdot b) = e = e \cdot e = \varphi(a) \cdot \varphi(b)$

Ejemplo

G: Palabras en español

$\cdot$ = '␣'

El␣carro␣es␣grande español.

G' La␣voiture␣est␣grande francés

$\varphi : G \to G'$

φ(El␣carro␣es␣grande)
$= \varphi$(El)␣φ(carro)␣φ(es)␣φ(grande).

3) $(\mathbb{R}, +)$ $(\mathbb{R}^+, \cdot)$
$\varphi : \mathbb{R} \to \mathbb{R}^+$
$x \mapsto 2^x$

$\varphi(x+y) = 2^{x+y} = 2^x 2^y = \varphi(x) \cdot \varphi(y)$

4) $\varphi : \mathbb{R}^+ \to \mathbb{R}$
$x \mapsto \log_{10}(x)$

$\varphi(x \cdot y) = \log_{10}(x \cdot y) = \log_{10}(x) + \log_{10}(y)$
$= \varphi(x) + \varphi(y)$

$\varphi : \mathbb{Z} \to G$ $G = \{e, a\} = C_2$

$\varphi(x+y) = e$ si $x+y$ es par

$\varphi(x+y) = a$ si $x+y$ es impar

Demostración
1) $x, y \in \mathbb{Z}$
2) x, y pares

Demostración
P.D. $\mathcal{R} \subseteq \mathcal{U}$

1) $\mathcal{U}$ ideal de $\mathcal{R}$	Hipótesis
2) $r \in \mathcal{R}$	Hipótesis
3) $1 \in \mathcal{U}$	Hipótesis
4) $1 \cdot r \in \mathcal{U}$	Hipótesis
5) $1 \cdot r = r$	(2), (3) y def de ideal
6) $r \in \mathcal{U}$	(4) y (5)
7) $\mathcal{R} \subseteq \mathcal{U}$	(1) - (6)

Clase · lunes 23 de agosto

Ejercicio: Si F es un campo, entonces (0) y F son sus únicos ideales.

Demostración: (Por absurdo)

1) F es un campo	Hipótesis
2) $\mathcal{U}$ ideal de F	Hipótesis
P.D. $\mathcal{U} = \{0\}$ ó $\mathcal{U} = F$	
3) $ur \in \mathcal{U}$ para todo $u \in \mathcal{U}$ y $r \in F$	(2) y def de ideal
4) $u \neq 0$, $u \in \mathcal{U}$	Hip
5) $uu^{-1} = 1$	(4), F campo y prop
6) $1 \in \mathcal{U}$	(5) y (3)
7) $\mathcal{U} = F$	(6) y ejer anterior
8) $\{0\}$ es ideal de F	def de ideal
9) F es ideal de F	def de ideal
10) $\{0\}$ y F son los únicos ideales de F	(7), (8) y (9)

Ejercicio:
Sea R un anillo conmutativo con unidad cuyos únicos ideales son (0) y R. Entonces R es un campo

Demostración:
R es un anillo conmutativo con unidad
Los únicos ideales de R son $\{0\}$ y R

1) $a \in R$ y $r \neq 0$
2) $Ra = \{ra \mid r \in R\}$
P.D. Ra es ideal de R
3) $u_1, u_2 \in Ra$ P.D. $u_1 + u_2 \in Ra$
4) $u_1 = r_1 a$ y $u_2 = r_2 a$
5) $u_1 + u_2 = r_1 a + r_2 a$
6) $= (r_1 + r_2) \cdot a$
7) $u_1 + u_2 \in Ra$

Inverso
8) $u \in Ra$ P.D u tiene inverso
9) $u = ra$ con $r \in R$
10) $ra + (-(ra)) = 0$
11) $ra + ((-r) \cdot (a)) = 0$
12) $u^{-1} = (-r) \cdot a$

Segunda parte de ideal
$u \in Ra$ y $r \in R$ $ur \in Ra$
13) $u \in Ra$ y
14) $u = r'a$
15) $ur = (r'a)r$
16) $= (rr')a$
17) $= r''a$
18) $ur \in Ra$

3) $x+y$ par
4) $\varphi(x+y) = e$
5) $= e \cdot e$
6) $= \varphi(x) \cdot \varphi(y)$

7) x impar , y par
8) $x+y$ impar
9) $\varphi(x+y) = a$
10) $= a \cdot e$
11) $= \varphi(x) \cdot \varphi(y)$

El resto de casos son similares

Clase · miércoles 25 de agosto de 2021

```
typedef  int  (*fncion_de_S3)(int);

int  Id(int);
int  r (int);
 :
class  S3
{
   public

      operator *
      igualdad , inuevo   }  tabla  imprimir tablc

   private

      función_de_S3  nombre;
};
```

Clase · viernes 27 de agosto.

Teorema
Sea G un grupo y N un subgrupo normal de G, entonces existe un homeomorfismo $\varnothing: G \to G/N$

→ Ejemplo ① $G = \mathbb{Z}$ y $N =$ pares $\quad \phi: \mathbb{Z} \to \{\text{Pares, Impares}\}$

$(\mathbb{Z}, +)$ $\quad$ $(\{\text{Pares, Impares}\}, \cdot)$,

→ Ejemplo

$$\varphi(n+m) = \begin{cases} n+m & \text{si } n \text{ y } m \text{ es par} \\ \vdots \end{cases} \qquad n \mapsto \begin{cases} \text{Para} & \text{si } n \text{ es par} \\ \text{Impar} & \text{si } n \text{ es impar} \end{cases}$$

→ Ejemplo ②
$G = S_3$, $N = \{Id, r, s\}$ $\quad \varnothing: S_3 \to S_3/N = \{N, Nf\}$

$Id \mapsto N$
$s \mapsto N$
$f \mapsto Nf$
$g \mapsto Nf$
$h \mapsto Nf$

Demostración

1) $\phi: G \to G/N$
   $g \mapsto Ng$

P.D. ϕ es un homomorfismo

2) $\phi(g \cdot h) = Ngh$
3) $= Ng\, Nh$
4) $= \varphi(g) \cdot \varphi(h)$

P.D. ϕ es sobreyectiva

5) $x \in G/N$
6) $x = Ng$
7) $\phi(g) = Ng$
8) ϕ es sobre

metáfora = lo más importante
coin kernel
la parte comible del chocho

Definición (Núcleo) (Kernel)

Sea $\Phi: G \to \overline{G}$ un homeomorfismo entre grupos G y $\overline{G}$

$K_\Phi = \{ x \in G \mid \Phi(x) = e \}$ se lee el kernel de Φ

Ejemplo ② $\Phi: S_3 \to \{N, Nf\}$

$K_\Phi = \{Id, r, s\}$ $\Phi(x) = N$ $x \in K_\Phi$ N es el elemento identidad en G/N

Ejemplo $\Phi: \mathbb{Z} \to \{Pares, Impares\}$

$K_\Phi = \{Pares\}$

Teorema Sea $\Phi: G \to \overline{G}$ un homeomorfismo

i) $\Phi(e) = \bar{e}$
ii) $\Phi(ex^{-1}) = (\Phi(x))^{-1}$

Demostración

1) $\phi(e) = \phi(e \cdot e)$
2) $= \phi(e) \cdot \phi(e)$
3) $\phi(e) = \bar{e}$

$e = ex$ para todo x
ϕ es homeo
2 unicidad de la identidad

1) $x \in G$
2) $e = x x^{-1}$
3) $\phi(e) = \bar{e}$
4) $\phi(e) = \phi(x x^{-1})$
5) $= \phi(x) \cdot \phi(x^{-1})$
6) $\phi(x^{-1}) = (\phi(x))^{-1}$

(5), (3) y unicidad del inverso

Ejercicio.

