Groups, rings and fields

$\mathfrak{H}.\mathfrak{C}$

12 décembre 2023

1 Groups, rings and fields

1.1 Groups

1.1.1 Definitions and Examples

Definition 1.1.1 *A group is a set G which is **CLOSED** under an operation $*$ (that is, for any $x, y \in G, x * y \in G$) and satisfies the following properties :*

1. ***(Associativity)*** *For all $x, y, z \in G, (x * y) * z = x * (y * z)$,*
2. *There exists an element $e \in G$ such that :*

a/ ***(Identity)*** $\forall x \in G, e * x = x * e = x$ *; and*

b/ ***(Inverses)***$\forall x \in G, \exists x' \in G$ *such that* $x * x' = x' * x = e$.

If in addition the following holds :
Commutativity : $x * y = y * x$ *for all* $x, y \in G$, *then* $(G, *)$ *is called an **abelian group**, or simply **a commutative group.***

Remark 1.1.1 *if $(G, *)$ is a group then the identity e is unique and the inverse of any x in G is uniquely determined by x.*

Example 1.1.1
1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ *and* $(\mathbb{C}, +)$ *are abelian groups* ($e = 0, \quad x' = -x$).
2. $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ *are abelian groups* ($e = 1, \quad x' = \frac{1}{x}$).
3. $(\mathbb{Z}, \cdot)$ *is not a group.*
4. $(\mathbb{N}, +)$ *is not a group.*
5. ***bijections on a set** E.*
   Fix a non-empty set E and let

$$\mathcal{B}(E, E) = \{f : E \to E / \quad f \text{ is a bijection }\},$$

   and let "$\circ$" denote composition of maps.

a/ $(\mathcal{B}(E, E), \circ)$ *is a group that is not abelian.*
Indeed, let $E = \mathbb{R}$, we consider the following applications :

$$f : \begin{array}{rcl} \mathbb{R} & \to & \mathbb{R} \\ x & \longmapsto & 2x \end{array} \quad \text{and}$$

$$g : \begin{array}{rcl} \mathbb{R} & \to & \mathbb{R} \\ x & \longmapsto & 1 - x. \end{array} \quad \text{Then } f \circ g \neq g \circ f.$$

6. *Let $\mathcal{R}$ be the set of rotations of the plane whose center is at the origin O.*
Then for two rotations R_θ and R_α, the composite $R_\theta \circ R_\alpha$ is still a rotation with center the origin and angle $\theta + \alpha$. Thus $(\mathcal{R}, \circ)$ forms a group (which is even commutative). For this law the identity is the rotation of angle 0 (it is the identity of the plane). The inverse of a rotation R_θ is the rotation $R_{-\theta}$

7. *For any natural number n, the set $G = \mathbb{Z}/n\mathbb{Z}$ of equivalence classes modulo n defined by*

$$\forall x \in \mathbb{Z}, \quad \overline{x} \in \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \overline{x} = \{y \in \mathbb{Z}/ \quad y - x \equiv 0\,[n]\} = \{y \in \mathbb{Z}/y - x \in n\mathbb{Z}\}\,.$$

We define the additive law denoted $\dot{+}$ as follows

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}, \quad \overline{x} \dot{+} \overline{y} = \overline{x+y}.$$

$(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ is an abelian group. Indeed :

a/ *G is closed under $\dot{+}$, since $x + y \in \mathbb{Z}$ and therefore $x \dot{+} y = \overline{x+y} \in \mathbb{Z}/n\mathbb{Z} = G$.*

b/ *$\dot{+}$ is associative, since $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}/n\mathbb{Z}$,*

$$\begin{aligned}(\overline{x} \dot{+} \overline{y}) \dot{+} \overline{z} &= \overline{(x+y)} \dot{+} \overline{z} \\ &= \overline{(x+y)+z} \\ &= \overline{x+(y+z)} \\ &= \overline{x} \dot{+} \overline{(y+z)} \\ &= \overline{x} \dot{+} (\overline{y} \dot{+} \overline{z})\,.\end{aligned}$$

c/ *Knowing that $+$ is commutative in $\mathbb{Z}$, the law $\dot{+}$ satisfies,*
$\overline{x} \dot{+} \overline{y} = \overline{(x+y)} = \overline{(y+x)} = (\overline{y} \dot{+} \overline{x})$. which shows that $\dot{+}$ is commutative

d/ *The identity element $\overline{0}$ given by :*
$\overline{x} \dot{+} \overline{0} = \overline{x+0} = \overline{x}$.
is well defined, since 0 is the identity element of $\mathbb{Z}$ for the law $+$, and therefore $\overline{0}$ is the identity element of G for the law $\dot{+}$.

