TP5 – Estructuras Algebraicas - Teoría de Grupos

Agustina Sol Rojas

Ejercicio 1.

Determinar cuáles de las siguientes operaciones están bien definidas sobre el conjunto A dado. Analizar las propiedades en los casos afirmativos

a) $A = N, a * b = 3ab$

Dado que el producto es una operación cerrada en N, para todo $a, b \in N$, se cumple que $ab \in N$. Además, como $3 \in N$, al multiplicarlo por otro número natural (nuevamente porque el producto es una operación cerrada) el resultado sigue siendo un número natural. Por lo tanto, la operación $a * b = 3ab$ está bien definida en N.

Conmutativa:
Como el producto es conmutativo en N se cumple para todo $a, b \in N$ que $a * b = 3ab = 3ba = b * a$

Asociativa:
Como el producto es asociativo y conmutativo en N se cumple para todo $a, b, c \in N$ que $(a * b) * c = (3ab) * c = 3(3ab)c = 3a(3bc) = a * (3bc) = a * (b * c)$

Elemento neutro:
Se debe probar que existe en N un elemento e tal que para todo a en N valga que $a * e = e * a = a$:

1. Teniendo en cuenta lo siguiente:
    i. $a * e = 3ae$
    ii. $e * a = 3ea$
2. Se debe encontrar un $e \in N$ tal que
    i. $3ae = a$

ii. $3ea = a$

3. Despejando las ecuaciones queda:
   i. $3e = 1$
   ii. $3e = 1$
4. Como ningún número natural multiplicado por 3 da como resultado 1, no existe un $e \in N$ tal que $a * e = e * a = a$. Por lo tanto * no tiene un elemento neutro.

Elemento inverso:

Como * no tiene elemento neutro, no tiene elemento inverso.

b) $A = Z, a * b = \frac{a+b}{3+ab}$

Contraejemplo:

1. Dados $a, b \in Z$ tal que $a = -3$ y $b = 1$:

$$-3 * 1 = \frac{-3+1}{3+(-3).1} = -\frac{2}{3-3} = \frac{2}{0}$$

2. $\frac{2}{0} \notin Z$, por lo tanto la operación $a * b$ no está bien definida en Z.

c) $A = R, x * y = x + y - xy$

Dado que la suma y el producto son operaciones cerradas en N, para todo $x, y \in R$, se cumple que $x + y - xy \in N$. Por lo tanto, la operación $x * y = x + y - xy$ está bien definida en R.

Conmutativa:

Como el producto es conmutativo en R se cumple para todo $x, y \in R$ que $x * y = x + y - xy = y + x - yx = y * x$

Asociativa:

Como la suma y producto son asociativos y conmutativos en R, y además se cumple la propiedad distributiva se cumple para todo $x, y, z \in R$ que

$$x * (y * z) = x * (y + z - yz) =$$
$$= x + (y + z - yz) - x(y + z - yz) =$$
$$= x + y + z - yz - xy - xz + xyz =$$

$= x + y - xy + z - xz - yz + xyz =$

$= (x + y - xy) + z - (xz + yz - xyz) =$

$= (x + y - xy) + z - (x + y - xy)z$

$= (x + y - xy) * z = (x * y) * z$

Elemento neutro:

Se debe probar que existe en R un elemento e tal que para todo x en R valga que $x * e = e * x = x$:

1. Teniendo en cuenta lo siguiente:
    i. $x * e = x + e - xe$
    ii. $e * x = e + x - ex$
2. Se debe encontrar un $e \in N$ tal que
    i. $x + e - xe = x$
    ii. $e + x - ex = x$
3. Despejando las ecuaciones queda:
    i. $x + e - xe = x$
    $e - ex = 0$
    $e(1 - x) = 0$
    $e = 0$
    ii. $e + x - ex = x$
    $e - ex = 0$
    $e(1 - x) = 0$
    $e = 0$
4. Reemplazando en la expresión de 2. por e verificamos que se cumple lo siguiente para cualquier $x \in R$
    i. $x + 0 - x.0 = x + 0 = x$
    ii. $0 + x - 0.x = 0 + x = x$
5. Por lo tanto existe en R un elemento e tal que para todo x en R vale que $x * e = e * x = x$ y ese $e = 0$

Elemento inverso:

Un elemento x de R se tiene inverso si existe x' en R tal que $x * x' = x' * x = e$

1. Teniendo en cuenta lo siguiente
    i. $x * x' = x + x' - x\,.\,x'$
    ii. $x' * x = x' + x - x'.\,x$

2. Se debe encontrar un $e \in N$ tal que
    i. $x + x' - x \,.\, x' = e$
    ii. $x' + x - x' .\, x = e$
3. Despejando las ecuaciones y teniendo en cuenta que $e = 0$ queda:
    i. $x + x' - x \,.\, x' = 0$

    $x' - x \,.\, x' = -x$

    $x'(1 - x) = -x$

    $x' = \frac{-x}{1-x}$

    ii. $x' + x - x' .\, x = 0$

    $x' - x' . x = -x$

    $x'(1 - x) = -x$

    $x' = \frac{-x}{1-x}$
4. El inverso existe y es $\frac{-x}{1-x}$ para todo $x \neq 1 \in R$. Cuando $x = 1$ el denominador se hace cero y la expresión no puede resolverse, por lo que no existe inverso para $x = 1$.
    i. Esto último es válido.

d) $A = \{0, 1, 2, 3\}$

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	1	2	0	2
3	2	3	1	1

Se puede observar en el cuadro que para todo $a, b \in A$ se cumple que el resultado de $a * b \in A$.

