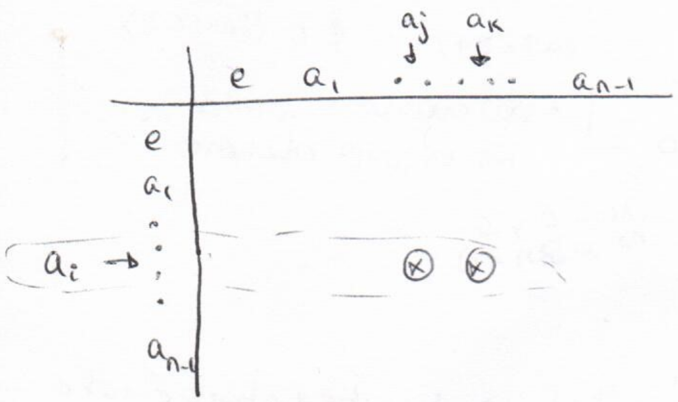
EJERCICIOS

20/2/2018

1.1.a

② Probar que la tabla de cayley de todo grupo finito forma ~~parte~~ una distribución en la que cada elemento del grupo aparece una y solo una vez en cada fila y columna (esta distrib.: Cuadrado Latino) ¿Es todo cuadrado latino la tabla de un grupo?

$G = \{e, a_1, \dots, a_{n-1}\}$



(por red. al absurdo)

suponemos que no todos los elementos son distintos $\Rightarrow \exists\, a_j$ y $a_k \in G$

$a_i * a_j = a_i * a_k \Rightarrow a_j = a_k$ (propiedad cancelativa)

pero entonces estas dos operaciones están en realidad en la misma columna (mismo elemento, si serían todos distintos)

(difícil)

⑨ Demostrar que si $(G, \cdot)$ es grupo finito de orden par, entonces existe un elemento $a \in G$ distinto del neutro, que verifica $a^2 = e$.

sabemos que G tiene orden par $\Rightarrow$ divido G en 2 apartados:

$G = H_1 \cup H_2$; $H_1 \cap H_2 = \emptyset \Rightarrow |H_1| + |H_2| = 2n = |G|$

ejercicios:

④, ⑤, ⑥

del tema $\boxed{1.1.a}$

1.1.b

① Estudiar en cada caso si la operación $*$ dota al conjunto correspondiente de estructura de grupo. En cada caso afirmativo, obtener el elemento neutro, el inverso de cada elemento, e indicar si el grupo es abeliano.

a En $\mathbb{Z}$, $a * b = a - b$

No es una operación asociativa $\rightarrow$ No es grupo abeliano.

ej: $(7-3)-2 = 4-2 = 2$
$7-(3-2) = 7-1 = 6$

b Es asociativa.
Comprobamos: operación interna? No $\rightarrow 3*3 = 3+3 = 6 \notin G$ $\overbrace{\{2n+1 \in \mathbb{Z}\}}^{\text{(impar)}}$
Hay elem. neutro? No $\rightarrow$ ej (sería 0 y 0 no es $2n+1$)
$\rightarrow$ por cualquiera de ellas, No es grupo abeliano.

En $G = \{2n+1 : n \in \mathbb{Z}\}$, se define $*$ por: $a * b = a + b$

c En $G = \mathbb{R} - \{-1\}$, $a * b = a + b + ab$

¿asociativa?: $a*(b*c) = a*(b+c+bc) = a+b+c+bc+ab+ac+abc$
$(a*b)*c = (a+b+ab)*c = a+b+ab+c+ac+bc+abc$ ✓ asociativa

¿op. interna?: $a*b = -1 \Leftrightarrow a+b+ab = -1 \Leftrightarrow a(1+b)+(1+b) = 0 \Leftrightarrow$
$\Leftrightarrow (1+b)(1+a) = 0 \Leftrightarrow \left\{\begin{array}{l} a=-1 \\ b=-1 \end{array}\right\}$ no posible pq entonces a ó b no serían parte del conjunto ✓ op interna

¿e. neutro?: $e*a = a \Leftrightarrow e+a+ea = a \Leftrightarrow$
$\Leftrightarrow e(1+a) = 0$
como a no puede ser $-1 \Rightarrow \underline{e = 0}$ ✓ e. neutro

¿inverso?: $a' * a = e \Rightarrow a' + a + a'a = 0$
$a'(1+a) = -a \Rightarrow a' = \frac{-a}{1+a}$ ✓ sí hay inverso
$1+a \neq 1$ siempre

Es grupo ✓
y además es abeliano (cumple la prop. conmutativa)

$b*a = b+a+ba = a+b+ab = a*b$

d $H = \left\{\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R}\right\}$ con la operación:

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} * \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{pmatrix}$$

(cont.) $\Rightarrow$

¿asociativa? (Ya lo habíamos visto en un ej. $\rightarrow$ sí ✓)

(cont.)

¿op. interna?

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & b+ax+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \in H$$ ✓ op. interna

¿e. neutro?

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H \quad (x,y,z=0)$$ ✓ e. neutro

del grupo general lineal

¿inverso?

$$A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in H \Rightarrow A^{-1} = \begin{pmatrix} 1 & -x & -y-zx \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \in H$$ cta. $A \cdot A^{-1} = e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$)

✓ inverso $\in G$

Es subgrupo ✓

No es abeliano (no es conmutativo) ✗

③ Demostrar que si H y K son subgrupos de un grupo abeliano $(G, *)$ entonces también es subgrupo de $(G,*)$ el conjunto:

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

hay que demostrar
① $HK \neq \phi$
② $\forall a,b \in HK \Rightarrow ab^{-1} \in HK$ — why? creo: pq si K es subgrupo, $b \in K$ y b^{-1} (su inverso) $\in K$

e neutro
① $H \leq G \Rightarrow H \neq \phi$ $\quad e_G \in H$
$K \leq G \Rightarrow G \neq \phi$ $\quad e_G \in K$ $\Rightarrow e_G * e_G = e_G \in HK \Rightarrow HK \neq \phi$ ✓

inverso
② $a,b \in HK \Rightarrow \begin{cases} a = h_1k_1 & \text{con } h_1 \in H, k_1 \in K \\ b = h_2k_2 & \text{con } h_2 \in H, k_2 \in K \end{cases}$ (notación: $hk = h*k$)

prop. grupo de G

$$ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = (h_1h_2^{-1})(k_1k_2^{-1}) \in HK$$

$(h_1h_2^{-1}) \in H$, $(k_1k_2^{-1}) \in K$ porque son subgrupos y por tanto verifican op. interna

$h_2, k_2 \in G$
$(h_2 * k_2)^{-1} = k_2^{-1} * h_2^{-1}$ pq. $\boxed{\text{inverso de un producto}}$!!! saber

operación de G (la misma!)

HK es subgrupo de $(G,*)$ ✓

④ Sea $(G,*)$ un grupo y $a \in G$, se llama centralizador de a al subconjunto $C(a) = \{g \in G : g*a = a*g\}$ (elementos de G que conmutan con a).
Demostrar que $C(a)$ es un subgrupo de G.

tengo que demostrar
$$\begin{cases} \forall g,h \in C(a),\ gh \in C(a) & \text{[op. interna]} \\ e_G \in C(a) & \text{[e. neutro]} \\ \forall g \in C(a) \Rightarrow g^{-1} \in C(a) & \text{[inverso]} \end{cases} \Rightarrow \text{subgrupo de } G$$

¿op. interna?

$\forall g,h \in C(a),\ gh \in C(a)$

$gh \in C(a)$; ¿ $(gh)a = a(gh)$? ($gh \in G$, $a \in G$ tb)

se utiliza la asociativa (porque G es grupo)

$$(gh)a \underset{\uparrow}{=} g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$$ ✓ op. interna ~~asociativa~~

$g,h,a \in G$ y G es grupo

¿e. neutro?

$e_G * a = a = a * e_G$; $e_G \in C(a)$ ✓ e. neutro

¿inverso?

$\forall g \in C(a) \Rightarrow$ ¿$g^{-1} \in C(a)$?

$g \in G \rightarrow g^{-1} \in G$

$g \in C(a)$: $g*a = a*g \Rightarrow (g*a)*g^{-1} = (a*g)*g^{-1} = a$

$\Downarrow$

$g^{-1}(gag^{-1}) = g^{-1}a \Rightarrow (g^{-1}g)(ag^{-1}) = g^{-1}a$

$\Downarrow$

$C(a)$ es subgrupo de G ✓

$ag^{-1} = g^{-1}a$ ✓ inverso

⑤ Sea $(G,*)$ un grupo, el conjunto $Z(G) = \{g \in G : x*g = g*x \text{ para todo } x \in G\}$ se denomina centro de G (mismo que antes? Creo q no, pq antes a no tenía p~~q~~ ser de G, lo especifica en el enunciado).

Demostrar las siguientes proposiciones:

a) $Z(G) \leq G$ (subgrupo) (este apartado es igual q. el anterior ejercicio, basically)

¿op. interna?

$\forall g,h \in Z(G),\ gh \in Z(G)$

$\forall x \in G$ ¿ $(gh)x = x(gh)$? hipótesis: $\forall x \in G\ \ gx = xg$
$\forall x \in G\ \ hx = xh$

$$\underset{\substack{\uparrow \\ \text{asociativa}}}{(gh)x =} g(hx) \underset{\substack{\uparrow \\ h \in Z(G)}}{=} g(xh) \underset{\substack{\uparrow \\ \text{asociativa}}}{=} (gx)h \underset{\substack{\uparrow \\ g \in Z(G)}}{=} (xg)h \underset{\substack{\uparrow \\ \text{asociativa}}}{=} x(gh)$$ ✓ op. interna

¿e.neutro?

