

## Chapitre 10

### Structures algébriques

#### 1 Loi de composition interne

##### Définition 1

Soit  $E$  un ensemble. Une loi de composition interne (parfois abrégée en l.c.i. ou l.d.c.i.) sur  $E$  est une application de  $E \times E$  dans  $E$ .

##### Remarque 2

On note une loi de composition interne sous la forme d'une **opération** entre deux éléments :  $x + y, x \times y, x * y, x.y, x \circ y, \dots$

##### Exemple 3

Quelques exemples.

- (i) L'addition,  $+$ , sur  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  est une loi de composition interne.
- (ii) La multiplication,  $\times$ , sur tous ces ensembles, est aussi une loi de composition interne.
- (iii) La multiplication est une loi de composition interne sur  $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ ,  $\mathbb{U}$ , sur  $\mathbb{U}_n$ .
- (iv) (pour celles et ceux qui ont des souvenirs sur les matrices) La multiplication est une loi de composition interne sur  $\mathcal{M}_2(\mathbb{R})$ , l'ensemble des matrices carrées de taille  $2 \times 2$  à coefficients réels.
- (v) La soustraction est une loi de composition interne sur  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , mais pas sur  $\mathbb{N}$ .
- (vi) La division est une loi de composition interne sur  $\mathbb{Q}^*$ , sur  $\mathbb{R}^*$ , sur  $\mathbb{C}^*$ , sur  $\{-1, 1\}$ .
- (vii) La loi  $\ominus$  définie par  $x \ominus y = |x - y|$  est une loi de composition interne sur  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ . (cette notation est une notation maison, qui servira juste pour cet exemple)
- (viii) Si  $E$  est un ensemble, la composition  $\circ$  est une loi de composition interne sur  $E^E$  : si  $f \in E^E$  et  $g \in E^E$ ,  $f \circ g$  est bien un élément de  $E^E$ .
- (ix) Soit  $\mathcal{B}$  l'ensemble des bijections d'un ensemble  $E$ . La composition est une loi de composition interne sur  $E$ .
- (x) Soit  $E$  un ensemble.  $\cup, \cap$  et  $\Delta$  sont des l.d.c.i. sur  $\mathcal{P}(E)$ .  
*On rappelle que  $A\Delta B = (A \cup B) \setminus (A \cap B)$ .*
- (xi) Sur  $\mathbb{Z}$ ,  $\wedge$  et  $\vee$  sont des lois de composition internes.

#### Définition 4

Soit  $(E, *)$  un ensemble muni d'une loi de composition interne.

- (i) La loi  $*$  est dite associative si

$$\forall (x, y, z) \in E^3, (x * y) * z = x * (y * z).$$

Dans ce cas, on note  $x * y * z$  sans mettre de parenthèse.

- (ii) Deux éléments  $x$  et  $y$  commutent pour  $*$  si  $x * y = y * x$ . Si tous les éléments de  $E$  commutent, on dit que  $*$  est commutative.

#### Exemple 5

Compléter le tableau suivant, en mettant OUI ou NON selon que la loi est associative et/ou commutative. Donne un contre-exemple lorsque ce n'est pas le cas.

Loi	Ensemble	Associative ?	Commutative ?
$+$	$\mathbb{R}$		
$\times$	$\mathbb{R}$		
$\times$	$\mathcal{M}_2(\mathbb{R})$		
$-$	$\mathbb{R}$		
$\div$	$\mathbb{R}$		
$\div$	$\{-1, 1\}$		
$\ominus$	$\mathbb{R}$		
$\circ$	$E^E$		
$\cap$	$\mathcal{P}(E)$		
$\cup$	$\mathcal{P}(E)$		
$\Delta$	$\mathcal{P}(E)$		
$\wedge$	$\mathbb{N}$		
$\vee$	$\mathbb{N}$		

Contre-exemples éventuels ?

#### Remarque 6 (À retenir)

- (i) Toutes les lois « normales » sont associatives (il faut chercher à faire une loi tordue pour avoir quelque chose de pas associatif).  
(ii) En revanche, certaines lois importantes ne sont pas commutatives ! (la composition et le produit matriciel).  
(iii) Il n'y a aucun lien entre commutativité et associativité.

#### Définition 7

Soit  $(E, *)$  un ensemble muni d'une loi. Un élément  $e$  de  $E$  est appelé élément neutre pour  $*$  si

$$\forall x \in E, x * e = e * x = x.$$

**Proposition 8**

Un élément neutre, s'il existe, est unique.

**Démonstration**

Soient  $e$  et  $e'$  deux éléments neutres de  $(E, *)$ . Alors

$$e * e' = e \text{ car } e' \text{ est élément neutre}$$

mais

$$e * e' = e' \text{ car } e \text{ est élément neutre}$$

Donc  $e = e'$ . ■

**Remarque 9**

L'élément neutre, s'il existe, commute avec tous les autres éléments, mais cela ne signifie pas que la loi est commutative.

