STRUCTURES ALGEBRIQUES

1 Lois de composition interne

1.1 Généralités

Définition 1 Une loi de composition interne sur un ensemble E est une application de $E \times E$ vers E.
$*$ LCI sur E : Application $E \times E \longrightarrow E,\ (x, y) \longmapsto x * y$

Exemple 1
- Addition et multiplication dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- Division sur $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$.
- Intersection, réunion, différence sur $\mathcal{P}(E)$, ensemble des parties d'un ensemble E.
- Composée des applications dans E^E ensemble des applications de l'ensemble E vers lui même.

Propriété 1 Une loi de composition interne $*$ sur l'ensemble E peut être :

- Associative si : $\forall (x, y, z) \in E^3,\ x * (y * z) = (x * y) * z$.
- Commutative si : $\forall (x, y) \in E^2,\ x * y = y * x$.
- Un élément $a \in E$ est régulier pour $*$ (ou simplifiable) si : $\forall (x, y) \in E^2, a*x = a*y \Longrightarrow x = y$ et $x*a = y*a \Longrightarrow x = y$. Si $*$ est commutative les deux implications sont équivalentes.
- Un élément e de E est élément neutre pour $*$ si : $\forall x \in E,\ a * e = e * a = a$. Un tel élément s'il existe est unique.
- Un élément $x \in E$ admet un symétrique pour la loi $*$ s'il existe $y \in E$ tel que : $x * y = y * x = e$ où e est l'élément neutre pour $*$.
  Si la loi $*$ est associative et si x admet un symétrique, il est unique.
  Le symétrique de x est noté $y = x^{-1}$ en général, mais $y = \frac{1}{x}$ si $*$ est la multilpication dans un ensemble de nombres et $y = -x$ si c'est l'addition, dans le cas de la multiplication on parle d'inverse et d'opposé dans le cas de l'addition.

Exemple 2 Sur E^E la composée des applications est associative.
Remarque Pour montrer que deux applications sont différentes il suffit de montrer qu'elles diffèrent pour une seule valeur de $x \in E$.
Ainsi, en général, la composée des applications n'est pas commutative :
Si $E = \mathbb{R}$, n$f : x \mapsto 3x + 2,\ g : x \mapsto x^2$ on pourrra vérifier que $g \circ f(0) = 4$ et $f \circ g(0) = 2$ ce qui montre que $g \circ f \neq f \circ g$.
Sur $\mathbb{R}$ (resp. sur $\mathbb{R}^*$) la soustraction (resp. la multilication) n'est pas associative ni commutative.
0 et 1 sont éléments neutres pour l'addition et la multiplication respectivement sur les ensembles de nombres.
Id_E est élément neutre pour $\circ$ dans E^E, les éléments inversibles sont les bijections.
E est élément neutre pour $\cap$ dans $\mathcal{P}(E)$.
Si a et b inversibles pour $*$ alors $a * b$ est inversible et $(a * b)^{-1} = b^{-1} * a^{-1}$, en particulier si f et g sont des bijections de E^E, $g \circ f$ est une bijection dont la bijection réciproque est $f^{-1} \circ g^{-1}$.
Si $*$ est associative, tout élément inversible est régulier.

Propriété 2 La loi de composition interne $*$ est distributive par rapport à la loi de composition interne T si :
$\forall (x, y, z) \in E^3,\ x * (y\,T\,z) = (x * y)\,T\,(x * z)$ et $(y\,T\,z) * x = (y * x)\,T\,(z * x)$, une seule de ces égalité étant nécessaire si $*$ est commutative.

Exemple 3 Sur $\mathbb{R}$ la multiplication est distributive par rapport à l'addition.
Sur $\mathcal{P}(E)$ $\cap$ (resp. $\cup$) est distributive par rapport à $\cup$ (resp. $\cap$. Par exemple :
$\forall A, B, C \in \mathcal{P}(E),\ A \cap (B \cup C) = (A \cap B)\ \cup\ (A \cap C)$.

1.2 Itérés d'un élément

Notation multiplicative.
Soit E un ensemble muni d'une loi de composition interne $*$, associative et admettant un élément neutre e. On définit :
$x^0 = e,\ x^2 = x * x$ et par récurrrence $x^{n+1} = x^n * x$.

Propriété 3 Si x est inversible et $n \in \mathbb{N},\ x^n$ l'est également et $(x^n)^{-1} = \left(x^{-1}\right)^n$.
$p, q \in \mathbb{N},\ x \in E,\ x^p * x^q = x^{p+q}$.

Notation additive.
Soit E un ensemble muni d'une loi de composition interne notée $+$, aasociative, commutative et admeetant 0 comme élément neutre.
On définit $nx, x \in E,\ n \in \mathbb{N}$ par : $0x = 0,\ 2x = x + x,\ (n+1)x = nx + x$.

Propriété 4 $p, q \in \mathbb{N},\ (p+q)x = px + qx,\ p(qx) = (pq)x$.