e/ *For all x, we have*
$\overline{x} \dot{+} \overline{-x} = \overline{x + (-x)} = \overline{0}$,
since the symmetric of x in $\mathbb{Z}$ for the law $+$ is $-x$. Thus, $\overline{x}$ admits as symmetric the element $\overline{-x}$ for the law $\dot{+}$.
Therefore, $\mathbb{Z}/n\mathbb{Z}$, is an abelian group.

For example *in $\mathbb{Z}/60\mathbb{Z}$, we have $\overline{31} \dot{+} \overline{46} = \overline{31+46} = \overline{77} = \overline{60+17} = \overline{60} \dot{+} \overline{17} = \overline{0} \dot{+} \overline{17} = \overline{17}$.*

Proposition 1.1.1 *Let $(G, *)$ be a group then*

1. *$\forall a, b \in G$ the equation $a * x = b$ (respectively $x * a = b$) admits a unique solution in G, $\quad x = a^{-1}b$ (respectively $x = b * a^{-1}$).*
2. *$\forall a, b, c \in G$ such that*
$a * b = a * c$ (respectively $b * a = c * a$) we have $b = c$.

1.2 Subgroups

Definition 1.2.1 *Let $(G, *)$ be a group. We say that a non-empty part H of G is a subgroup of G if $(H, *)$ is itself a group.*

Proposition 1.2.1 *Let G be a group, with identity e, and H a part of G, then the following properties are equivalent :*

1. *H is a subgroup of G,*
2. *$e \in H$ and $\forall x, y \in H$ we have $x * y^{-1} \in H$.*

Remark 1.2.1 *G and $\{e\}$ are so-called trivial subgroups of G.*

Théorème 1.2.1 *Additive subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, where n is a positive integer.*

Proof 1.2.1 *For $n = 0$, $\{0\} = 0\mathbb{Z}$ is, by the previous remark, a subgroup of $\mathbb{Z}$.*
Let $H = n\mathbb{Z}, \quad n > 0$. So we have

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

b/ Let $x, y \in H$, then $\exists k, l \in \mathbb{Z}$ such that $x = nk$ and $y = nl$. Thus, $y^{-1} = -y = n(-l)$ and we have

$$x + (-y) = nk + n(-l) = n(k - l) \in n\mathbb{Z}.$$

Which shows that $H = n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Théorème 1.2.2 *Let G be a group and $(H_i)_{i\in I}$ a family of subgroups of G, then $\cap_{i\in I} H_i$ is a subgroup of G.*

Proof 1.2.2 *Given that $\forall i, H_i$ is a subgroup of G, then $e \in H_i \quad \forall i$.*
Thus, $e \in \cap_{i\in I} H_i$ On the other hand, $\forall x, y \in \cap_{i\in I} H_i$ we have $x, y \in H_i$ for all $i \in I$, and H_i a subgroup of G, then $\forall i \in I$ we have $x * y^{-1} \in H_i$. Which leads to $x * y^{-1} \in \cap_{i\in I} H_i$.

Remark 1.2.2 *The union of subgroups is not a subgroup.*

Indeed, consider $H_1 = 3\mathbb{Z}$ and $H_2 = 5\mathbb{Z}$ two subgroups of $\mathbb{Z}$. If $H_1 \cup H_2$ was a subgroup, then $8 = 3 + 5 \in H_1 \cup H_2$ which is impossible since $8 \notin H_1$ and $8 \notin H_2$.
Let us give in what follows a necessary and sufficient condition for the union of subgroups to be a subgroup.

Théorème 1.2.3 *Let H_1 and H_2 be two subgroups of a group G. $H_1 \cup H_2$ is a subgroup of G if and only if $H_1 \subseteq H_2$ or $H_1 \subseteq H_2$.*

1.3 Group homomorphisms

Given two groups $(G, *)$ and $(G', \top)$ two respective groups of identities elements e and e'.