**Exemple 10**

Déterminer, pour chaque loi, l'élément neutre. S'il n'y en a pas, le démontrer !

Loi	Ensemble	Neutre
+	$\mathbb{R}$	
$\times$	$\mathbb{R}$	
$\times$	$\mathcal{M}_2(\mathbb{R})$	
$-$	$\mathbb{R}$	
$\div$	$\mathbb{R}$	
$\div$	$\{-1, 1\}$	
$\ominus$	$\mathbb{R}$	
$\circ$	$E^E$	
$\cap$	$\mathcal{P}(E)$	
$\cup$	$\mathcal{P}(E)$	
$\Delta$	$\mathcal{P}(E)$	
$\wedge$	$\mathbb{N}$	
$\vee$	$\mathbb{N}$	

Contre-exemples éventuels ?

**Définition 11**

Soit  $(E, *)$  un ensemble muni d'une loi,  $x$  un élément de  $E$ .

- (i)  $x$  est dit inversible pour  $*$  s'il existe  $y$  dans  $E$  tel que  $x * y = y * x = e$ .
- (ii) dans ce cas, on dit que  $y$  est un inverse de  $x$  pour  $*$ .

**Proposition 12 (Quelques propriétés des inverses)**

Soit  $(E, *)$  un ensemble muni d'une loi,  $e$  son neutre,  $(x, y, z)$  trois éléments de  $E$ .

- (i) Si un élément  $x$  de  $E$  admet un inverse, alors cet inverse est unique. On le notera  $x^{-1}$ .
- (ii)  $e$  est inversible d'inverse  $e^{-1} = e$ .
- (iii)  $x^{-1}$  est inversible d'inverse  $x$ .
- (iv) Si  $x$  et  $y$  sont deux éléments inversibles, alors  $x * y$  est inversible et  $(x * y)^{-1} = y^{-1} * x^{-1}$ .

**(v)** Si  $x$  est inversible, alors

$$(x * y = x * z) \Rightarrow (y = z)$$

$$(y * x = z * x) \Rightarrow (y = z).$$

### Démonstration

**(i)** Soient  $a$  et  $b$  deux inverses de  $x$  pour  $*$ . Posons  $c = a * x * b$ . Comme  $a * x = e$ ,

$$c = e * b = b.$$

Comme  $x * b = e$ ,

$$c = a * e = a.$$

Donc  $b = a$ . D'où l'unicité de l'inverse.

**(ii)**  $e * e = e$  donc  $e^{-1} = e$ .

**(iii)**  $x^{-1} * x = x * x^{-1} = e$  donc, par définition de l'inverse,  $x^{-1}$  est inversible, d'inverse  $x$ .

**(iv)** on calcule

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e,$$

et, de même,

$$(y^{-1} * x^{-1}) * (x * y) = e,$$

donc  $x * y$  est inversible d'inverse  $y^{-1} * x^{-1}$ .

**(v)** Supposons que  $x$  est inversible, et que  $x * y = x * z$ . Alors

$$x^{-1} * x * y = x^{-1} * x * z,$$

donc  $e * y = e * z$ , donc  $y = z$ .

■

### Remarque 13

**(i)**  $x^{-1}$  est une **NOTATION** ! Il faut l'adapter au cadre considéré.

**(ii)** La dernière proposition est importante : elle assure que, pour un élément inversible, on peut « simplifier » les équations.

### Exemple 14

Recherchons les éléments admettant un inverse pour les lois précédentes :

**(i)** pour  $+$ , tout élément admet un inverse dans  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  : c'est son opposé. En revanche, seul  $0$  est inversible dans  $(\mathbb{N}, +)$ .

**(ii)** pour  $\times$ , dans  $\mathbb{Z}$ , seuls  $1$  et  $-1$  sont inversibles. Dans  $\mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$ , tous les éléments non nuls sont inversibles.

**(iii)** dans  $E^E$ , les éléments inversibles sont les bijections !

**(iv)** dans  $(\mathcal{P}(E), \cap)$ , le seul élément inversible est  $E$  ! Dans  $(\mathcal{P}(E), \cup)$ , le seul élément inversible est  $\emptyset$ .

(v) en revanche, dans  $(\mathcal{P}(E), \Delta)$ , tout élément est son propre inverse ! (le vérifier)

### Exercice 15

- (i) (exercice **fondamental**) Soit  $(E, *)$  un ensemble muni d'une ldci associative, d'élément neutre  $e$ . Soit  $x \in E$ , inversible. Montrer que

$$\varphi : \begin{cases} E \rightarrow E \\ y \mapsto x * y \end{cases}$$

est une bijection.

- (ii) Soit  $E = \mathbb{R}^{\mathbb{R}}$ , muni de la loi  $\times$  (produit de fonctions). Déterminer le neutre et les inversibles de  $(E, \times)$ .