2 Groupes

Définition 2 Soit E un ensemble non vide **une loi de composition interne** sur E est une application de $E \times E$ dans E.

Définition 3 Soit E un ensemble muni d'une loi de composition interne * on dit que **(E,*) est un groupe** si
1. * est associative
2. * admet un élément neutre : $\exists e \in E \ \ \forall x \in E \ \ e * x = x * e = x$
3. tout élément est inversible (admet un symétrique) :$\forall x \in E \ \ \exists x' \in E \ \ x * x' = x' * x = e$
Si de plus la loi est commutative on dit que le groupe est **commutatif** ou **abélien**.

Proposition 4 Soit $(E, *)$ un groupe :
1. l'élément neutre est unique
2. le symétrique de tout élément est unique
3. tout les éléments de E sont réguliers
4. $\forall (x, y) \in E^2 \quad (x * y)^{-1} = y^{-1} * x^{-1}$

Proposition 5 Soit $(E, *)$ un groupe et H une partie de E. On dit que H est un sous groupe de E si H est stable pour $*$ c'est à dire $\forall (x, y) \in H^2 \quad x * y \in H$ et si H muni de la loi induite par * est un groupe.

Proposition 6 Si H est un sous groupe de E alors l'élément neutre de H est le même que celui de E.

Proposition 7 Soit $(E, *)$ un groupe et H une partie de E

$$H\ est\ un\ sous-groupe \Leftrightarrow \begin{cases} 1)\ e \in H \quad (H \neq \emptyset) \\ 2)\ \forall x \in H \ \ x^{-1} \in H \\ 3)\ \forall (x, y) \in H^2\ x * y \in H \end{cases}$$

$$H\ est\ un\ sous-groupe \Leftrightarrow \begin{cases} 1)\ H \neq \emptyset \\ 2)\ \forall (x, y) \in H^2\ x * y^{-1} \in H \end{cases}$$

Exemple 4 1. $\{e\}$ et E sont des sous-groupes de E

Proposition 8 L'intersection d'une famille non vide de sous-groupes d'un groupe est un sous-groupe, mais attention c'est faux pour la réunion.

3 Morphisme de groupes

Définition 9 Soit $(E, *)$ et (F, T) 2 groupes et f une application de E dans F. On dit que f est un **morphisme de groupe** si

$$\forall (x, y) \in E^2 \quad f(x * y) = f(x) T f(y)$$

Si de plus f est bijective on dit que f est un **isomorphisme**
Si de plus $E = F$ on dit que f est un **endomorphisme**
Si de plus f est bijective et $E = F$ on dit que f est un **automorphisme**

Proposition 10 Si f est un **morphisme de groupe** de $(E, *)$ vers (F, T) alors en notant e l'élément neutre de E et e' l'élément neutre de F

$$\begin{array}{rcll} f(e) & = & e' & \\ \forall x & \in & E & f(x^{-1}) = [f(x)]^{-1} \end{array}$$

Proposition 11 La composée de deux morphismes de groupes est un morphisme de groupe. La réciproque d'un isomorphisme est un isomorphisme.

Proposition 12 Soit $(E,*)$ et (F,T) 2 groupes et f un morphisme de groupes E dans F
1. l'image par f d'un sous-groupe de E est un sous-groupe de F.
2. l'image réciproque par f d'un sous-groupe de F est un sous-groupe de E.

Définition 13 Soit $(E,*)$ et (F,T) 2 groupes et f un morphisme de groupes E dans F , soit e' l'élément neutre de F et e celui de E.
L'ensemble des antécédents de e , $f^{-1}(\{e'\})$ est appelé noyau de f et est noté $\ker f$.

Proposition 14 f est injectif si et seulement si $\ker f = \{e\}$

Proposition 15 $\ker f$ est un sous-groupe de E et $f(E)$ est un sous-groupe de F

4 Anneaux

4.1 Définitions

Définition 16 Soit A un ensemble non vide muni de deux lois de compositions internes $+$ et $\times$ on dit que $(A,+,\times)$ est un **anneau** si

$(A,+)$ est un groupe commutatif
$\times$ est associative
$\times$ possède un élément neutre 1_A
$\times$ est distributive par rapport à $+$ c-a-d : $\forall (x,y,z)\in A^3$, $\begin{cases} x\times(y+z)=x\times y+x\times z \\ (y+z)\times x=y\times x+z\times x \end{cases}$

L'anneau est dit commutatif si $\times$ est commutative.

Notation L'élément neutre de $(A,+)$ est noté 0_A ou 0 si il n'y a pas de risque de confusion.
Exemple : $(\mathbb{Z},+,\times)$, $(\mathbb{C},+,\times)$,

Proposition 17 Soit $(A,+,\times)$ un anneau.
1. Pour tout x de A on a $0_A\times x = x\times 0_A = 0_A$.
2. Pour tout x et y de A on a $-(x\times y)=(-x)\times y = x\times(-y)$.