Definition 1.3.1 *We call **homomorphism** groups G and G' any map $f : G \to G'$ verifying*

$$f(a * b) = f(a) \top f(b), \quad \forall a, b \in G.$$

*If moreover $G = G'$, f is said to be **an endomorphism** of G.*

Example 1.3.1 *1. let $G = G' = \mathbb{R}$ be an additive group and let the map $f : \mathbb{R} \to \mathbb{R}/ \quad f(x) = 2x$. We have : $\forall x, y \in \mathbb{R}$*

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y).$$

f is therefore an homomorphism of groups.

*2. Consider the application
$f : \mathbb{R}^3 \to \mathbb{R}^2, \quad f(x, y, z) = (x + y, y - z)$ where $\mathbb{R}^2, \mathbb{R}^3$ are considered additive groups.
Let $X = (x, y, z)$ and $X' = (x', y', z') \in \mathbb{R}^3$, then*

$$\begin{aligned} f(X + X') &= f((x + x', y + y', z + z')) \\ &= ((x + x') + (y + y'), (y + y') - (z + z')) \\ &= ((x + y) + (x' + y'), (y - z) + (y' - z')) = (x + y, y - z) + (x' + y', y' - z') \\ &= f((x, y, z)) + f((x', y', z')). \end{aligned}$$

Proposition 1.3.1 *Let $f : G \to G'$ be a homomorphism of groups, then*

1. *$f(e) = e'$.*
2. *$(f(x^{-1})) = (f(x))^{-1}, \quad \forall x \in G$.*

Proof 1.3.1 *Since f is an homomorphism, then $f(a * b) = f(a) \top f(b), \forall a, b \in G$. Then :*

1. *we have : $f(e) = f(e * e) = f(e) \top f(e), with f(e) \in G'$, then $f(e) = e'$.*
2. *Like $e' = f(e) = f(x * x^{-1}) = f(x) \top f(x^{-1}), \forall x \in G$, then $f(x^{-1})$ is the symmetric of $f(x)$ for the operation $\top$. Thus $f(x^{-1}) = (f(x))^{-1}$.*

Example 1.3.2 *Let's take the example of the function $f : \mathbb{R} \to \mathbb{R}_+^*$ defined by $f(x) = exp(x)$.
We indeed have $f(0) = 1$: the identity of $(\mathbb{R}, +)$ has as its image the identity of $(\mathbb{R}_+^*, .)$.
For $x \in \mathbb{R}$ its inverse in $(\mathbb{R}, +)$ is here its opposite $-x$, then $f(-x) = exp(-x) = \frac{1}{exp(x)} = \frac{1}{f(x)}$ is indeed the opposite (in $(\mathbb{R}_+^*, .)$ $\quad of \quad$ $f(x)$).*

Proposition 1.3.2 *1. Let two morphisms of groups $f : G \to G'$ and $g : G' \to G"$. Then $g \circ f : G \to G"$ is a morphism of groups.*

2. If $f : G \to G'$ is a bijective morphism then $f^{-1} : G' \to G$ is also a group morphism.

Proof 1.3.2 *The first part is easy. Let's show the second part :
Let $y, y' \in G'$. Since f is bijective, there exists $x, x' \in G$ such that $f(x) = y$ and $f(x') = y'$.
Then $f^{-1}(y \top y') = f^{-1}(f(x) \top f(x')) = f^{-1}(f(x * x')) = x * x' = f^{-1}(y) * f^{-1}(y')$. And therefore f^{-1} is a morphism from G' to G.*

Definition 1.3.2 *A bijective morphism is an **isomorphism**, if in addition $G = G'$, we say that f is **an automorphism**.
Two groups G, G' are isomorphic if there exists a morphism bijective $f : G \to G'$.*

Example 1.3.3 *Still continuing the example $f(x) = exp(x), \quad f : \mathbb{R} \to \mathbb{R}_+^*$ is a bijective map.
Its reciprocal bijection $f^{-1} : \mathbb{R}_+^* \to \mathbb{R}$ is defined by $f^{-1}(x) = ln(x)$.
According to the proposition above, f^{-1} is also a morphism from $(\mathbb{R}_+^*, \times)$ to $(\mathbb{R}, +)$ so $f^{-1}(x \times x') = f^{-1}(x) + f^{-1}(x')$, what is expressed here by the well-known formula : $ln(x \times x') = ln(x) + ln(x')$. Thus f is an isomorphism and the groups $(\mathbb{R}_+^*, \times)$ and $(\mathbb{R}, +)$ are isomorphic.*

1.4 Kernel and image

Let $f : G \to G'$ be a group morphism. We define two important subsets which will be subgroups.