### Définition 16

Soit  $(E, *)$  un ensemble muni d'une Ici. Soit  $A$  un sous-ensemble de  $E$ .  $A$  est dite stable par \*

\* si

$$\forall (x, y) \in A^2, x * y \in A.$$

### Exemple 17

- (i) pour tout entier  $a$ ,  $a\mathbb{Z}$  est une partie stable par addition de  $\mathbb{Z}$ .  
(ii)  $\mathbb{Q}$  est une partie stable par addition et par multiplication de  $\mathbb{R}$ .  
(iii) en revanche,  $\mathbb{R} \setminus \mathbb{Q}$  n'est pas stable par  $\times$  dans  $\mathbb{R}$ .  
(iv)  $\mathbb{U}, \mathbb{U}_n$ , stables par la multiplication.

### Définition 18

Soit  $(E, *)$  un ensemble muni d'une ldci, associative, possédant un neutre  $e$ . Soit  $x \in E$  et  $n \in \mathbb{N}$ . On note

$$x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}},$$

avec comme convention  $x^0 = e$ .

Si de plus,  $x$  est inversible, on note  $x^{-n} = (x^{-1})^n$ .

### Remarque 19

- (i) Attention, la notation  ${}^n$  est une notation ! Il faut pouvoir l'adapter en  ${}^{nx}$  si la loi est + par exemple.  
(ii) On a clairement  $x^{n+m} = x^n * x^m$ .  
(iii) On n'a pas, en général,  $(x * y)^n = x^n * y^n$  : il faut que  $x$  et  $y$  commutent !



**Proposition 20**

Soit  $(E, *)$  un ensemble muni d'une ldci, associative, possédant un neutre  $e$ . Soient  $(x, y) \in E^2$ .

- (i) Si  $x * y = y * x$ , alors pour tout  $n$  dans  $\mathbb{N}$ ,  $(x * y)^n = x^n * y^n$ .
- (ii) Si  $x * y = y * x$  et si  $x$  et  $y$  sont inversibles,  $(x * y)^{-1} = x^{-1} * y^{-1}$ .

**Démonstration**

On prouve ce résultat par récurrence, en démontrant d'abord le Lemme  $\forall k \in \mathbb{N}, x * y^k = y^k * x$ .

■

**Proposition 21 (Une propriété importante)**

Soit  $(E, *)$  un ensemble muni d'une ldci, associative, possédant un neutre  $e$ . Soit  $x$  un élément **inversible** de  $E$ ,  $a \in E$ . On note  $b = x * a * x^{-1}$ . Alors, pour tout  $n$  dans  $\mathbb{N}$ ,

$$b^n = x * a^n * x^{-1}.$$

**Démonstration**

On démontre le résultat par récurrence sur  $n$ .

Pour l'**initialisation**, on remarque que  $b^0 = e$  et  $x * a^0 * x^{-1} = x * x^{-1} = e$ .

Pour l'hérédité, soit  $n$  dans  $\mathbb{N}$  tel que  $b^n = x * a^n * x^{-1}$ . Alors

$$\begin{aligned} b^{n+1} &= b * b^n \\ &= (x * a * x^{-1}) * (x * a^n * x^{-1}) \\ &= x * a * x^{-1} * x * a^n * x^{-1} \\ &= x * a * a^n * x^{-1} \\ &= x * a^{n+1} * x^{-1}. \end{aligned}$$

D'où l'hérédité et le résultat ! ■

**Remarque 22**

Cette propriété sera **très importante** lorsqu'on fera des matrices. Gardez-la en tête !

**Exercice 23**

Dans  $\mathcal{M}_2(\mathbb{R})$ , muni de la multiplication, on pose

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \text{ et } C = \begin{pmatrix} -1 & -1 \\ 6 & 4 \end{pmatrix}.$$

- (i) Démontrer que  $B$  est l'inverse de  $A$  pour  $\times$ .
- (ii) Calculer  $A \times C \times B$ , et en déduire une formule assez simple pour  $C^n$ .

## 2 Groupes

### 2.1 Groupes, sous-groupes

#### Définition 24

Un groupe est un ensemble non vide  $G$ , muni d'une loi de composition interne  $*$ , vérifiant les propriétés suivantes :

- (i)  $*$  est associative.
- (ii)  $(G, *)$  admet un élément neutre.
- (iii) Tout élément de  $G$  admet un inverse pour  $*$ .

Si  $*$  est commutative, on dit que  $G$  est un groupe commutatif ou, plus couramment, on dira que  $G$  est un groupe abélien.

#### Exemple 25

Dans les exemples précédents, assez peu sont des groupes.

- (i)  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  sont des groupes abéliens.
- (ii)  $(\mathbb{C}^*, \times)$ ,  $(\mathbb{R}^*, \times)$ ,  $(\mathbb{Q}^*, \times)$  aussi.
- (iii)  $(\mathbb{U}, \times)$  et  $(\mathbb{U}_n, \times)$  sont des groupes abéliens.
- (iv) si  $E$  est un ensemble,  $(\mathcal{P}(E), \Delta)$  est un groupe abélien.

#### Définition 26 (et prop)

Soit  $E$  un ensemble. On note  $\mathcal{S}_E$  l'ensemble des bijections de  $E$  dans  $E$  et on appelle cet ensemble ensemble des permutations de  $E$ .