4.2 Simplification

Définition 18 Un élément non nul x d'un anneau A tel qu'il existe $y\in A$ $y\neq 0$ avec $x\times y = 0$ s'appelle un diviseur de 0.

Remarque 1 Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ne possède pas de diviseurs de 0.

Définition 19 Soit x est un élément d'un anneau A. Si x possède un symétrique pour la multiplication, c'est-a-dire si il existe $x'\in A$ tel que $x\times x' = x'\times x = 1$, alors on dit que x est inversible et on note $x^{-1}=x'$ son inverse.

Remarque 2 Un élément inversible n'est jamais un diviseur de 0 .De plus si x est inversible alors $x\times y = x\times z \Rightarrow y = z$.

4.3 Calcul dans un anneau.

Notation Soit $(A,+,.)$ un anneau, $n\in\mathbb{N}$ et $x\in A$. on pose $nx = 0_A$ si $n=0$ et $nx = x+(n-1)x$ si $n\geq 1$ et $(-n)x = -(nx)$. De même on pose $x^n = 1_A$ si $n=0$ et $x^n = xx^{n-1}$ si $n\geq 1$.

Théorème 20 Si $(A,+,)$ est un anneau et si x et y sont deux éléments de A tels que $xy=yx$ (on dit que x et y commute) alors pour tout $n\in\mathbb{N}$ on a

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}.$$

La démonstration se fait par récurrence sur n et est identique à celle réalisée dans $\mathbb{C}$ en début d'année.

Théorème 21 Si $(A,+,\times)$ est un anneau et si x et y sont deux éléments de A tels que $x\times y = y\times x$ (on dit que x et y commute) alors pour tout $n\in\mathbb{N}$ on a

$$x^{n+1}-y^{n+1} = (x-y)\left(\sum_{k=0}^{n} x^{n-k}y^k\right).$$

Démonstration. Comme $xy=yx$ on a

$$\begin{aligned}(x-y)\left(\sum_{k=0}^{n} x^{n-k}y^k\right) &= x\sum_{k=0}^{n} x^{n-k}y^k - y\sum_{k=0}^{n} x^{n-k}y^k\\ &= \sum_{k=0}^{n} x^{n+1-k}y^k - \sum_{k=0}^{n} x^{n-k}y^{k+1}\\ &= \sum_{k=0}^{n} x^{n+1-k}y^k - \sum_{k=1}^{n+1} x^{n-(k-1)}y^k\\ &= \sum_{k=0}^{n} x^{n+1-k}y^k - \sum_{k=1}^{n+1} x^{n+1-k}y^k = x^{n+1}-y^{n+1}.\end{aligned}$$

4.4 Sous-anneaux

Définition 22 Soit $(A,+,\times)$ un anneau et B une partie de A, on dit que B est un sous-anneau de A si
B est un sous-groupe de $(A,+)$
B est stable pour $\times$
$1\in B$

Toute intersection de sous-anneaux est un sous-anneau.

Exemple 5 $\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$

4.5 Morphisme d'anneau

Définition 23 Soit $(A,+,\times)$ et $(A',+',\times')$ 2 anneaux et f une application de A dans A'. On dit que $f$est un **morphisme d'anneaux** si
1. *f est un morphisme de groupes*
2. $f(1_A)=1_{A'}$
3.$\forall (x,y)\in A^2 \quad f(x\times y) = f(x)\times' f(y)$

Si de plus f est bijective on dit que f est un **isomorphisme**
Si de plus $A=A'$ on dit que f est un **endomorphisme**
Si de plus f est bijective et $A=A'$ on dit que f est un **automorphisme**

Proposition 24 La composée de deux morphismes d'anneaux est un morphisme d'anneaux. La réciproque d'un isomorphisme est un isomorphisme.

Proposition 25 Soit $(A,+,\times)$ et $(A',+',\times')$ 2 anneaux et f un morphisme d'anneaux de A dans A'
1. l'image par f d'un sous-anneau de A est un sous-anneau de A'.
2. l'image réciproque par f d'un sous-anneau de A' est un sous-anneau de A.

4.6 Idéal d'un anneau

Définition 26 Une partie non vide $\mathcal{I}$ de l'anneau A est un idéal de cet anneau si :
— $(\mathcal{I},+)$ est un sous groupe de $(A,+)$.
— $A\mathcal{I}\subset\mathcal{I}$ c'est à dire :$\forall (a,x)\in A\times\mathcal{I},\ ax\in\mathcal{I}$.

Exemple 6 $a\in\mathbb{Z}$, $a\mathbb{Z}=\{ak|k\in\mathbb{Z}\}$ est un idéal de $\mathbb{Z}$, c'est l'ensemble des multiples de a.

On verra que tous les idéaux de $\mathbb{Z}$ sont de ce type.

Définition 27 Un corps $\mathbb{K}$ est un anneau tel que $(\mathbb{K}-\{0\},\times)$ a une structure de groupe commutatif. C'est un anneau commutatif dans lequel tous les éléments non nuls ont un inverse pour la multiplication.