Definition 1.4.1 *The kernel of f is*

$$Kerf = \{x \in G / \quad f(x) = e_{G'} = e'\}.$$

So it's a subset of G. In terms of reciprocal image we have by definition $Kerf = f^{-1}(\{e'\})$ (**Attention**, the notation f^{-1} here denotes the reciprocal image, and does not mean that f is bijective.)

Definition 1.4.2 *The image of f is*

$$Imf = \{f(x)/ \quad x \in G\}.$$

It is therefore a subset of G' and in terms of direct image we have $Imf = f(G)$.

Proposition 1.4.1 *Let $f : G \to G'$ be a group morphism.*

1. *$Kerf$ is a subgroup of G.*
2. *Imf is a subgroup of G'.*
3. *f is injective if and only if $Kerf = \{e\}$.*
4. *f is surjective if and only if $Imf = G'$.*

Example 1.4.1 *Consider the following homomorphism :*
$f : \mathbb{R}^2 \to \mathbb{R}^2, \quad f(x, y) = (x + y, x - y)$.
SO

$$kerf = \{(x, y)/ \quad f(x, y) = (0, 0)\},$$

$f(x, y) = (0, 0) \Leftrightarrow x + y = 0$ *and* $x - y = 0$, *thus* $x = y = 0$, *therefore*

$$kerf = \{(0, 0)\}.$$

So according to the proposition above f is injective.

$$Imf = \left\{f(x, y)/ \quad (x, y) \in \mathbb{R}^2\right\}.$$

We have $(X, Y) \in \mathbb{R}^2, suchthat (X, Y) = f(x, y) = (x + y, x - y)$,
therefore $x = \frac{1}{2}X + \frac{1}{2}Y$ *and* $y = \frac{1}{2}X - \frac{1}{2}Y$.
This system admits a unique solution (X, Y) for each value of (x, y), therefore $Imf = \mathbb{R}^2$, and f is surjective.

2 Rings

2.1 The definition of a ring.

Let $+$ and $\cdot$ be two binary operations defined on a non-empty set A.

Definition 2.1.1 *A structure $(A, +, \cdot)$ is a ring if we have the following properties :*

1. ***Addition :***
   $(A, +)$ is an abelian group :

a/ ***Associativity.***

b/ ***Zero :*** *there exists $0 \in A$ such that for all $a \in A$ we have $a + 0 = 0 + a = a$.*

c/ ***Inverses :*** *for any $a \in A$ there exists $-a \in A$ such that $a + (-a) = (-a) + a = 0$.*
Commutativity : *for all $a, b \in A$ we have $a + b = b + a$.*

2. ***Multiplication :***
   The law " $\cdot$ " is associative : for all $a, b, c \in A$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3. ***Addition and multiplication together.***
   For all $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad et \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

We sometimes say A is a ring, taken it as given that the ring operations are denoted " $+$ " and " $\cdot$ " As in ordinary arithmetic we shall frequently suppress $\cdot$ and write ab instead of $a \cdot b$. We do NOT demand that multiplication in a ring be commutative.
Notation : subtraction and division We write $a - b$ as shorthand for $a + (-b)$ and a/b as shorthand for $a \cdot (1/b)$ when $1/b$ exists.

Remark 2.1.1

1. *If furthermore there exists $1_A \in A$ such that $a \cdot 1_A = 1_A \cdot a = a, \forall a \in A$, we say that $(A, +, \cdot)$ is a unit ring.*
2. *If the law " $\cdot$ " is commutative, A is called a commutative ring.*

Considérations.

1. In the following, the rings considered are unitary.
2. We define a^n for $n \in \mathbb{N}$ as follows : $a^n = \{ \begin{array}{lll} 1_A & if & n = 0 \\ a & if & n = 1 \\ a \cdot a \cdots a \quad (n \quad times) & if & n \geq 2 \end{array}$

Examples of rings.