$(\mathcal{S}_E, \circ)$  est un groupe, non abélien en général.

#### Exemple 27

Décrire  $\mathcal{S}_E$  lorsque  $E = \{a, b, c\}$ .

#### Définition 28

Soit  $(G, *)$  un groupe. Un sous-groupe de  $H$  est un sous-ensemble  $H$  de  $G$  tel que

- (i)  $H$  est stable par  $*$ .
- (ii)  $(H, *)$  est un sous-groupe.

#### Remarque 29

Si  $H$  est un sous-groupe de  $G$ , alors pour tout  $x$  de  $H$ ,  $x$  admet un inverse *dans*  $H$  : mais il s'agit aussi de l'inverse dans  $G$  (par unicité de l'inverse).

Cette définition n'est pas la plus pratique... donnons une propriété pratique des sous-groupes.

### Proposition 30

Soit  $(G, *)$  un groupe,  $H \subset G$ . Les assertions suivantes sont équivalentes :

- (i)  $H$  est un sous-groupe de  $(G, *)$ .
- (ii)  $H$  est non vide et pour tous  $(x, y)$  de  $H^2$ ,  $x * y$  et  $x^{-1}$  appartiennent à  $H$ .
- (iii)  $H$  est non vide et pour tous  $(x, y)$  de  $H^2$ ,  $x * y^{-1}$  appartient à  $H$ .

### Démonstration

Démonstration complètement inutile... Remarquons juste pourquoi les deux derniers points sont équivalents. La première implication est évidente, pour la réciproque,

- comme  $H \neq \emptyset$ ,  $H$  contient un élément  $x_0$  donc  $H$  contient  $x_0 * x_0^{-1}$  donc il contient  $e$ .
- soit  $x \in H$ . Alors  $e * x^{-1} \in H$  donc  $x^{-1} \in H$ .
- soit  $(x, y) \in H^2$ . Alors  $y^{-1} \in H$ , donc  $x * (y^{-1})^{-1} \in H$ , i.e.  $x * y \in H$ .

■

### Point de méthode 31

Les sous-structures, c'est plus sûr !

Pour montrer qu'un ensemble est un groupe, dans 90% des cas, on n'utilisera pas la définition mais la caractérisation !

### Exemple 32

- (i)  $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$  sont des sous-groupes de  $(\mathbb{C}, +)$  (on dit que ce sont des sous-groupes additifs de  $\mathbb{C}$ ).
- (ii)  $\mathbb{R}^*, \mathbb{Q}^*$  sont des sous-groupes de  $(\mathbb{C}^*, \times)$  (on dit que ce sont des sous-groupes multiplicatifs de  $\mathbb{C}$ ).
- (iii) On a déjà démontré que  $\mathbb{U}$  et  $\mathbb{U}_n$  étaient des sous-groupes de  $(\mathbb{C}, \times)$ .
- (iv) Si  $G$  est un groupe, alors  $\{e\}$  et  $G$  sont des sous-groupes de  $G$ , appelés sous-groupes triviaux de  $G$ .

### Proposition 33

Soit  $(G, *)$  un groupe.

- (i) Si  $H$  et  $K$  sont deux sous-groupes de  $G$ ,  $H \cap K$  est un sous-groupe de  $G$ .
- (ii) Si  $I$  est un ensemble et  $(H_i)_{i \in I}$  est une famille de sous-groupes de  $G$ , alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .
- (iii) Si  $H$  et  $K$  sont deux sous-groupes de  $G$ ,  $H \cup K$  est un sous-groupe de  $G$  si et seulement si  $H \subset K$  ou  $K \subset H$ .

### Démonstration

- (i) • déjà,  $e_G \in H$  et  $e_G \in K$  donc  $e_G \in H \cap K$ .

- ensuite, soit  $(x, y) \in (H \cap K)^2$ . Alors
  - $H$  est un sous-groupe de  $G$  donc  $x * y^{-1} \in H$ ,
  - $K$  est un sous-groupe de  $G$  donc  $x * y^{-1} \in K$ ,

donc  $x * y^{-1} \in H \cap K$ .

Donc  $H \cap K$  est un sous-groupe de  $(G, *)$ .

**(ii)** À adapter.

**(iii)** Supposons que  $H \cup K$  est un sous-groupe de  $G$ . On veut démontrer que  $H \subset K$  ou  $K \subset H$ .

**Supposons**  $H \not\subset K$ . Alors on dispose de  $h \in H$  tel que  $h \notin K$ .

Soit  $x \in K$ . Alors  $h \in H \cup K$ ,  $x \in H \cup K$  donc  $h * x \in H \cup K$  (car  $H \cup K$  est un sous-groupe de  $G$ )

- si  $h * x \in H$ , alors comme  $h \in H$ , et  $H$  est un sous-groupe de  $G$ ,  $h^{-1} * (h * x) \in H$ , donc  $x \in H$ ,
- si  $h * x \in K$ , alors, comme  $K$  est un sous-groupe de  $G$ ,  $(h * x) * x^{-1} \in K$ , i.e.  $h \in K$ , **IMPOSSIBLE**.

