1) a) i) $x \longmapsto ax$

<u>inyectiva</u> $ax = ay \Leftrightarrow a^{-1}ax = a^{-1}ay \Leftrightarrow x = y$

<u>sobre</u> $g \in G \Rightarrow g = aa^{-1}g$

$\Rightarrow$ preimagen de g es $a^{-1}g \in G$

además esa es la inversa

$$x \longmapsto a^{-1}x$$

ii) $x \longmapsto a.x.b$

<u>inyectiva</u> $ax.b = ay.b \Leftrightarrow$ igual que antes

$\Leftrightarrow x = y$

damos la inversa directo

$$x \longmapsto a^{-1}xb^{-1}$$

$\Rightarrow$ es sobre

iii) $x \longmapsto axa^{-1}$

<u>inyectiva</u> igual

inversa $x \longmapsto a^{-1}xa$

iv) $x \longmapsto x^{-1}$

<u>inyectiva</u> $x^{-1} = y^{-1} \Leftrightarrow e = xy^{-1}$

$\Leftrightarrow ey = xe \Leftrightarrow y = x$

<u>inversa</u> $x \longmapsto x^{-1}$

$x \longmapsto x^{-1} \longmapsto (x^{-1})^{-1} = x$ ✓

v) $x \longmapsto ax^{-1}a^{-1}$

<u>iny</u>: $ax^{-1}a^{-1} = ay^{-1}a^{-1} \Leftrightarrow x^{-1} = y^{-1}$

$\Leftrightarrow e = y^{-1}x$

$\Leftrightarrow y = x$

<u>inversa</u> $x \longmapsto a^{-1}x^{-1}a$

$x \longmapsto ax^{-1}a^{-1} \longmapsto a^{-1}(ax^{-1}a^{-1})^{-1}a$

$= a^{-1}a\,x\,a^{-1}a$

$= x$

b) i) $x \overset{\varphi}{\longmapsto} ax$ → si $a \neq e$ no es homo

$\varphi(x \cdot y) = a \cdot xy \neq ax \cdot ay = \varphi(x)\varphi(y)$

ii) $x \overset{\varphi}{\longmapsto} axb$ $\varphi(xy) = axyb$

$b \neq e$ $a \neq e \to \neq axbayb = \varphi(x)\varphi(y)$

además ↙

$b \neq a^{-1} \wedge b \neq a \wedge a^2 = e$

si no, si es homo

iii) $x \overset{\varphi}{\longmapsto} a x a^{-1}$

$$\varphi(xy) = axya^{-1} = axa^{-1}aya^{-1}$$
$$= \varphi(x)\varphi(y) \quad \text{es homo}$$

iv) $x \overset{\varphi}{\longmapsto} x^{-1}$

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

si G abeliano $= \varphi(x)\varphi(y)$

sería homo $\Leftrightarrow$ G abel

v) $x \overset{\varphi}{\longmapsto} ax^{-1}a^{-1}$

$$\varphi(xy) = axya^{-1} = axa^{-1}aya^{-1}$$
$$= \varphi(x)\varphi(y)$$

es homomorfismo

2) a) $(\mathbb{Z}, +)$ $f: \mathbb{Z} \to \mathbb{Z}$ $f(a) = na$

$$f(a+b) = n(a+b) = (a+b) + \dots + (a+b)$$
↳ notación aditiva

asoc y conmut $= a + \dots a + b + \dots + b$

$$= na + nb = f(a) + f(b)$$

mono $f(a) = f(b) \Leftrightarrow na = nb \Leftrightarrow a + \dots + a = b + \dots b$

$\Leftrightarrow a + \dots + a + b^{-1} + \dots + b^{-1} = e$

(abel) $\Leftrightarrow n(a + b^{-1}) = e$

si $a+b^{-1} \neq e \in \mathbb{Z}$ ⊛ $\Leftrightarrow a + b^{-1} = e$

$\Rightarrow |a+b^{-1}| = \infty$ $\Leftrightarrow a = b$

$\Rightarrow n(a+b^{-1}) = e$ abs!