$\forall x \in G \quad x \cdot e_G = e_G \cdot x = x \Rightarrow e_G \in Z(G)$ ✓ e.neutro

¿inverso?

sea $g \in Z(G)$ ¿$g^{-1} \in Z(G)$?, $\forall x \in G \quad gx = xg$ hipótesis

$(gx)g^{-1} = (xg)g^{-1} = x \Rightarrow g^{-1}(gxg^{-1}) = g^{-1}x \Rightarrow \underline{xg^{-1} = g^{-1}x}$ ✓ inverso

$Z(G)$ es subgrupo ✓

$\boxed{1b}$ $Z(G) = \bigcap_{a \in G} C(a)$ (intersección de todos los centralizadores)

primero: $Z(G) \subseteq \bigcap_{a \in G} C(a)$: $g \in Z(G) \Rightarrow \forall a \in G$ $ga = ag \Rightarrow \forall a \in G \quad g \in C(a)$

ahora: $\bigcap_{a \in G} C(a) \subseteq Z(G)$: $\underbrace{\text{sea } b \in \bigcap_{a \in G} C(a)}_{\text{b pertenece a todos los centralizadores}} \Rightarrow \forall a \in G,\ a * b = b * a \Rightarrow$

$\Rightarrow b \in Z(G)$ ✓

$\boxed{1c}$ $a \in Z(G) \Leftrightarrow C(a) = G$

$a \in Z(G) \Leftrightarrow \underbrace{ax = xa \quad \forall x \in G}_{\text{TODOS los elementos de G conmutan con a}} \Leftrightarrow \underbrace{\forall x \in G \quad x \in C(a)}_{\text{todos los elem. de G están en el centralizador de G}}$ ✓

⑤ Sea $G = \{T_{a,b} : \mathbb{R} \to \mathbb{R},\ a,b \in \mathbb{R}$ con $a \neq 0$, aplicaciones definidas por $T_{a,b}(r) = ar + b\}$. Se considera en G la operación composición de funciones.

$\boxed{a}$ Demostrar que $(G, \circ)$ es un grupo. ¿Es grupo abeliano?

¿op. interna?

$T_{a,b} \circ T_{c,d}(r) = T_{a,b}(cr + d) = acr + ad + b = T_{ac,\, ad+b}(r) \in G$ ✓

¿asociativa?

$T_{a,b} \circ (T_{c,d} \circ T_{e,f}) = T_{a,b} \circ T_{ce,\, cf+d} = T_{ace,\, acf + ad + b}$ ✓

¿e.neutro?

$e \circ T_{a,b} = T_{a,b}$; $T_{e_0,e_1} \Rightarrow e_0 = 1,\ e_1 = 0$: $T_{1,0}$ ✓

$\Downarrow$

$T_{ae_0,\, ae_1 + b}$

(cont.)

(cont.)

¿inverso?

$T_{a',b'} \circ T_{a,b} = T_{1,0} \Leftrightarrow \underline{T_{a'a,\,a'b+b'}} = T_{1,0} \Leftrightarrow \begin{cases} a' = 1/a \\ b' = -b/a \end{cases}$ ✓ hay inverso

Es abeliano? No, $T_{c,d} \circ T_{a,b} = T_{ca,\,cb+d} \neq T_{a,b} \circ T_{c,d}$
(No conmutativo) (ya hecho)

1b) Demostrar que $H = \{T_{a,b} \in G : a \in \mathbb{Q}\}$ (racionales) es un subgrupo de G. ¿es (H, o) abeliano?

¿op. interna?

$T_{a,b} \circ T_{c,d} = T_{ac,\,ad+b}$

si $a, c \in \mathbb{Q}$

$\left.\begin{matrix} a \neq 0 \\ c \neq 0 \end{matrix}\right\} \Rightarrow \begin{matrix} ac \neq \mathbb{R} \\ ac \neq 0 \end{matrix} \Rightarrow T_{ac,\,ad+b} \in H$

¿e. neutro?

$e_G = T_{1,0} \in H$

$1 \in \mathbb{Q}$ (es racional)

¿inverso?

$(T_{a,b})^{-1} = T_{\frac{1}{a},\,-b/a}$

a es racional $\Rightarrow \frac{1}{a}$ es racional

b es racional $\Rightarrow -\frac{b}{a}$ es racional

$T_{\frac{1}{a},\,-\frac{b}{a}} \in H$ ✓

No es abeliano (por lo mismo que antes, solo q ahora en $\mathbb{Q}$, pero la justificación es la misma)

1.2.a

① Dado un grupo $(G,*)$, demostrar que $\forall a,b,g \in G$ se verifica:

ⓐ $|a| = |a^{-1}|$

recordar: orden de un elemento a: mín. entero positivo (n) que verifica $a^n = e$)

¿ $a^n = e \Leftrightarrow a^{-n} = e$?

¿ $a^n \cdot a^{-n} = e$?

$\underbrace{a^1 \cdot a^{n-1}}_{=a^n} \cdot \underbrace{a^{-1} \cdot a^{-n+1}}_{=a^{-n}} = e \cdot \overset{\overset{!}{=}}{a^0} = e$ ✓ (not sure)

corrección de clase: $a^n = e \Leftrightarrow (a^n)^{-1} = e^{-1} = e \Leftrightarrow \underline{a^{-n} = e}$ ✓

ⓑ $|a| = |g^{-1}ag|$

¿ $a^n = e \Leftrightarrow (g^{-1}ag)^n = e$?

esto es porque como g^{-1} y g son inversos no hace falta elevarlos a n

$(g^{-1}ag)^n = e \Leftrightarrow g^{-1}a^n g = e \Leftrightarrow gg^{-1}a^n g = g \Leftrightarrow a^n g g^{-1} = g \cdot g^{-1} \Leftrightarrow$

$\Leftrightarrow \underline{a^n = e}$ ✓

!!! $(ab)^n \neq a^n b^n$ NO SON EQUIVALENTES

ⓒ $|ab| = |ba|$

¿ $(ab)^n = e \Leftrightarrow (ba)^n = e$?

$(ab)^n = e \Leftrightarrow \left((ab)^n = abab ab \ldots = a(ba)^{n-1}b \right) \Leftrightarrow a(ba)^{n-1}b = e \Leftrightarrow$

$\Leftrightarrow (ba)^{n-1} = \underbrace{a^{-1}b^{-1}}_{\text{!!! propiedad saber!}} = (ba)^{-1} \Leftrightarrow (ba)^n \cdot (ba)^{-1} = (ba)^{-1} \Leftrightarrow$

$\Leftrightarrow \underline{(ba)^n = e}$ ✓

② ¿Qué orden puede tener el elemento $a \in G$ si $a^{24} = e$?

cualquier divisor de 24 puede ser el orden de a:

$24 = 2^3 \cdot 3$

$|a| \in \{1,2,3,4,6,8,12,24\}$]– uno de ellos es el orden de a (NO TODOS, LÓGICO)

(3) Sea $(G,*)$ un grupo y sean $a,b \in G$ tales que $b \neq e$. Si $|a|=2$ y $b^2 = aba$ ¿qué puede decirse del orden de b?

$$b^2 = aba \Rightarrow \underline{b} = a^{-1}b^2a^{-1} = \underline{ab^2a} \Rightarrow$$

$a^{-1}b^2 = a^{-1}aba \Rightarrow$
$\Rightarrow \underline{a^{-1}b^2a^{-1}} = baa^{-1} = \underline{b}$

$|a|=2$
$a*a=e$
$a=a^{-1}$

$$\Rightarrow b^2 = (ab^2a)(ab^2a) = ab^4a \Rightarrow b^2 = aba = ab^4a \Rightarrow b = b^4 \Rightarrow b^3 = e$$

y como $b \neq e$:

$$\underline{|b|=3}$$

(5) escribir al menos 5 elementos de cada uno de los siguientes subgrupos cíclicos:

① $(25) \leq (\mathbb{Z},+)$
② $(1/2) \leq (\mathbb{Q}^*,\cdot)$
③ $(\pi) \leq (\mathbb{R}^*,\cdot)$

reminder
(*) el mínimo subgrupo q. contiene a $\frac{1}{2}$ es el generado por $\frac{1}{2}$

② $H = \underbrace{\langle \tfrac{1}{2} \rangle}_{\text{subgrupo generado por } \frac{1}{2}} \leq \mathbb{Q}^*$

$\underbrace{\frac{1}{2} \in H,\ 1 \in H,\ \frac{1}{4} \in H,\ 2,4 \in H}_{\text{ver teoría}} \Rightarrow \frac{1}{2^n} \in H,\ n \in \mathbb{Z}$

$H = \left\{ \frac{1}{2^n} : n \in \mathbb{Z} \right\}$ ¿$H \leq G = \mathbb{Q}^*$?

~~si H es subgrupo de $\mathbb{Q}^*$, los elem $\in H$ $\forall b \in \mathbb{Q}^*$~~

• $H \neq \phi$ $1 \in H$
• $2^a * 2^b = 2^{a+b} \in H$

✓ H es subgrupo de G, lo cumple (ya tengo los elem)

① $H_2 = \langle 25 \rangle$ ($\leq \mathbb{Z}$ pero ¿$\leq \mathbb{Z}$?)

$25, 0 \in H_2$
$-25 \in H_2$
$25 * 25 \in H_2$

$\Rightarrow H_2 = \{ n \cdot 25 : n \in \mathbb{Z} \}$ $\leq \mathbb{Z}$?

✓ sí, ya tengo los elem

③ $H_3 = \langle \pi \rangle \therefore H_3 = \{ \pi^n : n \in \mathbb{Z} \} \leq \mathbb{R}$?

si ✓ si

5 elem: $\pi^2, 1, \frac{1}{\pi^2}, 1/\pi$ ....

