Complementos de matemática 2

Autor: Agustín Fernández Bergé

Indice

Demostraciones de teoria

¿(Z,<=) es isomorfo a (Q,<=)?

¿(Z,<=) es isomorfo a (Q,<=)?
NO, el retículo $(\mathbb{Z}, \leq)$ no es isomorfo a $(\mathbb{Q}, \leq)$.

Demostración

Lema 1: Si dos retículos $(A, \prec_A)$ y $(B, \prec_B)$ son isomorfos y $(A, \prec_A)$ satisface el axioma del supremo. Entonces $(B, \prec_B)$ también debe satisfacerlo.
Demostración:
Sea $C \subseteq B$ no vació y acotado superiormente por el elemento b.
Sea $f : B \to A$ un isomorfismo de retículos entre $(B, \prec_B)$ y $(A, \prec_A)$.
$f(C)$ es un subconjunto no vació de A. A su vez dicho conjunto esta acotado superiormente ya que:
$\forall x \in C : x \prec_B b \implies \forall f(x) \in f(C) : f(x) \prec_A f(b)$
Por lo tanto por axioma del supremo de $(A, \prec_A)$, $f(C)$ tiene un elemento supremo c y en particular $f^{-1}(c)$ es el elemento supremo de C.
Por lo tanto $(B, \prec_B)$ satisface el axioma del supremo.

Dado que $(Z, \leq)$ satisface el axioma del supremo y $(\mathbb{Q}, \leq)$ no lo satisface, entonces ambos retículos no pueden ser isomorfos.

Axioma del supremo en Z

Axioma del supremo en Z
El poset $(\mathbb{Z}, \leq)$ satisface el axioma del supremo.

Demostración

Sea un conjunto $A \subseteq \mathbb{Z}$ no vacio y acotado superiormente.

Sea $z \in \mathbb{Z}$ cota superior de A, construyo el conjunto B tal que:

$$B = \{z - a : a \in A\}$$

$B \subseteq N_0$, por principio del buen orden, B tiene un elemento mínimo. Sea $b = \min B$, existe un $a' \in A$ tal que $b = z - a'$. Por lo tanto
$\forall a \in A$:
$z - a \geq b = z - a_0$(porque $z - a \in B$)
$-a \geq -a_0$
$a \leq a_0$
Por lo tanto a_0 es una cota superior de A. Como $a_0 \in A$, a_0 es el máximo(y en particular el supremo) del conjunto A.

Por lo tanto, A satisface el axioma del supremo.
■

Lema A.5.6

Lema A.5.6
Sean $a, b \in \mathbb{N}$. $\operatorname{mcm}(a,b)$ es el producto de los factores primos comunes y no comunes de a y b, elevados al mayor exponente con el que aparecen en las respectivas descomposiciones dadas por el TFA.

Se puede probar este lema a partir del Lema A.5.5 y el siguiente resultado:

$$\operatorname{mcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

Primero demuestro (1), usando el Teorema A.3.6

Si $M = \dfrac{ab}{\gcd(a,b)}$, se tiene que M es múltiplo de a y b.

Esto es así ya que $a/\gcd(a,b)$ y $b/\gcd(a,b)$ son enteros, por lo que para ambos existe un entero que hace cumplir la definición de *es múltiplo de*.

Sea $G = \gcd(a,b)$
SI k es múltiplo de a y b entonces existen enteros p y q que cumplen que:
$pa = k \land qb = k$
$\implies$
$pa \cdot 1 \cdot 1 = k$
$\implies$
$pa\dfrac{qb}{k}\dfrac{G}{G} = \dfrac{pqG}{k}M = k$

$k \mid pqG$ ya que $k \mid p$.
Luego existe $k' = \dfrac{pqG}{k}$ tal que $k'M = k$. Por lo tanto k es múltiplo de M.

Esto prueba el Lema (1). Se tiene entonces que ab es el producto de los factores primos comunes y no comunes de a y b, elevados a la suma de los exponentes en los que aparecen en la descomposición del TFA. Al dividir por el gcd se resta a estos exponentes el mínimo exponente de las descomposiciones primas, el resultado es que en la descomposición queda el mayor exponente común a ambas descomposiciones.

Teorema A.2.3 Inciso 2

Teorema A.2.3 Inciso 2
Hay que probar que cualesquiera sean $a, b \in \mathbb{Z}$, se tiene que:

$$a \mid b \iff (-a) \mid b \iff (-a) \mid (-b)$$

Y en particular que:

$$\operatorname{Div}(b) = \operatorname{Div}(-b) = \operatorname{Div}_+(b) \cup \{-a : a \in \operatorname{Div}_+(b)\}$$

Demostración

Pruebo la linea de equivalencias:

1. $a \mid b \implies (-a) \mid b$
   Si $a \mid b$ entonces $\exists k \in \mathbb{Z} : ka = b$
   Luego $(-k)(-a) = ka = b$, por lo que existe un numero entero($-k$) que hace cumplir la definición de divisibilidad, $(-a) \mid b$
2. $(-a) \mid b \implies (-a) \mid (-b)$
   Si $(-a) \mid b$ entonces $\exists k \in \mathbb{Z} : k(-a) = b$

Luego $(-k)(-a) = -(k(-a)) = -b$, por lo que existe un numero entero($-k$) que hace cumplir la definición de divisibilidad, $(-a) \mid (-b)$

3. $(-a) \mid (-b) \implies a \mid b$
   Se tiene que $\exists k \in \mathbb{Z} : k(-a) = (-b)$
   Si se multiplica ambos lados por -1 se tiene que $\exists k \in \mathbb{Z} : ka = b$. Por lo que se cumple la implicancia.

Por lo tanto se cumplen las equivalencias y en particular se cumple la igualdad.

Teorema A.3.3 Incisos 1 y 2

Teorema A.3.3 Incisos 1 y 2
Sean a y b enteros. Entonces:

$$\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b) = \gcd(b,a)$$

$$\gcd(a,b) = |a| \iff a \mid b$$

En particular:

$$\gcd(a,0) = |a|$$

---

(1) se puede probar a partir de la definición de gcd y de Teorema A.2.3 Inciso 2 > (2).
La conmutatividad del gcd parte de la definición y de la conmutatividad de la intersección de conjuntos.

Para probar (2) se puede proceder como sigue:
$\implies$)
Si $\gcd(a,b) = |a|$ en particular $|a|$ es un divisor de a y de b.
Si $|a| = a$, $a \mid b$. Si $|a| = -a$, $(-a) \mid b$ y por lo tanto $a \mid b$.
Luego se cumple la implicancia.
$\impliedby$)
Como $a \mid b$, $\text{Div}(a) \subseteq \text{Div}(b)$.
Esto sale de que si $c \mid a \wedge a \mid b \implies c \mid b$.(Teorema A.2.4 inciso 2).
Por lo tanto $\max(\text{Div}(a) \cap \text{Div}(b)) = \max(\text{Div(a)})$.
Claramente $|a| = \max(\text{Div}(a))$.
Luego $|a| = \gcd(a,b)$.

(3) es consecuencia de (2) y del hecho de que si $a \neq 0 \wedge b = 0$ entonces $a \mid 0$.

Finales

Final 2020

Final 2020

2. Sea M un monoide finito.

Suponiendo que M es un grupo, si x es un elemento idempotente entonces:
$x^2 = x$
$\implies$
$x^2x^{-1} = xx^{-1}$
$\implies$
$x = e$

Por lo tanto e es el único elemento idempotente del grupo.

Suponiendo que $x \in M$ es el único elemento idempotente del monoide M.
e es un elemento idempotente de M, por lo tanto $x = e$.

Sea $g \in M$, si $g \neq e$, como M es finito existe $n \in \mathbb{N}$ tal que $g^n = e$.
Como M es finito las potencias g^n eventualmente se repiten, es decir, existen r y t tal que:
$g^r = g^{r+kt}$

En particular si $r + kt = k't$
$r = (k' - k)t$

Es decir, las potencias de r se repiten cada t pasos.

$n \neq 1$ ya que $g \neq e$.
$n \neq 2$ ya que si fuera así g seria un elemento idempotente distinto de e.
Por lo tanto $g^{n-1} \neq g$ y:
$g^{n-1}g = g^n = e$
$gg^{n-1} = g^n = e$
g^{n-1} es un elemento inverso de g y resulta M grupo.

Final 2021

Final 2021

2. a)
   La respuesta es la suma directa $\mathbb{Z} \oplus \mathbb{Z}_2$

Sea $(n, a) \in \mathbb{Z} \oplus \mathbb{Z}_2$, si (n, a) tiene orden 2 entonces se tiene que cumplir que:
$(n, a) + (n, a) = (0, \bar{0})$
$(n, a) + (n, a) = (2n + 2a)$

$2n = 0$
$2\bar{a} = 0$

Tanto $\bar{0}$ como $\bar{1}$ cumplen la segunda ecuación, mientras que $2n = 0$ si y solo si $n = 0$. Como $(0, \bar{0})$ es la identidad del grupo, el único elemento de orden 2 es $(0, \bar{1})$.

b)
Defino

$$H = \{(a_1, a_2, a_3, \ldots) : a_1 \in \mathbb{Z}_2\}$$

También definible como:
$H = \bigoplus_{i=1}^{\infty} \mathbb{Z}_2$
H es un grupo por ser una suma directa de grupos.
H es infinito ya que contiene el siguiente conjunto infinito de cardinal $\aleph_0$:
$H' = \{(a_1, a_2, a_3, \ldots) : \forall i \in \mathbb{N}, \exists n \in \mathbb{N}, i \leq n \implies a_i = \bar{1}\}$
Es decir, existe una función biyectiva de $\mathbb{N}$ a H' tal que:
$f(0) = (0, 0, 0, \ldots)$
$f(1) = (1, 0, 0, \ldots)$
$f(2) = (1, 1, 0, \ldots)$
Y así:

Sea $(a_1, a_2, a_3, \ldots) \in H$, como todos los elementos de $\mathbb{Z}_2$ tienen orden 2 se tiene que:
$(a_1, a_2, a_3, \ldots) + (a_1, a_2, a_3, \ldots) = (a_1 + a_1, a_2 + a_2, a_3 + a_3, \ldots) = (0, 0, 0, \ldots)$
Por lo tanto todos los elementos de H tienen orden 2.

c)
Esto es equivalente a probar que existe un epimorfismo de G a H o que dicho epimorfismo no existe.

