Structures

C. Susset

1 Groupes

1.1 Définition

Définition 1 *Soit G un ensemble non vide, on appelle loi de composition interne sur G, toute application $*$ de $G \times G$ dans G : $(a,b) \mapsto *(a,b)$. $*(a,b)$ se note en général $a * b$.*

Exemple 1

1. *L'addition et la multiplication sont des lois de composition interne dans $\mathbb{N}$, dans $\mathbb{Z}$, dans $\mathbb{Q}$, dans $\mathbb{R}$ ou dans $\mathbb{C}$.*
2. *Soit $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ (a,b) \in \mathbb{Z}^2\}$, l'addition est une loi de composition interne dans $\mathbb{Z}[\sqrt{2}]$*
3. *Soit $\mathcal{A}(\mathbb{R},\mathbb{R})$ l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$, l'addition des applications est une loi de composition interne dans $\mathcal{A}(\mathbb{R},\mathbb{R})$, pour $(f,g) \in \mathcal{A}(\mathbb{R},\mathbb{R})^2$, $\forall t \in \mathbb{R},\ (f+g)(t) = f(t) + g(t)$.*
4. *Soit $\mathcal{S}(\mathbb{R})$ l'ensemble des bijections de $\mathbb{R}$ dans $\mathbb{R}$, on a $\mathcal{S}(\mathbb{R}) \subset \mathcal{A}(\mathbb{R},\mathbb{R})$ mais l'addition n'est pas une loi de composition interne dans $\mathcal{S}(\mathbb{R})$*

Définition 2 (Groupe)
Un ensemble non-vide $(G,*)$ muni d'une loi de composition interne $*$ est un groupe si et seulement si

1. *$\forall (a,b,c) \in G^3,\ (a*b)*c = a*(b*c)$ (on dit que $*$ est associative)*
2. *$\exists e \in G,\ \forall x \in G,\ e*x = x*e = x$ (on dit que $(G,*)$ possède un élément neutre).*
3. *$\forall x \in G,\ \exists x' \in G,\ x*x' = x'*x = e$ (on dit que tout élément x de G possède un symétrique.)*

Si de plus :

- *$\forall (a,b) \in G^2,\ a*b = b*a$ (on dit que $*$ est une loi commutative)*
  $(G,*)$ est un groupe commutatif, on dit aussi groupe abélien.

Exemple 2

- *$(\mathbb{Z},+)$, $(Q,+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(Q^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$,*
  sont des groupes commutatifs.
- *$U = \{z \in \mathbb{C},\ |z| = 1\}$, $(U,.)$ est un groupe commutatif*
- *$(\mathbb{Z},.)$, $(\mathbb{Q},.)$, $(\mathbb{R},.)$, $(\mathbb{C},.)$ ne sont pas des groupes*
- *Soit E un ensemble non-vide et $\mathcal{S}(E)$ l'ensemble des bijections de E dans E. $(\mathcal{S}(E),\circ)$, où $\circ$ est la loi de composition des applications, est un groupe, ce groupe n'est pas commutatif dès que E contient au moins trois éléments.*

Notations

Additive Pour un groupe abélien, lorsque la loi de composition interne est une addition on note + cette loi et on parle de groupe additif. L'élément neutre est alors noté 0, et le symétrique d'un élément x du groupe est noté $-x$ et appelé "opposé" de x.

Multiplicative Pour un groupe abélien, lorsque la loi de composition interne est une multiplication on note . ou $\times$ cette loi et on parle de groupe multiplicatif. L'élément neutre est alors noté 1, et le symétrique d'un élément x du groupe est noté $\dfrac{1}{x}$ et appelé "inverse" de x.

