A. Mira-Bejaia university	**Faculty of Exact Sciences**	**Department of Mathematics**
First year of mathematics	**Algebra 1**	**2024-2025**
Tutorial Series N° 5	**Algebraic structures**	

Exercise 1 We define a binary operation $\star$ on the set $\mathbb{R}$ by: $x \star y = x + y + 1$.

❶ Show that $(\mathbb{R}, \star)$ is an abelian group.

❷ Let $H = \{2k+1,\ \text{such that } k \in \mathbb{Z}\}$ be a subset of $\mathbb{R}$. Show that $(H, \star)$ is a subgroup of $(\mathbb{R}, \star)$.

❸ Let $\lambda \in \mathbb{R}$ and f be a function from the group $(\mathbb{R}, +)$ to the group $(\mathbb{R}, \star)$ defined by:

$$\forall x \in \mathbb{R},\ f(x) = x + \lambda.$$

Determine λ for which f be a group homomorphism.

Exercise 2 Recall that $(\mathbb{R}, +, .)$ be a field, notice that 0 is an identity element and 1 a unit element of $\mathbb{R}$.

(I) We define on $\mathbb{R}$ two other binary operations by

$$\forall a, b \in \mathbb{R},\ a \oplus b = a + b + 1 \quad \text{and} \quad a \otimes b = ab + a + b$$

❶ Show that $(\mathbb{R}, \oplus, \otimes)$ is a ring with unity. Is it a field?

❷ Show that the function f defined by

$$\begin{aligned} f : (\mathbb{R}, \oplus, \otimes) &\longrightarrow (\mathbb{R}, +, .) \\ a &\longmapsto f(a) = a + 1 \end{aligned}$$

is a ring isomorphism.

(II) Let E be the subset of $\mathbb{R}$ defined by

$$E = \left\{x + y\sqrt{3} :\ x, y \in \mathbb{Q}\right\}$$

❶ Show that E is closed under " + " and "."

❷ Show that every element of $E \setminus \{0\}$ has an inverse (under the multiplication) in $E \setminus \{0\}$

❸ Show that E is a subfield of the field $(\mathbb{R}, +, .)$.

Homework

Exercise 1

1. Determine which of the following sets are group under addition :
   (a) the set of all rationals (including 0) in lowest term whose denominators are odd.
   (b) the set of all rationals (including 0) in lowest term whose denominators are even.
   (c) the set of rationals whose absolute value <1.
   (d) the set of rationals whose absolute value 1 together with 0.
2. Let $G := \left\{a + b\sqrt{2}\ a, b \in \mathbb{Q}\right\}$.
   (a) Show that G is a group under addition.
   (b) Show that non-zero elements of G forms a group under multiplication.
3. Let $G = \left\{z \in \mathbb{C} \text{ such that } z = 1 \text{ for some } n \in \mathbb{N}\right\}$
   (a) Show that G forms a group with respect to multiplication.
   (b) Show that G does not form a group with respect to addition.

Correction of tutorial series N°: 5 Algebra 1

Exercise 1:

1) we show that $(\mathbb{R}, *)$ is an abelian group.

$(\mathbb{R},*)$ is an abelian group $\Leftrightarrow$ $\begin{cases} i) \ \mathbb{R} \text{ is closed under } * \\ ii) \ * \text{ is associative.} \\ iii) \text{ Existence of identity element} \\ iv) \text{ Every element admits an inverse} \\ v) \ * \text{ is commutative.} \end{cases}$

i) $\mathbb{R}$ is closed under $*$.

$\forall x, y \in \mathbb{R} : x*y \in \mathbb{R}$?

Let $x, y \in \mathbb{R}$. $x*y = x+y+1 \in \mathbb{R}$.

ii) Associativity:

$\forall x,y,z \in \mathbb{R} : (x*y)*z = x*(y*z)$?

$$\begin{aligned}(x*y)*z &= (x+y+1)*z \\ &= (x+y+1)+z+1 \\ &= x+y+z+2 \quad \dots (1)\end{aligned}$$

$$\begin{aligned}x*(y*z) &= x*(y+z+1) \\ &= x+(y+z+1)+1 \\ &= x+y+z+2 \quad \dots (2)\end{aligned}$$

(1) = (2) then $*$ is associative.

iii) Identity element:

$\exists e \in \mathbb{R}, \forall x \in \mathbb{R}, x*e = e*x = x$?

