

VII) LOIS DE COMPOSITION INTERNES ; STRUCTURES ALGÈBRIQUES.

1) Définitions.

DEF : une *loi de composition (ou opération) interne* (ou en abrégé "loi") dans un ensemble E est une application de E^2 dans E ; au lieu d'utiliser une notation fonctionnelle ($f(x, y)$), on utilise une notation opératoire ($(x * y)$) : avec cette notation, $f(f(x, y), z)$ s'écrit plus simplement : $(x * y) * z$.

Q1 : combien existe-t-il donc de lois dans un ensemble E ayant n éléments ?

Table de la loi (!!) dans le cas fini :

2) Exemples.

a) Lois notées additivement.

Remarque : deux opérations n'ayant pas le même ensemble de définition ne devraient pas être notées de la même façon ; mais c'est ce que nous ferons tout de même pour toutes les opérations notées $+$, pour simplifier les notations.

L'addition $+$ est définie au départ dans \mathbb{N} par :

$$\forall n \in \mathbb{N} \begin{cases} 1. n + 0 = n \\ 2. \forall m \in \mathbb{N} n + m^+ = (n + m)^+ \end{cases}$$

La notation n^+ signifiant l'entier juste après n (que l'on ne peut pas noter $n + 1$, avant d'avoir défini $+$!!).

Elle est ensuite prolongée à \mathbb{Z} par :

$$\forall n, m \in \mathbb{N} \begin{cases} n + (-m) = (-m) + n = \begin{cases} n - m \text{ si } n \geq m \\ -(m - n) \text{ si } n \leq m \end{cases} \\ (-n) + (-m) = -(n + m) \end{cases}$$

Puis à \mathbb{Q} par :

$$\forall a, c \in \mathbb{Z}, \forall b, d \in \mathbb{N}^* \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Puis à \mathbb{R} par : (le réel x étant limite des rationnels $(r_n)_{n \in \mathbb{N}}$ et le réel y limite de $(s_n)_{n \in \mathbb{N}}$)

$$x + y = \lim (r_n + s_n)$$

Et enfin à \mathbb{C} par :

$$\operatorname{Re}(z + z') = \operatorname{Re}(z) + \operatorname{Re}(z'), \quad \operatorname{Im}(z + z') = \operatorname{Im}(z) + \operatorname{Im}(z')$$

On définit aussi $+$ dans \mathbb{R}^n par

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

Vous avez aussi défini une addition dans l'ensemble \vec{P} des vecteurs du plan, ainsi que dans l'ensemble \vec{E}_3 des vecteurs de l'espace.

b) Lois notées multiplicativement.

On rappelle que la multiplication est notée par \times , par $.$ ou par rien du tout, s'il n'y a pas d'ambiguïté.

La multiplication \times est définie au départ dans \mathbb{N} par :

$$\forall n \in \mathbb{N} \begin{cases} 1. n \times 0 = 0 \\ 2. \forall m \in \mathbb{N} n(m + 1) = nm + n \end{cases}$$

Elle est ensuite prolongée à \mathbb{Z} par :

$$\forall n, m \in \mathbb{N} \begin{cases} n(-m) = (-m)n = -nm \\ (-n)(-m) = nm \end{cases}$$

Puis à \mathbb{Q} par :

$$\forall a, c \in \mathbb{Z}, \forall b, d \in \mathbb{N}^* \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$$

Puis à \mathbb{R} par : (le réel x étant limite des rationnels $(r_n)_{n \in \mathbb{N}}$ et le réel y limite de $(s_n)_{n \in \mathbb{N}}$)

$$xy = \lim (r_n s_n)$$

Et enfin à \mathbb{C} par :

$$\operatorname{Re}(zz') = \operatorname{Re}(z)\operatorname{Re}(z') - \operatorname{Im}(z)\operatorname{Im}(z'), \quad \operatorname{Im}(zz') = \operatorname{Re}(z)\operatorname{Im}(z') + \operatorname{Im}(z)\operatorname{Re}(z')$$

ATTENTION : le produit scalaire des vecteurs n'est pas une loi de composition interne !!!

c) La soustraction.