<u>Conmutativa</u>:

La operación * sobre A es conmutativa si, para todo a y b en A, resulta $a * b = b * a$

Contraejemplo:

$2 * 0 = 1$

$0 * 2 = 0$

Se puede observar como $2 * 0 \neq 0 * 2$, por lo tanto, no es conmutativa.

Asociativa:

La operación * sobre A es asociativa si, cualesquiera sean a, b y c en A, resulta $a * (b * c) = (a * b) * c$

Contraejemplo:

$(3 * 3) * 1 = 1 * 1 = 1$

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

Se puede observar como $(3 * 3) * 1 \neq 3 * (3 * 2)$, por lo tanto, no es asociativa.

Elemento neutro:

Existe en A un elemento e tal que para todo x en R vale que $x * e = e * x = x$. Se puede observar en el grafico que ese elemento es 1, puesto que para todo $x \in A$ vale que $x * 1 = 1 * x = x$

Elemento inverso:

Un elemento x de R se tiene inverso si existe x' en R tal que $x * x' = x' * x = e$

1. $x = 0$

   0 no tiene inverso puesto que nunca sucede que para cualquier $x' \in A$ vale que $0 * x' = x' * 0 = 1$
2. $x = 1$

   1 tiene inverso y ese es 1 dado que $1 * 1 = 1 * 1 = 1$
3. $x = 2$

   0 no tiene inverso puesto que nunca sucede que para cualquier $x' \in A$ vale que $2 * x' = x' * 2 = 1$

   $2 * 0 = 1$, pero $0 * 2 = 0$.

   $3 * 2 = 1$, pero $2 * 3 = 2$
4. $x = 3$

   3 tiene inverso y ese es 3 dado que $3 * 3 = 3 * 3 = 1$

Ejercicio 2.

Demostrar que:

a) Dado $M = \{m \in N : m > 0\}, (M, +)$ es un semigrupo pero no es un monoide

Asociativa:

La operación $+$ sobre M es asociativa si, cualesquiera sean a, b y c en A, resulta $a + (b + c) = (a + b) + c$.

Como la operación $+$ es asociativa en N, $(N, +)$ es un semigrupo. Debido a que $M \subset N$, por definición 2.7, $(M, +)$ es un semigrupo (se puede pensar como que la asociatividad se "hereda" de N).

Elemento neutro

No existe en M un elemento e tal que para todo a en M vale que $a * e = e * a = a$.

El elemento neutro de $(N, +)$ es el 0 y este es único. Por definición del conjunto M, $0 \notin M$ por lo tanto no existe un elemento neutro para la operación $+$ sobre el conjunto M.

Como no existe en M elemento neutro para $+$, $(M, +)$ no es un monoide.

b) El conjunto de un solo elemento $M = \{e\}$ con la operación definida por $e * e = e$ es un monoide

Asociativa

La operación $*$ sobre M es asociativa si, cualesquiera sean a, b y c en M, resulta $a * (b * c) = (a * b) * c$

1. Sean a, b y $c \in M$
   i. $a * (b * c) = a * e = e$
   ii. $(a * b) * c = e * c = e$
2. Como $a * (b * c) = (a * b) * c$, la operación $*$ sobre M es asociativa

Elemento neutro:

Se debe demostrar que existe en M un elemento e tal que para todo a en M valga que $a * e = e * a = a$.

1. Sea $a \in M$
   i. $a * e = e$

ii. $e * a = e$

2. Como $a \in M$ y el unico elemento de M es e, necesariamente $a = e$
3. Por lo tanto existe en M un elemento neutro para $*$

Como $*$ es asociativa y existe un elemento neutro, $(M,*)$ es un monoide.

c) Dado un conjunto no vacío A, el conjunto de las partes de A $P(A)$ con la operación intersección de conjuntos es un monoide conmutativo

Asociativa:

La operación $\cap$ sobre $P(A)$ es asociativa si, cualesquiera sean X, Y y Z en $P(A)$, resulta $X \cap (Y \cap Z) = (X \cap Y) \cap Z$

1. Sean $X, Y, Z \in P(A)$, como la $\cap$ entre conjuntos es asociativa se cumple que $X \cap (Y \cap Z) = (X \cap Y) \cap Z$

Elemento neutro:

Se debe demostrar que existe en $P(A)$ un elemento E tal que para todo X en $P(A)$ valga que $X \cap E = E \cap X = X$.