$\Rightarrow a + b^{-1} = e$

⊛ $|a| = \infty$, $n(a+b) = e$

$\Rightarrow a + b = e$

dem 1) caso $b = a^{-1}$ ya está $a + b = e$

1) $|a| = \infty \Rightarrow |a+b| = \infty$ supongo que no $\Rightarrow |a+b| = m$

$\Rightarrow m(a+b) + (a+b) = e$

$(m+1)a + (m+1)b = e$

epi no es Sea $e \neq \tilde{m} < m$ $m \neq e (=1)$ si fuera epi

$\exists a \in \mathbb{Z} / ma = \tilde{m}$ ($a \neq e$ si no $\tilde{m} = e$)

$\Leftrightarrow \underbrace{a + \dots + a}_{m\text{-veces}} = \tilde{m}$

$\Leftrightarrow m = \underbrace{1 + \dots + 1}_{m\text{-veces}} \leq a + \dots + a = \tilde{m}$

$\Leftrightarrow m \leq \tilde{m}$ abs!

b) $f(a) = 2a$ $\quad \mathbb{Z}_6 \to \mathbb{Z}_{12}$ $\quad f(a+b) = 2(a+b) = a+b+a+b = a+a+b+b$
$= 2a+2b$
$= f(a)+f(b)$

$\mathbb{Z}_{12}$ es abeliano

mono $\quad f(a) = f(b) \Leftrightarrow 2a = 2b \quad \Leftrightarrow a+a = b+b$
$\Leftrightarrow a+a+b^{-1}+b^{-1} = e$
$2(a+b^{-1}) = e$

mismo argumento $\Rightarrow a+b^{-1} = e$
(si no $|a+b^{-1}| = 2$) $\quad a = b$
abs!

epi no es ningun impar b cumple $b = 2a$

$f(c)+1 \in \mathbb{Z} \Rightarrow \exists a \in \mathbb{Z} / \; f(a) = f(c)+1$
$\Leftrightarrow f(a)+f(c)^{-1} = 1$

$(f(c))^{-1} = (2c)^{-1}$
$= (c+c)^{-1}$
$= c^{-1}+c^{-1}$
$= 2c^{-1}$
$= f(c^{-1})$

$\Leftrightarrow f(a)+f(c^{-1}) = 1$

$\Leftrightarrow f(a+c^{-1}) = 1$ $\quad$ abs!

$\Leftrightarrow 2(a+c^{-1}) = 1$

$\Leftrightarrow 2b = 1$

$\Leftrightarrow b+b = 1$

$\Leftrightarrow b = 1+b^{-1}$

$e = 1+b^{-1}+b^{-1}$

$\Rightarrow 2b^{-1} = (1)^{-1}$

c) $f: \mathbb{Z}_5 \to \mathbb{Z}_5 \quad f(a) = 3a$

$f(a+b) = 3(a+b) \overset{\text{abel}}{=} 3a+3b = f(a)+f(b)$

mono

$\exists$ epi

$$\begin{cases} f(0)=0 & f(3)=4 \\ f(1)=3 & f(4)=2 \\ f(2)=1 & \end{cases}$$

4) G abel $\Rightarrow$ $f: G \to G$ $f(x) = x^{-1}$ es morfismo de grupo

$$f(x \cdot y) = (xy)^{-1} = x^{-1}y^{-1} = f(x)f(y)$$

$$(xy)(x^{-1}y^{-1}) = x(yy^{-1})x^{-1} = e$$

abel

f morfismo de grupos

si no $f(x \cdot y) = (xy)^{-1} = (y^{-1}x^{-1}) = \underset{\in G}{f(y)}\underset{\in G}{f(x)} = f(x)f(y)$ abel

sin abel $xy\,y^{-1}x^{-1} = e$

inversión es morfismo $\Rightarrow$ $f: G \to G$ $f(x) = x^2$ es morfismo

por (2) $a^{-1}b^{-1} = (ab)^{-1} \Leftrightarrow a^2b^2 = (ab)^2$

$$f(a)f(b) = f(ab)$$

$f(x) = x^2$ morfismo $\Rightarrow$ G abeliano

$(xy)^2 = x^2y^2$ pq f morfismo

$\Rightarrow$ por PRI ej (2)

G abeliano

4) a) Sean $a, b \in H_1 \cap H_2$

Como $b \in H_1 \Rightarrow b^{-1} \in H_1$

$a \in H_1 \cap H_2 \Rightarrow a \in H_1$

$\Rightarrow ab^{-1} \in H_1$ (por ser H_1 sub

Análogo $ab^{-1} \in H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

$\Rightarrow H_1 \cap H_2$ subgrupo

b) Para finitos sale por inducción global

$H_1 \cap \dots \cap H_{n+1} = \underbrace{(H_1 \cap \dots H_n)}_{\text{sub g}} \cap \underbrace{H_{n+1}}_{\text{sub g}}$ $\Rightarrow$ por hipótesis

