Instituto Tecnológico de Estudios Superiores de Monterrey, Campus Guadalajara

MA2006B.401

Actividad 0 - Curvas Elípticas

Uso de álgebras modernas para seguridad y criptografía

Equipo:
Alberto Cortés
Diego Pérez
Luis Ramírez
Mariana Rizo

13 de Marzo del 2022

Ejercicios de Grupos

2.1

Para cada operación binaria $*$ definida en el conjunto señalado dígase cuándo $*$ dota al conjunto de una estructura de grupo. De no resultar grupo, dése el primer axioma que no se cumpla.

a. Definase $*$ en $\mathbb{Z}$ por $a * b = ab$
En este caso la operación $a * b = ab$ no resulta en un grupo para $\mathbb{Z}$ ya que no se cumple que $\forall a \in \mathbb{Z}\ \exists a^{-1} \in \mathbb{Z}$ ya que para encontrar el inverso de a se debe cumplir $aa^{-1} = 1 \implies a^{-1} = \frac{1}{a} \notin \mathbb{Z}$.

b. Definase $*$ en $\mathbb{Z}$ por $a * b = a - b$
En este caso la operación de la resta no resulta en un grupo, ya que no se cumple la asociatividad. Esto se puede observar con un contra-ejemplo:

$$\text{Tomemos } 1,\ 2 \text{ y } 3\ \in \mathbb{Z}$$

$$1 - (2 - 3) = 1 - (-1) = 0$$

$$(1 - 2) - 3 = (-1) - 3 = -4 \neq 0$$

c. Definase $*$ en $\mathbb{R}^+$ por $a * b = ab$
La operación $a * b = ab$ en $\mathbb{R}^+$ resulta en un grupo ya que cumple con todos los axiomas:

I. Cerradura

$$\forall a, b \in \mathbb{R}^+$$

$$ab = c \in \mathbb{R}^+$$

II. Identidad
La identidad es 1 y se prueba que

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

$$1a = a1 = a$$

III. Inverso

$$aa^{-1} = 1$$

$$a^{-1} = \frac{1}{a} \in \mathbb{R}^+$$

IV. Asociatividad

$$\forall a, b, c \in \mathbb{R}^+$$

$$(ab)c = a(bc)$$

d. Definase $*$ en $\mathbb{Q}$ por $a * b = ab$
El conjunto $\mathbb{Q}$ no forma un grupo con la operación $a * b = ab$ ya que no cumple con la existencia de un inverso. Basta con el siguiente contra-ejemplo:

$$0 \in \mathbb{Q}$$

$$\text{Sea } x^{-1} \text{ el inverso de } 0$$

$$x^{-1} = \frac{1}{0} \text{ el cual es indefinido.}$$

e. Definase $*$ en el conjunto de todos los números reales distintos de cero por $a * b = ab$
La operación $a * b = ab$ resulta en un grupo en $\mathbb{R} \setminus \{0\}$ ya que cumple con todos los axiomas:

I. Cerradura

$$\forall a, b \in \mathbb{R} \setminus \{0\}$$

$$ab = c \in \mathbb{R} \setminus \{0\}$$

II. Identidad
La identidad es 1 y se prueba que

$$\forall a \in \mathbb{R} \setminus \{0\}$$
$$1a = a1 = a$$

III. Inverso

$$aa^{-1} = 1$$
$$a^{-1} = \frac{1}{a} \in \mathbb{R} \setminus \{0\} \text{ ya que } a \neq 0$$

IV. Asociatividad

$$\forall a, b, c \in \mathbb{R} \setminus \{0\}$$
$$(ab)c = a(bc)$$

f. Definase $*$ en C por $a * b = a + b$
La operación $a * b = a + b$ resulta en un grupo en $\mathbb{C}$ ya que cumple con todos los axiomas:

I. Cerradura

$$\forall a, b \in \mathbb{C}$$
$$a + b = c \in \mathbb{C}$$

II. Identidad
La identidad es 0 y se prueba que

$$\forall a \in \mathbb{C}$$
$$0 + a = a + 0 = a$$

III. Inverso

$$a + a^{-1} = 0$$
$$a^{-1} = 0 - a = -a \in \mathbb{C}$$

IV. Asociatividad

$$\forall a, b, c \in \mathbb{C}$$
$$(a + b) + c = a + (b + c)$$

2.9

Sea S el conjunto de todos los números reales excepto -1. Definase $*$ en S por $a * b = a + b + ab$

a. Muéstrese que $*$ da una operación binaria en S.
Debemos comprobar que $ab \neq -1 \ \forall a, b \in \mathbb{R} \setminus \{-1\}$

$$\forall a, b \in S$$

$$a + b + ab = -1$$
$$a(1 + b) + b = -1$$
$$-a(1 + b) = 1 + b$$
$$-a = \frac{1 + b}{1 + b} = 1$$
$$a = -1 \text{ lo cual es absurdo ya que } a \in S$$

Similarmente, lo mismo sucede con b:

$$a + b + ab = -1$$

$$a + b(1 + a) = -1$$
$$-b(1 + a) = a + 1$$
$$-b = \frac{a + 1}{a + 1} = 1$$
$$b = -1 \text{ lo cual es absurdo ya que } b \in S$$

b. Muéstrese que $\langle S, *\rangle$ es un grupo.
En este caso, se puede probar la existencia del inverso de la siguiente manera, tomando a 0 como el elemento identidad:

$$a + a^{-1} + aa^{-1} = 0$$
$$a^{-1}(1 + a) = -a$$
$$a^{-1} = \frac{-a}{1+a} \text{ donde } a \neq -1 \text{ ya que pertenece a } S$$

De igual manera, se puede probar asociatividad:

$$\forall a, b, c \in S$$

$$a(bc) = a(b + c + bc) = a + b + c + bc + ab + ac + abc$$
$$(ab)c = (a + b + ab)c = a + b + ab + c + ac + bc + abc$$
$$a(bc) = (ab)c$$

c. Encuéntrese la solución de la ecuación $2 * x * 3 = 7$ en S.
Expandiendo la ecuación tenemos lo siguiente:

$$(2 + x + 2x) * 3 = 7$$

$$2 + x + 2x + 3 + 6 + 3x + 6x = 7$$
$$11 + 12x = 7$$
$$12x = -4$$
$$x = -\frac{1}{3}$$

Comprobando:

$$\left(2 + \left(-\frac{1}{3}\right) + \left(-\frac{2}{3}\right)\right) * 3$$
$$= (1) * 3$$
$$= 1 + 3 + 1(3)$$
$$= 7$$

Ejercicios de Anillos

23.1

Digase para cuáles de los siguientes conjuntos las operaciones indicadas de suma y multiplicación están definidas (el conjunto es cerrado) y dan estructura de anillo. Si el anillo no se forma, explíquese por qué.

a. $n\mathbb{Z}$ con la suma y multiplicación usuales.

I. Abeliano, bajo la suma.
En este caso sabemos que $n\mathbb{Z}$ bajo la suma forma un grupo abeliano ya que cumple con la cerradura

$$\forall x, y \in n\mathbb{Z}$$

Consideremos $x = nz_1, y = nz_2$, con $z_1, z_2 \in \mathbb{Z}$. Como la suma usual es distributiva:

$$nz_1 + nz_2 = n(z_1 + z_2) \in n\mathbb{Z}$$

tiene un elemento identidad (0)

$$\forall x \in n\mathbb{Z}$$

$$x + 0 = 0 + x = x$$

existe un inverso para cada elemento Tenemos que $\forall x \in n\mathbb{Z}$:

$$x + x^{-1} = 0$$

$$nz + n(-z) = 0$$

Ya que $z, -z \in \mathbb{Z}$

$$x^{-1} = -nz = -x$$

es asociativo

$$\forall x, y, z \in n\mathbb{Z}$$

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

y es conmutativo

$$\forall x, y \in n\mathbb{Z}$$

$$nz_1 + nz_2 = n(z_1 + z_2)$$

$$nz_2 + nz_1 = n(z_2 + z_1)$$

Como la suma usual en $\mathbb{Z}$ es conmutativa, tenemos que $nz_1 + nz_2 = nz_2 + nz_1$, por lo tanto $n\mathbb{Z}$ es conmutativo bajo la suma.