1. Sea X un elemento cualquiera de $P(A)$. Para que se cumpla $X \cap E = E \cap X = X$, a E deben pertenecer los mismos elementos que pertenecen a X. Los únicos conjuntos que cumplen con esto son el propio X y A. Si se toma como elemento neutro a X siendo X cualquier elemento de $P(A)$, este no va a ser único, puesto que va a haber un elemento neutro distinto para cada elemento de $P(A)$ por lo que se toma como elemento neutro a A.
2. Para cualquier $X \in P(A)$, al ser $X \subseteq A$ se cumple que:
   i. $X \cap A = X$
      a. La intersección entre un conjunto y su subconjunto da el subconjunto.
   ii. $A \cap X = X$
      a. La intersección entre un conjunto y su subconjunto da el subconjunto.

Conmutativa

La operación ∩ sobre $P(A)$ es conmutativa si, cualesquiera sean X y Y en $P(A)$, resulta $X \cap Y = Y \cap X$

1. Sean $X, Y \in P(A)$, como la ∩ entre conjuntos es conmutativa se cumple que $X \cap Y = Y \cap X$

Como ∩ es asociativa, existe un elemento neutro y es conmutativa $(P(A),\cap)$ es un monoide conmutativo.

Ejercicio 3.

Demostrar que si para una operación asociativa $*$ en A existe un elemento neutro e un elemento del conjunto, a, tiene inverso entonces este es único.

1. Sean $a, b, c \in A$, suponiendo que $b \neq c$ y ambos son inversos de a se cumple:
   i. $a * b = b * a = e$
   ii. $a * c = c * a = e$.
2. Como e es el elemento neutro del conjunto se cumple:
   i. $b = b * e$
3. Como por 1.i. $e = a * c$:
   i. $b * e = b * (a * c)$
4. Por asociatividad:
   i. $b * (a * c) = (b * a) * c$
5. Por hipótesis $(b * a) = e$
   i. $(b * a) * c = e * c$
6. Como e es el elemento neutro del conjunto se cumple:
   i. $e * c = c$
7. Se llego a que $b = c$, por lo tanto si para una operación asociativa $*$ en A existe un elemento neutro e un elemento del conjunto y a tiene inverso entonces este es único.

Ejercicio 4.

Sea R una relación de congruencia sobre un semigrupo $(S,*)$ demostrar que $(S/R,\circledast)$ (el conjunto cociente y la operación inducida por $*$ sobre las clases de equivalencia) es un semigrupo llamado Semigrupo Cociente

1. Teniendo en cuenta que $S/R = \{\bar{s} \in S\}$ y siendo $a, b \in S$, $\bar{a} \in S/R$ y $\bar{b} \in S/R$
   i. $\bar{a} \circledast \bar{b} = \overline{a * b}$
2. $\circledast$ es una operación bien definida puesto que al ser $(S,*)$ un semigrupo, $a * b \in$ S, y por lo tanto $\overline{a * b} \in S/R$.
3. $\circledast$ es asociativa. Sean $\bar{a}, \bar{b}, \bar{c} \in S/R$ y teniendo en cuenta que $(S,*)$ es un semigrupo (asociatividad de *):
   i. $\bar{a} \circledast (\bar{b} \circledast \bar{c}) = \bar{a} \circledast (\overline{b * c}) = \overline{a * (b * c)} = \overline{(a * b) * c} = (\overline{a * b}) \circledast \bar{c} = (\bar{a} \circledast \bar{b}) \circledast \bar{c}$
   ii. Como se llega a que $\bar{a} \circledast (\bar{b} \circledast \bar{c}) = (\bar{a} \circledast \bar{b}) \circledast \bar{c}$, $\circledast$ es asociativa.
4. Como $\circledast$ es una operación bien definida y $\circledast$ es asociativa, $(S/R,\circledast)$ es un semigrupo llamado Semigrupo Cociente.

Ejercicio 5.

Analizar si las siguientes son estructuras de grupo:

a) $(Z, +)$, los enteros con la suma usual

Asociativa:
La operación $+$ sobre Z es asociativa ya que para cualesquiera sean a, b y c en Z, se cumple que $a + (b + c) = (a + b) + c$.

Elemento neutro:
Existe en Z un elemento e tal que para todo a en Z vale que $a + e = e + a = a$ y ese $e = 0$.

Elemento inverso:
Para todo elemento a de Z existe a' en Z tal que $a + a' = a' + a = e$ y ese $a' = -a$

Como $+$ es asociativa, existe un elemento neutro y todos los elementos de Z tienen un inverso $(Z, +)$ es un grupo.

b) $(Z,\cdot)$, los enteros con el producto usual

Asociativa:

La operación $\cdot$ sobre Z es asociativa ya que para cualesquiera sean a, b y c en Z, se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Elemento neutro:

Existe en Z un elemento e tal que para todo a en Z vale que $a \cdot e = e \cdot a = a$ y ese $e = 1$.

Elemento inverso:

No se cumple que para todo elemento a de Z existe a' en Z tal que $a \cdot a' = a' \cdot a = 1$. Esto solamente se cumple para $a = 1$ y $a = -1$.