$\Rightarrow$ sub g

$a, b \in \bigcap^{\infty} H_i \Rightarrow a, b \in H_i$ para cada i

$\Rightarrow a \cdot b^{-1} \in H_i$ para cada i

$\Rightarrow ab^{-1} \in \bigcap^{\infty} H_i$

c) ($\Rightarrow$) Supongo $H_1 \not\subseteq H_2 \wedge H_2 \not\subseteq H_1$

$\Rightarrow \exists\, a \in H_1 / a \notin H_2 \wedge b \in H_2 / b \notin H_1$
($\Rightarrow a^{-1} \in H_1$) ($b^{-1} \in H_2$)

$\Rightarrow a, b \in H_1 \cup H_2 \Rightarrow a \cdot b \in H_1 \cup H_2$

supongo $a \cdot b \in H_1$

$\Rightarrow a^{-1} a b \in H_1$

$\Rightarrow b \in H_1$ abs!

supongo $a \cdot b \in H_2$

$\Rightarrow a b b^{-1} \in H_2$

$\Rightarrow a \in H_2$ abs!

$\Rightarrow a.b \notin H_1 \wedge a.b \notin H_2$

$\Rightarrow ab \notin H_1 \cup H_2$ abs!

$\Rightarrow H_1 \subseteq H_2$ o $H_2 \subseteq H_1$

$(\Leftarrow)$ Spd $H_1 \subseteq H_2$

$\Rightarrow H_1 \cup H_2 = H_2$

$\Rightarrow H_1 \cup H_2$ es grupo

d) Si estan encajados, $\{H_i\}_{i \in \mathbb{N}}$ subgrupos

tq $H_i \subseteq H_{i+1}$

$\Rightarrow \bigcup H_i$ grupo

<u>demo</u> sean $a, b \in \bigcup H_i$

$\Rightarrow a \in H_j \quad b \in H_k$

$(a^{-1} \in H_j) \quad (b^{-1} \in H_k)$

$\Rightarrow a, b \in H_l$ con $l = \max\{k, j\}$

$\Rightarrow ab^{-1} \in H_l$ (pq $a \in H_l$ y $b^{-1} \in H_l$)

$\Rightarrow a.b^{-1} \in \bigcup H_i$

-) Si no estan encajados no vale

se ve igual que para finitos

5) A mismo

6) Sea $\tilde{G} \leq \mathbb{Z} \Rightarrow \tilde{G} = n\mathbb{Z}$ con $n = \min\{x \mid x \in \tilde{G}_{>0}\}$

Sea $n \in \min\{x \mid x \in \tilde{G}_{>0}\}$ $\exists$ por buen orden de $\mathbb{Z}$

·) $(\supseteq)$ afirmo $n\mathbb{Z}_{>0} \subseteq \tilde{G}$

Sea $x \in n\mathbb{Z} \Rightarrow x = n \cdot a \quad a \in \mathbb{Z}$

$(n \in \tilde{G})$

$$= \underbrace{n + \cdots + n}_{a \text{ veces}}$$

$$\Rightarrow x \in \tilde{G}$$

Análogo $n\mathbb{Z}_{\leq 0}$ ·) $x = n \cdot a = (\underbrace{n + \cdots + n}_{a \text{ veces}})^{-1} \in \tilde{G}$

$a < 0$

·) $x = n \cdot 0 \rightarrow x = 0 \in \tilde{G}$

$$\Rightarrow \tilde{G} \supseteq n\mathbb{Z}$$

·) $(\subseteq)$ Sea $x \in \tilde{G}$

$(x \neq n$ trivial$)$

·) caso $x > 0 \Rightarrow x \geq n \quad (x \in \tilde{G}) \Rightarrow x = hn + r$

$0 \leq r < n \qquad h \in \mathbb{Z}$

como $x \in \tilde{G}$ $\underset{\in \tilde{G}}{hn} + r \in \tilde{G} \Rightarrow \underset{\in \tilde{G}}{x} + \underset{\in \tilde{G}}{(hn)^{-1}} = r \Rightarrow r \in \tilde{G}$

$$\Rightarrow r = 0 \quad (r < n)$$

$$\Rightarrow x = hn$$
$$= nh \Rightarrow x \in n\mathbb{Z}$$

Caso $x \leq 0$ (supongo $x \neq 0$, si $x=0$ trivial)