II. Asociatividad bajo la multiplicación.

$$\forall x, y, z \in n\mathbb{Z}$$

Como la multiplicación usual en $\mathbb{Z}$ es asociativa:

$$x(yz) = (xy)z$$

III. Distributividad, multiplicación sobre suma.

$$\forall x, y, z \in n\mathbb{Z}$$

$$x(y + z) = xy + xz = (xy) + (xz) \mod n$$

$$(y + z)x = yx + zx = (yx) + (zx) \mod n$$

Por lo anterior, se comprueba que $n\mathbb{Z}$ forma un anillo bajo la suma y multiplicación usual.

b. $\mathbb{Z}^+$ con la suma y multiplicación usuales.
En el conjunto $\mathbb{Z}^+$ no se forma un anillo, ya que no se forma un grupo bajo la suma porque no existen inversos para los elementos de $\mathbb{Z}^+$.

$$\forall x \in \mathbb{Z}^+$$

$$x + x^{-1} = 0 \implies x^{-1} = -x$$

$$\text{Pero } -x \notin \mathbb{Z}^+$$

c. $\mathbb{Z} \times \mathbb{Z}$ con la suma y multiplicación por componentes.

I. Abeliano, bajo la suma.
En este caso sabemos que $\mathbb{Z} \times \mathbb{Z}$ bajo la suma forma un grupo abeliano ya que cumple con la cerradura

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

como $x_1 + x_2, y_1 + y_2 \in \mathbb{Z}$ tenemos cerradura bajo la suma.

tiene un elemento identidad (0,0)

$$\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}$$

:

$$(x, y) + (0, 0) = (x + 0, y + 0) = (x, y)$$
$$(0, 0) + (x, y) = (0 + x, 0 + y) = (x, y)$$

existe un inverso para cada elemento $\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}$:

$$(x, y) + (x, y)^{-1} = (0, 0)$$
$$(x, y)^{-1} = (0 - x, 0 - y)$$
$$(x, y)^{-1} = (-x, -y)$$

es asociativo

$$\forall (x_1, y_1), (x_2, y_2)(x_3, y_3) \in \mathbb{Z} \times \mathbb{Z}$$
$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1 + x_2 + x_3, y_1 + y_2 + y_3)$$
$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1 + x_2 + x_3, y_1 + y_2 + y_3)$$

y es conmutativo

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$$
$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$(x_2, y_2) + (x_1, y_1) = (x_2 + x_1, y_2 + y_1)$$

Como la suma usual es conmutativa tenemos que

$$(x_1, y_1) + (x_2, y_2) = (x_2, y_2) + (x_1, y_1)$$

II. Asociatividad bajo la multiplicación.

$$\forall (x_1, y_1), (x_2, y_2)(x_3, y_3) \in \mathbb{Z} \times \mathbb{Z}$$
$$((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) = (x_1 \cdot x_2 \cdot x_3, y_1 \cdot y_2 \cdot y_3)$$
$$(x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)) = (x_1 \cdot x_2 \cdot x_3, y_1 \cdot y_2 \cdot y_3)$$

III. Distributividad, multiplicación sobre suma.

$$\forall (x_1, y_1), (x_2, y_2)(x_3, y_3) \in \mathbb{Z} \times \mathbb{Z}$$
$$(x_1, y_1) \cdot ((x_2, y_2) + (x_3, y_3)) = (x_1 \cdot (x_2 + x_3), y_1 \cdot (y_2 + y_3))$$
$$(x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3) = (x_1 \cdot x_2 + x_1 \cdot x_3, y_1 \cdot y_2 + y_1 \cdot y_3)$$

Como existe distributividad de la multiplicación sobre la suma en $\mathbb{Z}$, tenemos que:

$$(x_1, y_1) \cdot ((x_2, y_2) + (x_3, y_3)) = (x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3)$$

Por lo anterior, se comprueba que $\mathbb{Z} \times \mathbb{Z}$ forma un anillo bajo la suma y multiplicación usual.

d. $2\mathbb{Z} \times \mathbb{Z}$ con la suma y multiplicación por componentes.