Contraejemplo:

Sea $a \in Z$ con $a = 2$, no existe ningún $a' \in Z$ tal que $2 \cdot a' = a' \cdot 2 = 1$. Por lo tanto no se cumple que para todo elemento a de Z existe a' en Z tal que $a \cdot a' = a' \cdot a = 1$.

Como no todos los elementos de Z tienen un inverso $(Z, \cdot)$ no es un grupo.

c) $(R^2, +)$, los pares ordenados de reales con la suma usual

Asociativa:

La operación $+$ sobre R^2 es asociativa ya que para cualesquiera sean a, b y c en R^2, se cumple que $a + (b + c) = (a + b) + c$. Esto sucede debido a que la operación $+$ es asociativa en R.

Demostración:

1. Sean a, b y $c \in R^2$, con $a = (a_1, a_2)$, $b = (b_1, b_2)$, $c = (c_1, c_2)$. Dado a que la operación $+$ es asociativa en R se cumple que:

$$a + (b + c) = (a_1, a_2) + \big((b_1, b_2) + (c_1, c_2)\big) = \big(a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)\big)$$
$$= \big((a_1 + b_1) + c_1, (a_2 + b_2) + c_2\big) = \big((a_1, a_2) + (b_1, b_2)\big) + (c_1, c_2)$$
$$= (a + b) + c$$

Elemento neutro:

Existe en Z un elemento e tal que para todo a en Z vale que $a + e = e + a = a$ y ese $e = (0,0)$.

Demostración:

1. Sea $a \in R^2$, con $a = (a_1, a_2)$. Dado a que el elemento neutro para la operación $+$ en R es 0 se cumple que:
   i. $a + e = (a_1, a_2) + (0,0) = (a_1 + 0, a_2 + 0) = (a_1, a_2)$
   ii. $e + a = (0,0) + (a_1, a_2) = (0 + a_1, 0 + a_2) = (a_1, a_2)$

Elemento inverso:

Para todo elemento a de Z existe a' en Z tal que $a + a' = a' + a = e$ y ese $a' = -a$

Demostración:

1. Sea $a \in R^2$, con $a = (a_1, a_2)$ y $-a = (-a_1, -a_2)$. Dado a que para todo elemento $x \in R$ se verifica que $x + (-x) = 0$ se cumple que:
   i. $a + (-a) = (a_1, a_2) + (-a_1, -a_2) = (a_1 + (-a_1), a_2 + (-a_2)) = (0,0)$
   ii. $-a + a = (-a_1, -a_2) + (a_1, a_2) = (-a_1 + a_1, -a_2 + a_2) = (0,0)$

Como $+$ es asociativa, existe un elemento neutro y todos los elementos de R^2 tienen un inverso $(R^2, +)$ es un grupo.

d) $(M_{2x2}, +)$, las matrices de 2x2 con la suma usual de matrices

Asociativa:

La operación $+$ sobre M_{2x2} es asociativa ya que para cualesquiera sean a, b y c en M_{2x2}, se cumple que $a + (b + c) = (a + b) + c$. Esto sucede debido a que la operación $+$ es asociativa en R.

Elemento neutro:

Existe en M_{2x2} un elemento e tal que para todo a en M_{2x2} vale que $a + e = e + a = a$ y ese $e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Esto se cumple debido a que el elemento neutro para la operación $+$ en R es 0.

Elemento inverso:

Para todo elemento $a = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ de M_{2x2} existe a' en M_{2x2} tal que $a + a' = a' + a = e$ y ese $a' = -a$ siendo $-a = \begin{pmatrix} -a_1 & -a_2 \\ -a_3 & -a_4 \end{pmatrix}$. Esto sucede dado que para todo elemento $x \in R$ se verifica que $x + (-x) = 0$.

Como $+$ es asociativa, existe un elemento neutro y todos los elementos de M_{2x2} tienen un inverso $(M_{2x2}, +)$ es un grupo.

e) $(P(A),\cup)$, A cualquier conjunto y $P(A)$ indica el conjunto de partes de A

Asociativa:

La operación $\cup$ sobre $P(A)$ es asociativa ya que para cualesquiera sean X, Y y Z en Z, se cumple que $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.

Elemento neutro:

Existe en $P(A)$ un elemento E tal que para todo X en $P(A)$ vale que $X \cup E = E \cup X = X$ y ese $E = \emptyset$.

Elemento inverso:

No se cumple que para todo elemento X de $P(A)$ existe X' en $P(A)$ tal que $X \cup X' = X \cup X' = \emptyset$. Nunca sucede que la unión de un conjunto con otro del vacío, salvo que ambos conjuntos sean el vacío.

Como no todos los elementos de $P(A)$ tienen un inverso $(P(A),\cup)$ no es un grupo.

Ejercicio 6.