FALSO:
Suponiendo que existe un subgrupo K de G tal que $H \cong G/K$
K es un subgrupo normal, luego la operación de G se induce al cociente.
Sea f dicho isomorfismo y $g \in G$
$f([g]^2) = f([g][g]) = f([g])f([g]) = f([g])^2 = e_H$
Como f es un monomorfismo, para todo $g, g' \in G$:
$f([g]^2) = f([g']^2)$
$\implies$
$[g]^2 = [g']^2$
$\implies$
$[g^2] = [g'^2]$

En particular $\forall g : g^2 \in K$

Tomando $G = \mathbb{Z} \times \mathbb{Z}_2$ se tiene que si k es par entonces $(k/2, \bar{0})$ y $(k/2, \bar{1})$ están en K.

G/K tiene una única clase de equivalencia y es un conjunto finito, pero H es infinito. ABS!
Luego no existe un subgrupo K que cumpla lo pedido.

Final 2021 2

Final 2021 2

2. a) Si KN es un subgrupo de G entonces:
   $\forall a, b \in KN, ab^{-1} \in G$

Sean $n \in N$ y $k \in K$:

Como NK es un subgrupo se tiene que:
$(nk)^{-1} = k^{-1}n^{-1} \in NK$
Pero $k^{-1} \in K$ y $n^{-1} \in N$, por lo tanto $(nk)^{-1} \in KN$ y de manera analoga se puede probar que
$kn \in KN \implies (kn)^{-1} \in NK$

Se tiene que $\forall g \in G$:
$g \in NK \implies g^{-1} \in KN$
$g \in KN \implies g^{-1} \in NK$

Reemplazando g con su inverso se tiene que:
$g^{-1} \in NK \implies g \in KN$
$g^{-1} \in KN \implies g \in NK$

Entonces:
$g \in NK \wedge g^{-1} \in NK \iff g \in KN \wedge g^{-1} \in NK$

Si $g \in NK$, como NK es grupo se tiene que $g^{-1} \in NK$ así que la proposición anterior se reemplaza como:
$g \in NK \iff g \in KN$

De donde sale que $NK = KN$
□

Suponiendo que $NK = KN$,
Sean $a, b \in NK$
Para que $NK < G$ se tiene que cumplir que:
$ab^{-1} \in G$
Existen $n_1, n_2 \in N$ y $k_1, k_2 \in K$ tal que $a = n_1k_1$ y $b = n_2k_2$
$ab^{-1} = (n_1k_1)(n_2k_2)^{-1} = n_1k_1k_2^{-1}n_2$
$k_2^{-1}n_2 \in KN \implies k_2n_2 \in NK$
$n_1k_1 \in NK$

Por lo tanto $n_1k_1k_2^{-1}n_2 \in NK \subseteq G$ y $NK < G$

□

b)
Sean $k \in K$ y $n \in N$:
Se tiene que:
$nk = kn \iff nkn^{-1}k^{-1} = e$

$nk(n^{-1}k^{-1})$
$=$
$(nkn^{-1})k^{-1}$
$=$
$n(kn^{-1}k^{-1})$

Por normalidad de K, $nkn^{-1} \in K$ y como $k^{-1} \in K$ se tiene que $nkn^{-1}k^{-1} \in K$
Pero por normalidad de N, $kn^{-1}k^{-1} \in N$ y resulta $n(kn^{-1}k^{-1}) \in N$
Entonces $nkn^{-1}k^{-1} \in N \cap K$, de donde resulta que $nkn^{-1}k^{-1} = e$ y $nk = kn$.
□

c)
$\varphi : K \times N \to KN$
$\varphi(k, n) = kn$

φ es morfi de grupos:
$\varphi((k_1, n_1)(k_2, n_2)) = \varphi(k_1k_2, n_1n_2) = (k_1k_2)(n_1n_2)$
$= k_1(k_2n_1)n_2 = k_1(n_1k_2)n_2 = (k_1n_1)(k_2n_2) = \varphi(k_1, n_1)\varphi(k_2, n_2)$

φ es mono de grupos:
$\varphi(k_1, n_1) = e$
$\implies$
$k_1n_1 = e$
$\implies$
$k_1 = n_1^{-1}$

Entonces:
$k_1 \in N \cap K$
$n_1 \in N \cap K$
Por lo tanto $(k_1, n_1) = (e, e)$ y φ es mono de grupos.

φ es epi de grupos:
Sea $kn \in KN$ entonces:
$\varphi(k, n) = kn$

Entonces φ es un morfi de grupos biyectivo. Por lo tanto es φ es un isomorfismo.
■

Final dic 2

Final dic 2

2. a)
   Sea la relación $a \sim b$ tal que $\exists g \in G : gag^{-1} = b$

$\sim$ es reflexiva, $eae^{-1} = a$
$\sim$ es simétrica, $gag^{-1} = b \implies a = g^{-1}bg \implies a = g^{-1}b(g^{-1})^{-1}$
$\sim$ es transitiva, $gag^{-1} = b \land hbh^{-1} = c \implies (hg)a(hg)^{-1} = c$

Por lo tanto $\sim$ es una relación de equivalencia.

b)
Sea $a, b \in G$, la función:
$f : \langle a \rangle \to \langle bab^{-1} \rangle$
$f(a^k) = ba^kb^{-1}$
Es una función biyectiva,

Es inyectiva:
$f(a^k) = f(a^j)$
$\implies$
$ba^kb^{-1} = ba^jb^{-1}$
$\implies$
$a^k = a^j$

Es sobreyectiva:
$(bab^{-1})^k = ba^kb^{-1}$, por lo tanto
$f(a^k) = (bab^{-1})^k$

De donde sale que $o(a) = o(bab^{-1})$

c)
FALSO
Considerar el grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$:
$o(0,1) = o(1,0)$

Para cualesquiera $a, b \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$:
$(-b) + a + b = ((-b) + b) + a = (0,0) + a = a$
Luego la clase de conjugación de cualquier elemento a contiene solo al elemento a y por lo tanto las clases de conjugación de $(0,1)$ y $(1,0)$ son diferentes.

Parciales

2do Parcial 2014

2do Parcial 2014

1. $f(e)$ es el neutro de S donde e es el neutro de G.

Sea $s \in S$, como f es un epimorfismo s tiene al menos una preimagen.
Sea $g \in G$ tal que $f(g) = s$:
$f(e)s = f(e)f(g) = f(eg) = f(g) = s$
$sf(e) = f(g)f(e) = f(ge) = f(g) = s$
Luego $f(e)$ es neutro en S y S es un monoide.

De la misma forma:
$sf(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e)$
$f(g^{-1})$ es inverso a derecha de s.
Como S es un monoide, el inverso a derecha es también el inverso a izquierda y resulta S grupo.

2. a)
   Analizando el termino:
   $h_1k_1 = h_2k_2$
   $\implies$
   $h_1 = h_2k_2k_1^{-1}$
   $\implies$
   $h_2^{-1}h_1 = k_2k_1^{-1}$

$k_2k_1^{-1} \in K$
$h_2^{-1}h_1 \in H$
Luego $h_2^{-1}h_1 \in K \cap H$, por lo tanto $h_2^{-1}h_1 = e$ y $h_1 = h_2$.

b)
Del ejercicio anterior sale que si $g = h_1k_1 = h_2k_2$ entonces $h_1 = h_2$ y $k_1 = k_2$.
Por lo que g se puede escribir de una única forma como un producto de un elemento H y un elemento de G.
Luego sea:
$f : G/K \to H$
$f([hk]) = h$

Pruebo que f esta bien definida:
$[hk] = hkK = hK = [h]$
Luego $[h_1k_1] = [h_2k_2] \implies [h_1] = [h_2] \implies h_1K = h_2K$
$h_1K = h_2K$ implica que existen $k_1, k_2 \in K$ tal que:
$h_1k_1 = h_2k_2$ de donde sale que $h_1 = h_2$ y por lo tanto f esta bien definida.

f es morfi de grupos:
$f([h_1k_1][h_2k_2])$
$=$
$f([h_1][h_2])$
$=$
$f([h_1h_2])$
$=$
h_1h_2
$=$

$f([h_1])f([h_2])$
$=$
$f([h_1k_1])f([h_2k_2])$

f es epi de grupos:
Sea $h \in H$ entonces:
$f([he]) = f([h]) = h$

f es mono de grupos:
$f([h_1k_1]) = f([h_2k_2])$
$\implies$
$f([h_1]) = f([h_2])$
$\implies$
$h_1 = h_2$
De donde sale que $[h_1k_1] = [h_2k_2]$

Por lo tanto f es un isomorfismo de grupos y $G/K \cong H$.
■

2do Parcial 2015

2do Parcial 2015

1. Sea $f : G \to G^n$ tal que
   $f(x) = x^n$

$G^n = \text{Im}(f)$ y $\ker f = G_n$ por definición.

Suponiendo que G es abeliano.
G^n es un grupo:

- $x^n y^n = (xy)^n$, G^n es magma.
- G es semigrupo porque la asociatividad es heredada de G.
- $e^n x^n = (ex)^n = x^n$, e^n es neutro a izquierda y derecha(se prueba de manera analoga) y en particular $e^n = e$. Por lo que G^n es un monoide.
- $((x^{-1})^n)x^n = ((x^{-1})x)^n = e^n$, todo x^n tiene inverso y resulta G^n grupo.

Además f es morfi de grupos:
$f(xy) = (xy)^n = x^n y^n = f(x)f(y)$

f es un epimorfismo y por primer teorema del isomorfismo $G^n \cong G/G_n$.
■

2. Sea $n \in Z(G)$ y $a \in G$
   $ana^{-1} = aa^{-1}n = n \in N$.
   Por lo tanto $Z(G) \triangleleft G$.
3. a) VERDADERO, Todo grupo de orden 4 es o isomorfo a $\mathbb{Z}_4$ o isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Ambos son abelianos así que un grupo de orden 4 debe ser abeliano.
   b) FALSO, S_3 es el grupo de funciones biyectivas de $\{1, 2, 3\}$ en si mismo. $o(S_3) = 3! = 6$ y $o(\mathbb{Z}_6) = 6$, sin embargo S_3 no es abeliano y $\mathbb{Z}_6$ si así que ambos no pueden ser isomorfos.
   c) VERDADERO, si G tiene orden primo p entonces tiene al menos dos elementos. Sea $g \neq e$, $\langle g \rangle$ es un subgrupo de G. Por teorema de Lagrange, $o(g) = 1$ o $o(g) = p$. Como $o(g) \neq_1$, $o(g) = o(G) = p$ y G es cíclico.