⑥ Indicar cuáles de los siguientes grupos son cíclicos y obtener los generadores

$(H_1, *_1) = (\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

$(H_2, *_2) = (\mathbb{Q}, +)$

$(\mathbb{Q}, +)$ no es cíclico: supongamos que $\mathbb{Q} = \langle \frac{p}{q} \rangle$

$\langle p/q \rangle = \{ \frac{p}{q} n : n \in \mathbb{Z} \}$ $\quad \frac{1}{q+1} \notin \frac{p}{q} n$

$(H_3, *_3) = (\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$

$(\mathbb{Q}^*, \cdot)$ $\quad \mathbb{Q}^* = \langle \frac{p}{q} \rangle = \{ (\frac{p}{q})^n : n \in \mathbb{Z} \}$

sea $h \in \mathbb{N}$ primo tq mcd $(h, p) = 1$ y mcd $(q, h) = 1$

No es cíclico

$(H_4, *_4) = (6\mathbb{Z}, +) = \langle 6 \rangle = \langle -6 \rangle$

$(H_5, *_5) = (\{6^n : n \in \mathbb{Z}\}, \cdot) = \langle 6 \rangle = \langle 1/6 \rangle$

¡Matchit!

(10) Encontrar el nº de generadores de los grupos cíclicos de órdenes 6, 8, 12, 60

para 12:

$(G,*)$ con $|G|=12$ $\quad G=\langle a\rangle$ pq es cíclico

$G=\{e, a, a^2, \ldots, a^{11}\}$ ← orden 12, $a^{12}=e$, $a^{13}=a$ etc

$$|a^r| = \frac{12}{mcd(12,r)} = 12 \iff mcd(12,r)=1$$

sabemos · si y solo si · el orden del grupo será 12

tenemos que buscar por tanto cuántas unidades en 12 hay: $|U_{12}|$?

$U_{12}=\{r\in\{1,\ldots,n\}$ tq $mcd(r,n)=1\}$

unid. de 12

$$\to |U_{12}| = \frac{12}{1} - \frac{12}{2} - \frac{12}{3} + \frac{12}{6} = 4 \text{ unidades}$$

sus divisores!

no sé pq un +

⇓

4 generadores del grupo cíclico de 12

||

4 r's ≠ porque $|a^r|=12$ siendo $\langle a\rangle$ generador de 12, $\langle a^r\rangle$ tb generador

(4) Sea $(G,*)$ un grupo y sean $a,b\in G$, tales que $b\neq e$

a) Demostrar que si $aba^{-1}=b^k$ entonces $a^rba^{-r}=b^{k^r}$

Por inducción sobre r:

a) $r=1$ $\quad a^1ba^{-1}=b^k \to$ ✓

b) sup $a^{r-1}ba^{-r+1}=b^{k^{r-1}}$ cierto

c) ¿$a^rba^{-r+1}=b^{k^r}$? despejo b en la 2ª

$$\left.\begin{array}{l} aba^{-1}=b^k \\ a^{r-1}ba^{-r+1}=b^{k^{r-1}} \end{array}\right\} \Rightarrow b=a^{-r+1}b^{k^{r-1}}a^{r-1} \Rightarrow b^k=(a^{-r+1}b^{k^{r-1}}a^{r-1})^k=$$

$$= a^{-r+1}(b^{k^{r-1}})^k a^{r-1} = a^{-r+1}b^{k^{r-1}k}a^{r-1} =$$

$$\left.\begin{array}{l} = a^{-r+1}b^{k^r}a^{r-1} \\ b^k = aba^{-1} \end{array}\right\} \Rightarrow aba^{-1} = a^{-r+1}b^{k^r}a^{r-1} \Rightarrow$$

$$\Rightarrow b^{k^r} = a^rba^{-r}$$ ✓

b) Si $|a| = 5$ y $b^2 = aba^{-1}$ ¿ que puede decirse sobre el orden de b?

$$a^5 b^5 a^{-5} = b^{\cancel{2}^5} = b^{2^5} \Rightarrow b = b^{32} \Rightarrow \underline{\underline{b^{31} = e}}$$

$$|b| = 31$$

$\boxed{1.2.b}$

① Encontrar el nº de elementos de cada uno de los subgrupos cíclicos indicados:

a) $H_a = \langle 25 \rangle \leq \mathbb{Z}_{30}$

$$|25| = \frac{30}{mcd(30,25)} = \frac{30}{5} = \underline{\underline{6}}$$

b) $H_b = \langle 30 \rangle \leq \mathbb{Z}_{42}$

" "

c) $H_c = \langle i \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$

$$\langle i \rangle = \{ i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1 \}$$

Grupo generado por i tiene 4 elementos

hemos llegado al e. neutro, los siguientes ya se repetirían so we stop.

d) $H_d = \frac{1+i}{\sqrt{2}} \leq \mathbb{C}^* = \mathbb{C} - \{0\}$

$$\left\langle \frac{1+i}{\sqrt{2}} \right\rangle = \left\{ \frac{1+i}{\sqrt{2}},\ \left(\frac{1+i}{\sqrt{2}}\right)^2 = i,\ \left(\frac{1+i}{\sqrt{2}}\right)^3 = \frac{i-1}{\sqrt{2}},\ \left(\frac{1+i}{\sqrt{2}}\right)^4 = -1,\ \left(\frac{1+i}{\sqrt{2}}\right)^5 = \frac{-1-i}{\sqrt{2}},\right.$$
$$\left. \left(\frac{1+i}{\sqrt{2}}\right)^6 = -i,\ \left(\frac{1+i}{\sqrt{2}}\right)^7 = \frac{-1+i}{\sqrt{2}},\ \left(\frac{1+i}{\sqrt{2}}\right)^8 = 1 \right\}$$

e. neutro, fin.

② Sea $n \in \mathbb{N}$, demostrar que para todo K divisor n, el grupo $(\mathbb{Z}_n, +_n)$, tiene un único subgrupo de orden K, que es $H_K = \langle \frac{n}{K} \rangle$.

Sea K divisor de n $\rightarrow h = \frac{n}{K} \in \mathbb{N}$

orden de h: $\underline{\underline{|h|}} = \frac{n}{mcd(n,h)} = \frac{n}{mcd(n, \frac{n}{K})} = \frac{n}{\frac{n}{K}} = \underline{\underline{K}} \Rightarrow$

$\Rightarrow H_K = \langle h \rangle = \langle \frac{n}{K} \rangle$ tiene orden K ✓

cont. →

cont. $\rightarrow$ Ahora veremos que también es único:

sup H' otro subgrupo: tq:

sea $H' \leq \mathbb{Z}_n$ con orden $|H'| = K$

H' tiene que estar generado por un elemento, que tendrá el mismo orden que el orden del grupo (teoría).

$H' = \langle h' \rangle$ con $|h'| = K$ (múltiplo de $\frac{n}{K}$)

y además $\frac{n}{mcd(n,h')} \Rightarrow mcd(n,h') = \frac{n}{K} \Rightarrow h' = \frac{n}{K} \cdot q \Rightarrow$

$\Rightarrow h' \in \langle \frac{n}{K} \rangle \Rightarrow \langle h' \rangle \subseteq \langle \frac{n}{K} \rangle$

pertenece al subg. generado por $\frac{n}{K}$

y como tienen el mismo orden:

$|\langle h' \rangle| = |\langle \frac{n}{K} \rangle| \Rightarrow \langle h' \rangle = \langle \frac{n}{K} \rangle$

son el mismo

es único ✓

watch it tut.

③ Sea H un subgrupo propio de $(\mathbb{Z}, +)$. Estudiar si puede determinarse el subgrupo H en cada uno de los siguientes casos:

a) si $18, 30, 40 \in H$

si H contiene a estos nº's, también va a contener a sus combinaciones lineales ($\equiv$ múltiplos)

(reminder:) th. Bezout: $d = ax + by$

siendo $d = mcd(a,b)$ = mínimo entero no negativo que se puede escribir como combinación lineal de dos enteros

so: mcd en a: mínima combinación lineal (max. común divisor) $= 2$

y $2 \in H \Rightarrow \langle 2 \rangle \subseteq H$

subg. generado por 2 $\Rightarrow \langle 2 \rangle = \{0, 2, 4, 6 \ldots\} \subseteq \mathbb{Z}$

sea $\langle 2 \rangle \subsetneq H \subseteq \mathbb{Z}$ (contenido y distinto de) si $2n+1 \in H$, $2n \in H$ $\Rightarrow$ $1 \in H$ $(\frac{1}{2} \cdot 2 = 1)$ $\Rightarrow H \in \mathbb{Z}$ ↯ pq $\in \langle 2 \rangle$

b) $12, 30, 54 \in H$

mcd $= 6 \in H \Rightarrow \langle 6 \rangle \subseteq H$

$\langle 6 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$

$\langle 6 \rangle \subsetneq \langle 3 \rangle \subsetneq \mathbb{Z}$

$H = \begin{cases} \langle 2 \rangle \\ \langle 3 \rangle \\ \langle 6 \rangle \end{cases}$ No se determina cual es el subgrupo

⊛₁

(5) Demostrar que se cumple $Y^2 = J^2 = K^2 = -q_0$, $YJ = K$, $JK = Y$, $KY = J$, $JY = -K$, $KJ = -Y$ y $YK = -J$. obtener el orden de cada elemento y un cjto. generador del grupo $(Q, \cdot)$.

$$Q = \left\{ q_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, -q_0 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right.$$

$$\left. -Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, -J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, -K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\}$$

a) por cuentas básicas, like:

$$Y^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = J^2$$

b) orden:

$|q_0| = 1$ ↑ por ser identidad $(q_0^1 = e)$

$|-q_0| = 2$ $\quad (-q_0)^2 = e$

orden de J:

$J^2 = -q_0$

$(-q_0)^2 = q_0 = e$

⇕

$(-J^2)^2 = q_0 = e$

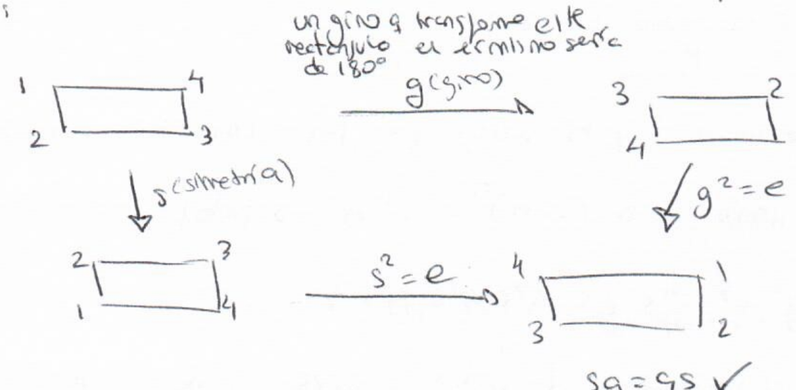
orden de J: $\underline{|J| = 4}$

watchititot.

c) un cjto generador del grupo:

$Q = \langle Y, J \rangle = \langle Y, K \rangle = \langle J, K \rangle = \langle Y, J \rangle = \ldots$ ⊛₁ viendo esta op.