Probar que en todo Grupo el único elemento idempotente es el neutro

1. Existe un elemento $a \in G$, siendo $(G,*)$ un grupo, tal que a es idempotente:
   $a * a = a$.
2. Como $(G,*)$ es un grupo entonces existe un $a^{-1} \in G$ tal que:
   $a^{-1} * (a * a) = a^{-1} * a$.
3. Como $(G,*)$ es un grupo, * es asociativa:
   $(a^{-1} * a) * a = a^{-1} * a$
4. Teniendo en cuenta que $a^{-1} * a = e$, remplazando queda:
   $e * a = e$
5. Teniendo en cuenta que $e * a = a$
   $a = e$
6. Esto nos deja que el a idempotente es e, por lo tanto el único elemento idempotente es el elemento neutro.

Ejercicio 7.

Mostrar que en todo grupo vale la propiedad cancelativa

1. Sea $a, b, c \in G$ y siendo $(G,*)$ un grupo valiendo que:
   $a * b = a * c$
2. Como $(G,*)$ es un grupo, todo elemento de G tiene un inverso por la operación *, operando en ambos lados de la igualdad con el inverso de a nos queda:
   $a' * (a * b) = a' * (a * c)$
3. Como $*$ es asociativa:
   $(a' * a) * b = (a' * a) * c$
4. Como $a' * a = e$
   $e * b = e * c$
5. Como $e * b = b$ y $e * c = c$:
   $b = c$
6. Por lo tanto vale la propiedad cancelativa.
7. De modo similar se prueba para:
   $b * a = c * a$
   i. $(b * a) * a' = (c * a) * a'$
   ii. $b * (a * a') = c * (a * a')$
   iii. $b * e = c * e$
   iv. $b = c$

Ejercicio 8.

Sea $(G,*)$ un grupo tal que todo elemento es su propio inverso, probar que G es abeliano

1. Sea $a, b \in G$ y siendo $(G,*)$ un grupo valiendo que para todo $x \in G$ se cumple que: $x = x^{-1}$
2. Teniendo en cuenta que $a * a^{-1} = a^{-1} * a = e, b * b^{-1} = b^{-1} * b = e, a = a^{-1}$, $b = b^{-1}$ y la asociatividad de $*$:
   $a * b = e * (a * b) * e = (b^{-1} * b) * (a * b) * (a * a^{-1}) = b * (b * a) * (b * a) * a$
   $= b * (b * a) * (b * a)^{-1} * a = b * e * a = b * a$
3. Por lo tanto $a * b = b * a$, valiendo la conmutatividad para $*$ haciendo que G sea abeliano.

Ejercicio 9.

Dado un grupo $(G,*)$, probar que G es abeliano si y sólo si para cualquier x, y en G vale que: $(x * y)^2 = x^2 * y^2$

Se quiere demostrar que G es abeliano ↔ para cualquier x, y en G vale que: $(x * y)^2 = x^2 * y^2$

- $(x * y)^2 = (x * y) * (x * y)$
- $x^2 * y^2 = (x * x) * (y * y)$

1. Se quiere demostrar que G es abeliano → para cualquier x, y en G vale que: $(x * y)^2 = x^2 * y^2$
   i. Suponiendo que G es abeliano, por asociatividad vale que:
   $(x * y)^2 = (x * y) * (x * y) = x * (y * x) * y$
   ii. Por conmutatividad vale que:
   $x * (y * x) * y = x * (x * y) * y$
   iii. Por asociatividad vale que:
   $x * (x * y) * y = (x * x) * (y * y)$
   iv. Teniendo en cuenta que $(x * x) * (y * y) = x^2 * y^2$ se cumple que
   $(x * y)^2 = x^2 * y^2$

2. Se quiere demostrar que G es abeliano ← para cualquier x, y en G vale que:

   $(x * y)^2 = x^2 * y^2$

   i. Si se tiene $(a * b) * (a * b)$ se cumple por definición e hipótesis que:

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

   ii. Entonces se tiene la siguiente igualdad:

   $(a * b) * (a * b) = (a * a) * (b * b)$

   iii. Como G es un grupo, cada elemento tiene su inverso para la operación $*$, multiplicando por el inverso de a en ambos lados de la igualdad queda:

   $a^{-1} * \big((a * b) * (a * b)\big) = a^{-1} * \big((a * a) * (b * b)\big)$

   iv. Por asociatividad vale que:

   $(a^{-1} * a) * b * (a * b) = (a^{-1} * a) * a * (b * b)$

   v. Teniendo en cuenta que $a * a^{-1} = e$ nos queda:

   $e * \ b * (a * b) = e * a * (b * b)$

   vi. Como G es un grupo, para cualquier x en G vale que $x * e = e * x = x$, esto nos deja:

   $b * (a * b) = a * (b * b)$

   vii. Por asociatividad:

   $(b * a) * b = (a * b) * b$

   viii. Multiplicando en ambos lados de la igualdad por el inverso de b nos queda:

   $(b * a) * b * b^{-1} = (a * b) * b * b^{-1}$

   ix. Teniendo en cuenta que $b * b^{-1} = e$ nos queda:

   $(b * a) * e = (a * b) * e$

   x. Como G es un grupo, para cualquier x en G vale que $x * e = e * x = x$, esto nos deja:

   $b * a = a * b$

   xi. Como $b * a = a * b$, al ser G un grupo y conmutativo, G es abeliano.