1) Por analogía, definir homomorfismo de anillos.
2) Definir kernel de anillos
3) Enunciar el teorema anterior para anillos

1) Sea R un anillo y $\mathcal{U}$ un ideal, entonces existe un homomorfismo ente $R \to R/\mathcal{U}$ donde $R/\mathcal{U}$ es un anillo.

2) $K_\Phi = \{ x \in \mathcal{U} \mid \Phi(x) = 0 \}$

(Parte 3) Teorema

- $\bar{\Phi}(0) = \bar{0}$
- $\bar{I}(-x) = -\bar{\Phi}(x)$

Definición

Sean R y $\bar{R}$ anillos $\bar{\Phi}: R \to \bar{R}$ es un homeomorfismo si y solo si

i) $\bar{\Phi}(x+y) = \bar{\Phi}(x) + \bar{\Phi}(y)$
ii) $\bar{\Phi}(x \cdot y) = \bar{\Phi}(x) \cdot \bar{\Phi}(y)$

Definición (Kernel de anillos)

Sea $\bar{\Phi}: R \to \bar{R}$ un homeomorfismo

$$I\bar{\Phi} = \{ x \mid \bar{\Phi}(x) = \bar{e} \}$$

Teorema

Sea $\bar{\Phi}: R \to \bar{R}$

i) $\bar{\Phi}(0) = 0$
ii) $\bar{\Phi}(-x) = -\bar{\Phi}(x)$

Clase • lunes 30 de agosto de 2021

Definición -Isomorfismo-

Definición: Un isomorfismo es un homeomorfismo 1-1

Definición (Grupos isomorfos)

Sean G y $\bar{G}$ dos grupos y $\Phi: G \to \bar{G}$, sea Φ un isomorfismo sobreyectivo, entonces G y $\bar{G}$ se nota por $G \approx \bar{G}$ (se lee G es isomorfo a $\bar{G}$)

Ejemplo

$$H = \{ e, a, a^2, \ldots, a^{n-1}, a^n = e \} = C_n$$

(Es el mismo grupo salvo isomorfismos)

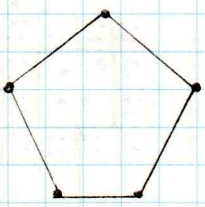
$$H \approx \mathbb{Z}_n$$

$$\mathbb{Z}_n = \{ [0], [1], \ldots, [n-1] \}$$

Todos los grupos isomorfos pueden representarse por el mismo diagrama de Caylay

Ejemplo

C_5:



Probar que $\times$ es una relación de equivalencia.

Sean G, G_1, G_2 grupos.

Reflexia

1. G un grupo
2. $Id: G \to G$, $x \mapsto x$
3. Id. es un isomorfismo

Simetria

1. G, H grupos tq. G es isomorfo a H
2. Existe $\bar{\Phi}: G \to H$ $\bar{\Phi}$ iso. y sobre

3. Φ es biyectivo
4. Ψ es la inversa de Φ
5. $\Psi: H \to G$

P.D $\Psi(h_1 + h_2) = \Psi(h_1) + \Psi(h_2)$

6). $\Psi(h_1+h_2) = \Psi(\Phi(g_1) + \Phi(g_2))$
7) $= \Psi(\Phi(g_1+g_2))$
8) $= g_1 + g_2$
9) $= \Psi(h_1) + \Psi(h_2)$.
10) Ψ es biyectiva y homeomorfismo
11) Ψ es isomorfismo
12) $H \cong G$

Transitiva
1) G, H, F grupos
2) Existe $\Phi_1: G \to H$ y $\Phi_2: H \to F$ iso y sobre
3) $\Phi = \Phi_2 \circ \Phi_1 : G \to F$
4) Φ es uno a uno y sobre

P.D Φ es homeomorfismo
5) $x, y \in G$
6) $\Phi(x+y) = \Phi_2(\Phi_1(x_1 + y_1))$
7) $= \Phi_2(\Phi_1(x_1) + \Phi_1(y_1))$
8) $= \Phi_2(\Phi_1(x_1)) + \Phi_2(\Phi_1(y_1))$
9) $= \Phi(x_1) + \Phi(y)$
10) Φ es homo y biyectivo
11) $G \cong K$

Probar que $U_8 \cong V$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

	Id	h	v	r
Id	Id	h	v	r
h	h	Id	r	v
v	v	r	Id	h
r	r	v	h	Id

$\Phi =$

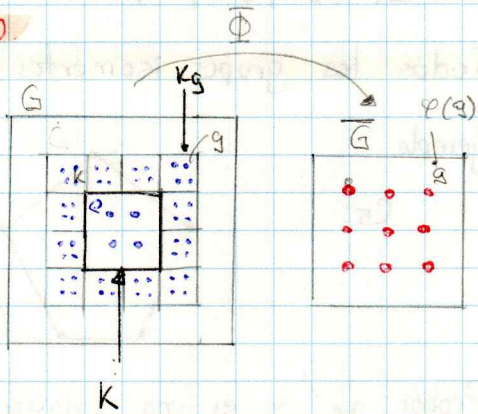
1	3	5	7
Id	h	v	r

$\Phi(7 \cdot 3) = \Phi(5) = v = r \cdot h = \Phi(7) \cdot \Phi(3)$

Clase - miércoles 1 de septiembre.

Teorema: Primer Teorema Fundamental de Homomorfismo
Sea $\Phi: G \to \overline{G}$ un homomorfismo sobreyectivo, entonces

$$G/K \cong \overline{G} \qquad [K = K_\Phi]$$



Ejemplo

$G = S_3$ $\qquad \Phi: S_3 \to C_2$
$\overline{G} = C_2 = (a)$
$K = K_\Phi = \{Id, r, s\}$

$$G/K = \{K, Kf\}$$

C_2 y G/K son isomorfos.

Demostración
- Debemos en primer lugar, encontrar $\Psi: G/K \to \overline{G}$ que sea isomorfismo.