Elle est définie par rapport à l'addition par $x - y = x + (-y)$.

Attention : la soustraction n'est pas une loi de composition interne dans \mathbb{N} !

d) La division \div .

Elle est définie par rapport à la multiplication par $x \div y \left(= \frac{x}{y} \right) = x \frac{1}{y}$ si $y \neq 0$.

Attention : c'est une loi de composition interne dans \mathbb{Q}^* , dans \mathbb{R}^* et dans \mathbb{C}^* , mais ni dans \mathbb{Z}^* , ni dans \mathbb{D}^* , ni dans \mathbb{Q} etc...

e) L'exponentiation.

Voir la définition de a^b dans le cours sur les fonctions usuelles.

C'est une loi de composition interne dans \mathbb{N} , et dans \mathbb{R}_+ , mais pas dans \mathbb{Z} , ni même \mathbb{Z}^* !!

f) Le produit vectoriel \wedge .

C'est une loi dans \overrightarrow{E}_3 .

g) La réunion \cup , l'intersection \cap , la différence \setminus , la différence symétrique Δ .

Ce sont des lois dans $\mathcal{P}(E)$ (il y en a donc autant que d'ensembles E).

h) La composition des applications \circ .

C'est une loi dans l'ensemble E^E des applications de E dans E (mais pas dans F^E avec $E \neq F$!!!)

i) min et max dans $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$.

Remarquer qu'ici, ces deux lois ont une notation fonctionnelle ; mais on emploie parfois une notation opératoire :

$$\min(x, y) = x \wedge y, \quad \max(x, y) = x \vee y$$

j) pgcd et ppcm dans \mathbb{N} .

On rappelle :

$d = \operatorname{pgcd}(a, b) \Leftrightarrow$	$\begin{cases} d \text{ divise } a \text{ et } b \\ \text{si } d' \text{ divise } a \text{ et } b \text{ alors } d' \text{ divise } d \end{cases}$
$m = \operatorname{ppcm}(a, b) \Leftrightarrow$	$\begin{cases} a \text{ et } b \text{ divisent } m \\ \text{si } a \text{ et } b \text{ divisent } m' \text{ alors } m \text{ divise } m' \end{cases}$

On emploie aussi une notation opératoire : $\operatorname{pgcd}(a, b) = a \wedge b$ et $\operatorname{ppcm}(a, b) = a \vee b$ (s'il n'y a pas de confusion possible avec min et max).

3) Commutativité.

DEF : une loi $*$ définie dans un ensemble E est dite *commutative* si

$$\forall x, y \in E \quad x * y = y * x$$

Q2 : Comment cette propriété se voit-elle dans la table de la loi (dans le cas fini) ?

Q3 : Déterminer parmi les exemples de lois donnés ci-dessus celles qui ne sont *pas* commutatives.

4) Associativité.

DEF : une loi $*$ définie dans un ensemble E est dite *associative* si

$$\forall x, y, z \in E \quad (x * y) * z = x * (y * z)$$

On supprime donc dans ce cas les parenthèses : $x * y * z$.

REMARQUE : Cette propriété ne se voit pas clairement dans la table de la loi dans le cas $|E| = n$; il faut donc vérifier la propriété $(x * y) * z = x * (y * z)$ pour les n^3 triplets (x, y, z) de E^3 .

Q4 : Déterminer parmi les lois internes définies ci-dessus celles qui ne sont *pas* associatives.

5) Distributivité d'une loi par rapport à une autre.

DEF : deux lois $*$ et Δ étant définies dans un ensemble E , on dit que $*$ est *distributive sur Δ* si

$$\forall x, y, z \in E \quad \begin{cases} x * (y \Delta z) = (x * y) \Delta (x * z) & (\text{distributivité à gauche de } * \text{ sur } \Delta) \\ (x \Delta y) * z = (x * z) \Delta (y * z) & (\text{distributivité à droite de } * \text{ sur } \Delta) \end{cases}$$

Q5 : Déterminer parmi les couples de lois internes définies ci-dessus ceux ayant cette propriété.