Ejercicio 10.

Dados los Grupos $(G,*)$ y $(F, \diamondsuit)$ se define en el conjunto $G \times F$ la ley • tal que (x, y) • $(z, t) = (x * z, y \diamondsuit t)$. Probar que $(G \times F,\bullet)$ es Grupo (Grupo Producto):

Sean $x, z \in G$ y $y, t \in F$, la operación • esta bien definida ya que al estar $*$ bien definido en G, $x * z \in G$ y al estar $\diamondsuit$ bien definido en F, $y \diamondsuit t \in F$, por lo tanto $(x * z, y \diamondsuit t) \in G \times F$.

Asociativa:

La operación • sobre $G \times F$ es asociativa ya que para cualesquiera sean a, b y c en $G \times F$, se cumple que $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.

Demostración:

1. Sean $a, b, c \in G \times F$, con $a = (a_1, a_2)$, $b = (b_1, b_2)$,$c = (c_1, c_2)$. Por asociatividad de $*$ y $\diamondsuit$ se cumple que:

$$a \bullet (b \bullet c) = (a_1, a_2) \bullet \big((b_1, b_2) \bullet (c_1, c_2)\big) = \big(a_1 * (b_1 * b_2), a_2 \diamondsuit (b_2 \diamondsuit c_2)\big)$$
$$= \big((a_1 * b_1) * c_1, (a_2 \diamondsuit b_2) \diamondsuit c_2\big) = \big((a_1, a_2) \bullet (b_1, b_2)\big) \bullet (c_1, c_2)$$
$$= (a \bullet b) \bullet c$$

Elemento neutro:

Existe en $G \times F$ un elemento e tal que para todo a en $G \times F$ vale que $a \bullet e = e \bullet a = a$ y ese $e = (e_G, e_F)$, siendo e_G y e_F los elementos neutros de G y F respectivamente.

Demostración:

1. Sea $a \in G \times F$, con $a = (a_1, a_2)$. Dado a que e_G y e_F son los elementos neutros para las operaciones $*$ en G y $\diamondsuit$ en F se cumple que:
   i. $a \bullet e = (a_1, a_2) \bullet (e_G, e_F) = (a_1 \bullet e_G, a_2 \bullet e_F) = (a_1, a_2)$
   ii. $e \bullet a = (e_G, e_F) \bullet (a_1, a_2) = (e_G \bullet a_1, e_F \bullet a_2) = (a_1, a_2)$

Elemento inverso:

Para todo elemento $a = (a_1, a_2)$ de $G \times F$ existe a' en $G \times F$ tal que $a \bullet a' = a' \bullet a = e$ y ese $a' = -a$, con $-a = (-a_1, -a_2)$ y $e = (e_G, e_F)$.

Demostración:

1. Sea $a \in G \times F$, con $a = (a_1, a_2)$ y $-a = (-a_1, -a_2)$. Dado a que para todo elemento $x \in G$ se verifica que $x * (-x) = e_G$ y para todo elemento $x \in F$ se verifica que $x \diamondsuit (-x) = e_F$ se cumple que:
   i. $a \bullet (-a) = (a_1, a_2) \bullet (-a_1, -a_2) = \big(a_1 * (-a_1), a_2 \diamondsuit (-a_2)\big) = (e_G, e_F)$
   ii. $-a \bullet a = (-a_1, -a_2) \bullet (a_1, a_2) = (-a_1 * a_1, -a_2 \diamondsuit a_2) = (e_G, e_F)$

Como • es asociativa, existe un elemento neutro y todos los elementos de $G \times F$ tienen un inverso $(G \times F\ ,\ \bullet)$ es un grupo.

Ejercicio 11.

Estudiar si son Subgrupos de los grupos indicados:

a. Los enteros pares de $(Z, +)$

$P = \{x\ \in Z : x = 2\ .\ k, k \in Z\}$

Asociativa:
La operación $+$ sobre P es asociativa ya que para cualesquiera sean a, b y c en Z, se cumple que $a + (b + c) = (a + b) + c$. Esto lo "hereda" de Z.

Elemento neutro:
Existe en P un elemento e tal que para todo a en P vale que $a + e = e + a = a$ y ese $e = 0$. El neutro $+$ en Z, es 0, como $0 = 2\ .\ 0$, este $\in P$.

Operación bien definida y elemento inverso:
Sean $a, b \in los\ enteros\ pares\ de\ Z$, como a, b son pares se puede escribir como $a = 2\ .\ m$ y $b = 2\ .\ n$. Se puede observar que se cumple que $b^{-1} \in P$ ya que este se puede escribir como $2\ .\ (-n)$
Por propiedad distributiva y asociativa de Z se cumple:
$a + b^{-1} = (2\ .\ m) + (2.\ -n) = 2.\ (m - n) = 2\ .\ k$ con $k \in Z$ ya que la resta es cerrada en Z.
Como $a + b^{-1} = 2\ .\ k, a + b^{-1} \in P$, por lo tanto $(P, +)$ es un subgrupo de Z.

b. Las matrices simétricas de 2x2

Ejercicio 12.