I. Abeliano, bajo la suma.
En este caso sabemos que $2\mathbb{Z} \times \mathbb{Z}$ bajo la suma forma un grupo abeliano ya que cumple con la cerradura

$$\forall (2x_1, y_1), (2x_2, y_2) \in 2\mathbb{Z} \times \mathbb{Z}$$
$$(2x_1, y_1) + (2x_2, y_2) = (2(x_1 + x_2), y_1 + y_2)$$

como $x_1 + x_2, y_1 + y_2 \in \mathbb{Z}$ tenemos cerradura bajo la suma.

tiene un elemento identidad (0,0)

$$\forall (2x, y) \in 2\mathbb{Z} \times \mathbb{Z}$$

:

$$(2x, y) + (0, 0) = (2x + 0, y + 0) = (2x, y)$$
$$(0, 0) + (2x, y) = (0 + 2x, 0 + y) = (2x, y)$$

existe un inverso para cada elemento $\forall (2x, y) \in 2\mathbb{Z} \times \mathbb{Z}$:

$$(2x, y) + (2x, y)^{-1} = (0, 0)$$
$$(2x, y)^{-1} = (0 - 2x, 0 - y)$$
$$(2x, y)^{-1} = (-2x, -y)$$

es asociativo

$$\forall (2x_1, y_1), (2x_2, y_2)(2x_3, y_3) \in 2\mathbb{Z} \times \mathbb{Z}$$
$$((2x_1, y_1) + (2x_2, y_2)) + (2x_3, y_3) = (2x_1 + 2x_2 + 2x_3, y_1 + y_2 + y_3)$$
$$(2x_1, y_1) + ((2x_2, y_2) + (2x_3, y_3)) = (2x_1 + 2x_2 + 2x_3, y_1 + y_2 + y_3)$$

y es conmutativo

$$\forall (2x_1, y_1), (2x_2, y_2) \in 2\mathbb{Z} \times \mathbb{Z}$$
$$(2x_1, y_1) + (2x_2, y_2) = (2x_1 + 2x_2, y_1 + y_2)$$
$$(2x_2, y_2) + (2x_1, y_1) = (2x_2 + 2x_1, y_2 + y_1)$$

Como la suma usual es conmutativa tenemos que

$$(2x_1, y_1) + (2x_2, y_2) = (2x_2, y_2) + (2x_1, y_1)$$

II. Asociatividad bajo la multiplicación.

$$\forall (2x_1, y_1), (2x_2, y_2)(2x_3, y_3) \in 2\mathbb{Z} \times \mathbb{Z}$$
$$((2x_1, y_1) \cdot (2x_2, y_2)) \cdot (2x_3, y_3) = (2x_1 \cdot 2x_2 \cdot 2x_3, y_1 \cdot y_2 \cdot y_3)$$
$$(2x_1, y_1) \cdot ((2x_2, y_2) \cdot (2x_3, y_3)) = (2x_1 \cdot 2x_2 \cdot 2x_3, y_1 \cdot y_2 \cdot y_3)$$

III. Distributividad, multiplicación sobre suma.

$$\forall (2x_1, y_1), (2x_2, y_2)(2x_3, y_3) \in 2\mathbb{Z} \times \mathbb{Z}$$
$$(2x_1, y_1) \cdot ((2x_2, y_2) + (2x_3, y_3)) = (2x_1 \cdot (2x_2 + 2x_3), y_1 \cdot (y_2 + y_3))$$
$$(2x_1, y_1) \cdot (2x_2, y_2) + (2x_1, y_1) \cdot (2x_3, y_3) = (2x_1 \cdot 2x_2 + 2x_1 \cdot 2x_3, y_1 \cdot y_2 + y_1 \cdot y_3)$$

Como existe distributividad de la multiplicación sobre la suma en $\mathbb{Z}$, tenemos que:

$$(2x_1, y_1) \cdot ((2x_2, y_2) + (2x_3, y_3)) = (2x_1, y_1) \cdot (2x_2, y_2) + (2x_1, y_1) \cdot (2x_3, y_3)$$

Por lo anterior, se comprueba que $2\mathbb{Z} \times \mathbb{Z}$ forma un anillo bajo la suma y multiplicación usual.

e. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ con la suma y multiplicación usuales.