6) Élément neutre.

DEF : un élément e d'un ensemble E muni d'une loi $*$ est dit *neutre* si :

$$\forall x \in E \quad \begin{cases} x * e = x & (e \text{ est neutre à droite}) \\ e * x = x & (e \text{ est neutre à gauche}) \end{cases}$$

Q6 : Comment remarque-t-on sur une table de loi qu'il y a un élément neutre ?

Q7 : Déterminer parmi les lois définies ci-dessus celles ayant un élément neutre.

PROP : une loi possède un élément neutre au plus.

D1

Notations : en notation additive, l'élément neutre, s'il existe, sera appelé l'élément *nul*, et noté 0_E , et en notation multiplicative, il sera appelé l'élément *unité*, et sera noté 1_E .

Exemples : E1

7) Élément absorbant.

DEF : un élément a d'un ensemble E muni d'une loi $*$ est dit *absorbant* si :

$$\forall x \in E \quad \begin{cases} x * a = a & (a \text{ est absorbant à droite}) \\ a * x = a & (a \text{ est absorbant à gauche}) \end{cases}$$

Q8 : Comment remarque-t-on sur une table de loi qu'il y a un élément absorbant ?

PROP : une loi possède un élément absorbant au plus.

D2

Exemples : E2

8) Symétrique d'un élément pour une loi possédant un élément neutre.

DEF : soient x et x' deux éléments d'un ensemble E possédant une loi $*$ ayant un élément neutre e . Alors on dit que x' est un symétrique de x pour la loi $*$ si

$$\boxed{\begin{cases} x * x' = e & (x' \text{ est symétrique à droite}) \\ x' * x = e & (x' \text{ est symétrique à gauche}) \end{cases}}$$

Un élément ayant au moins un symétrique est dit *symétrisable*.

Q9 : comment remarque-t-on dans une table de loi qu'un élément possède un ou plusieurs symétriques ?

Exemple de loi où un élément possède deux symétriques : E3.

PROP : si la loi $*$ est associative, un élément de E possède un symétrique au plus.

D3

Notation : dans ce cas, le symétrique de x pour la loi $*$ sera noté (s'il existe) : $sym_*(x)$ et simplifié en $-x$ (*opposé* de x) si la loi est additive, ou x^{-1} si la loi est multiplicative ; dans ce cas x^{-1} est appelé l'*inverse* de x et x est dit *inversible* au lieu de symétrisable ; mais la notation $\frac{1}{x}$, dangereuse, est strictement réservée au cas commutatif.

Remarque : $sym_*(e) = e$ et si x a un symétrique, $sym_*(sym_*(x)) = x$.

PROP : La loi $*$ étant supposée associative et d'élément neutre e , alors le composé par $*$ de deux éléments symétrisables est un élément symétrisable, et

$$\boxed{sym_*(x * y) = sym_*(y) * sym_*(x)} \text{ (attention à l'inversion de l'ordre)}$$

Ce qui, en notations additive et multiplicative, donne :

$$\boxed{-(x + y) = -y + (-x) \text{ et } (xy)^{-1} = y^{-1}x^{-1}}$$

D4

EXEMPLES : E4.

9) Éléments simplifiables (ou réguliers).

DEF : un élément x d'un ensemble muni d'une loi $*$ est dit *simplifiable* (ou *régulier*) pour $*$ si

$$\forall y_1, y_2 \in E \begin{cases} x * y_1 = x * y_2 \implies y_1 = y_2 & (x \text{ est simplifiable à gauche}) \\ y_1 * x = y_2 * x \implies y_1 = y_2 & (x \text{ est simplifiable à droite}) \end{cases}$$

Q10 : comment remarque-t-on que dans une table de loi un élément est simplifiable ?

PROP : si la loi est associative et possède un élément neutre, tout élément symétrisable est simplifiable, mais la réciproque est fausse.