Demostrar que si H y K son subgrupos de $(G, *)$ entonces $H\ \cap\ K$ es un subgrupo de $(G, *)$

Elemento neutro:

Se debe demostrar que existe en $H \cap K$ un elemento e tal que para todo a en $H \cap K$ valga que $a * e = e * a = a$.

1. Se sabe que al ser H y K subgrupos de $(G,*)$.
   i. Existe un $e \in H$ tal que para todo a en H vale $a * e = e * a = a$
   ii. Existe un $e \in K$ tal que para todo a en K vale $a * e = e * a = a$
2. Como $e \in K$ y $e \in H$, por definición de intersección $e \in H \cap K$
3. Por lo tanto existe en $\mathrm{H} \cap \mathrm{K}$ un elemento e tal que para todo a en $H \cap K$ valga que $a * e = e * a = a$

Operación bien definida y elemento inverso:

Sea desea demostrar que para si $a, b \in \mathrm{H} \cap \mathrm{K}$ entonces $a * b^{-1} \in H \cap K$:

1. Por hipótesis se sabe que $a, b \in \mathrm{H} \cap \mathrm{K}$, entonces, por definición de intersección:
   i. $a \in H$ y $a \in K$
   ii. $b \in H$ y $b \in K$
2. Como H y K son subgrupos de $(G,*)$ se cumple que.
   i. Existe un $b^{-1} \in H$ tal que para todo b en H vale $b * b^{-1} = b^{-1} * b = e$
   ii. Existe un $b^{-1} \in K$ tal que para todo b en K vale $b * b^{-1} = b^{-1} * b = e$
3. Como $b^{-1} \in K$ y $b^{-1} \in H$, por definición de intersección $b^{-1} \in H \cap K$
4. Como H y K son subgrupos de (G,*), la operación * está bien definida en H y en K, por hipótesis 1. se sabe que tanto a como b pertenecen a H y a K y que también sucede que b^{-1} pertenece a H y a K por lo tanto:
   i. $a * b^{-1} \in H$ y $a * b^{-1} \in K$
5. Como $a * b^{-1} \in H$ y $A * b^{-1} \in K$ por definición de intersección $a * b^{-1} \in H \cap K$

Ejercicio 13.

Sea $(G,*)$ un grupo, sea $a \in G$ y sea H un subgrupo de G. Demostrar que el conjunto $aHa^{+1} = \{a * h * a^{-1} : h \in H\}$ es un subgrupo de G.

Elemento neutro:

Se debe demostrar que existe en aHa^{+1} un elemento e tal que para todo x en aHa^{+1} valga que $x * e = e * x = x$.

1. Se sabe que al ser H un subgrupos de $(G,*)$.
   i. Existe un $e \in H$ tal que para todo a en H vale $a * e = e * a = a$
2. Como $e \in H$, podemos considerar que $h = e$. Reemplazando nos queda:
   i. $a * e * a^{-1} = a * a^{-1} = e$
4. Por lo tanto existe en aHa^{+1} un elemento e tal que para todo a en aHa^{+1} valga que $a * e = e * a = a$

Operación bien definida y elemento inverso:

Sea desea demostrar que para si $x, y \in aHa^{+1}$entonces $x * y^{-1} \in aHa^{+1}$:

1. Por hipótesis se sabe que $x, y \in aHa^{+1}$, entonces, por definición sabemos existe un h_1 y un h_2 tal que:
   i. $x = a * h_1 * a^{-1}$
   ii. $y = a * h_2 * a^{-1}$
2. Se quiere encontrar un $y^{-1} = (\, a * h_2 * a^{-1})^{-1}$. Desarrollando nos queda:
   i. $y^{-1} = (a^{-1})^{-1} * h_2^{-1} * a^{-1} = a * h_2^{-1} * a^{-1}$
3. Como al ser H un subgrupos de $(G,*)$. Si $h_2 \in H$ entonces también $h_2^{-1} \in H$, por lo tanto $y^{-1} \in aHa^{+1}$ (se cumple bien $a * h_2^{-1} * a^{-1}$).
4. Esto nos deja que
   i. $x * y^{-1} = (a * h_1 * a^{-1}) * (a * h_2^{-1} * a^{-1})$
5. Por asociatividad de * en G nos queda que:
   i. $x * y^{-1} = a * h_1 * (a^{-1} * a) * h_2^{-1} * a^{-1}$
6. Como $a^{-1} * a = e$ (neutro de G)
   i. $a * h_1 * e * h_2^{-1} * a^{-1} = a * h_1 * h_2^{-1} * a^{-1}$
7. Nuevamente asociatividad de * en G
   i. $a * (h_1 * h_2^{-1}) * a^{-1}$
8. Como H es un subgrupos de $(G,*)$ y tanto $h_1 \in H$ como $h_2^{-1} \in H$, sucede que $h_1 * h_2^{-1} \in H$. $h_1 * h_2^{-1} = h$ esto nos deja:
   i. $a * h * a^{-1}$
9. Entonces $x * y^{-1} = a * h * a^{-1} \in H$.