(6) Describir el grupo de simetrías de un rectangulo y encontrar un cjto. generador del grupo:



sg = gs ✓

$D_2 = \{e, g, s, gs\}$

	e	g	s	gs
e	e	g	s	gs
g	g	e	gs	s
s	s	gs	e	g
gs	gs	s	g	e

⑦ Describir el grupo de simetrías de un rombo y encontrar un gto. generador

(sabiendo hacer las simetr. de un rectángulo, las del rombo son fáciles)

⑧ Se considera el grupo diédrico $(D_n, \circ)$, $D_n = \{a, b : |a| = n, b^2 = e, ba = a^{-1}b\}$

a) Demostrar que $ba^r = a^{-r}b \quad \forall \quad 0 \leq r < n$

Inducción sobre r:

a) $r=1 \qquad ba = a^{-1}b$

b) sup $\qquad ba^{r-1} = a^{-r+1}b$

c) $ba^r = (ba^{r-1})a \underset{\substack{\uparrow \\ \text{hip. induc.}}}{=} (a^{-r+1}b)a = a^{-r+1}(ba) = a^{-r+1}a^{-1}b = a^{-r}b$

b) Demostrar que todo elemento de la forma $a^r b$ tiene orden 2

$(a^r b)(a^r b) = a^r(ba^r)b = a^r(a^{-r}b)b = (a^r a^{-r})(bb) = b^2 = \underline{\underline{e}}$

c) Encontrar el centro de D_n

$\underset{(\text{centro})}{Z(D_n)} = \{g \in D_n : gx = xg \ \forall x \in D_n\}$

$ba^r = a^{-r}b \underset{\substack{\uparrow \\ \text{para q } b \\ \text{y } a^r \text{ conmuten}}}{=} a^r b \iff a^{-r}b = a^r b \iff a^{2r} = e \iff$

$\iff n = 2r$, $\left.\begin{array}{l} n \text{ es par} \\ y\ r = \frac{n}{2} \end{array}\right\} \Rightarrow$

$\Rightarrow \left.\begin{array}{l} Z(D_{2n}) = \{e, a^n\} \\ Z(D_{n+1}) = \{e\} \end{array}\right\} n > 1$

⑨ Encontrar en cada caso, un grupo con las condiciones requeridas.

c) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 5$

si G es abeliano $\rightarrow (ab)^n = a^n b^n \Rightarrow |ab| = \text{mcm}(|a|, |b|)$

$D_5 = \{e, g, g^2, g^3, g^4, s, gs, g^2s, g^3s, g^4s\}$

Buscamos 2 elementos de orden 2 cuyo producto tenga orden 5

$|s| = 2$

$|gs| = 2$

(pq son giros)

$|(gs)s| = |g| = 5$

(10) Demostrar que D_6 tiene un subgrupo de orden 4.

$$D_6 = \{e, g, g^2, g^3, g^4, g^5, \underbrace{s, gs, g^2s, g^3s, g^4s, g^5s}_{\text{todos tienen orden 2 (que los giros)}}\}$$

orden 6 (g), orden 2 (g^3), orden 3, orden 6 (g^5)

p.ej.: metemos e g^2 y g^4, pero entonces tb:

$\{e, g^2, g^4, s, g^2s, g^4s\}$ → orden 6 no vale

$\{e, g^3, s, g^3s\}$ → orden 4 ✓

ó

$\{e, g^3, gs, g^4s\}$ → orden 4 ✓

$(g^3 \cdot gs = g^4s)$

(11) Demostrar que D_3 no tiene un subgrupo de orden 4.

$D_3 = \{e, g, g^2, s, gs, g^2s\}$

$\{e, g, g^2, g^3, s, gs\}$
$\{e, s, ss, g^2s, g, g^2\}$
→ en el momento en que ~~tienes~~ metes 4, tienen que entrar todos

1.3

(1) Escribir cada una de las siguientes permutaciones como producto de ciclos disjuntos y como producto de transposiciones.

b) ~~$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 & \end{pmatrix}$~~ $= (37)(2548)(6)(9) =$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9 \end{pmatrix} = \underbrace{(13)(37)}\ \underbrace{(25)(54)(48)}$

dos 2 ciclos disjuntos

Es una permutación impar

(2) Escribir como producto de ciclos disjuntos:

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$, $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix} \in S_6$

cont.

cont. ⟹ d) $\tau\sigma^{-2}$

1º, pasamos como producto de ciclos disjuntos:

$\tau = (1243)(56)$

$\sigma = (134562)$

Ahora, sabemos:

$\tau\sigma^{-2} = \tau(\sigma^{-1})^2 = \tau\cdot\sigma^{-1}\cdot\sigma^{-1}$ ← elegimos esta, p.ej

ó

$\tau(\sigma^2)^{-1} = \tau\cdot(\sigma\cdot\sigma)^{-1}$

$\sigma^{-1} = (1\,2\,6\,5\,4\,3)$ ¿how?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$$= \underline{(1\,2\,6\,5\,4\,3)}$$

$\tau\cdot\sigma^{-1}\cdot\sigma^{-1} = (1243)\underset{\text{ya están}}{(56)}(126543)(126543) =$

$= \underline{(15)(2634)}$ ✓ hasta q aparezcan todos los nºs

③

a) ¿Cuál es el orden del ciclo $(1,4,5,7) \in S_8$?

orden = longitud (en un ciclo) $\underline{\underline{4}}$

b) ¿Cuál es el orden de $\sigma = (45)(237)$ y de $\tau = (14)(3578)$ en S_8?

$|\sigma| = 6 = \text{mcm}\{\underbrace{|45|}_{2}, \underbrace{|237|}_{3}\}$ (mín. común múltiplo)

$|\tau| = \text{mcm}\{2,4\} = 4$

c) Expresar como producto de ciclos disjuntos y obtener el orden $v_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$

$v_4 = (124)(35)$

$|v_4| = \text{orden} = \text{mcm}\{3,2\} = 6$

④ Demostrar que A_8 contiene un elemento de orden 15.

$X = \{1\,2\,3\,4\,5\,6\,7\,8\}$ $(\notin A_8)$

$\sigma = (123)(45678)$ ~~$\in A_8$~~ cuyo orden $= \text{mcm}\{3,5\} = 15$

$\|$

$\sigma = (12)(23)(45)(56)(67)(78) \in A_8$

(5) a) sea $\beta = (1\ 3\ 5\ 7\ 9\ 8\ 6)(2\ 4\ 10)$ ¿cual es el menor entero positivo $n \in \mathbb{N}$ tal que $\beta^n = \beta^{-5}$.

$\beta^n = \beta^{-5} \Leftrightarrow \beta^{n+5} = e \Rightarrow n+5 = 21$ ya que $|\beta| = 21 = \text{mcm}\{7,3\}$

b) si $\alpha = (1\ 3\ 5\ 7\ 9)\overset{(2\,4\,6)}{(}8\ 10)$ y α^m es ciclo de longitud 5 ¿qué puede decirse sobre m?

$$|\alpha^m| = \frac{\overset{\text{mcm}\{5,3,2\}=|\alpha|}{\overset{\shortparallel}{30}}}{\text{mcd}(30,m)} = 5 \longrightarrow m \ast \text{mcd}(30,m) = 6$$

(4) ¿cuales de ~~se dispone~~ los siguientes son subgrupos de S_5?

$X_a = \{(1,2,3,4,5)(1,2,4),(3,5)\}$ No es subgrupo, $e \notin X_a$

$X_b = \{(1),(1,2,3,4,5),(1,3,5,2,4),(1,4,2,5,3)(1,5,4,3,2)\}$ Sí es subgrupo $\langle 12345\rangle \in X_b$ y su cuadrado $\langle 135\,24\rangle$ tb (+)

$X_c = \{(1),(1\,2)(3\,4\,5),(1\,3\,5),(2\,4),(1\,5,3,2,4),(1,2),(4,5),(1\,3,4)(2,5),$
$(1,4,3),(2,5)\}$ No es subgrupo pq. no está el elemento mas grande $(1\,5\,3\,2\,4)$ elevado al cuadrado $(1\,4\,2\,5\,3)$.