1) $\Psi: G/K \to \overline{G}$
$Kg \mapsto \Phi(g)$

P.D. Ψ está bien definido
2) $g, g' \in Kg$. P.D. $\Psi(Kg) = \Psi(Kg')$

3) $Kg = Kg'$
4) $g' = Kg \quad K \in K$
5) $\phi(g') = \phi(Kg)$
6) $= \phi(K) \cdot \phi(g)$
7) $= \bar{e} \cdot \phi(g)$
8) $= \phi(g)$
9) $\psi(Kg) = \psi(Kg')$

P. D. ψ es uno a uno
10) $Kg, Kh \in G/K$ con $\psi(Kg) = \psi(Kh)$ P.D. $Kg = Kh$
11) $\phi(g) = \phi(h)$
12) $\Phi(g)(\Phi(h))^{-1} = \bar{e}$
13) $\Phi(g)\Phi(h^{-1}) = \bar{e}$
14) $\Phi(gh^{-1}) = \bar{e}$
15) $gh^{-1} \in K$
16) $(gh^{-1})h \in Kh$
17) $g \in Kh$
18) $Kg = Kh$

P.D. ψ es sobre
19) $\bar{g} \in \bar{G}$ Hipótesis
P D Existe $X \in G/K$ tal que $\psi(x) = \bar{g}$
20) Existe $g \in G$ tal que $\Phi(g) = \bar{g}$
21) $X = Kg$
22) $\psi(x) = \psi(Kg)$
23) $= \Phi(g)$
24) $= \bar{g}$

P.D. ψ es un homomorfismo
P.D. $\psi(x \cdot y) = \psi(x) \cdot \psi(y)$ para $x, y \in G/K$
25) $x, y \in G/K$
26) $x = Kg \quad y = Kh$
27) $\psi(xy) = \psi(Kg Kh)$
28) $= \psi(Kgh)$
29) $= \phi(gh)$
30) $= \phi(g) \cdot \phi(h)$
31) $= \psi(Kg) \cdot \psi(Kh)$
32) $= \psi(x) \cdot \psi(y)$

Teorema
Sea $\Phi: G \to \bar{G}$, entonces $K = K_{\bar{e}}$ es un subgrupo normal de G.

Demostración
Clausura
1) $x, y \in K$
2) $\phi(x) = \bar{e}$
3) $\phi(y) = \bar{e}$
4) $\phi(xy) = \phi(x) \cdot \phi(y)$
5) $= \bar{e} \cdot \bar{e}$
6) $= \bar{e}$
7) $x \cdot y \in K$

Inverso
8) $\phi(x^{-1}) = (\phi(x))^{-1}$
9) $= e^{-1}$
10) $= e$
11) $x^{-1} \in K$

Demostración K sgn

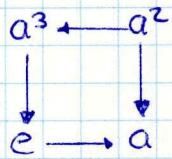
12) $g \in G$
13) $K \in K$
P.D. $gkg^{-1} \in K$
14) $\varnothing(k) = \varnothing(kgg^{-1})$
15) $= \bar{e}$
16) $= \varnothing(k)\varnothing(g)\varnothing(g^{-1})$
17) $= \varnothing(g)\varnothing(k)\varnothing(g^{-1})$
18) $= \varnothing(gkg^{-1})$
19) $gkg^{-1} \in K$
20) K es sgn.

Clase · viernes 3 de septiembre de 2021

$j^4 = 1$
$i^2 = j^2 = k^2 = i \cdot j \cdot k = -1$
$ij = k \quad jk = i \quad k \cdot i = j$

1	i	j	k
e	a	b	ab

$a^4 = e$
$b^4 = e$



Teorema de Cauchy

Si G es un grupo finito abeliano* y $p \mid o(G)$, siendo p - primo, entonces existe $g \in G$, con $g \neq e$ tal que $g^p = e$

* nuestra versión

Ejemplos:
① $G = S_3$, $o(G) = 6$ $p = 2$

$2 \mid 6$ ✓ Debe existir $x \neq Id$ tal que $x^2 = Id$ si hay $x = t$

$p = 3$

$3 \mid 6$ ✓ Debe existir $x \neq Id$ tal que $x^3 = Id$ si hay $x = r$.

② $G = \mathbb{Q}$ $o(\mathbb{Q}) = 8$

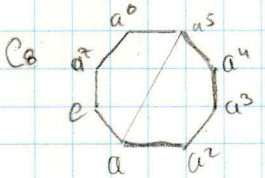
$p = 2$ $2 \mid 8$ ✓ Debe existir $x \in \mathbb{Q}$ tal que $x^2 = Id$ si hay $x = -1$

Para un cierto diagrama de Caylay donde g es un generador de G, hay un solo de orden p

Ejemplo Supongamos que G es de orden 60

$5 \mid 60$ G podría admitir un generador de orden 5.

Para orden de G igual a 8



Demostración: (Por inducción sobre o(G))
1) El antecedente es F, por lo que el teorema es verdadero (trivialmente)
2) Opcional $n = 2$
3) $o(G) = 2$
4) $G = \{e, a\}$ $a \neq e$

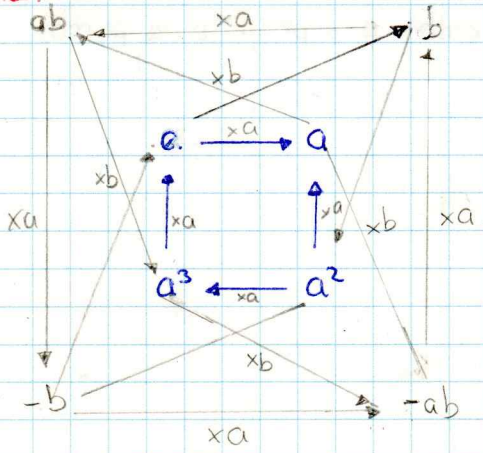
5) $p \mid o(G)$
6) $p = 2$
7) $a^2 = e$
8) El teorema es cierto para $n=2$
9) Suponemos que el teorema es cierto para todo grupo cuyo orden es menor que n
10) G tiene subgrupos no triviales o G no tiene subgrupos no triviales (Tercero excluido)
11) G no tiene subgrupos no triviales — Hipótesis.
12) $o(G)$ es primo
13) $p \mid o(G)$
14) $p = o(G)$
15) $a \in G \quad a \neq e$
16) $a^p = e$.
17) Si G si tiene subgrupos no triviales
18) N subgrupo no trivial — Nomenclatura
19) N es un subgrupo normal de G — Ejercicio
20) $p \mid o(N)$ ó $p \nmid o(N)$ — Tercero excluido
21) $p \nmid o(N)$ — (20)
22) $o(G/N) = o(G)/o(N)$
23) $o(G) = o(G/N) \cdot o(N)$
24) $p \mid o(G)$
25) $p \mid o(G/N)$
26) G/N es un grupo finito de orden — Hip inducción
27) Existe $X \in G/N$ con $X \neq N$ tal que $X^p = N$

Diagrama de Caylay de los Cuaterniones.