Donc  $x \in H$ , donc  $K \subset H$ .

D'où le résultat désiré!

■

### Proposition 34

Soit  $(G, *)$  un groupe,  $H$  un sous-groupe de  $G$ . Alors pour tout  $x$  de  $H$ , pour tout  $n$  dans  $\mathbb{Z}$ ,  $x^n \in H$ .

### Démonstration

C'est juste une récurrence! ■

### Exercice 35

- (i)** Je suis un sous-groupe de  $(\mathbb{Z}, +)$  contenant 1. Qui suis-je ?
- (ii)** Je suis un sous-groupe de  $(\mathbb{R}, +)$  contentant  $[a, b]$  avec  $a < b$ . Qui suis-je ?

### Proposition 36 (Sous-groupes additifs de $(\mathbb{Z}, +)$ )

Soit  $H$  un sous-groupe additif de  $(\mathbb{Z}, +)$ . Alors il existe un entier naturel  $a$  tel que

$$H = a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}.$$

### Remarque 37

Attention au contexte dans lequel on se place : ici, le groupe est **additif**. Le neutre est 0, l'inverse de  $x$  est  $-x$ , la notation «  $x^n$  » de la proposition précédente est  $nx$ , etc.

### Démonstration

- Déjà, si  $H$  est réduit à  $\{0\}$ ,  $H = 0\mathbb{Z}$ .
- Sinon, la partie  $\mathbb{N}^* \cap H$  est non vide (en effet,  $H$  contient un élément non nul : s'il est positif, c'est gagné, sinon, comme son opposé est aussi dans  $H$ , c'est aussi gagné). Soit  $a = \min(\mathbb{N}^* \cap H)$ . On montre que  $H = a\mathbb{Z}$ .
  - déjà, par la proposition précédente (réurrence), pour tout  $n$  dans  $\mathbb{N}$ ,  $an \in H$ .
  - ensuite, soit  $x \in H$ . Effectuons la division euclidienne de  $x$  par  $a$  :

$$x = aq + r \text{ avec } r \in \llbracket 0, a-1 \rrbracket.$$

Comme  $x \in H$ , comme  $aq \in H$ ,  $r \in H$  et  $r \in \mathbb{N}$ .

Si  $r \neq 0$ , alors  $r \in \mathbb{N}^* \cap H$  et  $r < a$ , absurde !

Donc  $r = 0$ , donc  $a$  divise  $x$ .

Donc  $x \in a\mathbb{Z}$ .

D'où l'inclusion réciproque et l'égalité !



### Proposition 38 (Sous-groupes additifs de $(\mathbb{R}, +)$ , HP)

Soit  $A$  un sous-groupe additif de  $(\mathbb{R}, +)$ . Alors

- (i) Soit il existe un réel  $a > 0$  tel que  $A = a\mathbb{Z}$ .
- (ii) Soit  $A$  est dense dans  $\mathbb{R}$ .

### Démonstration

La preuve constitue un des exercices corrigés en classe dans le TD. ■

## 2.2 Générateurs, sous-groupe engendré

### Définition 39

Soit  $(G, *)$  un groupe.

- (i) Si  $x \in G$ , le sous-groupe engendré par  $x$  est le sous-groupe de  $G$  noté  $\langle x \rangle$  et défini par

$$\langle x \rangle = \{x^k, k \in \mathbb{Z}\}.$$

- (ii) Soit  $\mathcal{A}$  une partie de  $G$ . Le sous-groupe engendré par  $\mathcal{A}$  est l'ensemble des produits d'éléments de  $\mathcal{A}$  ou de leurs inverses

$$\langle \mathcal{A} \rangle = \{a_1^{\varepsilon_1} * a_2^{\varepsilon_2} * \dots * a_r^{\varepsilon_r}, (a_1, \dots, a_r) \in \mathcal{A}^r, (\varepsilon_1, \dots, \varepsilon_r) \in \{-1, 1\}^r\}.$$

- (iii) Si  $G$  est abélien, et si  $\mathcal{A} = \{x_1, \dots, x_r\}$  est finie, alors le sous-groupe engendré par  $\mathcal{A}$  est

$$\langle \mathcal{A} \rangle = \{x_1^{k_1} * x_2^{k_2} * \dots * x_r^{k_r}, (k_1, \dots, k_r) \in \mathbb{Z}^r\}.$$

### Proposition 40

Soit  $(G, *)$  un groupe,  $\mathcal{A}$  une partie de  $G$ .  $\langle \mathcal{A} \rangle$  est le plus petit sous-groupe de  $G$  contenant  $\mathcal{A}$ .

### Remarque 41

- (i) Pour le moment, en MPSI, garder la définition du sous-groupe engendré par un élément, et la définition dans le cas abélien.
- (ii) La proposition, que l'on ne démontre pas là, est à garder dans un coin de la tête quand nous définirons la notion de sous-espace vectoriel.