(+) y su cuadrado tb y su cuadrado (vuelve a ser (12345))+

Problemas Tema 2

2.1

① En $(\mathbb{Z},+)$ se considera el subgrupo $H=\{3n : n\in\mathbb{Z}\}$. Decidir cuales de los siguientes pares de clases laterales son las mismas.

a) $11+H$ y $17+H$ $\quad 11H \quad 17H$

b) $-1+H$ y $5+H$ $\quad -1H \quad 5H$

c) $7+H$ y $23+H$ $\quad 7H \quad 23H$

$a\,R_H\,b \iff a^{-1}b\in H$ [copiado de Alicia]

$(-1)^{-1}$ en $\mathbb{Z}$ $= -(-1)+5 = 6 \in H$ ✓

$-11+17 = 6 \in H$ ✓

$-7+23 = 16 \notin H$ ✗

2.2

④ Dados el grupo $(G,*)$ y el subg. $H\leq G$, demostrar que $H\trianglelefteq G$, construir la tabla de Cayley del grupo cociente G/H y encontrar un grupo isomorfo a G/H.

b) $(G,*)=(\mathbb{Z}_4\times\mathbb{Z}_4,(+_4,+_4))$ y $H=\{([0]_4,[0]_4),([2]_4,[0]_4),([0]_4,[2]_4),([2]_4,[2]_4)\}$

ser: clases lat de todos los elem de $\mathbb{Z}_4$, pero como buscamos el g. cociente: SOLO HASTA TENER TODOS LOS ELEM

$(0,0)H=\{(0,0),(2,0),(0,2),(2,2)\}$

$(0,1)H=\{(0,1),(2,1),(0,3),(2,3)\}$ el $(0,1)$ no está aquí

$(1,0)H=\{(1,0),(3,0),(1,2),(3,2)\}$ el $(1,0)$ no está aquí ni aquí

$(1,1)H=\{(1,1),(3,1),(1,3),(3,3)\}$ el $(1,1)$ no está en ninguno de los anteriores

Ya tengo todos los elementos (en $\mathbb{Z}_4\times\mathbb{Z}_4$):

$\frac{G}{H}=\{\underbrace{(0,0)H}_{e},\ \underbrace{(0,1)H}_{a},\ \underbrace{(1,0)H}_{b},\ \underbrace{(1,1)H}_{c}\}$ $\Rightarrow$ tabla:

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

$*: (0,1)\times(0,1)=(0,2)$ en $\mathbb{Z}_4\times\mathbb{Z}_4$ $\Rightarrow$ su clase $(0,0)=e$

$\Downarrow$

$\frac{G}{H}\cong$ grupo 4 de Klein

subgrupo generado por (1,2)

c) $(G,*) = (\mathbb{Z}_4\times\mathbb{Z}_4, (+_4,+_4))$ y $H = \langle\langle [1]_4, [2]_4 \rangle\rangle$

$$\left.\begin{array}{l} (1,2)*(1,2) = (2,0) \\ (2,0)*(1,2) = (3,2) \\ (3,2)*(1,2) = (0,0) \end{array}\right\} \Rightarrow H = \langle\langle (1,2) \rangle\rangle = \{(0,0),(1,2),(2,0),(3,2)\}$$

$(0,0)H = \{(0,0),(1,2),(2,0),(3,2)\}$

$(0,1)H = \{(0,1),(1,3),(2,1),(3,3)\}$

$(0,2)H = \{(0,2),(1,0),(2,2),(3,0)\} = (1,0)H$

$(0,3)H = \{(0,3),(1,1),(2,3),(3,1)\} = (1,1)H$

$G/H = \{\underbrace{(0,0)H}_{e}, \underbrace{(0,1)H}_{a}, \underbrace{(0,2)H}_{b}, \underbrace{(0,3)H}_{c}\}$

(ó $(1,0)H$, $(1,1)H$)

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

$G/H \approx \mathbb{Z}_4$ (isomorfo a)

d) $(G,*) = (\mathbb{Z}_4\times\mathbb{Z}_4^*, (+_4,\cdot_4))$ y $H = \langle\langle [2]_4, [3]_4 \rangle\rangle$

$\mathbb{Z}_4^* = U_4 = \{1,3\}$ = unidades módulo 4 $(mcd(4,x)=1)$ $(1,3,5,7,9,$ etc$)$

$(2,3)*(2,3) = (0,1)$

$(0,1)*(2,3) = (2,3)$ $\Rightarrow H = \{(0,1),(2,3)\}$

$(0,1)H = \{(0,1),(2,3)\}$

$(1,1)H = \{(1,1),(3,3)\}$

$(2,1)H = \{(2,1),(0,3)\}$

$(3,1)H = \{(3,1),(1,3)\}$

ya están todos ✓

(ej: $(0,0)$, $(0,2)$ no valdrían: $2 \notin U_4$, $\notin H$)

$G/H = \{\underbrace{(0,1)H}_{e}, \underbrace{(1,1)H}_{a}, \underbrace{(2,1)H}_{b}, \underbrace{(3,1)H}_{c}\}$

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

$G/H \approx \mathbb{Z}_4$ tb.

e) $(G,\circ) = (\mathbb{Z}_4 \times U_4, (+_4, \cdot_4))$ y $H = \langle\langle [2]_4, [1]_4 \rangle\rangle$ $\{1,3\}$

$\Downarrow$

$H = \{(0,1), (2,1)\}$

$(0,1)H = \{(0,1), (2,1)\}$

$(1,1)H = \{(1,1), (3,1)\}$

$(0,3)H = \{(0,3), (2,3)\}$

$(1,3)H = \{(1,3), (3,3)\}$

ya están todos:

$\frac{G}{H} = \{\underbrace{(0,1)H}_{\substack{H \\ e}}, \underbrace{(1,1)H}_{b}, \underbrace{(0,3)H}_{a}, \underbrace{(1,3)H}_{c}\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	
b	b		etc.	
c	c			

$\frac{G}{H} \approx$ grupo 4 de Klein $(\mathbb{Z}_2 \times \mathbb{Z}_2)$

"isomorfo a"

$\boxed{2.1}$ continuación y fin

(2) Dados $(G,*)$ y $H \leq G$, calcula $|H|$ y $[G:H]$ en cada caso:

a) $H = \langle [18]_{36} \rangle$, $(G,*) = (\mathbb{Z}_{36}, +_{36})$

$G = \mathbb{Z}_{36} \to G = \langle 1 \rangle$ ¿pq? el grupo cíclico)

$H \leq G$ $\quad H = \langle 18 \rangle$

por tanto $\underset{|H|}{=} |18| = \frac{36}{mcd(36,18)} = \frac{36}{18} = \underline{\underline{2}}$

$H = \{0, 18\}$

$\underline{\underline{[G:H]}} = \frac{|G|}{|H|} = \frac{36}{2} = \underline{\underline{18}}$

b) $H = \langle [3]_6 \rangle$, $(G,*) = (\mathbb{Z}_6, +_6)$

(same)

d) $H = \langle [12]_{60} \rangle$, $(G,*) = (\mathbb{Z}_{60}, +_{60})$

$G = \mathbb{Z}_{60} \longrightarrow G = \langle 1 \rangle$ $\quad H \leq G$ $\quad H = \langle 12 \rangle$

por tanto : $\underline{\underline{|H|}} = \frac{60}{mcd(60,12)} = \frac{60}{12} = \underline{\underline{5}}$

$\underline{\underline{[G:H]}} = \frac{|G|}{|H|} = \frac{60}{5} = \underline{\underline{12}}$

e) $H = \langle [2]_4 \rangle \times \langle [2]_{12} \rangle$, $(G,*) = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +_4 \times +_{12})$ // grupo no cíclico

$$[G:H] = \frac{|G|}{|H|} = \frac{4\cdot 12}{|H|} = \frac{4\cdot 12}{12} = 4$$

$$H = \langle 2 \rangle \times \langle 2 \rangle \Rightarrow |H| = |2|_4 \cdot |2|_{12} = 2\cdot 6 = 12$$
(en $\mathbb{Z}_4$) (en $\mathbb{Z}_{12}$)

rem: subgrupo generado por 2

en este caso: $H = \{(0,2)\,(0,4)\,(0,6)\,(0,8)\,(0,10)\,(2,2)\,(2,4)\,(2,6)\,(2,8)\,(2,10)\,(0,0)\,(2,0)\}$

f) $H = \langle ([2]_4, [2]_{12}) \rangle$, $(G,*) = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +_4 \times +_{12})$

$G = \mathbb{Z}_4 \times \mathbb{Z}_{12}$ // el grupo es el mismo q arriba, pero el subgrupo es distinto aunque ambos sean generados por 2,2 aquí es el grupo cíclico, y arriba es el producto de 2 cíclicos (*)

$H = \langle (2,2) \rangle$ (en $\mathbb{Z}_4$, en $\mathbb{Z}_{12}$) $\Rightarrow |H| = \text{mcm}(|2|_4, |2|_{12}) = \text{mcm}(2,6) = \underline{6}$

$$\underline{[G:H]} = \frac{|G|}{|H|} = \frac{4\times 12}{6} = \underline{8}$$

(*) q no es cíclico

en este caso: $H = \{(0,0)\ (2,2)\ (0,4)\ (2,6)\ (0,8)\ (2,10)\}$

$(2,2)*(2,2) = (0,4)$, $(0,4)*(2,2) = (2,6)$, $(2,2)*(2,6) = (0,8)$, $(2,2)*(0,8) = (2,10)$

$(2,10)*(2,2) = (0,0)$ ya incluido, FIN

g) $H = \langle [1]_3 \rangle \times \langle [0]_2 \rangle \times \langle [0]_4 \rangle$,
$(G,*) = (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4, +_3 \times +_2 \times +_4)$

$|H| = 3$ $\quad |G| = 3\cdot 2\cdot 4 \Rightarrow [G:H] = \frac{|G|}{|H|} = 2\cdot 4 = 8$

h) $H = \langle [0]_3 \rangle \times \langle [1]_2 \rangle \times \langle [2]_4 \rangle$, $(G,*) = (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4, +_3 \times +_2 \times +_4)$

H es producto de grupos cíclicos

$|H| = 4$ $\quad [G:H] = 6$

(3) Sean H y K dos subgrupos de un grupo $(G,\cdot)$ con $|G|=660$. Si $|K|=66$ y $K\subset H\subset G$ ¿que orden puede tener el grupo H?

si $H\in G \Rightarrow |H| \mid |G|$

$|K|=66 \mid |H| \Rightarrow |H|=66\cdot q$

$|H| \mid |G|=660 \Rightarrow 660=|H|\cdot h=66\cdot q\cdot h \Rightarrow 660=66q\, h \Rightarrow$
$\Rightarrow 10=q\cdot h$

$q\in\{1,2,5,10\}$

si $K \subsetneq H \subsetneq G \Rightarrow q\in\{2,5\}$
(contenido pero no igual)

$|H|\in\{2\cdot 66, 5\cdot 66\}$

(5) Sea $(G,*)$ un grupo y p un nº primo. Demostrar:

a) Si G tiene orden 2p entonces todo subgrupo propio de G es cíclico

$|G|=2p$ y $H\leq G$ $\quad H\neq G$

¿$|H|$? $\rightarrow H\in\{1,2,p\}$ pq $H\neq G$ por ser propio $\Rightarrow$
$\Rightarrow |H|\neq 2p$

si $|H|=1 \rightarrow H=\{e_G\}=\langle e_G\rangle \Rightarrow$ es cíclico

si $|H|\in\{2,p\} \rightarrow$ es cíclico (si un nº tiene orden primo, entonces necesariamente es primo pq:)

$\exists a\in H$ tq $a\neq e_G$

$|a|\neq 1$ pero $|a| \mid q$ con

$q\in\{2,p\} \Rightarrow |a|=q \Rightarrow$

$\Rightarrow H=\langle a\rangle \Rightarrow H$ es cíclico

b) Si G tiene orden p^2 entonces tiene un subgrupo de orden p.