Parcial 2 2024

Parcial 2 2024

1.

a)
La conjugación por a es un automorfismo de G, la conjugación se define como:
$f_a(g) = aga^{-1}$
Como H es un subgrupo característico entonces $\forall a \in G : f_a(H) \subset H$
O lo que es equivalente:
$\forall a \in G : aHa^{-1} \subset H$
De donde resulta que $H \triangleleft G$

b)
Como $H \triangleleft G$, la proyección al cociente $\pi : G \to G/H$ es un homomorfismo donde coso.

Defino:
$\overline{\varphi} : G/H \to G/H$
$\overline{\varphi}([x]) = [\varphi(x)]$

Sean $x, y \in G$ tal que $x \equiv y(H)$
$xy^{-1} \in H$
$\varphi(xy^{-1}) \in H$, por ser H es un subgrupo característico.
$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} \in H$
Por lo tanto $\varphi(x) \equiv \varphi(y)\ (H)$ y $\overline{\varphi}$ esta bien definida.

$\overline{\varphi}$ es un morfismo de grupos:
Como $H \triangleleft G$, la operación de G se induce al cociente.
$\overline{\varphi}([x][y]) = \overline{\varphi}([xy]) = [\varphi(xy)] = [\varphi(x)\varphi(y)] = [\varphi(x)][\varphi(y)] = \overline{\varphi}(x)\overline{\varphi}(y)$

Como φ^{-1} es un automorfismo se puede definir:
$\psi : G/H \to G/H$
$\psi([x]) = [\varphi^{-1}(x)]$

Usando métodos análogos a los anteriores se puede probar que ψ es un morfismo de grupos bien definido.

Entonces:
$\overline{\varphi}(\psi([x])) = \overline{\varphi}([\varphi^{-1}(x)]) = [\varphi(\varphi^{-1}(x))] = [x]$
$\psi(\overline{\varphi}([x])) = \psi([\varphi(x)]) = [\varphi^{-1}(\varphi(x))] = [x]$

$\overline{\varphi}$ es invertible, por lo tanto es biyectivo y $\overline{\varphi}$ es un automorfismo.

Ahora defino la asignación:
$f(\varphi) = \overline{\varphi}$

Sean φ y ψ automorfismos de G:

$f(\varphi \circ \psi)([x]) = \overline{\varphi \circ \psi}([x]) = [(\varphi \circ \psi)(x)] = [\varphi(\psi(x))] = \overline{\varphi}([\psi(x)])$
$= \overline{\varphi}(\overline{\psi}([x])) = (\overline{\varphi} \circ \overline{\psi})([x]) = (f(\varphi) \circ f(\psi))([x])$

La concatenación de automorfismos es un automorfismos y f preserva la operación de concatenación. Por lo tanto f es un homomorfismo de grupos.

c)

Sea $f : \mathbb{Z}_2 \oplus \mathbb{Z}_2 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ donde
$f(1,0) = (0,1)$
$f(0,1) = (1,0)$
$f(x) = x$, en cualquier otro caso.

f es una función biyectiva y también es un morfismo de grupos.
$f(0,0) = (0,0)$, luego para todo elemento x del grupo:
$f((0,0) + x) = f(x) = f(0,0) + x$

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

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

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

Considerando el subgrupo normal $\langle(1,0)\rangle = \{(0,0),(1,0)\}$ se tiene que:
$f(1,0) = (0,1) \notin \langle 1,0\rangle$.
Por lo tanto $\langle(1,0)\rangle$ no es un subgrupo caracteristico.

3. a) Verdadero.
   Sea $a \in R$:

$0a = (0+0)a = 0a + 0a$
$0a$ tiene un elemento inverso b.
$0a + b = 0a + 0a + b$
$0 = 0a + (0a + b) = 0a + 0 = 0a$
Luego
$0a = 0$

b) Verdadero
$n = o(x)$, entonces $x^n = e$
Luego:
$f(x^n) = f(e)$
$\implies$
$f(x)^n = e$

Si $m = o(f(x))$ entonces $m \mid n$.

Ya que si k cumple que $a^k = e$ entonces $o(a) \mid x$.

Sea $p = o(a)$, $a^p = a^k$

Parcial 2020

Parcial 2020

Ejercicio 1

¿Probar que $(\mathcal{A}, \subseteq)$ es un poset?

Sea la función:
$f : A \to \mathcal{A}$
$f(a) = A_a$

f es un morfismo de posets:
Sean $a, b \in A$ tal que $a \leq b$
$f(a) \subseteq f(b)$
$\iff$
$\{x \in A : x < a\} \subseteq \{x \in A : x < b\}$
$\iff$
$\forall x \in A : x < a \implies x < b$
□

Si $a < b$ se cumple $x < b$ por transitividad de $<$:
$x < a \wedge a < b \implies x < b$
Si $a = b$ y $x < a$ en particular se tiene que $x < b$, así que también vale la propiedad.

Luego $f(a) \subseteq f(b)$, f es un morfismo de posets.

f es sobreyectiva:
Vale ya que la definición de $\mathcal{A}$ coincide con la definición de $\mathrm{Im}(f)$
□

f es un isomorfismo de posets:
Alcanza con probar que $f(a) \subseteq f(b) \implies a \leq b$

Pruebo por el absurdo, suponiendo que $a \nleq b$, como $(A, \leq)$ es un orden total se tiene que $b > a$.

Si se tiene que $f(a) \subseteq f(b)$ entonces $\forall x \in A : x < a \implies x < b$, en particular reemplazando $x = b$ se tiene que $b < a \implies a < b$. Luego por antisimetría de $<$, $a = b$. ABS!!

Por lo tanto, $a \leq b$ y por lo tanto f es un isomorfismo de posets.
□

Como existe un isomorfismo entre ambos posets, se tiene que $(A, \leq) \simeq (\mathcal{A}, \subseteq)$

Parcial 2020 1

Parcial 2020 1

1.

a)
Para probar que $+$ es cerrado hay que probar que $\phi + \psi$ es un homomorfismo de grupo de G en A.
Sean $x, y \in G$
$(\phi + \psi)(xy) = \phi(xy) + \psi(xy) = (\phi(x) + \phi(y)) + (\psi(x) + \psi(y))$
$= (\phi(x) + \psi(x)) + (\phi(y) + \psi(y)) = (\phi + \psi)(x) + (\phi + \psi)(y)$

$\phi + \psi$ es morfi de grupos.

b)
$(\phi + \psi)(x) = \phi(x) + \psi(x) = \psi(x) + \phi(x) = (\psi + \phi)(x)$, vale conmutatividad

$((\phi + \psi) + \chi)(x) = (\phi + \psi)(x) + \chi(x) = \phi(x) + \psi(x) + \chi(x)$
$(\phi + (\psi + \chi)(x) = \phi(x) + (\psi + \chi)(x) = \phi(x) + \psi(x) + \chi(x)$
vale asociatividad

Sea $\epsilon : G \to A$, $\epsilon(x) = e$ donde e es neutro A.
ϵ es morfi de grupos:
$\epsilon(xy) = e = e + e = \epsilon(x) + \epsilon(y)$
Luego
$(\phi + \epsilon)(x) = \phi(x) + \epsilon(x) = \phi(x) + e = \phi(x)$
ϵ es neutro en $\mathrm{Hom}(G, A)$

Dado un morfi ϕ, defino $\phi^{-1}(g) = -\phi(g)$
ϕ^{-1} es morfi de grupos:
$\phi^{-1}(xy) = -\phi(xy) = -(\phi(x) + \phi(y)) = -\phi(x) + -\phi(y) = \phi^{-1}(x) + \phi^{-1}(y)$
Luego
$(\phi + \phi^{-1})(x) = \phi(x) + \phi^{-1}(x) = \phi(x) + -\phi(x) = e = \epsilon(x)$
$\mathrm{Hom}(G, A)$ admite inversos.

Por lo tanto $\mathrm{Hom}(G, A)$ es grupo.

c)
Dado $a \in A$, defino $g_a : \mathbb{Z} \to A$ como:
$g_a(k) = ka$

g_a esta bien definida y además es un morfi de grupos:
$g_a(n + m) = (n + m)a = na + ma = g_a(n) + g_a(m)$

Defino entonces la función:
$f : A \to \mathrm{Hom}(\mathbb{Z}, A)$
$f(a) = g_a$

f es morfi de grupos.
$(g_a + g_b)(n) = g_a(n) + g_b(n) = na + nb = n(a+b) = g_{a+b}(n)$
Por lo tanto:
$f(a+b) = g_{a+b} = g_a + g_b$

f es mono de grupos:
$f(a) = f(b)$
$\implies$
$g_a = g_b$
$\implies$
$g_a(1) = g_b(1)$
$\implies$
$a = b$

f es epi de grupos:
Sea $\varphi \in \mathrm{Hom}(\mathbb{Z}), \mathrm{A}$, $\mathbb{Z}$ es cíclico y es generado por 1.
Por lo tanto como g es morfi de grupos:
$\varphi(k) = \varphi(1^k) = (\varphi(1))^k = k(\varphi(1)) = g_{\varphi(1)}(k)$
Por lo tanto $f(\varphi(1)) = \varphi$

Por lo tanto f es un iso de grupos y $\mathrm{Hom}(\mathbb{Z}, A) \cong A$.
■

2. a)
   $(a,a), (b,b) \in \hat{G}$
   $(a,a)(b,b)^{-1} = (a,a)(b^{-1}, b^{-1}) = (ab^{-1}, ab^{-1}) \in \hat{G}$
   $\therefore \hat{G} < G \times G$

b)
$f : G \to \hat{G}$
$f(g) = (g,g)$

f morfi de grupos:
$f(gh) = (gh, gh) = (g,g)(h,h) = f(g)f(h)$

f invertible, por lo tanto biyectiva:
$\pi : \hat{G} \to G$
$\pi(g,g) = g$

$f(\pi(g,g)) = f(g) = (g,g)$
$\pi(f(g)) = \pi(g,g) = g$

Por lo tanto, f iso de grupos y $\hat{G} \cong G$

c)
Suponiendo G abeliano:
Sea $(n,n) \in \hat{G}$ y $(a,b) \in G \times G$
$(a,b)(n,n)(a,b)^{-1}$
$=$
(ana^{-1}, bnb^{-1})
$=$
$(aa^{-1}n, bb^{-1}n)$
$=$
(n,n)
$\in$
$\hat{G}$
$\therefore \hat{G} \triangleleft G \times G$

Suponiendo $\hat{G} \triangleleft G \times G$:
Sean $a, b \in G$, como $\hat{G}$ es normal se tiene que:
$(a,1)(b,b)(a,1)^{-1} \in \hat{G}$

$(a,1)(b,b)(a,1)^{-1} = (aba^{-1}, b) \in \hat{G}$
Por lo tanto
$aba^{-1} = b$
$\implies$
$ab = ba$

Por lo tanto $\hat{G}$ es abeliano.