### Exercice 42

Soient  $a$  et  $b$  deux entiers naturels. Comment décrire  $\langle a, b \rangle$ ? Comment décrire  $a\mathbb{Z} \cap b\mathbb{Z}$ ?

### Définition 43

Soit  $(G, *)$  un groupe.

- (i)  $G$  est dit **monogène** s'il existe  $x_0$  dans  $G$  tel que  $G = \langle x_0 \rangle$ .
- (ii)  $G$  est dit **cyclique** s'il est monogène et fini.

### Exemple 44

- (i)  $(\mathbb{U}_n, \times)$  est un groupe cyclique. On a vu dans le chapitre d'arithmétique que les générateurs de  $(\mathbb{U}_n, \times)$  sont les complexes de la forme  $e^{\frac{2ik\pi}{n}}$ , avec  $k \wedge n = 1$ .
- (ii)  $(\mathbb{Z}, +)$  est monogène mais pas cyclique.

## 2.3 Morphismes

### Définition 45

Soient  $(G, *)$  et  $(H, \cdot)$  deux groupes.  $\varphi$  une application de  $G$  dans  $H$ .

- (i) on dit que  $\varphi$  est un morphisme de groupes si
$$\forall (x, y) \in G^2, \varphi(x * y) = \varphi(x) \cdot \varphi(y)$$
- (ii) si  $\varphi$  est bijective, on dit que  $\varphi$  est un **isomorphisme de groupes**, et que  $G$  et  $H$  sont isomorphes.
- (iii) si  $\varphi : (G, *) \rightarrow (G, *)$ , on dit que  $\varphi$  est un **endomorphisme de groupes**
- (iv) si  $\varphi$  est un endomorphisme bijectif, on dit que c'est un **automorphisme de groupes**.

### Proposition 46

Soient  $(G, *)$  et  $(H, .)$  deux groupes.  $\varphi$  un morphisme de  $G$  dans  $H$ . Alors

- $\varphi(e_G) = e_H$ ,
- $\forall x \in G$ ,

$$\varphi(x^{-1}) = \varphi(x)^{-1},$$

le  $^{-1}$  étant à comprendre comme l'inverse dans le groupe considéré.

### Démonstration

- $e_G * e_G = e_G$  donc

$$\varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G).$$

En multipliant par l'inverse **dans**  $H$  de  $\varphi(e_G)$ , on obtient  $\varphi(e_G) = e_H$ .

- soit  $x \in G$ . Alors  $x * x^{-1} = e_G$  donc

$$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(e_G) = e_H,$$

$$\text{donc } \varphi(x^{-1}) = \varphi(x)^{-1}.$$

■

### Exemple 47

Il faut remarquer que l'on a déjà vu des morphismes de groupes :

- (i) toute application linéaire est un endomorphisme de groupes de  $(\mathbb{R}, +)$ .
- (ii) on a vu mieux : tout endomorphisme de groupe **continu** de  $(\mathbb{R}, +)$  est linéaire.
- (iii) l'exponentielle est un morphisme de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}_+^*, \times)$ .
- (iv)  $\ln$  est un morphisme de  $(\mathbb{R}_+^*, \times)$  dans  $(\mathbb{R}, +)$ .

- (v) si  $\omega = e^{\frac{2i\pi}{n}}$ , l'application

$$\varphi : \begin{cases} \mathbb{Z} \rightarrow \mathbb{U}_n \\ k \mapsto \omega^k \end{cases}$$

est un morphisme de groupes.

### Proposition 48

- (i) Une composée de morphismes de groupes est un morphisme de groupes.
- (ii) La réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

### Proposition 49

Soient  $(G, *)$  et  $(H, .)$  deux groupes,  $\varphi : G \rightarrow H$  un morphisme de groupes.

- (i) si  $A$  est un sous-groupe de  $G$ , alors  $\varphi(A)$  est un sous-groupe de  $H$ .
- (ii) si  $B$  est un sous-groupe de  $H$ , alors **l'image réciproque**  $\varphi^{-1}(B)$  est un sous-groupe de  $G$ .

Cette définition est utile pour **une notion fondamentale** notamment, celle de noyau.

**Définition 50**

Soient  $(G, *)$  et  $(H, .)$  deux groupes,  $\varphi : G \rightarrow H$  un morphisme de groupes.  
Le **noyau** de  $\varphi$  est l'ensemble noté  $\ker(\varphi)$  et défini par

$$\ker(\varphi) = \varphi^{-1}(\{e_H\}) = \{x \in G, \varphi(x) = e_H\}.$$

**Remarque 51**

Remarquons que  $\ker(\varphi)$  est toujours non vide car  $e_G \in \ker(\varphi)$ .