Number systems

1. All of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are commutative unit rings with identity 1.
2. $\mathbb{N}$ is NOT a ring for the usual addition and multiplication. These are binary operations and we do have a zero element, namely 0.
   The existence of additive inverses fails : there is no $n \in \mathbb{N}$ for which $1 + n = 0$, for example.
3. Consider the set of even integers, denoted $2\mathbb{Z}$, with the usual addition and multiplication. This is a commutative ring without an identity. To verify that this condition (of identity) fails it is just to say that the integer 1 does not belong to $2\mathbb{Z}$.
   Instead we argue as follows. Suppose for contradiction that there were an element $e \in 2\mathbb{Z}$ such that $n \cdot e = n$ for all $n \in 2\mathbb{Z}$. In particular $2e = 2$, from which we deduce that e would have to be 1. Since $1 \notin 2\mathbb{Z}$ we have a contradiction.

4. Let $A = C([0,1],\mathbb{R}) = \{f : [0,1] / \quad f \quad continue\}$.
   We define on A the following operations : " + "," · "
   $f+g : \quad [0,1] \to \mathbb{R}$, $x \mapsto (f+g)(x) = f(x)+g(x)$. $\qquad f\cdot g : \quad [0,1] \to \mathbb{R}$, $x \mapsto (f\cdot g)(x) = f(x)\cdot g(x)$.

We check that $(A,+,\cdot)$ is a commutative ring. The identity element for the addition " + " is the function :

$0 : \quad [0,1] \to \mathbb{R}$, $x \mapsto 0(x) = 0$. And the identity element 1_A for multiplication, is the function :

$1_A : \quad [0,1] \to \mathbb{R}$, $x \mapsto 1_A(x) = 1$.

Calculational rules for rings

Proposition 2.1.1 *Let $(A,+,\cdot)$ be a ring, then we have :*

1. $\forall a \in A, \quad 0\cdot a = a\cdot 0 = 0$,
2. $\forall a,b \in A, \quad a\cdot(-b) = (-a\cdot b)$,
3. $\forall a,b,c \in A, \quad a\cdot(b-c) = a\cdot b - a\cdot c$,
4. *Assume in addition that " · " is commutative, then $\forall n \in \mathbb{N}$ et $\forall a,b \in A$, we have :*

$$(a+b)^n = \sum_{k=0}^{n} \mathcal{C}_k^n a^k \cdot b^{n-k}. \qquad binôme \quad of \quad Newton.$$

Proof 2.1.1 *Let 0 denote the identity element of the first law " + " of A.*

1. *By distributivity of " · " with respect to " + " we have*

$$0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$$

   Since $(A,+)$ is a group, we can simplify on the left and right by $0\cdot a$, which gives $0 = 0\cdot a$. Similarly, if we write $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$, we obtain $a\cdot 0 = 0$
2. *Since $0 = a\cdot 0 = a\cdot(b+(-b))$, then $0 = a\cdot b + a\cdot(-b)$, which shows that $a\cdot(-b)$ is the inverse of $a\cdot b$. Thus, $a\cdot(-b) = -ab$.*
3. *Since $b-c = b+(-c)$ then*
   $a\cdot(b-c) = a\cdot(b+(-c)) = a\cdot b + a\cdot(-c) = a\cdot b - a\cdot c$
4. *To demonstrate Newton's binomial, we'll adopt reasoning by induction.*

a/ *For $n=0$, we have $(a+b)\cdot 0 = 1_A = \mathcal{C}_0^0 \cdot a^0 b^0$.*

b/ *We assume that $(a+b)^n = \sum_{k=0}^{n} \mathcal{C}_k^n a^k \cdot b^{n-k}$ and show that :*

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \mathcal{C}_k^{n+1} a^k \cdot b^{n+1-k} = \mathcal{C}_0^{n+1} b^{n+1} + \mathcal{C}_1^{n+1} a\cdot b^n + \mathcal{C}_2^{n+1} a^2\cdot b^{n-1} + \cdots + \mathcal{C}_n^{n+1} a^n b + \mathcal{C}_{n+1}^{n+1} a^{n+1}.$$

Since $(a+b)^{n+1} = (a+b)(a+b)^n = a\cdot(a+b)^n + b\cdot(a+b)^n$ then

$$a(a+b)^n = \mathcal{C}_0^n a\cdot b^n + \mathcal{C}_1^n a^2\cdot b^{n-1} + \mathcal{C}_2^n a^3\cdot b^{n-2} + \cdots + \mathcal{C}_n^{n-1} a^n b + \mathcal{C}_{n+1}^n a^{n+1}.$$

and

$$b(a+b)^n = \mathcal{C}_0^n \cdot b^{n+1} + \mathcal{C}_1^n ba \cdot b^{n-1} + \mathcal{C}_2^n ba^2 \cdot b^{n-2} + \cdots + \mathcal{C}_n^{n-1} ba^{n-1} b + \mathcal{C}_n^n ba^n.$$