3. $\sigma(n) = n$
   Sea $\tau \in S_n$ tal que:
   $\tau(1) = n$
   $\tau(n) = 1$
   $\tau(x) = x$, en cualquier otro caso.

Sea $\sigma \in H$:
$\tau^{-1}(\sigma(\tau(1))) = \tau^{-1}(\sigma(n)) = \tau^{-1}(n) = 1$
Por lo tanto, $\tau^{-1} \circ \sigma \circ \tau \in H'$. H' y H son conjugados.

Si $H \triangleleft S_n$ entonces $\forall \sigma \in H, a \in S_n$:
$a^{-1}\sigma a \in H$
Pero si $a = \tau$ entonces $\tau^{-1}\sigma\tau \in H'$ por lo tanto
$(\tau^{-1}\sigma\tau)(1) = 1$
$(\tau^{-1}\sigma\tau)(n) = n$
$\implies$
$\sigma(\tau(1)) = \tau(1) = n$
$\sigma(\tau(n)) = \tau(n) = 1$
$\implies$
$\sigma(n) = n$
$\sigma(1) = 1$
$\implies$
$H \subseteq H'$

En particular, si $n > 3$ la función
$\rho(1) = 2$
$\rho(2) = 1$
$\rho(x) = x$
Es una función que cumple que $\rho \in H$ pero $\rho \notin H'$
En el caso de $n = 2$, la única función que cumple $\sigma(n) = n$ es la identidad. Por lo tanto en este caso $H \triangleleft S_n$.

Si $n = 2$, entonces $H = \{\mathrm{Id}\}$ y $H \triangleleft S_n$
■

Practica 1

Ejercicio 7

Ejercicio 7

Reflexiva

Valen 1,2 y 3.

Se tiene que $\Delta \subseteq \mathcal{R} \land \Delta \subseteq \mathcal{S}$, por lo tanto:

1. $\Delta \subseteq \mathcal{R} \cup \mathcal{S}$, la unión es reflexiva.
2. $\Delta \subseteq \mathcal{R} \cap \mathcal{S}$, la intersección es reflexiva.
3. Para todo $a \in A$ se tiene que $(a,a) \in \mathcal{R} \land (a,a) \in \mathcal{S}$, por lo tanto $(a,a) \in \mathcal{R} \circ \mathcal{S}$

Simétrica

Valen 1 y 2
$\mathcal{R}$ es simétrica $\iff \mathcal{R} = \mathcal{R}^{-1}$
1 y 2 vale ya que $(\mathcal{R} \cup \mathcal{S})^{-1} = \mathcal{R}^{-1} \cup \mathcal{S}^{-1}$, lo mismo para la intersección.

3 es falso
Sea $A = a,b,c$, las relaciones $\mathcal{R} = \{(a,a),(a,b),(b,a)\}$ y $\mathcal{S} = \{(a,b),(b,a)\}$ son ambas simétricas pero su composición es $\{(a,b),(a,a),(b,b)\}$ la cual no es simétrica.

Transitiva

1 es falso
Sean las relaciones $\mathcal{R} = \{(b,c)\}$ y $\mathcal{S} = \{(a,b)\}$. La unión es $\{(a,b),(b,c)\}$ la cual no es transitiva.

2 es verdadero
Suponiendo que $(a,b) \in \mathcal{R} \cap \mathcal{S} \land (b,c) \in \mathcal{R} \cap \mathcal{S}$. Eso quiere decir que (a,b) y (b,c) pertenecen tanto a $\mathcal{R}$ como a $\mathcal{S}$. Por transitividad de ambas relaciones $(a,c) \in \mathcal{R} \cap \mathcal{S}$. La intersección es transitiva.

3 es falso
$\mathcal{R} = \{(a,b),(c,d)\}$ $\mathcal{S} = \{(b,c),(d,a)\}$
$\mathcal{R} \circ \mathcal{S} = \{(a,c),(c,a)\}$, no transitiva

Antisimétrica

1 es falso
$\mathcal{R} = \{(a,b)\}, \mathcal{S} = \{(b,a)\}$, $\mathcal{R} \cup \mathcal{S} = \{(a,b),(b,a)\}$, no es antisimétrica.

2 es verdadero
$\mathcal{R} \cap \mathcal{S} \cap (\mathcal{R} \cap \mathcal{S})^{-1}$
$= \mathcal{R} \cap \mathcal{S} \cap \mathcal{R}^{-1} \cap \mathcal{S}^{-1}$=(\mathcal{R} \cap \mathcal{R}^{-1}) \cap (\mathcal{S} \cap \mathcal{S}^{-1})\subseteq \Delta \cap \Delta=\Delta$

3 es falso, el ejemplo de transitividad para el 3 también es contraejemplo para este caso.

Teorema de factorización

Teorema de factorización
Dada una función $f : A \to B$ y una relación de equivalencia $\sim \subseteq \mathcal{K}_f$, probar que existe una única función $f : A/\sim \ \to B$ tal que $f = \bar{f} \circ \pi$, donde $\pi : A \to A/\sim$ se define como $\pi(a) = \bar{a}$ para todo $a \in A$.

Demostración

Existencia

La relación

$$\bar{f} = \{(\bar{a}, f(a)) : a \in A\}$$

cumple con la definición del teorema.

$\bar{f}$ es una función ya que $\mathrm{Dom}(f) = A/\sim$ y si $\bar{a} = \bar{b}$, por ser $\sim \subseteq \mathcal{K}_f$ se tiene que cumplir que $f(a) = f(b)$ y por ser f una función $\bar{f}(a)$ tiene una única imagen.

Luego se tiene que $\forall a \in A$:
$\bar{f}(\pi(a)) = \bar{f}(\bar{a}) = f(a)$.

Esto prueba la existencia de al menos una función que cumple el teorema.

Unicidad

Sean $\bar{g}$ una función que cumple el teorema y $\bar{f}$ la función definida anteriormente

$\bar{f} = \bar{g}$
$\iff$
$\forall a \in A : \bar{f}(\bar{a}) = \bar{g}(\bar{a})$
$\iff$
$\forall a \in A : f(a) = \bar{g}(\pi(a))$
$\iff$
$f = \bar{g} \circ \pi$

Practica 3

📄 Ejercicio 11

Ejercicio 11

Ejercicio 11
Sea $(L, \preceq)$ un retículo. Un polinomio en n-variables es una función $p : L^n \to L$ que pertenece al siguiente conjunto inductivo P_L:

- $i \in \{1 \dots n\}, \pi_i(x_1, \dots, x_n) = x_i$
- Si $f, g \in P_L$, entonces $(f \vee g)(\bar{x}) = f(\bar{x}) \vee g(\bar{x})$
- Si $f, g \in P_L$, entonces $(f \wedge g)(\bar{x}) = f(\bar{x}) \wedge g(\bar{x})$
  Probar que toda función $p \in P_L$, es un morfismo de orden entre $(L^n, \preceq_{prod})$ y $(L, \preceq)$

Pruebo por inducción sobre el conjunto P_L.

CB) $f = \pi_i$
Sean $\bar{x}$ y $\bar{y}$ elementos de L^n:
Si $\bar{x} \preceq_{prod} \bar{y}$ en particular se tiene que $x_i \preceq y_i$.
Por lo tanto, $\pi_i(\bar{x}) \preceq \pi_i(\bar{y})$

□

HI) Dadas $f, g \in P_L$, f y g son morfismos de orden entre $(L^n, \preceq_{prod})$ y $(L, \preceq)$

PI)
Sean $\bar{x}$ y $\bar{y}$ elementos de L^n:
$(f \vee g)(\bar{x}) \preceq (f \vee g)(\bar{y})$
$\iff$ (def de $f \vee g$)
$f(\bar{x}) \vee g(\bar{x}) \preceq f(\bar{y}) \vee g(\bar{y})$

Dado que por ser f y g morfismos de orden se tiene que $f(\bar{x}) \preceq g(\bar{x})$, $f(\bar{y}) \preceq g(\bar{y})$

Luego por ser $(L, \preceq)$ un retículo, el join es compatible con la relación de orden y por lo tanto vale que
$f(\bar{x}) \vee g(\bar{x}) \preceq f(\bar{y}) \vee g(\bar{y})$.

El caso de $(f \wedge g)$ es análogo.
□

Luego por inducción en P_L, todo polinomio es un morfismo de orden entre $(L^n, \preceq_{prod})$ y $(L, \preceq)$.

■

Practica 6

Ejercicio 1

> **Ejercicio 1**
> e es un elemento neutro del conjunto X' por definición.
>
> $\forall x, y, z \in X : x(yz) = (xy)z$, por ser X un semigrupo.
>
> Tomando $x, y \in X$, se tiene que:
>
> - $e(xy) = xy = (xy)e$
> - $x(ey) = xy = (ex)y$
> - $(xy)e = xy = x(ye)$
>
> Por lo tanto, $\forall x, y, z \in X'$ se cumple la asociatividad y X' es un monoide.