D5

EXEMPLES : E5

10) Partie stable pour une loi de composition interne ; loi induite.

DEF : une partie A d'un ensemble E muni d'une loi $*$ est dite *stable* pour la loi $*$ si

$$\forall x, y \in A \quad x * y \in A$$

Dans ce cas, on peut définir la loi $*_A$ dans l'ensemble A par

$$\forall x, y \in A \quad x *_A y = x * y$$

La loi $*_A$ est appelée la *loi induite* par $*$ sur la partie A .

Remarque : les lois $*_A$ et $*$ ne diffèrent que par leur ensemble de définition et, en général, on confond leur écriture, mais il faut faire attention que, par exemple, l'une peut avoir un élément neutre et l'autre pas !!!

EXEMPLES : E6.

PROP :

1. Les lois induites d'une loi commutative restent commutatives.
2. Idem pour l'associativité.
3. Si e est un élément neutre de $*$ ET SI e appartient à la partie stable A , alors e est neutre pour $*_A$.
4. Si de plus x est un élément de A ayant un symétrique x' pour $*$ QUI APPARTIENT À A , alors x' est un symétrique de x pour $*_A$.

D6

VIII. STRUCTURES ALGÈBRIQUES.

1) Groupes.

a) Définition.

DEF $*$ étant une loi de composition interne dans un ensemble G , on dit que $(G, *)$ est un groupe si

1. La loi $*$ est associative.
2. $*$ possède un élément neutre i.e. : $\exists e \in G / \forall x \in G \quad x * e = e * x = x$
3. Tout élément de G possède un symétrique pour la loi $*$ i.e. : $\forall x \in G \quad \exists x' \in G / x * x' = x' * x = e$

Si de plus la loi $*$ est commutative, le groupe est dit *commutatif* (ou *abélien* en l'honneur du mathématicien Abel).

Remarques :

R1. On dit "souvent G muni de $*$ " au lieu de $(G, *)$, et lorsqu'il n'y a pas d'ambiguïté, on écrit G tout court au lieu de $(G, *)$; par exemple, on parle du groupe \mathbb{R} au lieu de $(\mathbb{R}, +)$ ou du groupe \mathbb{R}^* au lieu de (\mathbb{R}^*, \times) .

R2. La loi de groupe $*$ étant associative, le symétrique de x est unique ; on le notera x^{-1} ; mais en notation additive, ce sera $-x$.

R3. On a toujours, dans un groupe :

$$e^{-1} = e, \quad (x^{-1})^{-1} = x \quad \text{et} \quad (x * y)^{-1} = y^{-1} * x^{-1}$$

Ce qui, en notation additive donne :

$$-0_G = 0_G, \quad -(-x) = x \quad \text{et} \quad -(x + y) = -y + (-x)$$

R4 : En notation additive, on définit la *soustraction* $-$ par :

$$\forall x, y \in G \quad x - y = x + (-y)$$

R5 : Dans un groupe tout élément est simplifiable (puisque symétrisable) ; donc dans la table d'un groupe fini, apparaît dans chaque ligne et dans chaque colonne tous les éléments de G une fois et une seule.

PROP : si E est un ensemble muni d'une loi associative $*$ possédant un élément neutre e , alors l'ensemble $S(E)$ des éléments symétrisables de E est stable par $*$ et $S(E)$ muni de la loi induite $*_{S(E)}$ est un groupe.

D7

Exemples : E7.

b) Itérés d'un élément.

DEF : x étant un élément d'un groupe $(G, *)$ d'élément neutre e , et n un entier naturel, on définit le n -ième itéré de x , noté x^n par

$$\boxed{\begin{array}{l} x^0 = e \\ \forall n \in \mathbb{N} \quad x^{n+1} = x^n * x \quad (\text{donc, si } n \geq 1 : x^n = \underbrace{x * x * \dots * x}_{n \text{ fois}}) \end{array}}$$

De plus : x^{-n} sera par définition $(x^{-1})^n$.

