OPERATIONS et STRUCTURES

Lois de composition interne, Groupes, Anneaux, Idéaux, Corps.

On appelle **E X F**, **ensemble produit** de E par F, l'ensemble des couples **(a , b)** tels **a∈E** et **b∈F**.
A ⇨ B se lit « A implique B »

Loi de composition interne dans E :

Définition application de **E X E** dans **E**

Exemple1 addition dans Z

(+2 , +3) ➔ (+2) + (+ 3) = +5

(–2 , +7) ➔ (–2)+(+7)= +5

Exemple 2 Opération modulo dans N* :
Opération qui a un couple d'entiers non nuls (a , b) fait correspondre le reste de la division entière de a par b
14 : 3 = 4 reste 2 d'où **14 mod 3 = 2**
Si a = bq + r avec r < q on écrit **a mod b = r**
Ce n'est pas une opération interne sur **N** car on ne peut pas diviser un nombre par **0**, ni sur **N*** car si **b** est un diviseur de **a**, le reste de la division de **a** par **b** est **0** (➔ On sort de **N***).

Loi de composition externe sur E :

Définition application de Ω X E dans **E**

Exemple : la multiplication d'un vecteur par scalaire
Je multiplie un vecteur $\vec{V}$ par un scalaire par exemple **8** , je trouve $8\vec{V}$ qui est un vecteur .

Propriétés des lois de composition internes :

Dans ce qui suit ● et ‡ sont des lois de composition interne quelconques qu'on peut lire respectivement « loi » et « loi 2 » par exemple

Associativité : tout (a,b,c) ∈ E^3 **(a ● b) ● c = a ● (b ● c)**

Commutativité : tout (a,b) ∈ E^2 **a ● b = b ● a**

Distributivité à gauche de ● par rapport à ‡ : tout (a,b,c) ∈ E^3 : **a●(b ‡ c) = (a ● b) ‡ (a ● c)**

Distributivité à droite de ● par rapport à ‡ : tout (a,b,c) ∈ E^3 : **(b ‡ c) ● a = (b ● a) ‡ (c ● a)**

Une loi est **distributive** par rapport à une autre si elle est distributive à gauche et à droite

Elément neutre : tout a ∈ E **a ● e = e ● a = a** (Dans R : e= 0 pour + et e = 1 pour le produit)

Symétrique : si pour a ∈ E , il existe $\mathbf{a^{-1}} \in$E tel que **a ● a^{-1} = a^{-1} ● a = e** a^{-1} symétrique de **a** pour ●
(Dans R, le symétrique de a pour + est l'opposé –a, dans R*, pour le produit c'est l'inverse de a (1/a))

a∈E simplifiable pour ● si tout (b,c)∈ E^2 **a ● b = a ●c ⇨b = c**
et **b ● a = c ● a ⇨ b = c**

Quelques remarques et trucs utiles pour résoudre les problèmes

Attention : tant qu'on n'a pas montré qu'une loi est commutative, on n'a pas le droit d'inverser l'ordre des éléments combinés par la loi

● L'associativité nous permet de combiner trois opérandes en commençant par l'association soit des 2 derniers, soit des 2 premiers, mais le résultat de cette association doit rester à sa place.
Par exemple si **a ● b = K** alors **(a ● b) ● c** est équivalent à **K ● c** en général différent de **c ● K**
Si **b ● c = Q** alors **a ● (b ● c)** est équivalent à **a ● Q** en général différent de **Q ● a**
Pour démontrer que la loi est associative il faut démontrer que **(a ● b) ● c = a ● (b ● c)**
Autrement dit que **K ● c = a ● Q** (l'ordre dans lequel on écrit ces opérandes étant primordial)