$i^2 = j^2 = k^2 = ijk = -1$

$ij = k \quad jk = i \quad k \cdot i = j$

1	i	j	k
e	a	b	ab



Clase. lunes 6 de septiembre de 2021

Continuación de la demostración
28) $X = Na, \quad a \in G \quad a \notin N$
29) $(Na)^p = N a^p$ — (19) y teorema $Nab = NaNb$
30) $= N$ — (27) y (29)
31) $a^p \in N$ — (29) y (30)
32) $(a^p)^{o(N)} = e$
33) $(a^{o(N)})^p = e$
34) $g = a^{o(N)}$
35) $g = e$ o $g \neq e$
36) $g = e$
37) $a^{o(N)} = e$
38) $Na^{o(N)} = Ne = N$
39) $(Na)^{o(N)} = N$
40) $p \mid o(N)$
41) Contradicción (21, 40)
42) $g \neq e$

43) $o(N) < o(G)$
44) Existe $g \in N$, $g \neq e$ tal que $g^p = e$.

Ejercicio.
Si G es un grupo finito, y $p \mid o(G)$, p-p primo, entonces existe H subgrupo de G con $o(H) = p$, H cíclico.
0) $p \mid o(G)$, $g \in G$ $g \neq e$
Demostración
1) Existe $g \in G$, $g \neq e$ tal que $g^p = e$ Teo Cauchy
2) $H = (g) = \{e, g, g^2, \ldots, g^{p-1}\}$
P.D. $o(H) = p$
3) (Por absurdo) $o(H) = m$ con $m \neq p$
4) $m \nmid p$
5) $p = km$ para algún k
6) p es primo
7) Contradicción

Clase • miércoles 8 de agosto de 2021.

Ejercicio Sea G un grupo de orden 12, ¿G tiene un subgrupo de orden 2?

Por el momento, no sabemos.

Ejercicio
Si G es un grupo finito de orden p o p^2, p- primo, entonces todos los elementos de G son de orden p o p^2, con g distinto de e.

Demostración.
1) G es un grupo finito de orden p o p^2 y p es primo. Hipótesis
2) $o(G) = p$ Hipótesis
3) $a \in G$, $a \neq e$ Hipótesis
4) $a^p = e$ Teorema $b^{o(G)} = e$
5) a es de orden p (4) y p es primo
6) $o(G) = p^2$ Hipótesis
7) $a^{p^2} = e$ Teorema $b^{o(G)} = e$
8) $m = o(a)$ (8)
9) $a^m = e$ (9)
10) $m < p^2$
11) $m \mid p^2$ (8) y def de orden
12) $m = p$ o $m = p^2$
13) $o(a) = p$ u $o(a) = p^2$

Teorema:
Si $\Phi : G \to \bar{G}$ es un homomorfismo uno a uno, entonces $K_\Phi = \{e\}$. si $K_\Phi = \{e\}$, entonces Φ es uno a uno.

Demostración
1) $\Phi : G \to \bar{G}$ es un homomorfismo 1 a 1 Hipótesis
2) $x \in K_\Phi$
3) $\Phi(x) = \bar{e}$
4) $\Phi(e) = \bar{e}$
5) $x = e$

7) Supongamos que $K_\Phi = \{e\}$
8) $\Phi(x) = \Phi(y)$ con $x, y \in G$
9) $\Phi(x)\Phi(y)^{-1} = e$
10) $= \Phi(x)\Phi(y^{-1})$
11) $= \Phi(x \cdot y^{-1})$
12) $x \cdot y^{-1} \in K_\Phi$

13) $xy^{-1} = e$
14) $x = y$

Teorema.
Si $\Phi: G \to \bar{G}$ es un homomorfismo sobreyectivo con $K_\Phi = K$, entonces $\Phi^{-1}(\bar{g}) = Kx$, donde $x \in \Phi^{-1}(\bar{g})$.

Demostración
1) $\Phi: G \to \bar{G}$, homomorfismo, sobre $K_\Phi = K$ Hipótesis.
2) $x \in \Phi^{-1}(\bar{g})$
P.D $x \in Kx$
3) $\Phi(x) = \bar{g}$
4) $g = g(xx^{-1})$
5) $\Phi(gx^{-1}) = \Phi(g)\Phi(x^{-1})$
6) $= \Phi(g)(\Phi(x))^{-1}$
7) $= \bar{g}(\bar{g})^{-1}$
8) $= \bar{e}$
9) $gx^{-1} \in K$
10) $g \in Kx$

"$\supseteq$"
2) $y \in Kx$
3) $y = kx$
P.D. $y \in \Phi^{-1}(\bar{g}) \Leftrightarrow \Phi(y) = \bar{g}$
4) $\Phi(kx) = \Phi(k) \cdot \Phi(x)$
5) $= \bar{e}\,\bar{g}$
6) $= \bar{g}$
7) $y \in \Phi^{-1}(\bar{g})$

Ejercicio.
Sea G un grupo abeliano de orden finito $o(G)$ y supongamos que el entero n es primo relativo de $o(G)$. Probar que para todo $g \in G$, se tiene que $g = x^n$ para cierto x

Demostración
I: Definir un homomorfismo.
II: Probar que el homomorfismo es uno a uno, concluir que es sobre
1) $\Phi: G \to G$
$x \mapsto \Phi(x) = x^n$
2) $\Phi(x \cdot y) = (x \cdot y)^n$
3) $= x^n y^n$
4) $= \Phi(x) \cdot \Phi(y)$.

P.D. Φ es inyectivo.
5) $x \in K_\Phi$
P.D. $x = e$
6) $\Phi(x) = e$
7) $x^n = e$
8) $x^{o(G)} = e$
9) $x = x^1$
10) $1 = an + bo(G)$
11) $x = x^{an + bo(G)}$
12) $= x^{an} \cdot x^{bo(G)}$
13) $= (x^n)^a \cdot (x^{o(G)})^b$
14) $= e^a \cdot e^b$
15) $= e$
16)

Clase. viernes 10 de septiembre de 2021.

Teorema de Sylow (consideremos el caso de que G es abeliano)
Si G es un grupo finito, de orden $o(G)$ y p un primo tal que $p^\alpha | o(G)$ y $p^{\alpha+1} \nmid o(G)$, siendo $\alpha \geq 0$ con $\alpha \in \mathbb{Z}$, entonces existe un subgrupo de G de orden p^α

Notemos que p en el teorema se tiene que $p | o(G)$, $p^2 | o(G)$, ..., $p^{\alpha-1} | o(G)$ $p^\alpha | o(G)$ y $p^{\alpha+1} | o(G)$, por lo que la propiedad de que $p^\alpha | o(G)$ es maximal

- Sea: G un grupo de orden (12), averiguar si tiene subgrupos de orden 4. Lo mismo para orden 3 y lo mismo para orden (6)

(a) $p=2$ $2|12$, $4|12$, $8 \nmid 12$ Concluimos que G tiene un subgrupo de orden 4.

(b) $p=3$ $3^1|12$, $3^2 \nmid 12$, Concluimos que G tiene un subgrupo de orden 3.