I. Abeliano, bajo la suma.
En este caso sabemos que el conjunto $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ forma un grupo abeliano bajo la suma ya que cumple con la cerradura

$$\forall a, b, c, d \in \mathbb{Z}$$
$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in G$$

tiene un elemento identidad ($a = 0, b = 0$)

$$\forall a, b \in \mathbb{Z}$$
$$(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (a + 0) + (b + 0)\sqrt{2} = a + b\sqrt{2}$$

existe un inverso para cada elemento. Tenemos que $\forall a, b \in \mathbb{Z}$:

$$(a + b\sqrt{2}) + (a^{-1} + b^{-1}\sqrt{2}) = 0 = 0 + 0\sqrt{2}$$

$$(a + b\sqrt{2}) + (a^{-1} + b^{-1}\sqrt{2} = (a + a^{-1}) + (b + b^{-1})\sqrt{2} = 0$$

$$(a + a^{-1}) = 0 \text{ y } (b + b^{-1}) = 0$$

$$\therefore \quad a^{-1} = -a \quad \text{y} \quad b^{-1} = -b$$

Como $a, b \in \mathbb{Z}$ tenemos que $-a, -b \in \mathbb{Z}$.
Es asociativo

$$\forall a, b, c, d, e, f \in \mathbb{Z}$$

$$((a+b\sqrt{2})+(c+d\sqrt{2}))+(e+f\sqrt{2}) = ((a+c)+(b+d)\sqrt{2})+(e+f\sqrt{2}) = (a+c+e)+(b+d+f)\sqrt{2}$$

$$(a+b\sqrt{2})+((c+d\sqrt{2})+(e+f\sqrt{2})) = (a)+(b)\sqrt{2}+((c+e)+(d+f)\sqrt{2}) = (a+c+e)+(b+d+f)\sqrt{2}$$

y es conmutativo

$$\forall a, b, c, d \in \mathbb{Z}$$

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

$$(c + d\sqrt{2}) + (a + b\sqrt{2}) = (c + a) + (d + b)\sqrt{2}$$

Como la suma usual es conmutativa en $\mathbb{Z}$, sabemos que $(a+c) = (c+a)$ y $(b+d) = (d+b)$.

II. Asociatividad bajo la multiplicación.

$$\forall a, b, c, d, e, f \in \mathbb{Z}$$

$$((a + b\sqrt{2})(c + d\sqrt{2}))(e + f\sqrt{2}) = ((ac + 2bd) + (ad + bc)\sqrt{2})(e + f\sqrt{2})$$

$$= (ace + 2(adf + bcf + bde)) + (acf + ade + bce + 2bdf)\sqrt{2}$$

$$(a + b\sqrt{2}) + ((c + d\sqrt{2})(e + f\sqrt{2})) = (a + b\sqrt{2})((ce + 2df) + (cf + de)\sqrt{2})$$

$$= (ace + 2(adf + bcf + bde)) + (acf + ade + bce + 2bdf)\sqrt{2}$$

$$\therefore \quad ((a + b\sqrt{2})(c + d\sqrt{2}))(e + f\sqrt{2}) = (a + b\sqrt{2}) + ((c + d\sqrt{2})(e + f\sqrt{2}))$$

III. Distributividad, multiplicación sobre suma.
Sea $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ y $z = e + f\sqrt{2}$, donde $a, b, c, d, e, f \in \mathbb{Z}$:

$$xy + xz = (ac + 2bd) + (ad + bc)\sqrt{2} + (ae + 2bf) + (af + be)\sqrt{2}$$

$$x(y+z) = (a+b\sqrt{2})((c+e)+(d+f)\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}+(ae+2bf)+(af+be)\sqrt{2}$$

$$\therefore \quad xy + xz = x(y + z)$$

Por lo anterior, se comprueba que $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ forma un anillo bajo la suma y multiplicación usuales.

f. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ con la suma y multiplicación usuales.