$(-x =)\ x^{-1} > 0$ $(x \in \tilde{G} \to x^{-1} \in \tilde{G})$ $\Rightarrow$ $x^{-1} \geq n$

$\Rightarrow$ por caso antes

$x^{-1} \in \underline{n\mathbb{Z}}$

subgrupo $\Rightarrow$ $x \in n\mathbb{Z}$

$\Rightarrow$ $n\mathbb{Z} = \tilde{G}$

y trivialmente $n\mathbb{Z} = \langle n \rangle \left(= \{ n^k \mid k \in \mathbb{Z} \} \right)$

$= \{ \underbrace{n + n + \cdots + n}_{k\text{-veces}} \mid k \in \mathbb{Z} \}$

$\Rightarrow$ $n\mathbb{Z}$ cíclico

7) $A = \{ a^k : k \in \mathbb{Z} \}$ $\quad$ $B = \{ (a^{-1})^k : k \in \mathbb{Z} \}$

i) $A = B$ $\quad (\subseteq)$ $\quad x \in A \Rightarrow x = a^k = \underbrace{a \cdots a}_{k\text{-veces}}$

$$= \Big(\underbrace{a^{-1} \cdots a^{-1}}_{k \text{ veces}}\Big)^{-1}$$

$$= \left((a^{-1})^k\right)^{-1}$$

def de teo dice $a^n = (a^{-1})^{-n}$
$= (a^{-1})^{n \cdot -1}$

$$= \underbrace{(a^{-1})^{\overbrace{k \cdot -1}^{\in \mathbb{Z}}}}_{\in B}$$

acá $(\mathbb{Z}, +)$?;

ii) $(\supseteq)$ Sale al revés $\quad x \in B \Rightarrow x = (a^{-1})^k = (k \cdot -1)^{-1}$

$$= a^{-n} \in A$$

$\therefore \ |a| = |A| = |B| = |a^{-1}|$

b) Sea $|a| = n$ $\quad \Rightarrow (bab^{-1})^n = b \underbrace{a^n}_{= e} b^{-1} = bb^{-1} = e$

$$\Rightarrow |bab^{-1}| \leq n$$

Supongo es menor $\Rightarrow \exists\, m < n$ tq $|bab^{-1}| = m$

$ba^m b^{-1} = e \Rightarrow a^m = b^{-1}b = e$
abs!

$\Rightarrow |bab^{-1}| = n$

Si $|a| = \infty \Rightarrow |bab^{-1}| = \infty$

pq si $ba^n b^{-1} = e$

$\Rightarrow a^n = e$ abs!

Supongo $|ab| = n$

$(ab)^n = e \quad (ba)^{n+1} = b\underbrace{aba \ldots b}a$

$b\, ab^n\, a = ba$

$\Rightarrow (ba)^{n+1} = ba$

$\Rightarrow (ba)^n = e$

$\Rightarrow |ba| \leq n$

Supongo $|ba| = m < n$

$(ba)^m = b(ab)^{m-1}a = e$

$\Rightarrow (ab)^{m-1} = b^{-1}a^{-1} = (ab)^{-1}$

$(ab)^m = (ab)^{-1}(ab)$

$= e$ abs!

11)

b) Como G es abeliano. Por inciso a), existe un elemento de orden $[P,q]$. Luego, Sabemos que: $Pq = (P,q)[P,q] = [P,q]$.

Luego, $\overset{a)}{\exists} x \in G$ tq $|\langle x\rangle| = Pq \Rightarrow \langle x\rangle = G$

$\therefore$ G cíclico

a) Consideremos $(m,n)a+b$. Como G es abeliano: $(ab)^2 = a^2b^2$

en nuestro caso: $(a+b)^2 = 2(a+b) = 2a+2b$. Luego

neutro de un abeliano

$$[m,n]((m,n)a+b) \underset{\text{abeliano}}{=} [m,n](m,n)a + [m,n]b = \underbrace{(m\,n)a}_{\substack{\text{multiplo}\\ \text{de } m\\ |a|=m}} + \underbrace{[m,n]b}_{\substack{\text{multiplo}\\ \text{de } n\\ |b|=n}} = 0+0=0.$$

Por lo tanto $[m,n]$ es multiplo del orden de $(m,n)a+b$, donde a tal orden lo denotaremos por k.