Groupe quelconque Pour un groupe $(G,*)$ muni d'une loi $*$, L'élément neutre est souvent noté e, et le symétrique d'un élément x du groupe est noté x^{-1}.
Propriété 1 *Si $(x,y) \in G^2$ Alors $(x*y)^{-1} = y^{-1}*x^{-1}$*

1.2 Sous groupes

Définition 3 *Soit $(G,\star)$ un groupe et $H \subset G$. On dit H est un sous-groupe de G si $(H,\star)$ est un groupe.*

Proposition 1 *Soit $(G,\star)$ un groupe et $H \subset G$. H est un sous-groupe de G si et seulement si*
- *H est non vide*
- *$\star$ est interne dans H, soit $\forall (x,y) \in H^2,\ x \star y \in H$*
- *Le symétrique de tout élément de H appartient à H, soit $\forall x \in H,\ x^{-1} \in H$*

On a aussi

Proposition 2 *Soit $(G,\star)$ un groupe et $H \subset G$. H est un sous-groupe de G si et seulement si*
- *H est non vide*
- *$\forall (x,y) \in H^2,\ x \star y^{-1} \in H$*

Exemple 3
- *$(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$ qui est lui même un sous-groupe de $(\mathbb{R},+)$, enfin $(\mathbb{R},+)$ est un sous-groupe de $(\mathbb{C},+)$.*
- *$(\mathbb{Q}^*,.)$ est sous-groupe de $(\mathbb{R}^*,.)$ et $(\mathbb{R}^*,.)$ est un sous-groupe de $(\mathbb{C}^{\cdot\cdot})$.*
- *Pour $n \in \mathbb{N}^*$ posons $U_n = \{w \in \mathbb{C} / w^n = 1\}$, $U = \{z \in \mathbb{C},\ |z| = 1\}$, U_n est un sous-groupe de $(U,.)$.*

1.3 Morphismes de groupe

Définition 4 *Soit $(G,*)$ et $(G',*')$ deux groupes et f une application de G dans G'.*
f est un morphisme de groupe si et seulement si $\forall (x,y) \in G \times G',\ f(x*y) = f(x) *' f(y)$.
- *Un morphisme de groupe est aussi appelé homomorphisme de groupe*
- *Un morphisme bijectif est appelé isomorphisme de groupe*
- *Un morphisme de G dans G est appelé endomorphisme de groupe*
- *Un endomorphisme de groupe bijectif est appelé un automorphisme de groupe.*

Propriété 2 *Soit f un morphisme de groupe de G (d'élément neutre e) dans G' (d'élément neutre e') on a :*
- *$f(e) = e'$*
- *$\forall x \in G,\ (f(x))^{-1} = f(x^{-1})$*

Proposition 3 **Si** *f est un morphisme d'un groupe G dans un groupe G' et g est un morphisme de groupe de G' dans un groupe $G"$* **Alors** *$g \circ f$ est un morphisme de groupe de G dans $G"$.*

Proposition 4 *Soit $(G,*)$ un groupe et $\mathcal{A}(G)$ l'ensemble des automorphismes de G, $(\mathcal{A}(G),\circ)$ est un groupe.*

1.4 Noyau, image

Soit G et G' deux groupes et f un morphisme de groupe de G dans G'.

Proposition 5
- *Si H est un sous-groupe de G, Alors $f(H)$ est un sous-groupe de G'*
- *Si H' est sous-groupe de G', Alors $f^{-1}(H')$ est un sous-groupe de G*

Conséquences :

Proposition 6
- *$f(G)$ est un sous-groupe de G' appelé image de f. On le note $\mathrm{Im}(f)$ ou $\mathrm{Im} f$*
- *L'ensemble $f^{-1}(\{e'\})$ est un sous-groupe de G on l'appelle le noyau de f. On le note $\ker(f)$ ou $\ker f$*

Proposition 7 *Le morphisme f est injectif si et seulement si $\ker f = \{e\}$*

1.5 Groupe additif $(\mathbb{Z},+)$

Proposition 8 *Pour $a \in \mathbb{Z}$, $a\mathbb{Z} = \{a.n,\ n \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z},+)$*

Proposition 9 *Si G est un sous-groupe de $(\mathbb{Z},+)$ alors il existe un unique $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$*

2 Anneaux

2.1 Définition

Définition 5 (Anneaux)
Un ensemble non-vide $(A,+,.)$ muni de deux lois de composition interne $+$ et $\cdot$ est un anneau si et seulement si