On the other hand we have $ba^k b^l = a^k b^{-l+1}$, *since* " $\cdot$ " *is commutative, and* $\mathcal{C}_n^m + \mathcal{C}_{n+1}^m = \mathcal{C}_{n+1}^{m+1}$, *by summing the two previous equalities we get :*

$$(a+b)^{n+1} = \mathcal{C}_0^n b^{n+1} + (\mathcal{C}_0^n + \mathcal{C}_1^n)\, a \cdot b^n + (\mathcal{C}_1^n + \mathcal{C}_2^n)\, a^2 \cdot b^{n-1} + \cdots + \left(\mathcal{C}_{n-1}^n + \mathcal{C}_n^n\right) a^n b + \mathcal{C}_n^n a^{n+1}.$$

This leads to

$$(a+b)^{n+1} = \mathcal{C}_0^{n+1} b^{n+1} + \mathcal{C}_1^{n+1} a \cdot b^n + \mathcal{C}_2^{n+1} a^2 \cdot b^{n-1} + \cdots + \mathcal{C}_n^{n+1} a^n b + \mathcal{C}_{n+1}^{n+1} a^{n+1}.$$

Hence the result.

Integral domain

Definition 2.1.2 *An integral domain is a nonzero commutative ring* A *in which the product of any two nonzero elements is nonzero i.e.*
$\forall a, b \in A, \quad a \cdot b = 0 \Rightarrow a = 0 \quad or \quad b = 0$

Example 2.1.1 *1.* $(A, +, \cdot)$ *is an integral domain for* $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *and* $\mathbb{C}$.

2. For $A = C([0,1], \mathbb{R}) = \{f : [0,1] / \quad f \quad continue\}$. *The ring* $(A, +, \cdot)$ *defined above is not an integral domain. Indeed Consider the functions* f *and* g *in* A *given by*
$f(x) = \left\{ \begin{array}{lll} x-1 & if & x \in \left[0, \frac{1}{2}\right[\\ 0 & if & x \in \left[\frac{1}{2}, 1\right]. \end{array} \right.$ $g(x) = \left\{ \begin{array}{lll} 0 & if & x \in \left[0, \frac{1}{2}\right[\\ -x+1 & if & x \in \left[\frac{1}{2}, 1\right]. \end{array} \right.$
We can see that $f \neq 0$ *and* $g \neq 0$ *but* $f \cdot g = 0$ *since* $forall x \in [0,1]$ *we have* $f(x) \cdot g(x) = 0$.

2.2 Subrings and the Subring Test.

Let $(A, +, \cdot)$ be a ring and let A' be a non-empty subset of A. Then $(A', +, \cdot)$ is a subring of A if it is a ring with respect to the operations it inherits from A.

The Subring Test

Let $(A, +, \cdot)$ be a ring and let $A' \subseteq A$. Then $(A, +, \cdot)$ is a subring of A if (and only if) A' is non-empty and the following hold :

1. $(A', +)$ is an abelian subgroup of $(A, +)$,
2. $\forall a, b \in A', a \cdot b \in A'$.

Example 2.2.1 *1.* $\mathbb{Z}$ *and* $\mathbb{Q}$ *are subrings of* $\mathbb{R}$,

2. $\mathbb{R}$, *regarded as numbers of the form* $a + 0i$ *for* $a \in \mathbb{R}$, *is a subring of* $\mathbb{C}$.

3. In the polynomial ring $\mathbb{R}[x]$, *the polynomials of even degree form a subring but the polynomials of odd degree do NOT form a subring because* $x \cdot x = x^2$ *is not of odd degree.*

4. $n\mathbb{Z} = \{nk | \quad k \in \mathbb{Z}\}$ *is a subring of* $\mathbb{Z}$ *for any* $n \in \mathbb{N}$.