$|G|=p^2$ y p primo $\Rightarrow \exists a\in G \; |a|\neq 1 \Rightarrow$
¡(propiedad)!

$\Rightarrow |a|\in\{p,p^2\}$ $\Rightarrow$ $\begin{cases} |a|=p \Rightarrow H=\langle a\rangle \text{ tiene orden } p \checkmark \\ |a|=p^2 \Rightarrow H=\langle a^p\rangle \text{ tiene orden } p \checkmark \end{cases}$

el orden de a tiene q dividir al orden del grupo $=p^2$

necesito un subgrupo que tenga p elementos,
¿como lo genero?: $\langle a^p\rangle$, ya q $|a^p|=\dfrac{|a|}{mcd(|a|,p)}=\dfrac{p^2}{p}=p$

⑥ Sean H y K dos subgrupos de $(G, *)$

a) Demostrar que si $|H| = 10$ y $|K| = 21$, entonces $H \cap K = \{e\}$

b) Demostrar que si $|H| = n$ y $|K| = m$ con $mcd(n, m) = 1$ entonces $H \cap K = \{e\}$

a) $|H| = 10$, $|K| = 21$ sea $a \in H \cap K \Rightarrow$ ¿$a = e_G$?

$$\left.\begin{array}{l} a \in H \quad |a| \,\big|\, |H| \Rightarrow \\ a \in K \Rightarrow |a| \,\big|\, |K| \Rightarrow \end{array}\right] \rightarrow |a| \,\big|\, mcd(|H|, |K|) \Rightarrow$$

$$\Rightarrow |a| \,\big|\, 1 \Rightarrow |a| = 1 \Rightarrow \underline{a = e_G}$$

b) (same thing)

$\boxed{2.2}$ continuación y fin

① Estudiar si H es un subgrupo normal de $(G, *)$ en cada caso

3 cond. suficientes: ⊛

① si $[G : H] = 2 \Rightarrow H \trianglelefteq G$

② $|H| = n$ y H es el único subgrupo de G con orden $n \Rightarrow$ $\Rightarrow H \trianglelefteq G$

③ si G es abeliano $\Rightarrow \forall H \leq G \Rightarrow$ $\Rightarrow H \trianglelefteq G$

* aunq no necesarias! (pero sí muy útiles a veces para caracterizar)

a) $H = \{(1), (1,2)\}$, $G = S_3$

$$\sigma \cdot (a_0, a_1, \dots, a_{n-1}) \sigma^{-1} = $$
$$= (\sigma(a_0), \sigma(a_1), \dots, \sigma(a_{n-1}))$$

$$(2,3)(1,2)(2,3)^{-1} = (1,3) \notin H \Rightarrow$$
$$\Rightarrow H \not\trianglelefteq G \qquad \text{(por esto) } ⊛_2$$

b) $H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \text{ tq } ac \neq 0 \right\}$

$G = GL_2(\mathbb{R}) \rightarrow \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathbb{R}^{2\times 2}$ tq $xt - yz \neq 0$ $⊛_3$

$⊛_2$ reminder: $H \trianglelefteq G \Leftrightarrow aha^{-1} \in H$ $\forall a \in G, h \in H$

$aha^{-1} \in H$ $\forall a \in G, h \in H$

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix}^{-1} =$$

del grupo general lineal orden 2 (GL_2)

$$= \frac{1}{xt - yz} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} t & -y \\ -z & x \end{pmatrix} =$$

tb. se puede hacer con ejemplos numéricos, pero así es + visual

por esto ← $⊛_3$ podemos usar esta fracción →

$$= \frac{1}{xt - yz} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} at - bz & -ay + bx \\ -cz & cx \end{pmatrix} =$$

$$= \frac{1}{xt - yz} \cdot \begin{pmatrix} (x) & (x) \\ \underbrace{zat - bz^2 - czt}_{\neq 0} & (x) \end{pmatrix} \longrightarrow \notin H \text{ por tanto } H \text{ no normal!}$$

c) $H = SL_2(\mathbb{R})$, $G = GL_2(\mathbb{R})$ determinantes G y H

$G = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2} : ad-bc \neq 0 \} = \underline{GL_2(\mathbb{R})}$ $\underline{(DEF.)}$

$H = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2} : ad-bc = 1 \} = \underline{SL_2(\mathbb{R})}$ $\underline{(DEF.)}$

$I \in H \neq \emptyset$

$\overset{\shortparallel}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}$

$A, B \in H \Rightarrow \det(A) = \det(B) = 1$

$\det(AB^{-1}) = \det(A) \cdot \det(B)^{-1} = 1 \cdot 1 = 1$

$B \in G$
$A \in H$ ¿ $\det(BAB^{-1})$?

$\det(BAB^{-1}) = \underbrace{\det(B)}_{=1} \cdot \underbrace{\det(A)}_{=1} \cdot \underbrace{\det(B)^{-1}}_{=1^{-1}=1} = 1 \Rightarrow$

$\Rightarrow BAB^{-1} \in H \Rightarrow$

$\Rightarrow \forall B \in GL_2(\mathbb{R})$,

$BHB^{-1} \subseteq H \Rightarrow$

$\Rightarrow H$ es subgrupo normal

$H \trianglelefteq GL_2(\mathbb{R})$

d) $H = A_4$, $G = S_4$

$[G:H] = \frac{|G|}{|H|} = 2 \Rightarrow H \trianglelefteq G$

e) $H = \{(1), (1,2,3), (1,3,2)\}$, $G = A_5$

$\sigma(a_0, a_1, \ldots, a_{n-1})\sigma^{-1} = (\sigma(a_0), \sigma(a_1), \ldots, \sigma(a_{n-1}))$

$\underbrace{(1,2,4)}_{\in G} \underbrace{(1,2,3)}_{\in H} \underbrace{(1,4,2)}_{(1,2,4)^{-1}} = \underline{(2\,4\,3)} \notin H$ No es subgrupo normal

producto de permutaciones [viewed]

f) $H = D_4$, $G = S_4$

$D_4 =$ 

$= \{ \underset{e}{(1)}, \underset{\text{giro}}{(1\,2\,3\,4)}, \underset{\text{giro}^2}{\underline{(1,3)(2,4)}}, \underset{\text{giro}^3}{(1,4,3,2)}, \underset{\text{simetría}}{\underline{(1,2)(3,4)}}, \underline{(1,4)(2,3)}, \underline{(1,3)}, \underline{(2,4)} \}$

$S_4 = \{$ permutaciones de 4 elementos $\}$ $|S_4| = 4! = 24$

$\underset{\shortparallel}{(1,2)}(1,2,3,4)\underset{(\text{inverso de } (1,2)^{-1})}{\overset{\shortparallel}{(1,2)}} = \underset{(1\,3\,4\,2)}{\overset{}{(2,1,3,4)}} \notin D_4$

I think [$(1,2)(2,1)$
en permutaciones
$\rightarrow$ 4 elem $\in S_4$

(2) Demostrar que $Z(G)$ es un subgrupo normal de G, siendo $Z(G)$ el centro de G : $Z(G) = \{g \in G : g * a = a * g \quad \forall a \in G\}$

$$¿aga^{-1} \in H = Z(G) \quad \forall a \in G,\ \forall g \in Z(G)?$$

sea $a \in G$ y sea $g \in Z(G)$

$$aga^{-1} \underset{\uparrow}{=} gaa^{-1} = g \in Z(G)$$

$$g \in Z(G) \Rightarrow ag = ga \quad \forall a \in G$$

(3) Sea $(G, *)$ un grupo y sea $H = \langle a * b * a^{-1} * b^{-1} : a, b \in G \rangle$. Demostrar que H es un subgrupo normal de G. H recibe el nombre de <u>subg. conmutador</u> de G. Demostrar que G/H es abeliano.

$$\forall a \in G \quad \forall h \in H \quad ¿aha^{-1} \in H?$$

sea $a \in G$, $h \in H$ $\underset{\uparrow}{\Rightarrow}$ $\left.\begin{array}{l} aha^{-1}h^{-1} \in H \\ h \in H \end{array}\right\} \Rightarrow (aha^{-1}h^{-1})h \in H \Rightarrow$

por la definición de subgrupo de H

$$\Rightarrow \underline{\underline{aha^{-1} \in H}}$$

$aH, bH \in G/H$

$$\left.\begin{array}{l} aH * bH = abH \\ bH * aH = baH \end{array}\right\} ¿abH = baH?$$

//¿cuando son 2 clases iguales? cuando el * 1er representante multiplicado por el segundo pertenece al subgrupo + inverso

$\Downarrow$

$aH = bH \Leftrightarrow a^{-1}b \in H$

$\Downarrow$

$$(ab)^{-1}(ba) =$$
$$= b^{-1}a^{-1}ba =$$
$$= (b^{-1})(a^{-1})(b^{-1})^{-1}(a^{-1})^{-1} =$$
$$= c\,d\,c^{-1}d^{-1} \in H \ \checkmark \Rightarrow abH = baH$$