**Exemple 52**

(i) si  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ ,

$$\ker(\exp) = \exp^{-1}(\{1\}) = \{0\}.$$

(ii) si  $\omega = e^{\frac{2i\pi}{n}}$  et

$$\varphi : \begin{cases} \mathbb{Z} \rightarrow \mathbb{U}_n \\ k \mapsto \omega^k \end{cases}$$

alors

$$\ker(\varphi) = \{k \in \mathbb{Z}, \omega^k = 1\} = n\mathbb{Z}.$$

Cette notion de noyau est très satisfaisante dans le sens où elle permet de caractériser l'injectivité d'un morphisme.

**Proposition 53**

Soient  $(G, *)$  et  $(H, .)$  deux groupes,  $\varphi : G \rightarrow H$  un morphisme de groupes.  
Alors  $\varphi$  est injectif si, et seulement si  $\ker(\varphi) = \{e_G\}$ .

**Démonstration**

$\Rightarrow$  Si  $\varphi$  est injectif, on sait déjà que  $e_G \in \ker(\varphi)$ . Démontrons l'inclusion réciproque.  
Soit  $x \in \ker(\varphi)$ . Alors

$$\varphi(x) = e_H = \varphi(e_G),$$

donc, par injectivité de  $\varphi$ ,  $x = e_G$ . Donc  $\ker(\varphi) = \{e_G\}$ .

$\Leftarrow$  Si  $\ker(\varphi) = \{e_G\}$ , montrons que  $\varphi$  est injectif.

Soit  $(x, x') \in G^2$  tels que  $\varphi(x) = \varphi(x')$ . Alors, en multipliant par l'inverse de  $\varphi(x')$ ,

$$\varphi(x) \cdot \varphi(x')^{-1} = e_H,$$

donc, comme  $\varphi$  est un morphisme,

$$\varphi(x * x'^{-1}) = e_H,$$

donc  $x * x'^{-1} \in \ker(\varphi) = \{e_G\}$ .  
Donc  $x * x'^{-1} = e_G$  donc  $x = x'$ .  
D'où l'injectivité de  $\varphi$  !

### 3 Groupe des permutations d'un ensemble fini

#### Définition 54

Une permutation d'un ensemble  $E$  est une bijection de  $E$  dans lui-même. L'ensemble des permutations de  $E$  est  $S_E$ . L'ensemble des permutations de  $\llbracket 1, n \rrbracket$  est noté  $S_n$ .

#### Proposition 55

$S_n$  est un groupe, de cardinal égal à  $n!$ .

#### Démonstration

Même si on n'a pas fait vraiment de dénombrement, on peut expliquer comment on peut obtenir ce cardinal.

Choisir une permutation de  $\llbracket 1, n \rrbracket$ , c'est

- d'abord choisir l'image de 1 :  $n$  possibilités,
- puis choisir l'image de 2 parmi les éléments de  $\llbracket 1, n \rrbracket$ , mais en ne prenant pas l'image choisie pour 1 :  $n - 1$  possibilités,
- puis choisir l'image de 3 parmi les éléments privés des images de 1 et de 2 :  $n - 2$  possibilités,
- ...
- puis choisir l'image de  $n$  : il ne reste plus qu'une possibilité.

D'où  $n \times (n - 1) \times \cdots \times 2 \times 1 = n!$  possibilités de choisir un élément de  $S_n$ . ■

#### Définition 56 (Notation)

On notera un élément  $\sigma$  de  $S_n$  sous la forme  $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ .

#### Exemple 57

(i) Soient  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$  et  $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ .  
Calculer  $\sigma^2$ ,  $\sigma^3$ ,  $\rho^2$ ,  $\sigma \circ \rho$ .

(ii) Décrivons  $S_3$ . Il a 6 éléments.  $S_3$  et  $\mathbb{U}_6$  sont-ils pour autant isomorphes ?

### Définition 58

Soit  $p$  dans  $\llbracket 2, n \rrbracket$ . On appelle  $p$ -cycle de  $\llbracket 1, n \rrbracket$  toute permutation  $\sigma$  telle qu'il existe  $i_1, \dots, i_p$   $p$  entiers de  $\llbracket 1, n \rrbracket$  tels que

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{p-1}) = i_p, \sigma(i_p) = i_1,$$

et pour tout  $j$  différent de  $(i_1, \dots, i_p)$ ,  $\sigma(j) = j$ .

$\{i_1, \dots, i_p\}$  est nommé support du cycle, et le cycle  $\sigma$  sera noté  $(i_1 \dots i_p)$ .  
Un 2-cycle est appelé transposition.

### Exemple 59

(i) Dans  $S_4$ , si  $\rho = (1 2 4)$ ,  $\rho$  est la permutation  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ . Son support est  $\{1, 2, 4\}$ .

(ii) Avant d'utiliser la notation  $(i_1 \dots i_p)$ , il faut préciser  $n$  :

- si  $n = 3$ ,  $(1 2)$  correspond à  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

- si  $n = 5$ ,  $(1 2)$  correspond à  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ .

(iii) Il n'y a pas unicité dans l'écriture de  $(i_1 \dots i_p)$ . En effet, dans  $S_4$ ,

$$(1 2 4) = (2 4 1) = (4 1 2).$$

### Proposition 60

(i) Deux cycles à support disjoints commutent.