5. The null ring is the ring $\{0\}$ *formed by a single element.*

Example 2.2.2 *1. Let be the set* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}/a \in \mathbb{Q}, \quad b \in \mathbb{Q}\}$.
$\mathbb{Q}[\sqrt{2}]$ *is a ring. We check that* $\mathbb{Q}$ *is a subring of* $\mathbb{Q}[\sqrt{2}]$ *for usual addition and multiplication.*

2. ***The ring*** $\mathbb{Z}/n\mathbb{Z}$
Let's fix an integer $n \geq 2$. *Consider the additive group* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$. *We've already seen that the additive group* $\mathbb{Z}/n\mathbb{Z}$ *is abelian. We define a multiplication in* $\mathbb{Z}/n\mathbb{Z}$ *from that in* $\mathbb{Z}$ *by posing :* $\overline{x}{\cdot}\overline{y} = \overline{xy}$ *for all* $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$. *This multiplication is well defined, regardless of the representatives chosen. It's immediate to check that* $\mathbb{Z}/n\mathbb{Z}$ *is a unitary commutative ring.*

2.3 Ring homomorphism

Definition 2.3.1 *Let* $(A, +, \cdot)$ *and* $(B, +, \cdot)$ *be two rings of identities elements* 1_A *and* 1_B *respectively and* $f : A \to B$ *be a map.*
We say that f *is a if* $\forall a, b \in A$ *we have*

1. $f(a + b) = f(a) + f(b)$,
2. $f(a \cdot b) = f(a) \cdot f(b)$,
3. $f(1_A) = 1_B$.

If in addition f *is a bijection, then its inverse* f^{-1} *is also a ring homomorphism. In this case,* f *is called a* ***ring isomorphism****, and the rings* A *and* B *are called* ***isomorphic.***
From the standpoint of ring theory, isomorphic rings cannot be distinguished.

3 Fields and integral domains

Definition of a field :

Definition 3.0.1 *Let* K *a set, a structure* $(K, +, \cdot)$, *where* $+$ *and* $\cdot$ *are binary operations on* K *is a field if :*

1. $(K, +)$ *is an abelian group. (Identity noted* 0_K*.),*
2. $(K - \{0\}, \cdot)$ *is an abelian group. (Identity noted* 1_K*.),*
3. *The distributive laws hold (the " · " is distributive with respect to +).*

Proposition 3.0.1 *Let* $(K, +, \cdot)$ *be a ring.*
$(K, +, \cdot)$ *is a field if, and only if, every non-zero element of* K *is invertible, i.e. for all* $a \in K$ *with* $a \neq 0$ *there exists* $1/a \in K$ *(alternatively written* a^{-1}*) such that* $a \cdot 1/a = 1/a \cdot a = 1$.

Definition 3.0.2 *In a commutative ring we call an element* $a \neq 0$ *a zero divisor if there exists* $b \neq 0$ *such that* $a \cdot b = 0$.
A commutative ring with identity in which $0 \neq 1$ *is an* ***integral domain (ID)*** *if it has no zero divisors.*

Examples of integral domains

1. *We claim that any field is an integral domain. To prove this, assume that* $(K, +, \cdot)$ *is a field and let* $a, b \in K$ *be such that* $a \cdot b = 0$. *If* $a \neq 0$ *then* a^{-1} *exists, and we have*

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = \big((a^{-1} \cdot a) \cdot b\big) = 1 \cdot b = b.$$

   and likewise with the roles of a *and* b *reversed.*

2. $\mathbb{Z}$ *and* $K[x]$ *are integral domains which fail to be fields.*
3. K^2, *with coordinatewise addition and multiplication is a commutative ring with identity which fails to be an integral domain (and so is not a field) :*

$$(0, 1) \cdot (1, 0) = (0, 0).$$

3.1 Subfield

If $(K, +, \cdot)$ *is a field, a sub-field of* K *is a sub-ring* K' *of* K *such that for any non-zero element* x *of* K', *we have* $x^{-1} \in K', (K', +, \cdot)$ *is then a field.*

Example 3.1.1

1. $\mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$ *are fields, but not* Z *(2 is not invertible).*
2. $\mathbb{Q}[\sqrt{2}]$ *is a subfield of* $\mathbb{R}$.

Proposition 3.1.1 ***Characterization of sub-fields*** *Let* $(K, +, \cdot)$ *a field. A non-empty part* K' *of* K *is a sub-field of* K, *if and only if*

1. $1_K \in K'$
2. $\forall x, y \in K'; \quad x - y \in K'$.
3. $\forall x, y \in K'; \quad x \cdot y \in K'$.
4. $\forall x \in K'; \quad x^{-1} \in K'$.