Luego, $k \mid [m,n]$. (1)

Como k es el orden de $(m,n)a+b \rightarrow k(m,n)a + kb = 0 \Rightarrow k(m,n)a = -kb$

ó $k(m,n)a = kb = 0$

En el primer caso a es generado por b, luego $|a| \mid |b|$ (teo de lagrange)

$\Rightarrow [m,n] = |b|$, luego b es el elemento que buscamos

NOTA

En el segundo caso, podemos concluir que:

$n|k$, $\frac{m}{(m,n)} | k \quad \Rightarrow [n, \frac{m}{(m,n)}] \mid k$

Pero, cualquier primo removido de m por (m,n), será reemplazado por su copia en n, entonces $[n, \frac{m}{(n,m)}] = [n,m] \Rightarrow [n,m] \mid k$ (2)

Por (1) y (2) $k = [m,n] \Rightarrow (m,n)a+b$ es de orden $[m,n]$ ∎

9) a) $\overbrace{(1235)(1378)} = (15)(2378) = a$

$a^2 = (15)(2378)(15)(2378) = (27)(38)$

$a^3 = (27)(38)(1235)(1378) = (15)(2873)$

$a^4 = \underbrace{(15)(2873)}_{a^3}\underbrace{(15)(2378)}_{a} = Id$

b) $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = a^2$

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = a^3$

$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e = a^4$

$\Rightarrow \left| \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right| = 4$

c) $z = \cos\left(\frac{2\pi}{n}\right) + i\,\text{sen}\left(\frac{2\pi}{n}\right) = e^{\frac{2\pi}{n}i}$

$$z^n = \left(e^{\frac{2\pi}{n}i}\right)^n = e^{2\pi i} = 0 = \text{neutro}$$

$\rightarrow |z| = n$

d) $z = \frac{1}{2}\cos\left(\frac{2\pi}{n}\right) + \frac{1}{2}i\,\text{sen}\left(\frac{2\pi}{n}\right) = \frac{1}{2}e^{\frac{2\pi}{n}i}$

$$z^n = \frac{1}{2^n}e^{2\pi i} = 0$$

$$|z| = n$$

e) $x = e^{\frac{m}{n}i}$

f) propriedade $|X| = \frac{n}{(x:n)}$

f) $\frac{n}{(x:n)}\bar{x} = \bar{x} + \quad + \bar{x} = \overline{x + \cdots + x}$

$$= \overline{\frac{n}{(x:n)}x} \in \mathbb{Z}$$

$$= \bar{0}$$

Veamos que es el mínimo

si $k \in \mathbb{N}$ / $k\overline{x} = \overline{0} \Rightarrow \overline{0} = k\overline{x} = \overline{x} + \dots + \overline{x}$

$= \overline{x + \dots + x}$

$= \overline{kx}$

$\Rightarrow n \mid kx$

$m' \perp m''$ $\quad \overset{n}{\overbrace{(n:x)\, m'}} \mid k \overset{x}{\overbrace{(n:x)\, m''}}$

$\Rightarrow m' \mid k m''$

$\Rightarrow m' \mid k$

$\Rightarrow m' < k$

$\dfrac{n}{(n:x)} = m' < k$

$a \neq 0$

$ab \mid ac \Rightarrow b \mid c$

demo $ac = jab$

$\Rightarrow ac - jab = 0$

$a(c - jb) = 0$

$\Rightarrow c - jb = 0$

$\Rightarrow c = jb$

11) -) $\mathbb{Z}_3$ por lagrange el orden de cualquier subgrupo finito a 3

=) es 1 o 3

=) únicos sgbs son

$\{e\}$ y $\mathbb{Z}_3$

•) $\mathbb{Z}_2 \times \mathbb{Z}_2$. tiene orden 4. pq es multiplicar orden de $\mathbb{Z}_2$ por orden de $\mathbb{Z}_2$

=) 1, 2, 4 orden de subgrupos

los de orden 2 son $\langle (0,1) \rangle$ $\langle (1,0) \rangle$ $\langle (1,1) \rangle$