1. *$(A,+)$ est un groupe commutatif dont l'élément neutre est souvent noté 0.*
2. *$\cdot$ est associative*
3. *$(A,\cdot)$ possède un élément neutre souvent noté 1*
4. *$\forall(a,b,c)\in A^3$, $(a+b)\cdot c = a\cdot c + b\cdot c$ (on dit que $\cdot$ est distributive à gauche sur l'addition $+$)*
5. *$\forall(a,b,c)\in A^3$, $c\cdot(a+b) = c\cdot a + c\cdot b$ (on dit que $\cdot$ est distributive à droite sur l'addition $+$)*

Si de plus :

- *$\cdot$ est commutative dans A, $(A,+,\cdot)$ est un anneau commutatif.*
- *$(A,+,\cdot)$ est un anneau commutatif tel que $A\neq\{0\}$ et $a\cdot b = 0 \Rightarrow a = 0$ ou $b = 0$ (on dit que $(A,+,\cdot)$ est sans diviseur de 0), $(A,+,\cdot)$ est un anneau intègre.*

Exemple 4

- *$(\mathbb{Z},+,\cdot)$, $(Q,+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des anneaux intègres.*
- *Soit $A(\mathbb{R},\mathbb{K})$ l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{K}$, $(A(\mathbb{R},\mathbb{K}),+,.)$ est un anneau commutatif non intègre.*

Définition 6
Soit $(A,+,\cdot)$ un anneau, on note A^* l'ensemble des éléments de A qui sont inversibles pour $\cdot$
$A^* = \{a\in A,\ \exists a'\in A,\ a\cdot a' = a'\cdot a = 1\}$

Proposition 10 *Si $(A,+,\cdot)$ est un anneau alors $(A^*,\cdot)$ est un groupe*

2.2 Règles de calculs

Soit $(A,+,.)$ un anneau, on a les propriétés suivantes :
P₁ $\forall a\in A,\ 0.a = a.0 = 0$ (on dit que 0 est absorbant)
P₂ $\forall(a,b)\in A^2,\ (-a).b = a.(-b) = -(a.b)$ (règle des signes)
P₃ Si $(a_i)_{i\in I}$ et $(bj)_{j\in J}$ sont deux familles de A, indexées par des ensembles finis I et J, Alors on a :

$$\left(\sum_{i\in I} a_i\right)\cdot\left(\sum_{j\in J} b_j\right) = \left(\sum_{(i,j)\in I\times J} a_i b_j\right).$$

P₄ Formule du binôme de Newton
Si $(a,b)\in A^2$ avec $a.b = b.a$ (on dit que a et b commutent)
Alors $\forall n\in\mathbb{N},\ (a+b)^n = \sum_{p=0}^{n}\binom{n}{p}a^p.b^{n-p}$
P₄ Si $(a,b)\in A^2$ avec $a.b = b.a$ **Alors** $a^n - b^n = (a-b).(a^{n-1} + a^{n-2}.b + \cdots + a.b^{n-2} + b^{n-1})$.

2.3 Sous-anneaux

Définition 7 *On appelle sous-anneau d'un anneau $(A,+,.)$ une partie A' de A telle que : $(A',+,.)$ est un anneau avec $1_A\in A'$ où 1_A est l'élément neutre de $.$ dans A.*

Proposition 11 *Soit $(A,+,.)$ un anneau et $A'\subset A$, A' est un sous-anneau de A si et seulement si*

1. *$A\neq\emptyset$*
2. *$\forall(a,b)\in A^2,\ a-b\in A$*
3. *$\forall(a,b)\in A^2,\ a.b\in A$*
4. *$1_A\in A'$*

3 Corps

Définition 8 (Corps)
Un ensemble non-vide $(\mathbf{K}, +, .)$ *muni de deux lois de composition interne* $+$ *et* $\cdot$ *est un corps si et seulement si*

1. $(\mathbf{K}, +, \cdot)$ *est un anneau.*
2. $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$

Si de plus :
$\cdot$ *est commutative dans* $\mathbf{K}$, $(\mathbf{K}, +, \cdot)$ *est un corps commutatif.*

Exemple 5 • $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *sont des corps commutatifs.*

Dans la suite du cours sauf mention du contraire nous ne considérerons que des corps commutatifs, le mot **corps** désignera donc un corps commutatif. **Notation** Si a et b sont deux éléments d'un corps $\mathbf{K}$ (commutatif) avec $b \neq 0$, on note $\dfrac{a}{b}$ l'élément $a.b^{-1} = b^{-1}.a$ de $\mathbf{K}$.