Ejercicio 11

> **Ejercicio 11**
> Para probarlo demuestro que $\forall a, b \in H : ab^{-1} \in H$
>
> Sea $n \in \mathbb{N}$ y $H = \{g \in G : g^n = e\}$
>
> Tomo $a, b \in H$
> $(ab^{-1})^n$
> $=$(G grupo abeliano)
> $a^n(b^{-1})^n$
> $=$
> $a^n(b^n)^{-1}$
> $=$($a, b \in H$)
> ee^{-1}
> $=$(operación sobre elementos inversos)
> e
>
> $e \in H$, ya que $e^1 = e$. Por lo tanto $ab^{-1} \in H$ y resulta ser H un subgrupo de G.

Ejercicio 15

> **Ejercicio 15**
> a)
> $h = f \times g$

$h((x,y)(x',y')) = h(xx', yy') = (f(xx'), g(yy')) = (f(x)f(x'), g(y)g(y')) = (f(x), g(y))(f(x'), g(y')) = h(x,y)h(x',y')$
h morfi de grupos

b)
Suponiendo f, g monos de grupos:
$h(x,y) = (e_x, e_y)$
$\iff$
$f(x) = e_x \wedge g(y) = e_y$
$\iff$
$(x,y) = (e_x, e_y)$
h mono de grupos

Suponiendo f, g epis de grupos:
$h(X \times Y) = (f(X), g(Y)) = (X', Y')$
h epi de grupos.

Luego si f, h son isos de grupo entonces h es iso de grupos.

c)
Sea $f : X \times Y \to Y \times X$ definida como:
$f(x,y) = (y,x)$

f es mono de grupos:
$f((x,y)(x',y')) = f(xx', yy') = (yy', xx') = (y,x)(y',x') = f(x,y)f(x',y')$

f es invertible ya que es su propia inversa:
$f(f(x,y)) = f(y,x) = (x,y)$
Luego f biye y por lo tanto f iso de grupos. $X \times Y \cong Y \times X$

d)
Pruebo para G y el caso de H es análogo:
G cumple que:

- $G = G \times \{e_g\}$
- $G \cap \{e_g\} = \{e_g\}$
- $\{e_g\} \triangleleft G \wedge G \triangleleft G$
  Por lo tanto $G \cong G \times \{e_g\}$

e)
Se tiene que:
$\mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{15}$
Pero ninguno de los grupos $\mathbb{Z}_n$ es isomorfo entre sí.

Ejercicio 16

Ejercicio 16
a)
$(\{-1,1\}, \cdot)$ es un grupo cíclico de orden 2, ya que:
$(-1)^0 = 1$
$(-1)^1 = (-1)$
Por lo tanto es isomorfo a $(\mathbb{Z}_2, +)$

b)
$\bar{1}$ es el neutro del grupo de elementos invertibles.

Se tiene que:
$xy \equiv 1(8)$
$\iff$
$xy = 8k + 1$ con $k \in \mathbb{Z}$.(O lo que es lo mismo, $xy - 1$ es múltiplo de 8)

Entonces:
Ningún elemento con representante par es invertible, si $\overline{2p}$ es invertible tendría que pasar que $2py = 8k + 1$, pero $2py$ es par mientras que $8k + 1$ es par.
Todos los demás elementos son invertibles:
$1 \cdot 1 = 8 \cdot 0 + 1$
$3 \cdot 3 = 9 = 8 \cdot 1 + 1$
$5 \cdot 5 = 25 = 8 \cdot 4 + 1$
$7 \cdot 7 = 49 = 8 \cdot 6 + 1$

Como se puede observar para cualquier elemento del grupo, $\bar{p} = \bar{1}$ por lo tanto el grupo es no cíclico y de orden 4 por lo que es isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

ALTERNATIVA:
Sea $8k + 1 \in \bar{1}$, sea p un elemento de $\bar{n}$, por algoritmo de la división $p = 8q + r$, entonces:

- $\bar{p} = \bar{r}$
- $(8k + 1) \cdot p = (8k + 1)(8q + r) = 8(8qk + r + q) + r \implies \bar{1}\bar{p} = \bar{r}$

$\bar{1}$ es neutro de la multiplicación.

Un elemento $\bar{n}$ de $\mathbb{Z}_m$ es invertible bajo la multiplicación si y solo si es m coprimo con n.
$\Longleftarrow$)
Si n y p son coprimos entonces por identidad de Benzout existen p y q tal que:
$pn + qm = 1$
$\implies$
$pn - 1 = (-q)m$
$\implies$
$pn \equiv 1(m)$
Induciendo la operación al cociente:
$\bar{p} \cdot \bar{n} = \bar{1}$

$\implies$)
Sea $\bar{n} \in \mathbb{Z}_m$ y $\bar{p}$ su inverso, entonces:
$np \equiv 1(m)$
$\implies$
$np + 1 = km$, con $k \in \mathbb{Z}$
$\implies$
$np - km = 1$
Entonces $\gcd(n, m)$ debe dividir a $np - km$ y a 1. La única posibilidad es $\gcd(n, m) = 1$ y resulta n coprimo con m.

Luego proceder como antes:

c)
Cualquier subgrupo no trivial de $(\mathbb{Z}, +)$ es cíclico, sea a un generador de dicho subgrupo entonces la función:
$f : \mathbb{Z} \to \langle a \rangle$
$f(k) = a$

Es morfi de grupos:
$f(pq) = a^{pq} = a^p a^q = f(p)f(q)$

Es trivialmente epi de grupos:

Es mono de grupos:
$f(k) = a^k = e$
Solo si $k = 0$ ya que un subgrupo cíclico de $(\mathbb{Z}, +)$ es infinito.

Luego f es iso de grupo y los grupos son isomorfos.

Ejercicio 17

Ejercicio 17
G es un grupo abeliano si y solo si la aplicación $f : G \to G$ dada por $f(a) = a^{-1}$ es un automorfismo en G.

Demostración

G es abeliano $\implies$)
f es un morfismo de semigrupos:
$f(xy)$
$=$
$(xy)^{-1}$
$=$
$y^{-1}x^{-1}$
$=$(G abeliano)
$x^{-1}y^{-1}$
$=$
$f(x)f(y)$
Por lo tanto también es un morfismo de grupos.

Luego f es invertible, ya que es su propia inversa.
$f(f(x)) = f(x^{-1}) = (x^{-1})^{-1} = x$

Por lo tanto f es biyectiva, f es un isomorfismo de grupos y en particular también es un automorfismo.

f automorfismo $\implies$)
Sean $x, y \in G$: ambos tienen inversos x^{-1} y y^{-1}:
$f(x^{-1}y^{-1})$
$=$(f morfismo de grupos)
$f(x^{-1})f(y^{-1})$
$=$
$(x^{-1})^{-1}(y^{-1})^{-1}$
$=$
xy

Pero también
$f(x^{-1}y^{-1})$
$=$
$(x^{-1}y^{-1})^{-1}$
$=$
$(y^{-1})^{-1}(x^{-1})^{-1}$
$=$
yx

Luego G es abeliano.

Ejercicio 2

Ejercicio 2
Sea G un monoide con inversos a derecha(resp. izquierda), probar que G es un grupo.

Caso derecha:
Sea x un elemento y l su inverso a derecha.
l también tiene un inverso a derecha, denomino r a dicho inverso.

$lx = (lx)e = (lx)(lr) = l(xl)r = ler = lr = e$

Por lo tanto, l es a su vez inverso a derecha e izquierda de x.
Como cada x tiene inverso, G es un grupo.

Caso izquierda:
Sea x un elemento y r su inverso a izquierda.
r también tiene un inverso a izquierda, denomino l a dicho inverso.

$xr = e(xr) = (lr)(xr) = l(rx)r = ler = lr = e$

Por lo tanto, r es a su vez inverso a derecha e izquierda de x.
Como cada x tiene inverso, G es un grupo.

Ejercicio 3

Ejercicio 3
El producto de elementos invertibles es invertible:
$xy(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$
Por lo tanto $xy \in G$ y la operación es cerrada en G.

Por lo tanto, G es subconjunto cerrado de M. La asociatividad se hereda en G así que G es un semigrupo.

$e \in G$, ya que e es su propio inverso. Por lo tanto, G es a su vez un monoide.

Por definición todos los elementos de G son invertibles, por lo tanto G es un grupo.

Ejercicio 5

Ejercicio 5

Enunciado

Probar que todo semigrupo cancelativo finito G es un grupo.

Demostración

Considero que G tiene al menos un elemento. Sea $x \in G$, defino la función:
$f : G \to G$
$f(y) = xy$

f es una función inyectiva:

- Si $f(x) = f(x') \implies xy = x'y$, por ser y un elemento cancelativo se tiene que $x = x'$.

Como f es inyectiva, también es biyectiva(por ser G finito).

Al ser f biyectiva, existe un elemento $e \in G$ tal que $f(e) = xe = x$(esto es, x tiene una preimagen).
Se tiene que:

- e es neutro a derecha: $xy = (xe)y = x(ey)$, por ser x elemento cancelativo, $y = ey$
- e es neutro a izquierda: $yy = y(ey) = (ye)y$, por ser y elemento cancelativo, $y = ye$
  Luego e es elemento neutro y G es un monoide.

Como f es biyectiva, existe un elemento $a \in G$ tal que $f(a) = e$(esto es, e tiene una preimagen), por lo tanto $f(a) = xa = e$ y a es un inverso a derecha de x.

Como x era un elemento genérico, todo elemento de G tiene inverso a derecha y por Ejercicio 1, G es un grupo.

Caso infinito

$(\mathbb{N}, +)$ es un caso de un semigrupo cancelativo infinito que no es un grupo.

Ejercicio 5 - Metodo delfina

Ejercicio 5 - Metodo delfina

Enunciado

Probar que todo semigrupo cancelativo finito G es un grupo.

Demostración

Sea $a \in G$ y sea $\langle a \rangle = \{a^n : n \in \mathbb{N}\}$

$\langle a \rangle$ es un subsemigrupo de G, como G es finito $\langle a \rangle$ también debe serlo. Por lo tanto tienen que existir distintos $i, j \in \mathbb{N}$ tal que $a^i = a^j$ lo que equivale a, suponiendo que $i < j$, que $a = a^{j-i+1}$(esto es así ya que se puede aplicar i veces la propiedad cancelativa sobre a).