•) $|S_3| = 3! = 6$ $S_3 = \{e, (1\,2\,3)\ (1\,2)\ (1\,3\,2)\ (1\,3)\ (2\,3)\}$

orden 1 $\langle (1)(2)(3) \rangle$

orden 2 $\langle (1\,2) \rangle$ $\langle (1\,3) \rangle$ $\langle (2\,3) \rangle$

las otras no son de orden 2

la única que queda es $\langle (1\,3\,2) \rangle$

$$(1\,3\,2)(1\,3\,2) = (1\,2\,3) \neq e$$

$$(1\,2\,3)(1\,3\,2) = (1)(2)(3) = e$$

$$\Rightarrow |\langle(1\,3\,2)\rangle| = 3$$

y notar $\langle(1\,2\,3)\rangle = \langle(1\,3\,2)\rangle$

$\Rightarrow$ de orden 3 $\langle(1\,2\,3)\rangle$ (o $\langle(1\,3\,2)\rangle$

orden 6 S_3

$\cdot)$ $|D_4| = 8$ $\quad D_4 = \begin{cases} \sigma^{j-1} & 1 \leq j \leq 4 \\ \sigma^{j-1} \circ \gamma \end{cases}$

orden 1 $\langle \sigma^0 \rangle$

orden 2 $\langle \gamma \rangle$ $\quad \langle \sigma^2 \circ \gamma \rangle$ $\quad \langle \sigma^2 \rangle$

orden 4 $\langle \sigma \rangle$ $\quad \langle \sigma^3 \rangle$

orden 8 D_4

12) $\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(1\ 4)\rangle, \langle(2\ 3)\rangle, \langle(2\ 4)\rangle$

$, \langle(3\ 4)\rangle, \langle(1\ 2)(3\ 4)\rangle, \langle(1\ 3)(2\ 4)\rangle$

$\langle(1\ 4)(2\ 3)\rangle$

Vemos que son isomorfos a S_2

i) $(1\ 4) \xmapsto{\varphi} (1\ 2)$

$\varphi((1\ 4)(1\ 4)) = \varphi(e) = (1\ 2)(1\ 2)$
$= \varphi((1\ 4))\varphi((1\ 4))$

i) $(1\ 2)(3\ 4) \xmapsto{\varphi} (1\ 2)$

análogo

i) Acá hay que probar que

$A = \{ \sigma \in S \mid \sigma(n) = n \}$ es subgrupo de S_n

isomorfo a S_{n-1}

esto en las soluciones pero parece que está mal

La idea es encontrar $f: S_n^k \longrightarrow S_{n-1}$

Con $S_n^k = \{ \sigma \in S_n \mid \sigma(k) = k \}$ fijar k

$f(\sigma)(x) =$

$$\begin{aligned} 1 &\longmapsto 4 \\ 2 &\longmapsto 2 \\ 3 &\longmapsto 3 \\ 4 &\longmapsto 1 \end{aligned}$$

(13) Dado $g \in G$ $\langle g \rangle$ es subgrupo

i) si $\langle g \rangle$ finito $\forall g \in G$

$\Rightarrow$ como tengo finitos sub

tengo finitos g

y $\langle g \rangle$ finito

$\Rightarrow \bigcup_{g \in G} \langle g \rangle$ finito

ii) si tengo $\langle g \rangle$ infinito (p 35 Hung) (teo 3.2)

$\Rightarrow$ es isomorfo a $\mathbb{Z}$

y $\mathbb{Z}$ tiene infinitos subgrupos

$\Rightarrow$ tendría infinitos sub abs!

(subgrupos infinitos $n\mathbb{Z}$)

14

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{A^2}$$

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{A^3}$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{A^4}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{B^2}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_{BA}$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}}_{BA^2}$$

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{BA^3}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{AB}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \left.\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\right\} A^2B = BA^2$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \left.\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right\} A^3B = BA$$

$$AB^2 = AB \wedge B^2A = BA \quad (B^2 = Id)$$

$$\langle A, B \rangle = \{e, A, B, A^2, A^3, BA, BA^2, AB\}$$

15)

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{Z}_p \right\}$$

2 $$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

3 $$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}$$

4 $$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix}$$

5 $$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5a & 5b+10ac \\ 0 & 1 & 5c \\ 0 & 0 & 1 \end{pmatrix}$$

6 $$\begin{pmatrix} 1 & 6a & 6b+15ac \\ 0 & 1 & 6c \\ 0 & 0 & 1 \end{pmatrix}$$ 7 $$\begin{pmatrix} 1 & 7a & 7b+21ac \\ 0 & 1 & 7c \\ 0 & 0 & 1 \end{pmatrix}$$

$$A^p ? \begin{pmatrix} 1 & pa & pb+S_p ac \\ 0 & 1 & pc \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbb{Z}_p$$

$$S_p = 3+3+4+5+6+\cdots+p-1$$

Ejemplo $S_7 = \underbrace{3+3}_{p-1}+\underbrace{4}_{p-2}+\underbrace{5}_{p-2}+\underbrace{6}_{p-1} = 21$