(c) $p=6$ $6^1|12$, $6^2 \nmid 12$ pero 6 no es primo

Demostración

1)	$\alpha \geq 0$	Hipótesis
2)	$\alpha = 0$ o $\alpha > 0$	(1)
3)	$\alpha = 0$	Hipótesis
4)	$p^\alpha = 1$	
5)	(e) sg de G, $o(e) = 1 = p^{(0)}$	(4)
6)	$\alpha > 0$	Hipótesis
7)	$p	o(G)$	Hipótesis
8)	Existe $a \in G$, $a \neq e$ tal que $a^p = e$	Teo Cauchy
9)	$S = \{x \in G \mid (x^p)^n = e$ para algún $n\}$	Hipótesis
10)	$a^{p^1} = e$	(8)
11)	$a \in S$	(10)
12)	$S \neq \emptyset$	
13)	$S \neq (e)$	

P.D. S. Subgrupo de G

14)	$x, y \in S$	Hipótesis
	P.D. $x \cdot y \in S$	
15)	Existen n, m enteros tales que $x^{p^n} = e$ $x^{p^m} = e$	
	P.D. $(x \cdot y)^{p^r} = e$ para algún r	
16)	$(x \cdot y)^{p^{(n+m)}} = x^{p^{n+m}} y^{p^{m+n}}$	
17)	$= x^{p^n p^m} \cdot y^{p^m p^n}$	
18)	$= (x^{p^n})^{p^m} \cdot (y^{p^m})^{p^n}$	
19)	$= e^{p^m} \cdot e^{p^n}$	
20)	$= e$	
21)	$x \cdot y \in S$	
22)	S es subgrupo de G	

P.D. $o(S) = p^\alpha$
P.D $o(S) = p^\beta$ $0 \leq \beta \leq \alpha$ (Por el absurdo)

23)	$o(S) \neq p^\beta$	
24)	$o(S)$ tiene un factor que no es p, q, así $q \neq p$ y q es primo	
25)	$q	o(S)$	
26)	Existe $c \in S$, $c \neq e$ tal que $c^q = e$	
27)	$c^{p^n} = e$ para algún n	
28)	$(q, p^n) = 1$ ya que q y p - primos	
29)	Existen $\mu q + \eta p^n = 1$	
30)	$e^1 = c^{\mu q + \eta p^n}$	
31)	$= c^{\mu q} \cdot c^{\eta p^n}$	
32)	$= (c^q)^\mu \cdot (c^{p^n})^\eta$	
33)	$= e^\mu \cdot e^\eta$	

34) $= e$
35) Contradicción (34, 26)
36) $o(S) = p^\beta$
37) $\beta > \alpha$
38) $p^\beta > p^\alpha$
39) $o(S) | o(G)$
40) $p^\beta \nmid o(G)$
41) $o(S) \nmid o(G)$
42) Contradicción (39, 41)
43) Supongamos que $\beta < \alpha$
44) S es es un subgrupo normal
45) G/S es grupo.
46) $o(G/S) = o(G)/o(S)$
47) $= kp^\alpha / p^\beta$ para algún k
48) $= kp^{\alpha-\beta}$
49) $p | o(G/S)$
50) Existe $X \in G/S$ tal que $X^p = S$
51) $X^p = S \quad X \neq S$
52) $Sx = S \quad x \in G, \ x \notin S$
53) $(Sx)^p = Sx^p$
54) $= S$
55) $x^p \in S$
56) $(x^p)^{o(S)} = e$
57) $(x^p)^{p^\beta} = e$
57) $x^{p \cdot p^\beta} = e$
58) $x^{p^{1+\beta}} = e$
59) $x \in S$
60) Contradicción (51, 59)
61) $\beta \not< \alpha$
62) $\beta = \alpha$
63) $o(S) = p^\alpha$
64) S es el subgrupo buscado.

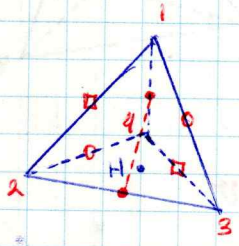
Hipótesis.

Teorema de Lagrange
Hipótesis maximal

G es abeliano

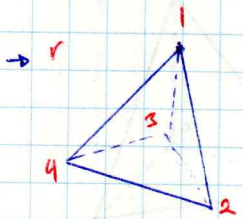
Clase - lunes 13 de septiembre de 2021

El grupo del tetraedro regular



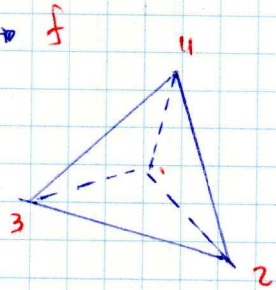
A_4 consiste de todas las rotaciones que mantendría la simetría del objeto.

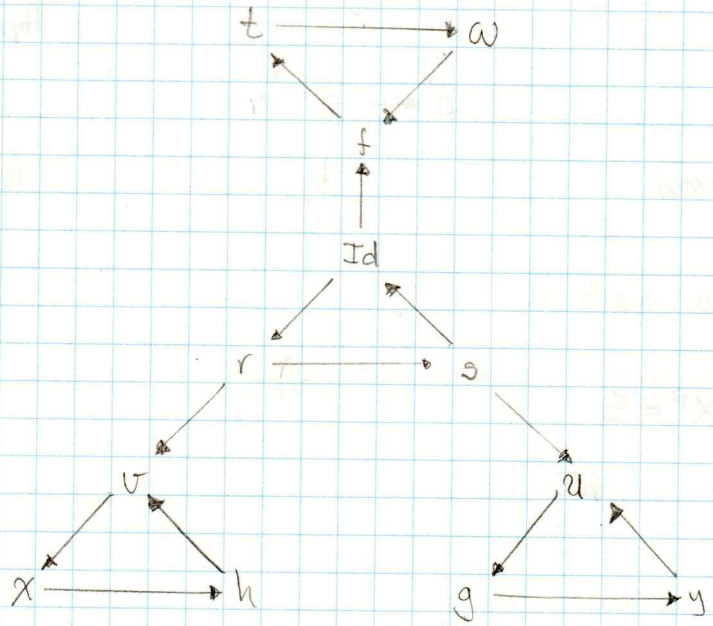
$A_4 = \{Id, \underbrace{r, s}_{1}, \underbrace{t, u}_{2}, \underbrace{v, w}_{3}, \underbrace{x, y}_{4}, f, g, h\}$



r = rotación 120° en el sentido antihorario alrededor de la altura $\overline{HI}$

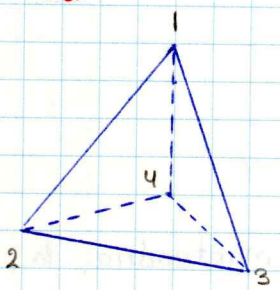
f = rotación 180° alrededor de $\overline{HN}$ donde H y N son puntos medios