$x*e = x \Leftrightarrow \cancel{x}+e+1 = \cancel{x} \Rightarrow e = -1 \in \mathbb{R}$.

we also have: $-1*x = x, \forall x \in \mathbb{R}$.

So $e=-1$ is the ~~element~~ identity element under $*$.

iv) Inverse element :

$\forall x \in \mathbb{R}, \exists x' \in \mathbb{R} : \quad x * x' = x' * x = e \, ?$

$x * x' = e = -1 \iff x + x' + 1 = -1$

$\iff x' = -x-2 \in \mathbb{R}$

we also have $(-x-2) * x = -1 \quad \forall x \in \mathbb{R}$.

So the inverse of x exist and equal to $(-x-2)$.

v) Commutativity :

$\forall x, y \in \mathbb{R} : \quad x * y = y * x \, ?$

$x * y = x + y + 1$

$= y + x + 1$ (because $+$ is commutative).

$= y * x$

. Conclusion :

from i), ii), iii) and iv) $(\mathbb{R}, *)$ is a group.

from i), ii), iii), iv), v) $(\mathbb{R}, *)$ is an abelian group.

2) We show that $(H, *)$ is a subgroup of $(\mathbb{R}, *)$.

H is an subgroup of $(\mathbb{R}, *) \iff \begin{cases} a) \; H \neq \phi \\ b) \; \forall x, y \in H : x * y^{-1} \in H \\ \quad (\text{where } y^{-1} \text{ is the Inverse of } y) \end{cases}$

a) $H \neq \phi$?

$e = -1 = 2(-1) + 1 = 2k + 1$ (with $k = -1$)

So $e \in H$, then $H \neq \phi$.

b) Let $x, y \in H$.

$x \in H \Rightarrow x = 2k + 1 \quad / \; k \in \mathbb{Z}$.

$y \in H \Rightarrow y = 2k' + 1 \quad / \; k' \in \mathbb{Z}$.

$y^{-1} = -y - 2 = -2k' - 3$.

$x * y^{-1} = x + y^{-1} + 1 = (2k+1) + (-2k'-3) + 1$

$= 2(k - k') - 1 = 2k'' - 1$

$x * y^{-1} = 2k'' - 1 \quad / \ k'' = k - k' \in \mathbb{Z}$

So $x * y^{-1} \in H$.

Conclusion :

from a) and b) H is a subgroup of $(\mathbb{R}, *)$.

3) f is a group homomorphism $\Leftrightarrow \forall x, y \in \mathbb{R} : f(x+y) = f(x) * f(y)$.

$$f(x+y) = f(x) * f(y) \Leftrightarrow (x+y) + \lambda = (x+\lambda) * (y+\lambda)$$
$$\Leftrightarrow x + y + \lambda = (x+\lambda) + (y+\lambda) + 1$$
$$\Leftrightarrow \cancel{x} + \cancel{y} + \lambda = \cancel{x} + \cancel{y} + 2\lambda + 1$$
$$\Rightarrow \boxed{\lambda = -1}$$

Exercise 02 :

1) we show that $(\mathbb{R}, \oplus, \otimes)$ is a ring with unity.

$(\mathbb{R}, \oplus, \otimes)$ is a ring with unity $\Leftrightarrow$
- i) $(\mathbb{R}, \oplus)$ is an abelian group
- ii) $\mathbb{R}$ is closed under $\otimes$
- iii) $\otimes$ is associative
- iv) $\otimes$ is distributive over $\oplus$
- v) Existence of identity element under $\otimes$

i) $(\mathbb{R}, \oplus)$ is an abelian group. (Already done. See exercise 1)

ii) $\mathbb{R}$ is closed under $\otimes$.

$\forall a, b \in \mathbb{R} : a \otimes b \in \mathbb{R}$?

$a \otimes b = a \cdot b + a + b \in \mathbb{R}$

iii) Associativity :

$\forall a, b, c \in \mathbb{R} : (a \otimes b) \otimes c = a \otimes (b \otimes c)$?

$$(a \otimes b) \otimes c = (ab + a + b) \otimes c$$
$$= (ab + a + b) \cdot c + (ab + a + b) + c$$
$$= abc + ac + ac + ab + a + b + c \quad \ldots (1)$$

$$a\otimes(b\otimes c) = a\otimes(bc+b+c)$$
$$= a\cdot(bc+b+c) + a + (bc+b+c)$$
$$= abc + ab + ac + bc + a + b + c \quad \ldots (2)$$

(1) = (2) then $\otimes$ is associative.

iv) $\otimes$ distributive over $\oplus$:

$\forall a,b,c \in \mathbb{R}$: $a\otimes(b\oplus c) = (a\otimes b)\oplus(a\otimes c)$.
and $(b\oplus c)\otimes a = (b\otimes a)\oplus(c\otimes a)$.