$=$

16) a) $(i_1, \dots, i_r) = (i_1\ i_2)(i_2\ i_3) \dots (i_{r-1}\ i_r)$

b) $(1\ i)(1\ j)(1\ i) = (i\ j)$

c) Sea $\sigma \in S_n \Rightarrow \sigma = (i_1 \dots i_r)$

por a) $\sigma = (i_1\ i_2) \dots (i_{r-1}\ i_r)$ algún $i_j = 1$

por b) $= (1\ i_1)(1\ i_2)(1\ i_1) \dots (1\ i_{r-1})(1\ i_r)(1\ i_{r-1})$

y es claro que pertenece al generador $<(1\ i_1) \dots (1\ i_n)>$

que tiene n elementos

pq $i = 1, \dots, n$

$\Rightarrow i_j = 1$ por algún j

d) $(1\ i_{j-1})(i_{j-1}\ i_j)(1\ i_{j-1}) = (1\ i_j)$ $j = 3 \dots r$

e) $(i_1, \dots i_r) = (1\ i_1)(1\ i_2)(1\ i_1) \dots (1\ i_{r-1})(1\ i_r)(1\ i_{r-1})$

$= \overbrace{(1\ i_1 - 1)}^{\text{MALO}}\underbrace{(i_1 - 1\ \ i_1)}_{\text{BUENO}}(1\ i_1 - 1)$

$$(1\ \ i_1-2)\underbrace{(i_1-2\ \ i_1-1)}_{\text{Bueno}}(1\ \ i_1-2)$$

en algún momento llegamos a

$$\hookrightarrow (1\ \ i_1-j)(i_1-j\ \ i_1-j+1)(1\ \ i_1-j+1)$$

$$i_1-j \overset{\shortparallel}{=} 1$$

$$= (\cancel{1\ 1})\underline{(1\ \ 2)}(\cancel{1\ 1})$$

$\Rightarrow$ todos los ciclos terminan siendo de la pinta

$$(j\ \ j+1)$$

$$f)\ \overset{\sigma}{(1\,2\,3\,4\,5)}(1\,2)\overset{\sigma^{-1}}{(1\,5\,4\,3\,2)} = (2\,1)$$

otro ejemplo $\quad (1\ 3\ 4\ 2)(1\,2)(1\ 2\ 4\ 3) = (3\ 1)$

$$(1\ 3\ 2\ 4)(1\,2)(1\ 4\ 2\ 3) = (4\ 3)$$

17) $(4267)(4267) = (27)(46) \quad \sigma^2$

$(4267)(27)(46) = (2476) \quad \sigma^3$

$(4267)(2476) = e$

$\Rightarrow \quad |\langle 4267 \rangle| = 4$

$\hookrightarrow = \{e, \sigma, \sigma^2, \sigma^3\}$

$Sg(4267) = -1$ pq es n-ciclo con n par

18) Todos tienen orden 8

i) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ cumple que $a^2 = e$

$(0,1,0) + (0,1,0) = (0,0,0)$

etc

$$\varphi(\underbrace{a+a}_{\in \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2}) = \varphi(a) + \varphi(a)$$

$\hookrightarrow e = \varphi(a) + \varphi(a)$

pero $\varphi(a) + \varphi(a) = e$ no necesariamente vale para $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$

$\mathbb{Z}_2 \times G_4$, D_4, G_8, Q_8

$$G_4 = \{e^0, e^{\frac{1\pi i}{2}}, e^{\pi i}, e^{\frac{3}{2}\pi i}\} \qquad e^{\frac{2k\pi i}{4}}$$

$$\quad 1 \quad\; i \quad -i \quad -1$$

- $f: \mathbb{Z}_2 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times G_4$

$$(a, b) \longmapsto \left(a, e^{\frac{b\pi i}{4}}\right)$$

$$f((a,b)+(c,d)) = \left(a+c, e^{\frac{(b+d)\pi i}{4}}\right)$$

$$= \left(a, e^{\frac{b\pi i}{4}}\right) + \left(c, e^{\frac{d\pi i}{4}}\right)$$