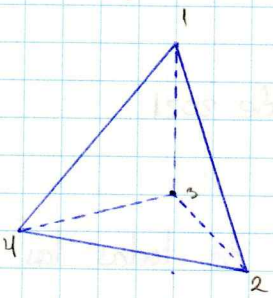


$Au = \{ Id, r, s, t, u, v, w, x, y, f, g, h \}$

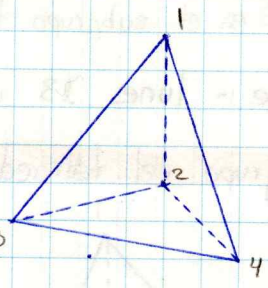
Id



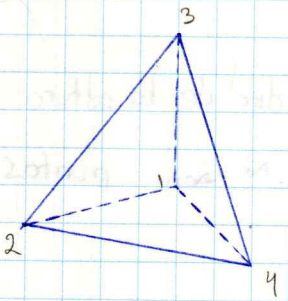
r



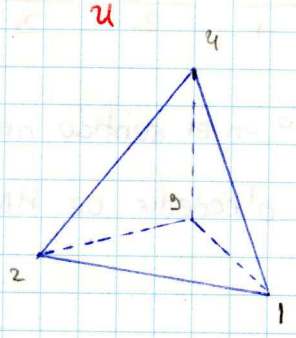
s



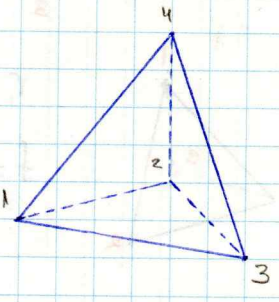
t



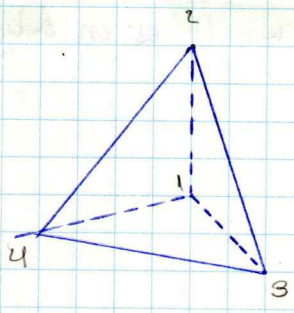
u



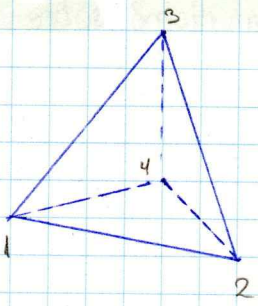
v



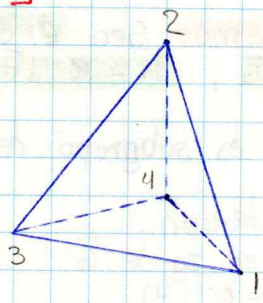
w



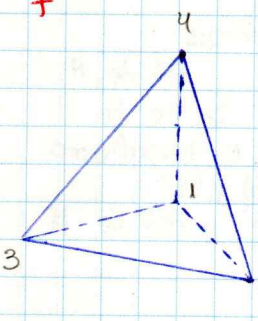
x



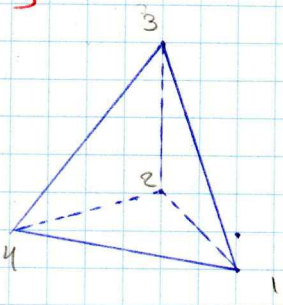
y



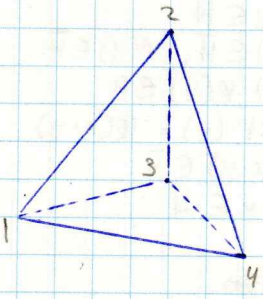
f



g



h



Clase · miercoles 15 de septiembre de 2021

Ejercicio: ¿Cuántos subgrupos de orden 2 tiene C_6?

- $C_6 = \{e, a, a^2, a^3, a^4, a^5\}$

  $H = \{e, a^3\}$ H es subgrupo de orden 2.

Respuesta: SI tiene y es único.

Por otro lado, también se puede concluir que hay subgrupos de orden 2.

- lo mismo pero para S_3

  Respuesta si tiene, pero no es único. $\{Id, f\}$, $\{Id, g\}$.

Ejercicio:
Probar que si un grupo G satisface las hipótesis del teorema de Sylow y es Abeliano, entonces el subgrupo de la conclusión es único.

Demostración (Por absurdo)

1) G es finito, abeliano — Hipótesis
2) Existe p primo tal que $p^\alpha \mid o(G)$ y $p^{\alpha+1} \nmid o(G)$ para algún $\alpha \in \mathbb{N}$ — Hipótesis
3) Existen H, K, $K \neq K$ H, K subgrupos de G con $o(H) = o(K) = p^\alpha$ — Hipótesis
4) HK es subgrupo de G
5) $o(HK) = o(H)o(K) / o(H \cap K)$
6) $= p^\alpha p^\alpha / o(H \cap K)$
7) $= p^{2\alpha} / o(H \cap K)$
8) $o(HK) \mid o(G)$
9) $H \cap K$ es subgrupo de G
10) $o(H \cap K) \mid o(G)$
11) $o(HK) = p^\beta$
12) $o(H \cap K) = p^\alpha$
13) $o(HK) = p^{2\alpha - \alpha}$
14) $p^\beta = p^{2\alpha - \alpha}$

14) $2\alpha - \gamma > \alpha$
15) $p^{2\alpha-\gamma} \mid o(G)$
16) Contradicción (15, 2)

Teorema: Sea $\varphi: G \to \bar{G}$ un homomorfismo sobreyectivo con $K_\varphi = K$, $\bar{H}$ es un subgrupo de $\bar{G}$, $H = \varphi^{-1}(\bar{H})$, entonces

1) H es subgrupo de G

Demostración
1) $\bar{H}$ es sg de $\bar{G}$
2) $H = \varphi^{-1}(H)$
   P.D. H sg de G

Clausura
3) $x, y \in H$
4) $\varphi(x) \in \bar{H}$, $\varphi(y) \in \bar{H}$
5) $\varphi(x) \cdot \varphi(y) \in \bar{H}$
6) $\varphi(x)\cdot(y) = \varphi(x \cdot y)$
7) $\varphi(x \cdot y) \in \bar{H}$
8) $x \cdot y \in H$

Hipótesis
(3) y def de H
$\bar{H}$ sg de G
φ es homomorfismo
(6) y (5)
(7) y def de H

Inverso
9) $x \in H$
10) $\varphi(x) \in \bar{H}$
11) $(\varphi(x))^{-1} \in \bar{H}$
12) $\varphi(x^{-1}) \in \bar{H}$
13) $x^{-1} \in H$

2) $K \subseteq H$

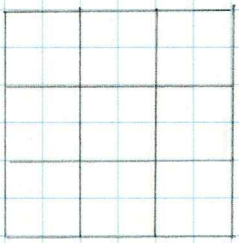
Demostración
1) $x \in K$
2) $\varphi(x) \in \bar{e}$
3) $\bar{e} \in \bar{H}$
4) $\varphi(x) \in \bar{H}$
5) $x \in H$