Proposition 12 *Soit* $\mathbf{K}$ *un corps,* $a \in \mathbf{K} \setminus \{1\}$ *et* $n \in \mathbb{N}$*, on a :*

$$1 + a + \cdots + a^n = \frac{1 - a^n}{1 - a}$$

Définition 9 *Soit* $\mathbf{K}$ *un corps. On appelle sous-corps de* $\mathbf{K}$ *un sous-anneau de* $\mathbf{K}$ *qui est un corps.*

Exemple 6 $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$ *sont trois sous-corps de* $(\mathbb{C}, +, .)$

4 Arithmétique dans $\mathbb{Z}$

Définition 10 *Soit* $(a, b) \in \mathbb{Z}^2$*, on dit que* b *divise* a *(on dit aussi* b *est un diviseur de* a*),* $b|a$ *si* $\exists c \in A,\ a = b \cdot c$*, on dit aussi que* a *est un multiple de* b*.*

Définition 11 *Soit* $a \in \mathbb{Z}$*, on dit que* a *est irréductible ou premier si* a *n'est pas inversible et les seuls diviseurs de* a *sont les éléments inversibles de* $\mathbb{Z}$ *et les éléments associés de* a*, c'est à dire le produit de* a *par un élément inversible, c'est à dire* $a \in \mathbb{Z}$ *est premier si et seulement si* a *admet exactement 4 diviseurs :* $a, -a, 1, -1$

Définition 12
Deux éléments a, b *de* $\mathbb{Z}$ *sont premiers entre eux si et seulement si les seuls diviseurs communs à* a *et* b *sont les éléments inversibles de* $\mathbb{Z}$ *c'est à dire* 1 *et* -1*, on note alors* $a \wedge b = 1$

Théorème 1 (décomposition en produit de facteurs premiers)
Si $a \in \mathbb{N}$*,* a *non-inversible, il existe une décomposition de* a *en produit de facteurs premiers :*
$a = \prod_{i=1}^{n} p_i^{\alpha_i}$ *avec* $\forall i,\ p_i \in \mathbb{N}$*,* p_i *premier,* $\alpha_i \in \mathbb{N}, \alpha_i \geq 1$*. Cette décomposition est unique à l'ordre près.*

Proposition 13 *Soit* $(a, b) \in \mathbb{N}^2$*, avec* a, b *non-nuls et non-inversibles ayant pour décomposition en produit de facteurs premiers :* $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ *et* $b = \prod_{j=1}^{m} q_j^{\beta_j}$ *on a :*

1. *a divise b si et seulement si tout diviseur premier de la décomposition de a apparait dans la décomposition de b avec un exposant supérieur ou égal.*
2. *Le* **pgcd** *de a et b (Plus Grand Commun Diviseur) est* $a \wedge b = \prod_{k=1}^{l} r_k^{\gamma_k}$ *avec*
   $\{r_1, \cdots, r_l\} = \{p_1, \cdots, p_n\} \cap \{q_1, \cdots, q_m\}$ *et* γ_k *est le plus petit des exposants de* r_k *apparaissant dans les décompositions de a et b.*
3. *Un* **ppcm** *de a et b (Plus Petit Commun Multiple) est* $a \vee b = \prod_{k=1}^{l} r_k^{\gamma_k}$ *avec*
   $\{r_1, \cdots, r_l\} = \{p_1, \cdots, p_n\} \cup \{q_1, \cdots, q_m\}$ *et* γ_k *est le plus grand des exposants de* r_k *apparaissant dans les décompositions de a et b.*

Proposition 14 (Division euclidienne)
Pour $(a, b) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ *il existe un unique couple* $(q, r) \in \mathbb{Z}^2$ *tel que* $a = bq + r$ *avec* $0 \leq r < b$
L'entier q *est le quotient de la division,* r *le reste,* a *et le dividende et* b *est le diviseur.*

Proposition 15 (Algorithme d'Euclide)
Soit $(a, b) \in N^2$*, avec* $b \neq 0$*. Si* $a = bq + r$ *avec* $(q, r) \in N^2$ *Alors* $a \wedge b = b \wedge r$