$$= f(a,b) + f(c,d)$$

$\Rightarrow$ son

19) Peso motor

$$|f(x)| \leq |x|$$

pq si $x^n = e$

Morfismo

$$f(x)^n = f(x^n) = f(e) = e$$

$$\Rightarrow |f(x)| \leq n$$

Supongo $|f(x)| = j \leq n$ y $j \nmid n$

$$\Rightarrow n = kj + r \quad r < j \quad r \neq 0$$

$$e = x^n = x^{kj+r}$$

$$\Rightarrow e = f(x)^{kj} \cdot f(x)^r = \left(f(x)^j\right)^k f(x)^r$$

$$= f(x)^r$$

abs! $r < j$

$$\Rightarrow j \mid n \Rightarrow |f(x)| \,\big|\, |x|$$

20) e_4

b) $Hom(\mathbb{Q}, \mathbb{Z})$

Sea $\varphi: \mathbb{Q} \to \mathbb{Z}$ no trivial. Sea n el entero positivo más chico en $im(\varphi)$

Sea $a/b \in \varphi^{-1}(n)$ entonces

$$n = 2\varphi\left(\frac{a}{2b}\right)$$

$n = \varphi(a/b) = \varphi\left(\frac{a}{2b} + \frac{a}{2b}\right) = \varphi\left(\frac{a}{2b}\right) + \varphi\left(\frac{a}{2b}\right) \Rightarrow \varphi\left(\frac{a}{2b}\right) = \frac{n}{2}$. absurdo pues $\frac{n}{2} < n$ y habíamos supuesto n el más chico

y $\frac{n}{2} \in Im\, \varphi$

$\therefore Hom(\mathbb{Q}, \mathbb{Z}) = 0$

• $(\mathbb{Z}, \mathbb{Q})$

Sea $f: \mathbb{Z} \to \mathbb{Q}$ hom $\to f(n) = n f(1)$. Luego $f(1) = q \in \mathbb{Q} \to f(n) = nq$

$\therefore Hom(\mathbb{Z}, \mathbb{Q}) = \{f: \mathbb{Z} \to \mathbb{Q} \mid f(1) \in \mathbb{Q}\} \cap \{f: \mathbb{Z} \to \mathbb{Q} \mid f(n) = f(1)^n\}$

c) $(\mathbb{Z}, G)$ G grupo finito

Sea $f: \mathbb{Z} \to G$ homomorfismo

Como $\mathbb{Z}$ es cíclico, solo necesitamos determinar la imagen de $f(1)$. Pues $f(n) = f(1)^n = n f(1)$

Luego, el orden de $f(1)$ debe dividir el orden de G. Pues si n es múltiplo del orden de G ($|G| \cdot k$) $f(n) = f(1)^n = f(1)^k = e^m = e$.

Luego $Hom(\mathbb{Z}, G) = \{f: \mathbb{Z} \to G \mid |f(1)| \mid |G| \wedge f(n) = f(1)^n\}$

$(G, \mathbb{Z})$

Sea $f: G \to \mathbb{Z}$ homomorfismo. Como G es finito $\forall x \in G$, $\exists n > 0$ tq $x^n = e$

$\Rightarrow 0 = f(e) = f(x^n) = n f(x) \Rightarrow f(x) = 0$. Luego, f trivial $\to Hom(G, \mathbb{Z}) = 0$.

a) Como G es un grupo finito, entonces es análogo al caso en (c)

4) a) Endomorfismo $\mathbb{Z} = \langle 1 \rangle$

$f_i(n) = ni$

$n \in \mathbb{Z}$

$i \in \mathbb{N}$

$f(a+b) = (a+b)i$

$= ai + bi$

$= f(a) + f(b)$

Automorfismo

$\text{Ker}(f_i) = \{ n \in \mathbb{Z} \,/\, f_i(n) = 0 \}$

$i \in \mathbb{N}$

$= \{ n \in \mathbb{Z} \,/\, ni = 0 \}$

Si $i = 0 \Rightarrow \text{Ker } f_i = \mathbb{Z} \Rightarrow$ no es mono

$i \neq 0 \Rightarrow \text{Ker } f_i = \{0\}$

$\Rightarrow$ es mono

epi

es $f_i(\mathbb{Z}) = i\mathbb{Z} \neq \mathbb{Z}$ salvo que $i = 1$

$\Rightarrow$ único automorfismo es Id