● Si la loi n'est pas dotée de propriétés particulières, tout ce qu'on peut faire, à partir d'une égalité **A = B** c'est dire **(B) = (A)** ou **x ● (A) = x ● (B)** ou **(A) ● x = (B) ● x** (c'est la même opération qui figure dans chaque membre) mais on ne peut pas, par exemple inverser l'ordre des opérandes ou les associer autrement .
De **(A) = (B)** on ne peut pas déduire par exemple que **x ● (A) = (B) ● x**
Si la loi n'est pas simplifiable, on ne peut même pas déduire de **x ● (A) = x ● (B)** que **A = B** car il peut exister
A ≠ B tel que **x ● (A) = x ● (B).**

● L'associativité, combinée à l'existence d'un symétrique est souvent utilisée pour obtenir de nouvelles égalités en vue de démontrer un résultat.
Par exemple trouver la valeur de **b** si **a ● b = k**
On peut écrire $\mathbf{a^{-1} ● (a ● b) = a^{-1} ● k}$ (c'est toujours vrai)
Puis $\mathbf{(a^{-1} ● a) ● b = a^{-1} ● k}$ (associativité) et donc **e ● b** $\mathbf{= a^{-1} ● k}$ (symétrique)
Soit au final $b = a^{-1} ● k$ ce qui revient à calculer b à partir de l'équation initiale.
De même, on peut calculer **a** à partir de : puisque **a ● b = k**

$(a●b)●b^{-1} = k●b^{-1}$ (trivial)

$\mathbf{a● (b ● b^{-1}) = k ● b^{-1}}$ (associativité)

a ● (e) = k ● $\mathbf{b^{-1}}$ (élément neutre)

et donc **a = k ●** $\mathbf{b^{-1}}$

● L'associativité, combinée à la commutativité et à l'existence d'un symétrique ouvre de nouvelles voies .
Par exemple **(a ● b) ●** $\mathbf{a^{-1}}$ peut être modifiée en **a ● (b ●** $\mathbf{a^{-1}}$ **)** (associativité)
Puis en **a ● (**$\mathbf{a^{-1}}$ **● b)** (commutativité) puis en **(a ●** $\mathbf{a^{-1}}$ **) ● b** (associativité) puis en **e ● b** (symétrique) ce qui donne finalement b

● Enfin, si un élément a est simplifiable, et la loi associative, on peut par exemple déduire de **(a ● b) ● c = a ● K** que **a ● (b ● c) = a ● K** et donc que **b ● c = K** .
la commutativité ou l'existence d'un symétrique (et bien sûr d'un élément neutre) nous ouvriraient d'autres possibilités.

STRUCTURES

GROUPES

Soit **E** un ensemble muni d'une loi de composition interne ● .
On dit que **(E , ●) est un groupe si et seulement si**

La loi ● est associative dans E
La loi ● admet un élément neutre
Tout élément de E admet un symétrique pour ●

Si de plus ● est commutative, on dit qu'on a affaire à un groupe commutatif ou abélien

Propriétés des groupes :

Important : Tout élément est simplifiable : **a ● b = a ● c** implique **b = c**
Quand on construit la table du groupe , tout élément figure une fois et une seule dans chaque ligne ou chaque colonne sinon on aurait a ● b = a ● c avec **b** différent de **c**

Par exemple dans **C**, l'ensemble E = **{ 1 , i , –1 , – i }** forme un groupe pour la multiplication..
La multiplication de 2 complexes est associative (ab)c = a(bc) , c'est aussi le cas si a, b, c appartiennent à E.
1 est l'élément neutre de la multiplication a(1) = (1)a = a (1 appartient à E) .
Tout élément de **E** admet un symétrique dans E (son inverse). (1)(1) = 1 ; (–1)(–1) = 1 ; (**i**)(**– i**) = 1 ; (**– i**)(**i**)=1
La table du groupe pour la multiplication est la suivante

●	1	i	–1	– i
1	1	i	–1	– i
i	i	–1	– i	1
–1	–1	– i	1	i
– i	– i	1	i	–1

On remarque que tout élément figure une fois et une seule dans chaque ligne et chaque colonne. (Ce qui est caractéristique d'un groupe)
On remarque que chaque ligne est déduite de la précédente par une permutation simple (la case de rang n prend le rang n–1)
Ce groupe est fini (seulement 4 éléments) et abélien (commutatif / table symétrique par rapport à la diagonale principale) .