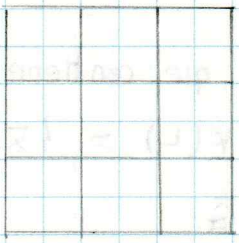
3) Si $\bar{H}$ es sgn de $\bar{G}$, entonces H es sgn de G

Demostración
1) $\bar{H}$ sgn $\bar{G}$
2) $g \in G$ y $n \in H$
3) $\varphi(gng^{-1}) = \varphi(g)\cdot\varphi(n)\cdot\varphi(g^{-1})$
4) $= \varphi(g)\cdot\varphi(n)\cdot[\varphi(g)]^{-1}$
5) $\varphi(n) \in \bar{H}$
6) $\varphi(g)\cdot\varphi(g)^{-1} \in \bar{G}$
7) $\varphi(g)\cdot\varphi(n)\cdot\varphi(g^{-1}) \in \bar{H}$
8) $\varphi(gng^{-1}) \in \bar{H}$
9) $gng^{-1} \in H$
10) H es normal

Teorema. - Segundo teorema fundamental de homomorfismos -
Sea $\varphi: G \to \bar{G}$ homo sobre con kernel K y sea $\bar{N}$ un sgn de $\bar{G}$ y $N = \varphi^{-1}(\bar{N})$, entonces $G/N \approx \bar{G}/\bar{N}$.

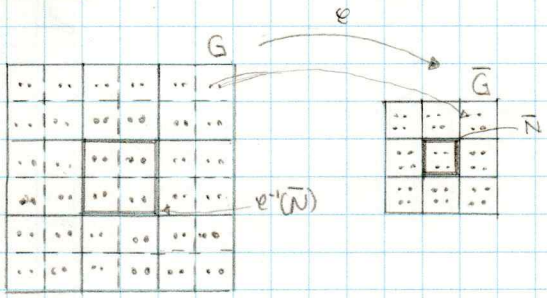
Ejecicio:
Haga un diagrama de Veen que ilustre el teorema anterior.





Clase . 17 de septiembre.

Teorema: - Segundo Teorema Fundamental de Homomorfismos -
Sea $\varphi: G \to \bar{G}$ un homomorfismo sobreyectivo y $\bar{N}$ un sgn de $\bar{G}$, entonces $G/N \approx \bar{G}/\bar{N}$, siendo $N = \varphi^{-1}(\bar{N})$



Idea demostración
Aplicar el primer teorema fundamental de homomorfismos a $G \to \bar{G}/\bar{N}$

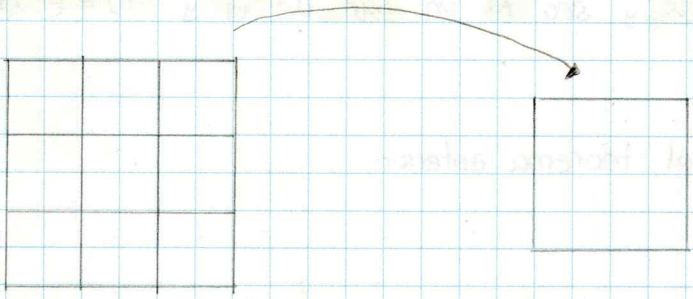
Demostración:
1) $\Psi: G \to \bar{G}/\bar{N}$
$\quad g \mapsto \bar{N}\varphi(g)$

2) $x, y \in G$
3) $\Psi(x \cdot y) = \bar{N}\varphi(x \cdot y)$
4) $\quad = \bar{N}\varphi(x) \cdot \varphi(y)$
5) $\quad = \bar{N}\varphi(x) \cdot \bar{N}\varphi(y)$
6) $\quad = \Psi(x) \cdot \Psi(y)$

P.D. Ψ es sobre
7) $Y \in \bar{G}/\bar{N}$
8) $Y = \bar{N}\bar{g}, \quad \bar{g} \in \bar{G}$
9) Existe $g \in G$ tal que $g = \varphi(\bar{g})$ — φ es sobre
10) $Y = \bar{N}\varphi(g)$
11) $\quad = \Psi(g)$

P.D. $K_\Psi = N$
($\in$)
12) $x \in K_\Psi$
13) $\Psi(x) = \bar{N}$ — Def de K_Ψ y elem identidad en $\bar{G}/\bar{N}$
14) $\quad = \bar{N}\varphi(x)$
15) $\varphi(x) \in \bar{N}$
16) $x \in N$

($\supseteq$)
17) $x \in N$
18) $\varphi(x) \in \bar{N}$



(iv) Si L un sg de G que contiene a K, entonces

$$\bar{L} = \varphi(L) = \{\bar{x} \in \bar{G} \mid \bar{x} = \varphi(\ell) \quad \ell \in L\}$$

es un subgrupo de $\bar{G}$

Demostración
($\bar{L}$ clausura)
1) $x, y \in \bar{L}$
2) $x = \varphi(\ell_1)$, $y = \varphi(\ell_2)$ $\quad \ell_1, \ell_2 \in L$
3) $xy = \varphi(\ell_1) \cdot \varphi(\ell_2)$
4) $\quad = \varphi(\ell_1 \ell_2)$
5) $\ell_1 \ell_2 \in L$
6) $x \cdot y \in \bar{L}$

Inverso
7) $x \in \bar{L}$ $\quad$ P.D $x^{-1} \in \bar{L}$
8) $x = \varphi(\ell)$
9) $x^{-1} = (\varphi(\ell))^{-1}$
10) $x^{-1} = \varphi(\ell^{-1})$
11) $\ell^{-1} \in L$
12) $x^{-1} \in \bar{L}$

v) $\varphi^{-1}(\bar{L}) = L$

Demostración
($\subseteq$)
1) $x \in \varphi^{-1}(\bar{L})$
2) $\varphi(x) \in \bar{L}$
3) $\varphi(x) = \bar{e}$ para algún $\ell \in L$
4) $\varphi(x) \cdot \varphi(\ell)^{-1} = \bar{e}$
5) $\varphi(x \cdot \ell^{-1}) = \bar{e}$
6) $x \cdot \ell^{-1} \in K$
7) $x \cdot \ell^{-1} \in L$
8) $x \in L\ell$
9) $x \in L$

($\supseteq$)
1) $x \in L$
2) $\varphi(x) \in \varphi(L)$
3) $\varphi(x) \in \bar{L}$
4) $x \in \varphi^{-1}(\bar{L})$

Existe
v) $\Psi : \mathcal{G} \to \bar{\mathcal{G}}$ siendo $\bar{\mathcal{G}}$ los subgrupos de $\bar{G}$ y $\mathcal{G}$ subgrupos de G que contienen a K, tal que Ψ es biyectiva.

19) $\Psi(x) = \bar{N}\varphi(x)$
20) $= \bar{N}$
21) $x \in K_\Psi$

22) $G/N \approx \bar{G}/\bar{N}$

Primer teorema fundamental de homomorfismos.