Remarque : en notation additive, tout ceci devient :

$$\boxed{\begin{array}{l} 0x = 0_G \\ \forall n \in \mathbb{N} \quad (n+1)x = nx + x \quad (\text{donc, si } n \geq 1 : nx = \underbrace{x + x + \dots + x}_{n \text{ fois}}) \\ (-n)x = -(nx) \end{array}}$$

On a alors les propriétés, pour x et y dans G et n entier relatif :

$$\boxed{\begin{array}{l} \text{P1. } x^n * x^m = x^{n+m} \quad (\text{qui donne en additif : } nx + mx = (n+m)x) \\ \text{P2. } (x^n)^m = x^{nm} = (x^m)^n \quad (\text{qui donne en additif : } m(nx) = (nm)x = n(mx)) \end{array}}$$

D8

c) Sous-groupes.

Soit $(G, *)$ un groupe d'élément neutre e et H une partie de G .

DEF : H est un *sous-groupe* de G si H est stable pour la loi $*$, et si H muni de la loi induite $*_H$ est un groupe.

CNS1 : H est un *sous-groupe* de G ssi

$$\boxed{\begin{array}{l} 1. e \in H \\ 2. \forall x, y \in H \quad x * y \in H \quad (\text{autrement dit } H \text{ est stable}) \\ 3. \forall x \in H \quad x^{-1} \in H \end{array}}$$

REM : en notation additive, ceci devient :

$$\boxed{\begin{array}{l} 1. 0_G \in H \\ 2. \forall x, y \in H \quad x + y \in H \quad (\text{autrement dit } H \text{ est stable}) \\ 3. \forall x \in H \quad -x \in H \end{array}}$$

CNS2 : H est un *sous-groupe* de G ssi

$$\boxed{\begin{array}{l} 1. e \in H \\ 2'. \forall x, y \in H \quad x * y^{-1} \in H \end{array}}$$

D9

REM : la CNS 2 est plus compacte, mais je conseille quand même d'utiliser la CNS1, plus facile à mettre en oeuvre.

Exemples triviaux : $\{e\}$ et G sont des sous groupes de G ; les autres sous-groupes sont dits "non triviaux".

Autres exemples : E8.

2) Anneaux.

a) Définition.

DEF Un ensemble A muni de deux lois notées $+$ et \times est appelé un *anneau* si

1. $(A, +)$ est un groupe commutatif (ce qui fait 4 propriétés).
2. La loi \times est associative.
3. Elle est aussi distributive sur $+$.
4. La loi \times possède un élément neutre différent de celui de $+$.

Si de plus la multiplication est commutative, l'anneau est dit *commutatif*.

Notation : l'élément nul (i.e. neutre pour l'addition) sera noté 0_A et l'élément unité (i.e. neutre pour \times) noté 1_A .

REM : l'appellation "anneau" est la traduction de l'allemand "Ring" qui peut signifier "cercle d'habitues".

Exemples : E9.

b) Calculs dans un anneau.

On définit la soustraction dans A par $a - b = a + (-b)$, l'itération additive na (n entier relatif et $a \in A$) comme on a dit ci-dessus, et l'exponentiation a^n pour n entier NATUREL par

$a^0 = 1_A$
$\forall n \in \mathbb{N} \quad a^{n+1} = a^n a$ (donc, si $n \geq 1 : a^n = \underbrace{a \times a \times \dots \times a}_{n \text{ fois}}$)

Sauf pour la commutativité de \times et autres exceptions dûment signalées ci-dessous, presque tous les réflexes acquis pour les calculs dans les réels pourront être conservés pour les calculs dans un anneau ; on a en particulier les propriétés pour a et b dans A :