(4) Dados $(G, *)$ y $H \leq G$, demostrar que $H \trianglelefteq G$, construir la tabla de Cayley de G/H y encontrar un grupo isomorfo a G/H.

a) $(G, *) = (\mathbb{Z}, +)$ y $H = 5\mathbb{Z}$

tabla

$$\mathbb{Z}/5\mathbb{Z} = \{0H, 1H, 2H, 3H, 4H\}$$

$0H = \{5n : n \in \mathbb{Z}\}$
$1H = \{1 + 5n : n \in \mathbb{Z}\}$
$2H = \{2 + 5n : n \in \mathbb{Z}\}$
$3H = \{3 + 5n : n \in \mathbb{Z}\}$
$4H = \{4 + 5n : n \in \mathbb{Z}\}$

//hasta que aparecen todos!

b, c, d, e (hechos en el primer $\boxed{2.2}$)

f) $(G,*) = (Q_8, \cdot)$ y $H = \{1,-1\}$

$Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$

$H = \{1,-1\}$ único subgrupo de Q_8 que tiene orden 2

$\Downarrow$

$H \trianglelefteq G$

$|1| = -1$

$|-1| = 2$

$|i| = |-i| = |j| = |-j| = |k| = |-k|$

$\shortparallel$

4 (ver ejemplo en apuntes teoría)

$1H = \{1,-1\}$

$iH = \{i,-i\}$

$jH = \{j,-j\}$

$kH = \{k,-k\}$

// ya están todos $\Rightarrow G/H = \{1H, iH, jH, kH\} \approx \mathbb{Z}_2 \times \mathbb{Z}_2$

$iH * iH = (i^2)H = (-1)H = 1H$

$jH * jH = (j*j)H = (-1)H = 1H$

$kH * kH = (k*k)H = (-1)H = 1H$

tb se puede sacar con su tabla de Cayley

⑤ a) Encontrar todos los subgrupos de D_4 y estudiar cuales son normales.

b) Calcular, salvo isomorfismos, todos los posibles grupos cocientes con el grupo D_4 y sus subgrupos normales.

a) $D_4 = \{e, g, g^2, g^3, s, gs, g^2s, g^3s\}$

$aHa^{-1} = H \;\; \forall a \in G$

- $H_0 = \{e\} = \langle e \rangle \trianglelefteq D_4$

cíclicos:

- $H_1 = \{e, g, g^2, g^3\} = \langle g \rangle \trianglelefteq D_4$ pq $[D_4 : H_1] = 2 \;(= \frac{8}{4})$
- $H_2 = \{e, g^2\} = \langle g^2 \rangle \trianglelefteq D_4$ pq g^2 conmuta con todos los elem. de G (y e tb) $\Rightarrow aga^{-1} = (*)$, $aea^{-1} = (*)$
- $H_3 = \{e, s\} = \langle s \rangle$ $(*)_1$
- $H_4 = \{e, gs\} = \langle gs \rangle$ $(*)_2$
- $H_5 = \{e, g^2s\} = \langle g^2s \rangle$ $(*)_3$
- $H_6 = \{e, g^3s\} = \langle g^3s \rangle$ $(*)_4$

si alguno de estos fuese el único con orden 2, tb sería directamente $\trianglelefteq G$ (prop ②)

no cojo $\langle g^3 \rangle$ pq es $= \langle g \rangle$ guessing

$H_7 = \{e, g^2, s, g^2s\} \trianglelefteq D_4$

$H_8 = \{e, g^2, gs, g^3s\} \trianglelefteq D_4$

$H_9 = \langle s, g \rangle = D_4 \trianglelefteq D_4$

$(*) = g^2aa^{-1} = g^2 \in H_2$
$= eaa^{-1} = e \in H_2$

$(*)_1 \rightarrow gsg^{-1} = gsg^3 = sss =$
$= g^3s \notin H_3$
$\Downarrow$
No es normal

$(*)_2 \rightarrow ggsg^{-1} = g^2sg^3 = g^2gs =$
$= g^3s \notin H_4$
$\Downarrow$
No es normal

$(*)_3 \rightarrow gg^2sg^{-1} = g^2sg^3 =$
$= g^2gs = s \notin H_5$

$(*)_4 \rightarrow gs^3sg^{-1} \ldots$
(incompleto)

b)

$D_4/\{e_4\} \cong D_4$ $\qquad$ $D_4/D_4 \approx \{e_4\}$

D_4/H_1

$H = \{e, g, g^2, g^3\}$

$D_4/H = \{eH, sH\} \approx \mathbb{Z}_2$

D_4/H_2

$H = \{e, g^2\}$

$D_4/H = \{eH, gH, sH, gsH\}$

$eH = \{e, g^2\}$

$gH = \{g, g^3\}$

$sH = \{s, sg^2 = g^2 s\}$

$gsH = \{gs, g^3 s\}$

¿isomorfo a?

- puedo hacer tabla cayley
- puedo ver orden elem. ④

$- gH * gH = g^2 H = eH$

$- gsH * gsH = (gsgs)H =$
$= (g g^{-1} s s) H = eH$

por tanto el orden es 2 (no hay ningún elem de orden 4, no puede ser $\approx \mathbb{Z}_4$)

④ pq ve:

$\left| D_4/H \right| = 4$

por tanto $D_4/H \approx \mathbb{Z}_4$ ó $\mathbb{Z}_2 \times \mathbb{Z}_2$

para saber cual es → orden elem.

como nos da 2:

$D_4/H \approx \mathbb{Z}_2 \times \mathbb{Z}_2$

quedan:

D_4/H_7 y D_4/H_8

(skipping)

2.3

(2) Sea $\varphi: \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ homomorfismo de grupos, tq $\ker(\varphi) = \{[0]_{30}, [10]_{30}, [20]_{30}\}$ y $\varphi([23]_{30}) = [9]_{30}$.

Determinar todos los grupos

$(\mathbb{Z}_{30}, +_{30})$ $\quad A = \{23, 3, 13\}$

$\ker\varphi = \{0, 10, 20\}$

$$\left.\begin{array}{l}\varphi(23) = 9 \\ \varphi(a) = 9\end{array}\right\} \Rightarrow \varphi(23) - \varphi(a) = 0 \Rightarrow$$

$$\underset{\text{prop. homomorf.}}{\Rightarrow} \varphi(23-a) = 0 \Rightarrow 23 - a \in \ker\varphi \Rightarrow a \in 23 - \ker\varphi$$

(3) Sea $\varphi: \mathbb{Z}_{30} \to G$ homomorfismo supreyectivo de grupos. Sabiendo que $|G| = 5$, calcular $\ker(\varphi)$.

$|G| = 5$

$\varphi: \mathbb{Z}_{30} \to G$ supreyectivo $\to$

$$\mathbb{Z}_{30}/\ker\varphi \underset{\substack{\text{isomorfo} \\ \text{(1}^{er}\text{ teo. de} \\ \text{isomorfía)}}}{\cong} \varphi(\mathbb{Z}_{30}) \underset{\substack{\text{pq es} \\ \text{supreyectivo} \\ \text{(Imagen = G)}}}{=} G \Rightarrow \frac{\overset{|\mathbb{Z}_{30}|}{30}}{|\ker\varphi|} = |G| = 5 \Rightarrow$$

$$\Rightarrow |\ker\varphi| = 6$$

y como $\ker\varphi \leq \mathbb{Z}_{30}$,

$\ker\varphi = \langle 5 \rangle$ pq el subgrupo generado por 5 es el único en $\mathbb{Z}_{30}$ que tiene orden 6 (pq $5 \cdot 6 = 30$ y ya sería e. neutro)

(4) Sea $\varphi: \mathbb{Z}_{17} \to G$ un homomorfismo de grupos. Determina φ sabiendo que no es inyectivo.

"Lo mismo q antes, tenemos q comprobar las propiedades

$\varphi: \mathbb{Z}_{17} \to G$ no es inyectivo] — te dicen

$\mathbb{Z}_{17}/\ker\varphi \underset{\substack{\uparrow \\ 1^{er}\text{ teo isomorfía}}}{\approx} \varphi(G)$, $\ker\varphi = \mathbb{Z}_{17} \Rightarrow \varphi(a) = e_G \ \forall a \in \mathbb{Z}_{17}$

⑤ ¿cuántos homomorfismos existen de $(\mathbb{Z}_{20}, +_{20})$ en $(\mathbb{Z}_8, +_8)$? ¿cuántos de ellos son suprayectivos?

sabemos que $\varphi: \mathbb{Z}_n \to \mathbb{Z}_m$ es homomorfismo de grupos $\Leftrightarrow \varphi(a) = ka$
$nk \equiv 0 \mod m$

$\Rightarrow 20k \equiv 0 \mod 8 \Leftrightarrow k \in \{0,2,4,6\}$

$\varphi(a) = ka \quad k \in \{0,2,4,6\}$ // hay 4

¿cuántos son suprayectivos = imagen = 1?

Ninguno, porq k siempre es par y $\varphi(a)$ vale ka — siempre par.

⑥ Estudiar si existe un homomorfismo suprayectivo $\varphi: G \to G'$, sabiendo que $(G, *)$ y $(G', *)$ son dos grupos de órdenes 24 y 7 respectivamente. ¿Existe un homomorfismo inyectivo de G' en G?

Si el 1 tiene imagen (reminder: 1 = generador del grupo pq $\langle 1 \rangle = \mathbb{Z}_n$) entonces va a ser suprayectivo pq $\varphi(1) = \mathbb{Z}_n$)

Kind of

$\varphi: G_{24} \to G'_7$ suprayectivo $\Rightarrow$

$\Rightarrow G_{24}/\ker\varphi \underset{1^{\circ}\text{ theo.}}{\approx} \varphi(G_{24}) = G'_7$

orden de G y orden H
$[G:H] = \frac{|G|}{|H|}$

$\frac{|G_{24}|}{|\ker\varphi|} = |G'_7| \Rightarrow \underset{\text{CONTRADICCIÓN}}{24 = |\ker\varphi| \cdot 7} \Rightarrow$ No existe ningún homomorfismo

* $\overset{\text{inyectivo}}{\Leftrightarrow} \ker\varphi = \{e_{G'_7}\} \Rightarrow |\ker\varphi| = 1$

$\frac{G'_7}{\ker\varphi} \approx \varphi(G'_7) \leq G_{24}$

inyectivo $\Rightarrow |\ker\varphi| = 1$

¡pq es de G' en G!