Du groupe E à un groupe d'isométries

Dans le plan des complexes, à toute multiplication d'un nombre quelconque Z par un complexe donné K, correspond une transformation du point d'affixe Z (composée d'une rotation et d'une homothétie de centre O).

En effet rappelons que si on écrit les nombres complexes sous leur forme (module, argument) on a
$Z \,.\, K = (\rho_Z \ ; \ \theta_Z).(\rho_K \ ; \ \theta_K) = (\rho_Z \ \rho_K \ ; \ \theta_Z + \theta_K)$
Or ajouter θ_K à l'argument de Z revient à faire effectuer une rotation de centre O et d'angle θ_K au point d'affixe Z .
Et multiplier le module de Z par ρ_K revient à appliquer au point d'affixe Z une homothétie (similitude) de centre O et de rapport ρ_K.

Si le module de K est 1, comme c'est le cas pour les 4 nombres de **E**, la transformation en question se résout à une rotation.
On peut donc associer la multiplication par l'un des nombres du groupe **E** à une isométrie particulière du plan des complexes.
Multiplication par 1 ➜ identité (rotation de centre O d'angle 0° ou 360°)
Multiplication par –1 ➜ symétrie de centre O (rotation de centre O et d'angle 180°)
Multiplication par **i** ➜ Rotation de centre O et d'angle + 90°
Multiplication par – **i** ➜ Rotation de centre O et d'angle –90°
Multiplier un nombre Z successivement par 2 de ces nombres revient à transformer le point d'affixe Z par la composition des deux isométries correspondantes.
C'est donc que ces 4 isométries forment un groupe qu'on peut appeler **H** pour la composition de 2 transformations.
On va trouver que la composition de deux isométries parmi celles du groupe **H** donne une isométrie du groupe **H**.
Que la composition est associative, que l'identité est l'élément neutre pour la composition, que chaque isométrie admet une isométrie réciproque (un symétrique)

Anneaux

Soit E un ensemble muni d'une loi interne multiplicative (●) et d'une loi interne additive (‡)
On dit que **(E, ●,‡) est un anneau si**

(E, ‡) est un **groupe commutatif**
● est **associative** et **distributive** par rapport à ‡

Si de plus ● admet un élément neutre, il est noté 1 et l'anneau est dit **unitaire**.
Si de plus ● est commutative l'anneau est dit commutatif

Z, Q, R et **C** sont des anneaux mais pas **N** .

Dans un anneau on peut définir **f ● g** application produit de deux applications x **→ f ● g (x) =** f(x) ● g(x)
et **f ‡ g** application somme de deux applications x **→f ‡ g** (x) = **f**(x) ‡ **g**(x).

Idéal dans un anneau A

J est un idéal à gauche si

J est un sous groupe de (A , ‡**)**
Tout x ∈ A et tout y ∈ J **→** x ● y ∈ J

Pour un **idéal à droite** il faut **y ● x ∈ J**
Idéal à droite et à gauche = idéal bilatère
Si l'anneau est commutatif tout idéal est bilatère et on dit prosaïquement que c'est un idéal.

Corps

Soit **K** un ensemble muni d'une loi interne multiplicative (●) et d'une loi interne additive (‡)
On dit que (K, ●,‡) est un corps si

(K, ●,‡**)** est un anneau
K* = K – {0} est stable pour la multiplication ●
(K* , ●) est un groupe dont l'élément neutre est noté 1.

Q, R, C sont des corps mais pas **Z** . (en général l'inverse d'un nombre de Z n'appartient pas à Z)