$G/K \approx \bar{G}$
$N/K \approx \bar{N}$

Ejercicio

Sea $\varphi: G \to G$, $x \mapsto x^5$, Averiguar si φ es un homeomorfismo y encontrar el K $\forall$

a)
a) $G = \mathbb{R}\setminus\{0\}$
b) $G = \mathbb{C}\setminus\{0\}$
c) $G = C_{10}$
d) $G = C_5$

Cuando G es abeliano.

a) $\mathbb{R}\setminus\{0\}$ es un grupo abeliano

$$K_\varphi = \{x \mid \varphi(x) = 1\} = \{x \mid x^5 = 1\} = \{1\}$$

b)
$$K_\varphi = \{x \mid \varphi(x) = 1\} = \{x \mid x^5 = 1\} = \left\{1, e^{\frac{2\pi n}{5}}, e^{\frac{3\pi n}{5}}, e^{\frac{4\pi n}{5}}, e^{\frac{\pi}{5}}\right\}$$

c) $C_{10} = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$

$K_\varphi = \{e, a^2, a^4, a^6, a^8\}$

d) $C_5 = \{e, a, a^2, a^3, a^4\}$

$K_\varphi = \{e, a, a^2, a^3, a^4\}$

Si N y H son subgrupos normales de G, probar que $NH/H \approx N/(N \cap H)$

① Probar que NH sg de G
② $N \cap H$ es sg de N
③ H sgn de NM

④ Aplicar el primer teorema
②
Demostración
1) $x \in N \cap H$, $n \in N$
2) $x \in N$
3) $x \in H$
4) $nx^{-1}n \in N$
5) $nx^{-1}n \in H$
6) $nx^{-1}n \in H \cap N$

1) $g \in H/N$
2) $m \in H$
3) $g = nm_1$, $n \in N$ $m \in H_1$
4) $(nm_1)m(nm_1)^{-1} = (nm_1)m(m_1^{-1}n^{-1})$
5) $= n(m_1 m m^{-1})n^{-1}$
6) $n(m_1 m m_1^{-1})n^{-1} \in H$

$\varphi: N \to NH/N$
$n \mapsto Hn$

1) Probar que φ es homomorfismo sobreyectivo.
2) Calcular K_φ

Clase - lunes 20 de septiembre de 2021

Automorfismos

Definición
$T: G \to G$ es un automorfismo si y sólo si T es un isomorfismo sobre.
Para automorfismos empleamos notación a la derecha

Ejemplo:
1) • La identidad es automorfismo. SÍ

2) La inversa
¿Homomorfismo?

$$\varphi(x,y) = (xy)^{-1} \neq x^{-1}y^{-1}$$

No es homomorfismo.

3) $\emptyset: G \to G$ con G-abeliano
• Homo
$$\emptyset(x,y) = (xy)^{-1} = x^{-1}y^{-1} = \varphi(x)\cdot\varphi(y)$$
- sobre. SÍ | SÍ es un automorfismo

Nota $A(S) = \{f \mid f: S \to S,\ f \text{ biyectiva}\}$. $A(S)$ es un grupo

$a(G) = \{T \mid T: G \to G \text{ y } T \text{ es automorfismo}\}$

$a(G) \subseteq A(G)$

Teorema. $a(G)$ es subgrupo de $A(G)$.

Demostración
1) $T_1, T_2 \in a(G)$ Hipótesis
P.D. $T_1T_2 \in a(G)$
1) T_1T_2 son biyectivas
2) T_1T_2 es biyectiva
P.D. T_1T_2 es homomorfismo
3) T_1, T_2 homomorfismo
4) $a,b \in G$
5) $(ab)(T_1T_2) = ((ab)T_1)T_2$
6) $= (aT_1\ bT_1)T_2$
7) $= (aT_1T_2)(bT_1T_2)$
8) $= a(T_1T_2)\ b\ (T_1T_2)$

• Inverso.
1) $T \in a(G)$
P.D. $T^{-1} \in a(G)$
2) T^{-1} es biyectiva
3) $a,b \in G$
4) $abT^{-1} = ((aT^{-1}T)(bT^{-1}T))T^{-1}$
5) $= (aT^{-1}\ bT^{-1})TT^{-1}$
6) $= aT^{-1}\ bT^{-1}$

$T: G \to G$, $g \in G$
$z \mapsto g^{-1} z g$

Demostremos que T es auto

$e(x) = x-1$
P.D. T es sobre
1) $y \in G$
2) $x = gyg^{-1}$
3) $xT = (gyg^{-1})T$
4) $= g^{-1}(gyg^{-1})g$
5) $= y$

P.D. T es homomorfismo
6) $x, y \in G$.
P.D. $(xy)T = (xT)(yT)$
7) $(xy)T = g^{-1}(xy)g$
8) $= g^{-1}(x \cdot (gg^{-1}) \cdot y) \cdot g$
9) $= (g^{-1} \cdot x \cdot g)(g^{-1} y \cdot g)$
10) $= (xT)(yT)$

Nota. El automorfismo anterior depende de $g \in G$. Por tal motivo a T lo llamamos T_g

$I(G) = \{T_g \mid g \in G\}$ ← Grupo de los automorfismos internos.

↑ Deber, probar que G es grupo

Ejercicio.

Calcular $I(V)$

$T \in I(V)$ $\quad V = \{Id, v, h, r\}$, $a, b \in V$, $g \in V$

$a T_g = g^{-1} a g$
$= a g^{-1} g$
$= a$

Entonces $T_g = Id_V$

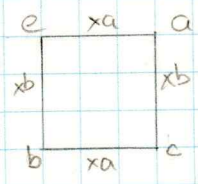
Ejercicio Encontrar un automorfismo no trivial en V

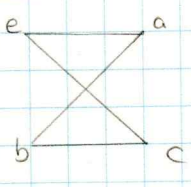
$V = \{e, a, b, c\}$

	e	a	b	c
e	e	b	a	c

T automorfismo no trivial

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e





Teorema.
Sea G y $\varphi: G \to G$ un automorfismo, $a \in G$, $o(a) = n$, entonces $o(\varphi(a)) = n$
Demostración

1) $\varphi: G \to G$ es automorfismo
2) $a \in G$
3) $o(a) = n$
4) $a^n = e$
5) $o(a^n) = o(a \cdots a)$
6) $= o(a) \cdots o(a)$
7) $o(a) = o(e) = e$

8) $\varphi(a)^n = e$
9) $m < n \quad (\varphi(a))^m = e$
10) $\varphi(a)^m = e$
11) $\varphi(a^m) = \varphi(a)^m$
12) $a^m \in K_\varphi$
13) φ es uno a uno
14) $K_\varphi = (e)$
15) $a^m = e$
16) Contradicción (3, 15)

$G(\mathbb{F}\bar{V}) = \{Id, \varphi_1$

φ_1	e	a	b	c
φ_2	e	b	a	c
φ_3	e	c	b	a
φ_4	e	a	c	b
φ_5	e	b	c	a
φ_6	e	c	a	b

$\varphi : C_7 \to C_7$
$x \mapsto x^2$