$7 = |\varphi(G_7)| \overset{|G_{24}|}{\neq} \Rightarrow \varphi(G'_7)$ no puede ser subgrupo de G_{24}

pq 7 no divide a 24

⑦ Estudiar si existe algún homomorfismo inyectivo $\varphi : D_4 \to \mathbb{Z}_{16}$

$\varphi : D_4 \to \mathbb{Z}_{16}$ inyectivo

1er th. isomorfía

$$\underbrace{D_4}_{\text{inyectivo}} \approx D_4/\ker\varphi \approx \varphi(D_4) \leq \mathbb{Z}_{16}$$

$\Rightarrow D_4 \approx \varphi(D_4) \leq \mathbb{Z}_{16}$

contradicción, pq D_4 no es abeliano ni cíclico, y esto dice q D_4 es isomorfo a un subgrupo de $\mathbb{Z}_{16}$ que es abeliano y cíclico. (y todo subgrupo de un grupo cíclico es cíclico!!)

⑧ Describir los posibles homomorfismos (de $\mathbb{Z}_{24}$ en $\mathbb{Z}_{18}$) $\varphi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$

$\varphi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$

para q φ sea homomorf. } $\varphi(a) = ka$ siendo $\underbrace{24}_{2^3 \cdot 3} k \equiv 0 \bmod \underbrace{18}_{2 \cdot 3^2}$ falta una pot. de 3

(k múltiplo de 3)

⇓

$k \in \{0, 3, 6, 9, 12, 15\}$ // 6 en total

⇓

cada uno de ellos ka

⑨ Construir un homomorfismo de grupos $\varphi : G \to G'$ tal que $\ker(\varphi) \approx \mathbb{Z}_3$.
Otro con núcleo isomorfo a $\mathbb{Z}_4$.
Otro con núcleo isomorfo a $\mathbb{Z}_6$.

$\varphi : \mathbb{Z}_3 \to G$, $\varphi(a) = e_G \Rightarrow \ker\varphi = \mathbb{Z}_3$ } (trivial)

$\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2$

$a \longmapsto \varphi(a) = a$

$\ker\varphi = \{0, 2, 4\} \approx \mathbb{Z}_3$

$\varphi : \mathbb{Z}_8 \to \mathbb{Z}_2 : \varphi(a) = a$

$\ker\varphi = \{0, 2, 4, 6\} \approx \mathbb{Z}_4$

24

① señalar cuáles de los siguientes grupos son cíclicos

ⓐ $\mathbb{Z}_6 \times \mathbb{Z}_5 \approx \mathbb{Z}_{30}$

ⓑ $\mathbb{Z}_7 \times \mathbb{Z}_6 \times \mathbb{Z}_4$ ¡no se repite 4 es pq potencia de un primo!

$\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$

$W_7 \times W_2 \times W_3$

este no es cíclico ⇒ Nuestro grupo NO es cíclico

$(\mathbb{Z}_7 \times \mathbb{Z}_6 \times \mathbb{Z}_2)$

fact. invariantes → $(\mathbb{Z}_{84} \times \mathbb{Z}_2)$

③ $\mathbb{Z}_{nm} \approx \mathbb{Z}_n \times \mathbb{Z}_m \Leftrightarrow \operatorname{mcd}(n,m) = 1$

② cada uno de los grupos de Sylow no tiene pq ser cíclico, tb puede ser producto de grupos cíclicos. And:

$|W_{p_1}| = p_1^{r_1}$

$|W_{p_2}| = p_2^{r_2}$

etc

① reminder: (prop. para ser cíclico)

Todo grupo abeliano es ≅ a un prod. de grupos de Sylow. Además un grupo de Sylow ...

⇓

si orden de G (G abeliano) es $p_1^{r_1} p_2^{r_2} p_3^{r_3} \Rightarrow G \approx W_{p_1} \times W_{p_2} \times W_{p_3}$

(c) $\mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_2$ ya está descompuesto por sus subgrupos de Sylow, cada uno de ellos es cíclico.

sí es cíclico

(d) $\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_2$

No es cíclico, y sus divisores elementales serían:

$$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \approx$$

$$\approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \approx$$

$$\approx \underline{W_2 \times W_3 \times W_5} \to \text{único cíclico}$$

$$\begin{pmatrix} |W_5| = 5^1 \\ |W_3| = 3^2 = 6 \\ |W_2| = 2^2 = 4 \end{pmatrix}$$ Not Sure

(*) factores invariantes : $\underline{\mathbb{Z}_{30} \times \mathbb{Z}_6}$

(q verifican q cada uno de ellos divide al anterior)

"elijen un factor de cada grupo de Sylow con la más potencia : $(2,3,5)$ $\quad (2,3)$ lo q todavía no elijo $\quad$ y ya no quedaría ninguno"

$\mathbb{Z}_{30} \quad \mathbb{Z}_6$

(2) Determinar salvo isomorfismos, todos los grupos abelianos de orden n

(*) cuando quede solo 1 factor invariante es cíclico!

a) $1 < n < 20$

$n=1 \quad \mathbb{Z}_1 = \{0\}$

$n=p$ (primo) $(\mathbb{Z}_p, +_p)$ cíclico

$n=4$ (el primero no primo) : $\mathbb{Z}_4$ (abeliano y cíclico) y $\mathbb{Z}_2 \times \mathbb{Z}_2$ (abeliano aunq no cíclico)

$n=6 \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \to$ fact invariantes: $\mathbb{Z}_6$ cíclico ✓

$W_2 \times W_3$

$n=8 \Rightarrow \underset{\text{abeliano no cíclico}}{\mathbb{Z}_2 \times \mathbb{Z}_4}$ ó $\underset{\text{abeliano no cíclico}}{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}$ ó $\underset{\text{cíclico y abeliano}}{\mathbb{Z}_8}$ $\Big] - W_2$

$n=9 \Rightarrow W_3 - \Big[\underset{\text{cíclico y abeliano}}{\mathbb{Z}_9}$ ó $\underset{\text{abeliano no cíclico}}{\mathbb{Z}_3 \times \mathbb{Z}_3}$

$n=10 \Rightarrow W_2 \times W_5 - \Big[\underset{\text{cíclico y abeliano}}{\mathbb{Z}_2 \times \mathbb{Z}_5} \Rightarrow$ fact. invariante: $\mathbb{Z}_{10} \approx \mathbb{Z}_{10}$ cíclico ✓

$2^2 \cdot 3$

$n=12$ $W_2 \times W_3$

$\left[\underbrace{\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3}_{\text{abeliano no cíclico}} \approx \mathbb{Z}_6\times\mathbb{Z}_2 \right]$ inv ó $\underbrace{\mathbb{Z}_4\times\mathbb{Z}_3}_{\text{cíclico y abeliano}} \approx \mathbb{Z}_{12}$ inv ó $\cancel{\mathbb{Z}_6\times\mathbb{Z}_2}$ 6 no es primo ni potencia de primo

$n=14 = 2\cdot 7 \approx \mathbb{Z}_2\times\mathbb{Z}_7 \approx \mathbb{Z}_{14}$ cíclico y abeliano

$W_2 \times W_7$

$n=15 = 3\cdot 5 \approx \mathbb{Z}_{15}$ cíclico y abeliano

$W_3\times W_5$

$n=16=2^4$

W_2

- $\mathbb{Z}_{16}$ abe y cíclico
- $\mathbb{Z}_8\times\mathbb{Z}_2$
- $\mathbb{Z}_4\times\mathbb{Z}_4$
- $\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$
- $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$

(abelianos no cíclicos)

$n=18 = 2\cdot 3^2$

$W_2\times W_3$

$\underbrace{\mathbb{Z}_2\times\mathbb{Z}_9}_{\text{cíclico y abeliano}} \approx \mathbb{Z}_{18}$ inv ó $\underbrace{\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3}_{\text{cíclico no abeliano}} \approx \mathbb{Z}_6\times\mathbb{Z}_3$ inv] — div elem.

b) $n=64=2^6$

- $\mathbb{Z}_{2^6}$ cíclico abeliano $\approx \mathbb{Z}_{64}$
- $\mathbb{Z}_{2^5}\times\mathbb{Z}_2$
- $\mathbb{Z}_{2^4}\times\mathbb{Z}_{2^2}$
- $\mathbb{Z}_{2^4}\times\mathbb{Z}_2\times\mathbb{Z}_2$
- $\mathbb{Z}_{2^3}\times\mathbb{Z}_{2^3}$
- $\mathbb{Z}_{2^3}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_2$
- $\mathbb{Z}_{2^3}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$
- $\mathbb{Z}_{2^2}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_{2^2}$
- $\mathbb{Z}_{2^2}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_2\times\mathbb{Z}_2$
- $\mathbb{Z}_{2^2}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$
- $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$

¿Cuáles de ellos tienen un elem de orden 4?

$\mathbb{Z}_{2^6}$ (2^4) 2^2 ó 4 es divisor de 64)

$\mathbb{Z}_{2^5}\times\mathbb{Z}_2$ (4 es divisor de 32)

$\mathbb{Z}_{2^4}\times\mathbb{Z}_{2^2}$
$\mathbb{Z}_{2^4}\times\mathbb{Z}_2\times\mathbb{Z}_2$ (4 divide a 16)

$\mathbb{Z}_{2^3}\times\mathbb{Z}_{2^3}$ (4 divide a 8)

$\mathbb{Z}_{2^3}\times\mathbb{Z}_{2^2}\times\mathbb{Z}_2$ " "

$\mathbb{Z}_{2^3}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ " "

etc

todos excepto

→ pq 4 no divide a 2