P1 : $a0_A = 0_A a = 0_A$ (0_A est absorbant)
P2 : $a(-b) = (-a)b = -(ab)$ (donc simplifié en $-ab$)
P3 : $a(b-c) = ab - ac$ et $(a-b)c = ac - bc$.
P4 : $(a+b)^2 = \begin{cases} a^2 + b^2 + ab + ba \\ a^2 + b^2 + 2ab \text{ seulement si } a \text{ et } b \text{ commutent (i.e. } ab = ba) \end{cases}$
P5 : $(a+b)(a-b) = \begin{cases} a^2 - b^2 + ba - ab \\ a^2 - b^2 \text{ seulement si } a \text{ et } b \text{ commutent} \end{cases}$
P6 : $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$ si a et b commutent
P7 : $a^n - b^n = (a-b) \left(\sum_{k=0}^{n-1} a^{n-1-k} b^k \right)$ si a et b commutent.

D10

c) Problème des diviseurs de zéro ; anneaux intègres.

On était habitués à ce que dans \mathbb{R} on ait : $ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$, propriété utilisée lors de la résolution des équations ; ceci n'est malheureusement plus exact dans un anneau quelconque (et en particulier dans l'anneau des matrices qui sera étudié cet année).

DEF : un élément non nul a de l'anneau A tel qu'il existe un élément b non nul de A tel que $ab = 0_A$, s'appelle un *diviseur de zéro* de A ; un anneau sans diviseur de zéro est dit *intègre*.

PROP : A est intègre $\Leftrightarrow \forall a, b \in A \quad ab = 0 \Rightarrow (a = 0_A \text{ ou } b = 0_A)$.

D11

CNS : a est un diviseur de zéro ssi a est non nul et non simplifiable ; un anneau intègre est donc un anneau où tout élément non nul est simplifiable.

D12

d) Sous-anneaux.

Soit A un anneau et B une partie de A .

DEF : B est un *sous-anneau* de A si B est stable pour l'addition et la multiplication, et si B muni des lois induites $+_B$ et \times_B est un anneau ayant le même élément unité que A .

CNS : B est un *sous-anneau* de A ssi

$$\left\{ \begin{array}{l} 1. -1_A \in B \\ 2. \forall a, b \in B \ a + b \in B \text{ (autrement dit } B \text{ est stable pour } +) \\ 3. \forall a, b \in B \ ab \in B \text{ (autrement dit } B \text{ est stable pour } \times) \end{array} \right.$$

Exemples : $\mathbb{Z}1_A = \{n1_A / n \in \mathbb{Z}\}$ et A sont des sous-anneaux de A .

Autres exemples : E10.

3) Corps.

a) Définition.

DEF : un corps K est un anneau où tous les éléments non nuls sont inversibles :

$$\forall x \in K \setminus \{0_K\} \ \exists x' \in K / xx' = x'x = 1_K$$

L'ensemble $K \setminus \{0_K\}$ est noté traditionnellement K^* .

Exemples : E11

CNS : $(K, +, \times)$ est un corps ssi

$$\left\{ \begin{array}{l} 1. (K, +, \times) \text{ est un anneau} \\ 2. (K^*, \times) \text{ est un groupe} \end{array} \right.$$

D13

Remarque : un corps est un anneau intègre, mais la réciproque est fautive (contre-exemple \mathbb{Z}).

b) Sous-corps.

Soit K un anneau et L une partie de K .

DEF : L est un *sous-corps* de K si L est stable pour l'addition et la multiplication, et si L muni des lois induites $+_L$ et \times_L est un corps.

CNS : L est un *sous-corps* de K ssi

$$\left\{ \begin{array}{l} 1. L \text{ est un sous-anneau de } K \\ 2. \forall x \in L \setminus \{0_K\} \ x^{-1} \in L \end{array} \right.$$

D14

4) Morphismes (hors programme).

a) Définitions.

DEF : l'ensemble E étant muni d'une loi $*$ et F d'une loi Δ , on dit qu'une application f de E vers F est un *morphisme* de $(E, *)$ vers (F, Δ) si elle vérifie :

$$\forall x, y \in E \quad f(x * y) = f(x) \Delta f(y)$$

Lorsque $E = F$ et $*$ = Δ on parle d'*endomorphisme* de $(E, *)$.