Defino entonces $e = a^{j-i}$:

- $ea = a^{j-i}a = a^{j-i+1} = a$
- Sea $y \in G$: $ya = y(ea) = (ye)a$, por propiedad cancelativa sobre a, $y = ye$
- De la misma forma: $yy = (ye)y = y(ey)$, por propiedad cancelativa sobre y, $y = ey$

Por lo tanto, e es un elemento neutro de G.

Al ser G un monoide se puede extender $\langle a \rangle = \{a^n : n \in \mathbb{N}_0\}$

De la misma forma, defino $a' = a^{j-i-1}$. Como $i < j$, $j - i > 0$ o equivalentemente $j - i \geq 1$. Por lo tanto $j - i - 1 \geq 0$ y a' esta bien definido.
Por lo tanto:

- $a'a = a^{j-i-1}a = a^{j-i} = e$
- $aa' = aa^{j-i-1} = a^{j-i} = e$
  a' es un inverso de a. Por lo tanto todo elemento $a \in G$ tiene un inverso.

Ejercicio 7

Ejercicio 7

Enunciado

Probar que $\forall k \in \mathbb{Z}, \forall \bar{a} \in \mathbb{Z}_m, k\bar{a} = \overline{ka}$

Demostración

Pruebo que vale $\forall k \in \mathbb{N}_0$, por inducción en k:
CB) $k = 0$
$0\bar{a} = \bar{0} = \overline{0a}$
HI) $\forall k \in \mathbb{N}_0, k\bar{a} = \overline{ka}$
PI)
$(k+1)\bar{a} = k\bar{a} + \bar{a} = \overline{ka + a} = \overline{(k+1)a}$

Luego si $k < 0, -k \in \mathbb{N}$:
$k\bar{a} = (-k)(-\bar{a}) = (-k)\overline{-a} = \overline{(-k)(-a)} = \overline{ka}$

Ejercicio 9

Ejercicio 9
Sea S es un subconjunto finito de un grupo G, S es subgrupo de $G \iff$ La operación de G es cerrada en S

Demostración

SI S es subgrupo de G entonces la operación de G tiene que ser cerrada en S.

Suponiendo que la operación de G es cerrada en S(es decir, S es un subconjunto cerrado en S).

Por lo tanto S es un subsemigrupo de G.
Todo elemento de G es a su vez un elemento cancelativo: sea $a \in S$, tomo dos elementos $b, c \in S$
Suponiendo que $ab = ac$, a tiene un inverso en G, luego:
$a^{-1}(ab) = a^{-1}(ac)$
$\implies$ (asociatividad)
$(a^{-1}a)b = (a^{-1}a)c$
$\implies$ (elementos inversos)
$eb = ec$
$\implies$ (elementos neutros)
$b = c$

Luego a es un elemento cancelativo en S y S es un semigrupo cancelativo finito. Por lo tanto S es un grupo y resulta también ser un subgrupo de G.
■

Practica 7

Ejercicio 10

> **Ejercicio 10**
> a)
> $G = \{t_{ab} : a \in \mathbb{R} - \{0\}, b \in \mathbb{R}\}$
> $(t_{ab} \circ t_{cd})(x) = t_{ab}(t_{cd}(x)) = t_{ab}(cx + d) = a(cx + d) + b = acx + ad + b = t_{(ac)(ad+b)}(x)$
>
> La composición es cerrada en G.
> Como la composición es asociativa, G es un semigrupo.
>
> Sea $e = t_{1,0}$
> $t_{1,0} \circ t_{ab} = t_{1a,1b+0} = t_{ab}$
> $t_{ab} \circ t_{10} = t_{a1,a0+b} = t_{ab}$
> e es neutro bilatero, G es un monoide.
>
> Dado t_{ab}, defino $(t_{ab})^{-1} = t_{a^{-1}-\frac{b}{a}}$
> $t_{ab}\left(t_{a^{-1},-\frac{b}{a}}\right) = t_{aa^{-1},a-\frac{b}{a}+b} = t_{10}$
> $t_{a^{-1},-\frac{b}{a}}$ es inverso a derecha, como G es monoide también es inverso a izquierda y resulta G grupo.
>
> b)
> Se tiene que los racionales son cerrados bajo sumas y productos, $t_{10} \in H$ y los racionales excluyendo el 0 son cerrados bajo inversos. Luego H es un grupo y la inclusión canónica en G es un homomorfismo de grupos. Por lo tanto $H < G$.
>
> c)
> Sea $f : G \to \mathbb{R} - \{0\}$ definido por:
> $f(t_{ab}) = a$
>
> f esta bien definida y además es un homomorfismo de grupos, en efecto:
> $f(t_{ab} \circ t_{cd}) = f(t_{ac,ad+b}) = ac = f(t_{ab})f(cd)$
>
> Luego $\ker(f) = \{t_{ab} \in G : a = 1\} = N$
>
> De donde resulta que $N \triangleleft G$.
>
> d)
> La función f definida anteriormente es un epimorfismo. En efecto si $a \in \mathbb{R} - \{0\}$ entonces $f(t_{a0}) = a$. Luego por primer teorema del isomorfismo, $G/N \simeq \mathbb{R} - \{0\}$.

Ejercicio 11

> **Ejercicio 11**

Sea $X = \{z \in \mathbb{C} : \exists n \in \mathbb{N}, z^n = 1\}$

Sea $z, w \in X$ y w^{-1} el inverso de z en $\mathbb{C} - \{0\}$. Como $\mathbb{C} - \{0\}$ es un grupo abeliano la potencia es distribuible en la multiplicación.

Sea $n, m \in \mathbb{N}$ tal que $z^n = 1$ y $w^m = 1$. Existen k y k' tal que $kn = \text{mcm}(n, m)$ y $k'm = \text{mcm(n, m)}$.

Entonces $(zw^{-1})^{\text{mcm(n,m)}} = z^{\text{mcm(n,m)}}(w^{-1})^{\text{mcm(n,m)}} = z^{\text{mcm(n,m)}}(w^{\text{mcm(n,m)}})^{-1}$.
$z^{\text{mcm}(n,m)} = z^{kn} = (z^n)^k = 1^k = 1$. De manera analoga se llega a que $w^{\text{mcm}(n,m)} = 1$. Luego $(zw^{-1})^{\text{mcm}(n,m)} = 1$ y $zw^{-1} \in X$.
De donde resulta que $X < \mathbb{C} - \{0\}$.

Sea la función $f : \mathbb{Q} \to X$ definida como:
$f(x) = 1_{\pi x}$,
$1_{\pi x}$ esta representado en forma polar.

f es un homomorfismo de grupos:
$f(x + y) = 1_{2\pi(x+y)} = 1_{2\pi x + 2\pi y} = 1_{2\pi x} \cdot 1_{2\pi y} = f(x)f(y)$

f es un epimorfismo:
Sea $z \in X$, $z \neq 0$ ya que $0 \notin X$. Por lo tanto z tiene representación en forma polar. Sea $z = r_\theta$(donde $r \geq_0$ y $0 \leq \theta < 2\pi$) y n tal que $z^n = 1$. Se tiene que

$z^n = (r_\theta)^n = r^n{}_{n\theta} = 1$, luego:
$r^n = 1 \implies r = 1$, ya que $r \in \mathbb{R}$ y $r > 0$.
$n\theta = 2k\pi$
$\theta = \frac{2k}{n}\pi$

Luego $f(k/n) = 1_{\pi 2k/n} = z$

$\ker(f) = \mathbb{Z}$:
En efecto si $p \in \mathbb{Z}$:
$f(p) = 1_{2\pi p}$
$1_{2\pi p}$ en forma trigonométrica es 1, el neutro de X.

Luego, por primer teorema del isomorfismo:
$X \simeq \mathbb{Q}/\mathbb{Z}$
■

Ejercicio 12

Ejercicio 12
a)
Sea $f : A \times B \to A \times B$ definida como:
$f(a, b) = (e_A, b)$

f es un endomorfismo:
$f((a, b)(c, d)) = f(ac, bd) = (e_A, bd) = (e_A, b)(e_A, d) = f(a, b)f(c, d)$

$\ker(f) = A \times \{e_B\}$
Ya que $f(a, b) = (e_A, e_B) \iff b = e_B$

Por lo tanto, $A \times \{e_B\} \triangleleft A \times B$.
El otro caso es análogo usando el endomorfismo $g(a, b) = (a, e_B)$.

b)
Sea $a \in A, b \in B$, entonces:
$\pi(e_A, b) = b$
$\pi_B(a, e_B) = a$
Por lo tanto π_A y π_B son ambos epimorfismos.

c)
$\pi_A(a,b) = e_a \iff a = e_a$ por unicidad del neutro
$\pi_B(a,b) = e_b \iff b = e_B$, por la misma razón.

d)
Sean $\pi_N : A \to A/N$ y $\pi_M : B \to B/M$.
$\pi_N(a) = aN$
$\pi_M(b) = bM$
las respectivas proyecciones de N y M. Ambas son epimorfismos de grupos.

Luego
$\Pi : A \times B \to (A/N) \times (B/M)$
$\Pi(a,b) = (\pi_N(a), \pi_M(b))$ es también un epimorfismos de grupos(por ser un producto de epimorfismos).

Se tiene que:
$\Pi(a,b) = (N,M) \iff \pi_N(a) = N \wedge \pi_M(b) = M$
por lo tanto $\ker(\Pi) = N \times M$

Por primer teorema del isomorfismo, $(A \times B)/(N \times M) \simeq (A/N) \times (B/M)$

Ejercicio 13

Ejercicio 13
Sea G un grupo de orden infinito:
Si G es cíclico entonces es isomorfo a $\mathbb{Z}$, como $\mathbb{Z}$ tiene un subgrupo propio G también lo tiene.
Si G no es cíclico, basta con tomar un elemento $a \in G$ tal que $a \neq e$ y se tiene que $\langle a \rangle$ es un subgrupo propio de G.