Ejercicio 14.

Probar que todo grupo cíclico es abeliano

1. Sea $(G,*)$ un grupo cíclico, por definición existe un $g \in G$ tal que para todo elemento $t \in G$ existe un entero k tal que $t = g^k$
2. Se desea demostrar que para todo $a, b \in G$ se cumple que $a * b = b * a$
3. Sea $a, b \in G$ por definición:
   i. $a = g^k$ con $k \in Z$
   ii. $b = g^h$ con $h \in Z$
4. Entonces si partimos de $a * b$ y vamos desarrollando podemos ver cómo se llega a la igualdad. Para ello se utilizará una de las leyes de los exponentes y la suma usual de los naturales, junto con su propiedad conmutativa.
   $a * b = g^k * g^h = g^{k+h} = g^{h+k} = g^h * g^k = b * a$
5. Como $a * b = b * a$ para todos los $a, b \in G$ siendo G un grupo, todo grupo cíclico es abeliano.

Ejercicio 15.

Sea G un grupo cíclico de orden n, Si m es divisor de n entonces el elemento a^m y sus potencias generan un subgrupo

$G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

$H = \langle a^m \rangle = \{e, a^m, a^{2m}, \dots, a^{km}\}$

Como m es divisor de n, $n = m \,.\, d$ con $d \in Z$. Como G es de orden n, $a^n = e$, por lo que si en H se tiene $a^{dm} = a^n = e$, por lo tanto necesariamente H es de orden d. Como $d = \frac{n}{m}$ (despejo d en la igualdad $n = m \,.\, d$) H es de orden $\frac{n}{m}$.

Elemento neutro:

Se debe demostrar que existe en H un elemento e tal que para todo a en H valga que $a * e = e * a = a$.

1. Se sabe que G es un grupo cíclicos de orden n. Por lo tanto:
   i. Existe un $e \in G$ tal que para todo a en H vale $a * e = e * a = a$
2. Teniendo en cuenta que $e = a^0$. Si a a^m lo elevamos a 0 nos queda lo siguiente:
   i. $(a^m)^0 = a^{m0} = a^0 = e$

3. Por lo tanto existe en H un elemento e tal que para todo a en H valga que $a * e = e * a = a$.

- $e = a^0$ dado que para todo $a^k \in G$ se cumple que $a^k * a^0 = a^{k+0} = a^{0+k} = a^k$

Operación bien definida y elemento inverso:

Sea desea demostrar que para si $x, y \in H$ entonces $x * y^{-1} \in H$:

1. Por hipótesis se sabe que $x, y \in H$, entonces, por definición:
   i. $x = (a^m)^k$
   ii. $y = (a^m)^h$
2. Se quiere encontrar un $y^{-1} = \left((a^m)^h\right)^{-1}$. Desarrollando nos queda:
   i. $y^{-1} = \left((a^m)^h\right)^{-1} = \left(a^{mh}\right)^{-1} = a^{-mh} = (a^m)^{-h}$
3. Como H es de orden d, el inverso en realidad seria $(a^m)^{d-h}$ (ver nota de abajo).
4. Como a^{-mh} es una potencia de a^m, siendo esta misma $(a^m)^{-h}$, $a^{-mh} \in H$
5. Esto nos deja que:
   i. $x * y^{-1} = (a^m)^k * a^{-mh}$
   ii. $x * y^{-1} = a^{mk} * a^{-mh}$
   iii. $x * y^{-1} = a^{mk-mh}$
   iv. $x * y^{-1} = a^{m(k-h)}$
   v. $x * y^{-1} = (a^m)^{k-h}$
6. Como $(a^m)^{k-h}$ es una potencia de a^m, $(a^m)^{k-h} \in H$
7. Entonces $x * y^{-1} \in H$.

Nota:

Si el grupo es cíclico H tiene un generador a^m, cada elemento del grupo se puede escribir como $(a^m)^k$ para algún entero k. El inverso de$(a^m)^k$ sería otro elemento $(a^m)^h$ tal que:

$$(a^m)^k * (a^m)^h = a^{mk+mh} = a^0 = e$$

- $a^{mk+mh} = a^{mh+mk} = (a^m)^h * (a^m)^k$

Dado que el orden del grupo es d para que $a^{mk+mh} = a^0$, se necesita que:

$$mk + mh \equiv_d 0$$

Esto implica que:

$$mh \equiv_d - mk$$

Por lo tanto, el inverso de $(a^m)^k$ es $a^{-mk} = (a^m)^{-k}$ o, escrito de otra forma, $(a^m)^{d-k}$

Ejercicio 16.

Sea $(G,*)$ un grupo, sea $a \in G$ y sea H un subgrupo de G. Si $a, b \in G$, probar que la relación dada por $a \equiv b \, mod(H)$ si $a * b^{-1} \in H$ es una relación de equivalencia.