. $a\otimes(b\oplus c) = a\otimes(b+c+1)$
$$= a\cdot(b+c+1) + a + (b+c+1)$$
$$= ab + a\cdot c + 2a + b + c + 1 \quad \ldots (3).$$

. $(a\otimes b)\oplus(a\otimes c) = (a\otimes b) + (a\otimes c) + 1$
$$= (ab+a+b) + (ac+a+c) + 1$$
$$= ab + ac + 2a + b + c + 1 \quad \ldots (4)$$

(3) = (4) then $\otimes$ is distributive over $\oplus$.

v) Identity element under $\otimes$.

$\exists e' \in \mathbb{R}, \forall a \in \mathbb{R}$: $a\otimes e' = e'\otimes a = a$?

$a\otimes e' = a \iff ae' + a + e' = a$
$$\iff (a+1)\,e' = 0$$
$$\Rightarrow e' = 0.$$

we ~~also have~~ $0\otimes a = a \quad \forall a \in \mathbb{R}$.

So $e' = 0$ is the ~~elem~~ identity element of $\otimes$.

we also call this element, « unit element ».

conclusion:

from i), ii), iii), iv) $(\mathbb{R},\oplus,\otimes)$ is a ring.

from i), ii), iii), iv) and v) $(\mathbb{R},\oplus,\otimes)$ is a ring with unity.

2) f is a ring isomorphism $\Leftrightarrow \begin{cases} i)\ \forall a,b \in \mathbb{R}:\ f(a \oplus b) = f(a) + f(b) \\ ii)\ \forall a,b \in \mathbb{R}:\ f(a \otimes b) = f(a) \cdot f(b) \\ iii)\ f \text{ is bijective.} \end{cases}$

i) $\forall a,b \in \mathbb{R}:\ f(a \oplus b) = f(a) + f(b)$?

$$f(a \oplus b) = (a \oplus b) + 1$$
$$= (a+b+1) + 1$$
$$= a+b+2 \ \ldots \ (1).$$

$$f(a) + f(b) = (a+1) + (b+1)$$
$$= a+b+2 \ \ldots \ (2).$$

$(1) = (2)$.

ii) $\forall a,b \in \mathbb{R}:\ f(a \otimes b) = f(a) \cdot f(b)$?

$$f(a \otimes b) = (a \otimes b) + 1$$
$$= (ab + a + b) + 1$$
$$= ab + a + b + 1 \ \ldots \ (3)$$

$$f(a) \cdot f(b) = (a+1) \cdot (b+1).$$
$$= a \cdot b + a + b + 1 \ \ldots \ (4)$$

$(3) = (4)$

iii) f is bijective ?

$\forall y \in \mathbb{R},\ \exists!\, a \in \mathbb{R}:\ y = f(a)$?

Let $y \in \mathbb{R}$.

$y = f(a) \Leftrightarrow y = a+1 \Leftrightarrow a = y-1$

for all $y \in \mathbb{R}$, a exists and is unique in $\mathbb{R}$.

So f is bijective.

II) 1) Show that E is closed under $+$

$\forall a,b \in E : a+b \in E$?

Let $a,b \in E$.

$a \in E \Leftrightarrow a = x + y\sqrt{3} \quad / x,y \in \mathbb{Q}$

$b \in E \Leftrightarrow b = x' + y'\sqrt{3} \quad / x',y' \in \mathbb{Q}$.

$$a+b = (x+y\sqrt{3}) + (x'+y'\sqrt{3})$$
$$= (x+x') + (y+y')\sqrt{3}$$
$$= x'' + y''\sqrt{3} \quad \text{such that } x''=x+x' \in \mathbb{Q},\ y''=y+y' \in \mathbb{Q}$$

So $a+b \in E$.

ii) Show that E is closed under "$\circ$"

$\forall a,b \in E : a\cdot b \in E$?

Let $a,b \in E$.