Ejercicio 14

Ejercicio 14
G grupo, $a, b \in G$.
a)
Sea m tal que $a^m = e$.
$\langle a \rangle$ tiene orden finito, por lo que es isomorfo a $Z_{o(a)}$ mediante el isomorfismo:
$f(a^k) = \bar{k}$

$f(e) = \bar{0} = \overline{m} = f(a^m)$
$m \equiv 0 (o(a)) \implies o(a) \mid m$

b)
$o(a) = o(a^{-1})$:
Trivial ya que $\langle a \rangle = \langle a^{-1} \rangle$

Sea $b \in G$ un elemento. La función $f : G \to G$ definida como $f(x) = b^{-1}xb$ es un automorfismo de grupos:

- $f(xy) = b^{-1}xyb = b^{-1}xbb^{-1}yb = (b^{-1}xb)(b^{-1}yb) = f(x)f(y)$. f es un morfismo de grupos.
- $f(x) = f(y) \iff b^{-1}xb = b^{-1}yb$, aplicando cancelativa a ambos lados se tiene que $x = y$. f es un monomorfismo de grupos.
- Sea $a \in G$, $f(bab^{-1}) = b^{-1}(bab^{-1})b = (b^{-1}b)a(b^{-1}b) = eae = a$. f es un epimorfismo de grupos.
  Por lo tanto f es un isomorfismo y en particular es un automorfismo de grupos.

$o(a) = o(b^{-1}ab)$:
Por inducción, $(b^{-1}ab)^n = b^{-1}a^nb$
Si $n = 0 \implies e = (b^{-1}ab)^0$ y $b^{-1}a^0b = b^{-1}b = e$
Suponiendo que vale para n, entonces $(b^{-1}ab)^{n+1} = b^{-1}ab(b^{-1}ab)^n = b^{-1}abb^{-1}a^nb = b^{-1}aa^nb = b^{-1}a^nb$
Luego $f(x) = b^{-1}xb$ es un isomorfismo de $\langle a \rangle$ a $\langle b^{-1}ab \rangle$

$o(ab) = o(ba)$:
Sea $f(x) = a^{-1}xa$
$f((ab)^n) = (ba)^n$
Por inducción:
Si $n = 0$, vale porque f es un endomorfismo.
Para $n + 1$:
$f((ab)^{n+1}) = f((ab)(ab)^n) = f(ab)f((ab)^n)$
$f(ab) = a^{-1}(ab)a = (a^{-1}a)ba = ba$
Aplicando la igualdad anterior y la HI.
$f((ab)^{n+1}) = ba(ba)^n = (ba)^{n+1}$.
Luego como f es biyectiva, los cardinales de $\langle ab \rangle$ y $\langle ba \rangle$ coinciden.

Ejercicio 15

Ejercicio 15

Primer intento

p primo, $p \nmid a$, probar que $n \equiv r(p-1) \implies a^n \equiv a^r(p)$

Como $p \nmid a$ y p es primo, $\gcd(p, a) = 1$ y $[a]$ es un generador de $\mathbb{Z}_p$:

Luego la función:
$f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$
$f([n]) = [a^n]$

Es una función bien definida(¿¿??), de donde sale que:
$n \equiv r(p-1)$
$\implies$
$[n] = [r]$(en $\mathbb{Z}_{p-1}$)
$\implies$
$f([n]) = f([r])$
$\implies$
$[a^n] = [a^r]$(en $\mathbb{Z}_p$)
$\implies$
$a^n \equiv a^r(p)$

En particular, $n \equiv r_{p-1}(n)(p-1)$. De donde sale que $a^n \equiv a^{r_{p-1}(n)}(p)$

Demostración alternativa

Como p es primo, sea x tal que $p \nmid x$(ie, $\gcd(p, x) = 1$), por identidad de Benzout existen $y, k \in \mathbb{Z}$ tal que:
$xy + kp = 1$
$\implies$
$xy - 1 = kp$
$\implies$
$xy \equiv 1(p)$

Por lo tanto $\mathbb{Z}_p$ es un grupo bajo la multiplicación si se excluyen los múltiplos de p(la asociatividad se hereda y el neutro es 1). Denoto por $\mathbb{Z}_p^*$ a dicho grupo.

Como $p \nmid a$, $a \in \mathbb{Z}_p^*$. $\langle a \rangle$ es entonces un subgrupo de $\mathbb{Z}_p^*$:
$o(\mathbb{Z}_p^*) = p - 1$(no esta $\bar{0}$) y por teorema de Lagrange $o(a) \mid p - 1$ o, lo que es equivalente, $\exists k \in \mathbb{Z} : o(a)k = p - 1$

Como $n \equiv r(p-1)$, se tiene que $\exists k' \in \mathbb{Z} : (n - r) = k'(p-1) = k'o(a)k$
Esto quiere decir que $n \equiv r(o(a))$

Y por lo tanto
$[a]^n = [a]^r$

$\implies$
$[a^n] = [a^r]$
$\implies$
$a^n \equiv a^r (p)$
■

Ejercicio 16

Ejercicio 16

16. Una matriz siempre satisface su polinomio característico, esto es, si:
    $p_A(\lambda) = \det(\lambda I - A)$
    Entonces $p_A(A) = 0$.

Aplico con las matrices del ejemplo
$p_A(\lambda) = \det \begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} = \lambda^2 + I$
$p_B(\lambda) = \det \begin{pmatrix} \lambda & -1 \\ 1 & \lambda + 1 \end{pmatrix} = \lambda(\lambda + 1) + 1 = \lambda^2 + \lambda + I$

Entonces:

$p_A(A) = A^2 + I = 0 \implies A^2 = -I \implies A^4 = I$
$p_B(B) = B^2 + B + I = 0 \implies B^2 + B = -I$

$B^2 = -I - B$
$B^3 = (-I - B)B = -B - B^2 = -(B^2 + B) = - - I = I$

Luego A y B tienen orden 4 y 3 respectivamente.

El caso de:
$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
Se hace por inducción y coso.

Ejercicio 2

Ejercicio 2

a)
Sea $H = \langle (2,1,3) \rangle$ y sean $f, g \in S_3$(es decir, f y g son biyecciones de $\{1,2,3\}$ en si mismo). Probar que $fH \neq Hg$(excepto para el caso donde $f = g = \mathrm{Id}$).

Si $f, g \in H$ tal que $fH = Hg$, entonces $\forall h \in H$:
$fh = hg$, en particular para $h = e$ se tiene que $f = g$

$h^0 = (1,2,3)$
$h^1 = (2,1,3)$
$h^2 = (1,2,3)$

Por lo tanto, $H = \{(1,2,3), (2,1,3)\}$

$\mathrm{Id} = f^{-1} g \implies f = g$
$f(2,1,3) = (2,1,3)f$

Como $o(G) = 3! = 6$ y $o(H) = 2$, hay un total de 3 clases a izquierda y derecha diferentes.

1. El mismo conjunto H
2. $(3,2,1)H = \{(3,2,1), (2,3,1)\}$, $H(3,2,1) = \{(3,2,1), (3,1,2)\}$. Las coclases son diferentes.
3. $(1,3,2)H = \{(1,3,2), (3,1,2)\}$, $H(1,3,2) = \{(1,3,2), (2,3,1)\}$. Las coclases son diferentes.
   Por lo tanto, solo hay una coclase a derecha que es una coclase a izquierda, el conjunto H.

b)
Como $\mathrm{Id} \in H$, se cumple que $\forall a \in S_3$:
$a\,\mathrm{Id} = a = \mathrm{Id}\,a$
Por lo tanto la intersección de las coclases no es vacía.

Para que la intersección sea vacía tiene que cumplirse que $a(2,1,3) = (2,1,3)a$. Esto se cumple, por ejemplo, para $a = (3,2,1)$ o $a = (1,3,2)$(se puede ver esto analizando las coclases del ejemplo anterior).

c)
$H = \langle (2,3,1) \rangle$
$O(G) = 3! = 2 \cdot 3$, por lo tanto $O(H) = 3$ o $O(H) = 2$

$h^0 = (1,2,3)$
$h^1 = (2,3,1)$
$h^2 = (3,1,2)$

$O(H) = 3$, hay un total de 2 coclases a izquierda o derecha

1 es la misma clase H y otra esta dada por:
Las otras son
$(3,1,2)H = \{(3,1,2),(1,2,3),(2,3,1)\}$
$H(3,1,2) = \{(3,1,2),(1,2,3),(2,3,1)\}$

Luego todas las coclases a derecha coinciden con las coclases a izquierda y H es un subgrupo normal.

d)
Un grupo ciclico, es en particular, un grupo abeliano, pero S_n no es abeliano.
Sean f y g las funciones:
$$f(n) = \begin{cases} 2 & n = 1 \\ 1 & n = 2 \\ n & \text{en cualquier otro caso} \end{cases}$$
$$g(n) = \begin{cases} 3 & n = 2 \\ 2 & n = 3 \\ n & \text{en cualquier otro caso} \end{cases}$$

f y g son ambas funciones biyectivas.

$f(g(2)) = f(3) = 3$
$g(f(2)) = g(1) = 1$
$fg \neq gf$, S_n no es abeliano y por lo tanto no es ciclico.

Ejercicio 3

Ejercicio 3
FALSO
Sean $f = (3,2,1,4)$ y $g = (1,2,4,3)$

$g^{-1} = (1,2,4,3) = g$

$fg = (3,2,4,1)$
$g^{-1}(fg) = (4,2,3,1)$

Como $g^{-1}fg(4) \neq 4$, El conjunto $\{f \in S_4 : f(4) = 4\}$ NO es un subgrupo normal de G.

Ejercicio 4

Ejercicio 4
a)
Como N y K son subgrupos de G, su intersección es a su vez un subgrupo y por estar sus elementos contenidos en K, $N \cap K < K$.

$\forall a \in K, n \in N \cap K$:

- $ana^{-1} \in N$, ya que $n \in N$, $a \in G$ y N es normal en G.
- $ana^{-1} \in K$, ya que $n \in K$ y $a \in K$.