Un morphisme bijectif est appelé un *isomorphisme*.

Deux ensembles munis d'opération tels qu'il existe un isomorphisme de l'un vers l'autre sont dits *isomorphes*, et ceci se note :

$$(E, *) \approx (F, \Delta) \quad (\text{simplifié en } E \approx F \text{ s'il n'y a pas d'ambiguïté})$$

Un endomorphisme bijectif est appelé un *automorphisme*.

EXEMPLES :

- id_E est un automorphisme de $(E, *)$.
- \ln est un isomorphisme de (\mathbb{R}_+^*, \times) sur $(\mathbb{R}, +)$; ces deux ensembles sont donc isomorphes.
- deux ensembles finis munis de lois sont isomorphes si, au nom des éléments près, les tables sont identiques.
- autres exemples E12

b) Propriétés.

P1 : une composée de morphismes est un morphisme ; plus précisément, si f est un morphisme de $(E, *)$ vers (F, Δ) et g un morphisme de (F, Δ) vers (G, ∇) (prononcer "atled") alors $g \circ f$ est un morphisme de $(E, *)$ vers (G, ∇) .

D15

REM : une composée d'endo, iso, ou auto-morphismes est donc un endo, iso, ou auto-morphisme.

P2 : La réciproque d'un isomorphisme est un isomorphisme.

D16

CORO 1 : la relation d'isomorphie est une relation d'équivalence, à savoir :

$(E, *) \approx (E, *)$
$(E, *) \approx (F, \Delta) \Rightarrow (F, \Delta) \approx (E, *)$
$\left\{ \begin{array}{l} (E, *) \approx (F, \Delta) \\ (F, \Delta) \approx (G, \nabla) \end{array} \right. \Rightarrow (E, *) \approx (G, \nabla)$

CORO 2 : l'ensemble des automorphismes de $(E, *)$, noté $AUT_*(E)$, est un sous-groupe de $BIJ(E)$ muni de \circ .

D17

c) Morphismes de groupes.

DEF si $(G, *)$ et (H, Δ) sont deux groupes, un morphisme de groupe de G vers H est un morphisme de $(G, *)$ vers (H, Δ) .

REM : on a alors, avec des notations évidentes : $f(e_G) = e_H$ et $(f(x))^{-1} = f(x^{-1})$.

D18

PROP (transport de la structure de groupe) : si $(G, *)$ est un groupe et s'il existe un morphisme surjectif de $(G, *)$ sur (H, Δ) alors (H, Δ) est un groupe ; si f est bijective, ces deux groupes sont isomorphes.

D19

d) Morphismes d'anneaux.

DEF si $(A, +, \times)$ et $(B, +, \times)$ sont deux anneaux, un morphisme d'anneaux de A vers B est un morphisme f de $(A, +, \times)$ vers $(B, +, \times)$ vérifiant de plus $f(1_A) = 1_B$.

E13

REM : on a alors, avec des notations évidentes : $f(0_A) = 0_B$, $f(-x) = -f(x)$ et si x est inversible, $f(x)$ aussi et $(f(x))^{-1} = f(x^{-1})$.

D20

PROP (transport de la structure d'anneau) : si A est un anneau et s'il existe un morphisme surjectif non nul f de $(A, +, \times)$ sur $(B, +, \times)$ alors B est un anneau ; si f est bijective, ces deux anneaux sont isomorphes.

D21

e) Morphismes de corps.

DEF si K et L sont deux corps, un *morphisme de corps* de K vers L est un morphisme d'anneaux de K vers L .

REM : on a alors, avec des notations évidentes : $f(0_K) = 0_L$, $f(-x) = -f(x)$ et si $x \neq 0_K$ $(f(x))^{-1} = f(x^{-1})$.

D22

PROP : un morphisme de corps est toujours injectif.

D23

PROP (transport de la structure de corps) : si K est un corps et s'il existe un morphisme surjectif non nul de $(K, +, \times)$ sur $(L, +, \times)$ alors L est un corps isomorphe à K .

D24