$a \in E \Leftrightarrow a = x + y\sqrt{3} \quad , x,y \in \mathbb{Q}$

$b \in E \Leftrightarrow b = x' + y'\sqrt{3} \quad , x',y' \in \mathbb{Q}$.

$$a\circ b = (x+y\sqrt{3})\cdot(x'+y'\sqrt{3})$$
$$= (xx'+3yy') + (xy'+yx')\sqrt{3}.$$
$$= x''' + y'''\sqrt{3}$$

such that $x''' = xx'+3yy' \in \mathbb{Q}$

$y''' = xy'+yx' \in \mathbb{Q}$

So $a\cdot b \in E$.

II.2) Show that:

$\forall a \in E\setminus\{0\},\ \exists a^{-1} \in E\setminus\{0\} : a\circ a^{-1} = a^{-1}\cdot a = 1$.

where

. a^{-1} is the inverse element of a under the multiplicat

. 1 is the unit element of $\mathbb{R}$ under the multiplicatio

Let $a \in E\setminus\{0\}$. Then $a = x + y\sqrt{3}$ $/ \, x, y \in \mathbb{Q}\setminus\{0\}$.

$$a \cdot a^{-1} = 1 \Leftrightarrow a^{-1} = \frac{1}{a} = \frac{1}{x+y\sqrt{3}}.$$

$$\Leftrightarrow a^{-1} = \frac{1}{x+y\sqrt{3}} \cdot \frac{x-y\sqrt{3}}{x-y\sqrt{3}}.$$

$$\Rightarrow a^{-1} = \frac{x-y\sqrt{3}}{x^2-3y^2} = \frac{x}{x^2-3y^2} + \frac{-y}{x^2-3y^2}\cdot\sqrt{3}.$$

But do we have $x^2 - 3y^2 \neq 0$?

we prove by contradiction that : $x^2 - 3y^2 \neq 0$.

we suppose that : $\exists x, y \in \mathbb{Q}\setminus\{0\} : x^2 - 3y^2 = 0$.

$$x^2 - 3y^2 = 0 \Leftrightarrow \frac{x^2}{y^2} = 3 \Rightarrow \left|\frac{x}{y}\right| = \sqrt{3}.$$

$\sqrt{3} = \left|\frac{x}{y}\right| \Rightarrow \sqrt{3}$ is a rationnal number. (Impossible)

Contradiction because $\sqrt{3}$ is an irrationnal number.

we have

$$a^{-1} = \frac{x}{x^2-3y^2} + \frac{-y}{x^2-3y^2}\cdot\sqrt{3}.$$

$$= x' + y'\sqrt{3} \quad / \; x' = \frac{x}{x^2-3y^2} \in \mathbb{Q}\setminus\{0\}.$$

$$y' = \frac{-y}{x^2-3y^2} \in \mathbb{Q}\setminus\{0\}.$$

Then $a^{-1} \in E\setminus\{0\}$.

So the inverse of $a \in E\setminus\{0\}$ exists in $E\setminus\{0\}$.

3) E is a subfield of the field $(\mathbb{R},+,\cdot) \Leftrightarrow \begin{cases} i)\ E \neq \phi. \\ ii)\ E \text{ is closed under } + \\ iii)\ E \text{ is closed under } \cdot \\ iv)\ \forall a \in E,\ -a \in E. \\ v)\ \forall a \in E\setminus\{0\},\ a^{-1} \in E\setminus\{0\} \end{cases}$

where:

$-a$ is the inverse of a under $+$.

a^{-1} is the inverse of a under $\cdot$

0 is the identity element under $+$.

i) $E \neq \phi$.

$0 = 0 + 0\cdot\sqrt{3} \Rightarrow 0 \in E.$

$1 = 1 + 0\sqrt{3} \Rightarrow 1 \in E.$ $\Rightarrow E \neq \phi$.

ii)-iii) the properties ii) and iii) are already made. See II. 1).

iv) $\forall a \in E,\ -a \in E$?

Let $a \in E$, then $a = x + y\sqrt{3}$ $/\ x, y \in \mathbb{Q}$.

$-a = (-x) + (-y)\sqrt{3}$.

$= x' + y'\sqrt{3}$ $/\ x' = -x \in \mathbb{Q},\ y' = -y \in \mathbb{Q}$

So $-a \in E$.

v) the property v) is already made. See II.2).