Luego $ana^{-1} \in N \cap K$ y resulta $N \cap K$ normal en K.

b)
$knk^{-1} \in N$, para cualquier $k \in K$ por ser N normal en G
Además
$(knk^{-1})n^{-1} \in N$

Como K es normal en G, $nkn^{-1} \in K$ para cualquier $n \in N$ y siguiendo un razonamiento análogo al anterior $nkn^{-1}k^{-1} \in K$

$(knk^{-1})n^{-1} = kn(k^{-1}n^{-1}) = kn(nk)^{-1}$
El inverso de este elemento es:
$(kn(nk)^{-1})^{-1} = nk(kn)^{-1} = nkn^{-1}k^{-1} \in N$

Por lo tanto, $nkn^{-1}k^{-1} \in N \cap K$, pero $N \cap K = \{e\}$. Asi que:
$nkn^{-1}k^{-1} = e$
$\implies$
$nk = kn$

c)
PENDIENTE

Ejercicio 5

Ejercicio 5
a)
Sean N_1 y N_2 subgrupos normales de G

Sea $n \in N_1 \cap N_2$:

- Como $N_1 \triangleleft G$: $\forall a \in G : ana^{-1} \in N_1$
- Como $N_2 \triangleleft G : \forall a \in G : ana^{-1} \in N_2$

Luego $ana^{-1} \in N_1 \cap N_2$ y $N_1 \cap N_2 \triangleleft G$.

b)
Sean $n_1 \in N_1$ y $n_2 \in N2$
$n_1n_2n_1^{-1} \in N_2$
$\implies$
$n_1n_2n_1^{-1}n_2^{-1} \in N_2$
$\implies$ (aplico inverso)
$n_2n_1n_2^{-1}n_1^{-1} \in N_2$

$n_2n_1n_2^{-1} \in N_1$
$\implies$
$n_2n_1n_2^{-1}n_1^{-1} \in N_2$

Luego $n_2n_1n_2^{-1}n_1^{-1} \in N_1 \cap N_2$, pero si eso pasa entonces:
$n_2n_1n_2^{-1}n_1^{-1} = e$
De donde sale que:
$n_2n_1 = n_1n_2$

Ejercicio 8

Ejercicio 8

Sea $m, n \in \mathbb{N}$ con $m \mid n$ y $H = \langle \bar{n} \rangle \in \mathbb{Z}_m$, probar que $\mathbb{Z}_m / H \cong \mathbb{Z}_n$

$\mathbb{Z}_m$ y $\mathbb{Z}_n$ son subgrupos normales de $\mathbb{Z}$, por lo tanto la operación de $\mathbb{Z}$ se induce a $\mathbb{Z}_m$ y $\mathbb{Z}_n$

$f : \mathbb{Z}_m \to \mathbb{Z}_n$
$f([x]_m) = [x]_n$

f bien definido:
Sean x, y tal que:
$x \equiv y(m)$
$x - y = km$, con $k \in \mathbb{Z}$
$x - y = k(np) = (kp)n$, donde $p = m/n$
Luego $x \equiv y(n)$ y $f([x]_m) = f([x]_n)$

f morfi de grupos:
$f([x]_m + [y]_m) = f([x + y]_m) = [x + y]_n = [x]_n + [y]_n = f([x]_m) f([y]_m)$

f epimorfismo:
$\mathbb{Z}_n$ es ciclico, luego sea $[k]_n = k[1]_n$
$f(k[1]_m) = kf([1]_m) = k[1]_n = [k]_n$

$\ker f = H$:
Por inducción en k para los elementos $k\bar{n}$:
$f([n]_m) = [n]_n = [e]_n$
$f((k+1)[n]_m) = f(k[n]_m + [n]_m) = f(k[n]_m) + f([n]_m) = [e]_n + [e]_n = [e]_n$

Por primer teorema del isomorfismo, $\mathbb{Z}_m / H \cong \mathbb{Z}_n$

Alternativa:
Por teorema de Lagrange:
$m = o(\mathbb{Z}_m) = [\mathbb{Z}_m : H] o(H) = o(\mathbb{Z}_m / H)(m/n)$
Luego:
$o(\mathbb{Z}_m / H) = m/(m/n) = n$

$\mathbb{Z}_m / H$ es un grupo cíclico:

Entonces $\mathbb{Z}_m / H \cong \mathbb{Z}_n$

Ejercicio 9

Ejercicio 9
a)
$Z(G)$ es un subgrupo de G:

- $a, b \in Z(G), c \in G \implies c(ab) = acb = abc = (ab)c$
- $e \in Z(G), \forall c \in G : ce = c = ec$
- $a \in Z(G), b \in G \implies a^{-1}g = (g^{-1}a)^{-1}) = (ag^{-1})^{-1} = ga^{-1}$

Si $n \in Z(G)$ entonces $\forall a \in G$
$ana^{-1} = naa^{-1} = ne = n \in Z(G)$
Por lo tanto $Z(G) \triangleleft G$

Alternativamente:

b)
Sean $f \in Z(S_n)$ y suponiendo que $n \geq 3$,

Si $f \neq \mathrm{Id}$, $\exists x : x \neq f(x)$
Sea $y \notin \{x, f(x)\}$.

Defino:
$f'(x) = y$
$f'(y) = x$
$f'(n) = n$, si $n \neq x$ y $n \neq y$

f' es biyectiva.

Entonces:
$f(f'(x)) = f(y)$
$f'(f(x)) = f(x)$, por ser $f(x) \neq x$ y $f(x) \neq y$.

$f(y) = f(x) \iff x \neq y$ por ser f biyectiva. Por lo tanto $ff' \neq f'f$ y $f \notin Z(S_n)$.

d)

Sea $\bar{a} \in Z(G/Z(G))$, $\bar{b} \in G/Z(G)$, tiene que pasar que $\bar{a} = Z(G)$ o $G/Z(G)$ es abeliano.

$\bar{a}\bar{b}$
$=$
$\overline{ab}$
$=$
$abZ(G)$

Pero
$\bar{b}\bar{a}$
$=$

Practica 8

Ejercicio 11

> **Ejercicio 11**
> a)
> Sean P y P' posets y $F : \mathscr{C}_P \to \mathscr{C}_{P'}$ un funtor entre sus categorías asociadas.
> Considerar la función $f : P \to P'$ tal que $f(x) = F(x)$(el funtor aplicado a los objetos).
>
> Suponiendo que $x, y \in P$ y $x \preceq_P y$, se tiene que $(x, y) \in \operatorname{mor} \mathscr{C}_P$. Por la primera ley de los funtores, $(f(x), f(y)) \in \operatorname{mor} \mathscr{C}_{P'}$ y se tiene que $f(x) \preceq_{P'} f(y)$. Por lo tanto f es un morfi de orden.
>
> b)
> Suponiendo M y M' monoides y $F : \mathscr{C}_M \to \mathscr{C}_{M'}$ un funtor entre sus categorías asociadas. Considerar la función $f : M \to M'$ tal que $f(x) = F(x)$(el funtor aplicado a los monoides).
>
> Por la segunda ley de los funtores, $f(e_M) = F(e_M) = e_{M'}$.
> $a, b \in M \implies a, b \in \operatorname{mor} \mathscr{C}_M$
> Por la tercera ley de los funtores
> $f(ab) = F(a \circ b) = F(a) \circ F(b) = f(a)f(b)$
> Por lo tanto, f es morfi de monoides.

Ejercicio 12

> **Ejercicio 12**
> Sea $F : \operatorname{Rel} \to \operatorname{Rel}^{\operatorname{op}}$ tal que:
> $F(A) = A$, $\forall A \in ob\operatorname{Rel}$
> $F(\mathcal{R}) = \mathcal{R}^{-1}$, $\forall \mathcal{R} \in \operatorname{mor} \operatorname{Rel}$
>
> F es un funtor:
> Cumple la ley 1)
> Si $\mathcal{R} \in \operatorname{Hom}(A, B) \implies F(\mathcal{R}) = \mathcal{R}^{-1} \in \operatorname{Hom}(B, A) = \operatorname{Hom}^{\operatorname{op}}(F(A), F(B))$
> Cumple la ley 2), esto es así ya que $F(\operatorname{Id}) = \operatorname{Id}$
> Cumple la ley 3), esto es así ya que para dos relaciones $\mathcal{R}$ y $\mathcal{S}$: $F(\mathcal{R} \circ \mathcal{S}) = (\mathcal{R} \circ \mathcal{S})^{-1} = \mathcal{S}^{-1} \circ \mathcal{R}^{-1} = F(\mathcal{R}) \circ^{\operatorname{op}} F(\mathcal{S})$
>
> Por lo tanto, F es un funtor. Además F cumple que:
> $F(F(A)) = A$, $\forall A \in \operatorname{ob} \operatorname{Rel}$
> $F(F(\mathcal{R})) = \mathcal{R}$, $\forall \mathcal{R} \in \operatorname{mor} \operatorname{Rel}$
>
> Por lo tanto F es un isomorfismo de categorías.

Ejercicio 13

> **Ejercicio 13**
> a) Si f y g monos entonces $g \circ f$ es mono
> Sean a, b morfis de la categoría
> $(g \circ f) \circ a = (g \circ f) \circ b$
> $\implies$
> $g \circ (f \circ a) = g \circ (f \circ b)$
> $\implies$ (g mono)

$f \circ a = f \circ b$
$\implies$
$a = b$

$g \circ f$ mono

b)
$g \circ f$ mono, f es mono
Sean a, b morfis
$f \circ a = f \circ b$
$\implies$
$g \circ (f \circ a) = g \circ (f \circ b)$
$\implies$
$(g \circ f) \circ a = (g \circ f) \circ b$
$\implies$
$a = b$

f mono

c)
f y g epis, $g \circ f$ epi
Sean a, b morfis
$a \circ (g \circ f) = b \circ (g \circ f)$
$\implies$
$(a \circ g) \circ f = (b \circ g) \circ f$
$\implies$
$a \circ g = b \circ g$
$\implies$
$a = b$

$g \circ f$ epi

d)
$g \circ f$ epi, g epi
Sean a, b morfis
$a \circ g = b \circ g$
$\implies$
$(a \circ g) \circ f = (b \circ g) \circ f$
$\implies$
$a \circ (g \circ f) = b \circ (g \circ f)$
$\implies$
$a = b$

g epi

e)
$(f^{-1} \circ g^{-1}) \circ (g \circ f)$
$=$
$f^{-1} \circ (g^{-1} \circ g) \circ f$
$=$
$f^{-1} \circ \mathrm{Id} \circ f$
$=$
$f^{-1} \circ f$
$=$
Id
La reversa es analoga.