I. Abeliano, bajo la suma.
En este caso sabemos que el conjunto $H = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ forma un grupo abeliano bajo la suma ya que cumple con la cerradura

$$\forall a, b, c, d \in \mathbb{Q}$$

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in H$$

Ya que la suma de racionales es racional.
Tiene un elemento identidad $(a = 0, b = 0)$

$$\forall a, b \in \mathbb{Q}$$

$$(a+b\sqrt{2})+(0+0\sqrt{2})=(a+0)+(b+0)\sqrt{2}=a+b\sqrt{2}$$

existe un inverso para cada elemento. Tenemos que $\forall a,b\in\mathbb{Q}$:

$$(a+b\sqrt{2})+(a^{-1}+b^{-1}\sqrt{2})=0=0+0\sqrt{2}$$

$$(a+b\sqrt{2})+(a^{-1}+b^{-1}\sqrt{2}=(a+a^{-1})+(b+b^{-1})\sqrt{2}=0$$

$$(a+a^{-1})=0 \text{ y } (b+b^{-1})=0$$

$$\therefore \quad a^{-1}=-a \quad \text{y} \quad b^{-1}=-b$$

Como $a,b\in\mathbb{Q}$ tenemos que $-a,-b\in\mathbb{Q}$.
Es asociativo

$$\forall a,b,c,d,e,f\in\mathbb{Q}$$

$$((a+b\sqrt{2})+(c+d\sqrt{2}))+(e+f\sqrt{2})=((a+c)+(b+d)\sqrt{2})+(e+f\sqrt{2})=(a+c+e)+(b+d+f)\sqrt{2}$$

$$(a+b\sqrt{2})+((c+d\sqrt{2})+(e+f\sqrt{2}))=(a)+(b)\sqrt{2}+((c+e)+(d+f)\sqrt{2})=(a+c+e)+(b+d+f)\sqrt{2}$$

y es conmutativo

$$\forall a,b,c,d\in\mathbb{Q}$$

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$

$$(c+d\sqrt{2})+(a+b\sqrt{2})=(c+a)+(d+b)\sqrt{2}$$

Como la suma usual es conmutativa en $\mathbb{Q}$, sabemos que $(a+c)=(c+a)$ y $(b+d)=(d+b)$.

II. Asociatividad bajo la multiplicación.

$$\forall a,b,c,d,e,f\in\mathbb{Q}$$

$$((a+b\sqrt{2})(c+d\sqrt{2}))(e+f\sqrt{2})=((ac+2bd)+(ad+bc)\sqrt{2})(e+f\sqrt{2})$$

$$=(ace+2(adf+bcf+bde))+(acf+ade+bce+2bdf)\sqrt{2}$$

$$(a+b\sqrt{2})+((c+d\sqrt{2})(e+f\sqrt{2}))=(a+b\sqrt{2})((ce+2df)+(cf+de)\sqrt{2})$$

$$=(ace+2(adf+bcf+bde))+(acf+ade+bce+2bdf)\sqrt{2}$$

$$\therefore \quad ((a+b\sqrt{2})(c+d\sqrt{2}))(e+f\sqrt{2})=(a+b\sqrt{2})+((c+d\sqrt{2})(e+f\sqrt{2}))$$

III. Distributividad, multiplicación sobre suma.
Sea $x=a+b\sqrt{2}$, $y=c+d\sqrt{2}$ y $z=e+f\sqrt{2}$, donde $a,b,c,d,e,f\in\mathbb{Q}$:

$$xy+xz=(ac+2bd)+(ad+bc)\sqrt{2}+(ae+2bf)+(af+be)\sqrt{2}$$

$$x(y+z)=(a+b\sqrt{2})((c+e)+(d+f)\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}+(ae+2bf)+(af+be)\sqrt{2}$$

$$\therefore \quad xy+xz=x(y+z)$$

Por lo anterior, se comprueba que $\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ forma un anillo bajo la suma y multiplicación usuales.

g. El conjuntos de todos los números complejos imaginarios puros ri para $r\in\mathbb{R}$ con la suma y multiplicación usuales.

En este caso no se forma un anillo, ya que no existe cerradura bajo la multiplicación:

Sean $ai, bi\in\mathbb{R}i$

$$ai\cdot bi=ab(-1)=-ab$$

Pero $-ab\notin\mathbb{R}i$