(ii) Si  $\rho$  est un  $p$ -cycle, alors  $\rho^p = \text{Id}$ . En particulier, pour une transposition,  $\tau^{-1} = \tau$ .

Il est alors important de comprendre comment est engendré  $S_n$  s'il n'est pas engendré par un seul élément comme  $\mathbb{U}_n$ .

### Théorème 61

Soit  $\sigma \in S_n$ . Alors  $\sigma$  s'écrit de manière unique comme produit de cycles à supports disjoints (moyennant commutation et réordonnement interne des cycles).

### Démonstration

L'idée est de faire une récurrence, mais je ne considère pas ce résultat comme pertinent à prouver en détail (très technique). L'idée est importante tout de même : on considère les **orbites** des éléments de  $\llbracket 1, n \rrbracket$ , i.e., si  $x \in \llbracket 1, n \rrbracket$ , l'ensemble

$$\{\sigma^k(x), k \in \mathbb{Z}\}$$

On remarque que les orbites forment une partition de  $\llbracket 1, n \rrbracket$ , et chaque orbite donne le support du cycle intervenant dans la décomposition. ■

**Exemple 62**

Décomposer en cycle à supports disjoints

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 2 & 8 & 1 & 7 & 3 & 4 & 9 \end{pmatrix}$$

Il existe une autre manière de décomposer les permutations, c'est en produit de transpositions.

**Proposition 63**

Tout cycle  $(i_1 \dots i_p)$  se décompose ainsi :

$$(i_1 \ i_p) \circ (i_1 \ i_{p-1}) \circ \dots \circ (i_1 \ i_2) \text{ ou } (i_1 \ i_2) \circ (i_2 \ i_3) \circ \dots \circ (i_{p-1} \ i_p)$$

Ceci permet donc d'énoncer la proposition suivante

**Proposition 64**

Toute permutation se décompose comme produit de transpositions.

Nous allons terminer avec une grandeur caractéristique des permutations : la signature.

**Théorème 65 (et définition)**

Il existe une unique application  $\varepsilon$  de  $S_n$  dans  $\{-1, 1\}$  telle que

- (i)  $\forall \tau$  transposition,  $\varepsilon(\tau) = -1$ .
- (ii)  $\forall (\sigma, \sigma') \in S_n^2$ ,  $\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ .

Cette application est appellée signature.

**Démonstration**

- (i) Existence.** On pose, si  $\rho$  est un cycle de longueur  $p$ ,

$$\varepsilon(\rho) = (-1)^{p-1},$$

et, si  $\sigma \in S_n$  et  $(\rho_1, \dots, \rho_r)$  est sa décomposition en cycles à supports disjoints,

$$\varepsilon(\sigma) = \prod_{k=1}^r (-1)^{p_k-1},$$

où  $p_k$  est la taille du support de  $\rho_k$ . (avec comme convention  $\varepsilon(\text{Id}_{[1,n]}) = 1$  – produit vide)

- déjà,  $\tau$  est à valeurs dans  $\{-1, 1\}$ .
- ensuite, si  $\tau$  est une transposition, c'est un 2-cycle et donc  $\varepsilon(\tau) = -1$ .
- enfin, pour démontrer la multiplicativité, on va simplement démontrer que si  $\sigma$  est une permutation, et  $\tau$  est une transposition, alors  $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$ . Le reste s'en déduira en décomposant  $\sigma'$  comme produit de transpositions. On écrit  $\tau = (a \ b)$  et  $\sigma = \rho_1 \circ \dots \circ \rho_r$  sa décomposition en cycles à supports disjoints.
  - (a) si  $a$  et  $b$  sont deux points fixes de  $\sigma$ , ils n'interviennent pas dans la décomposition de  $\sigma$  en cycles à supports disjoints, donc la décomposition en cycles à supports disjoints de  $\sigma \circ \tau$  est  $\rho_1 \circ \dots \circ \rho_r \circ \tau$ , de signature  $\prod_{k=1}^r (-1)^{p_k-1} \times 2 = \varepsilon(\sigma)\varepsilon(\tau)$ .

- (b) si  $a$  est un point fixe de  $\sigma$  et  $b$  est un élément du support d'un des cycles de  $\sigma$ , disons  $\rho_r = (c_1 \dots c_s \ b)$ . Alors  $\rho_r \circ \tau = (c_1 \dots c_s \ b \ a)$ , donc la signature de  $\sigma \circ \tau$  est  $\prod_{k=1}^{r-1} (-1)^{p_k-1} \times (-1)^{p_r+1-1} = \prod_{k=1}^r (-1)^{p_k-1} \times (-1) = \varepsilon(\sigma)\varepsilon(\tau)$ .
- (c) si  $a$  et  $b$  sont deux éléments du même cycle,  $\rho_r$ , alors  $\rho_r \circ \tau$  est un produit de deux cycles à supports disjoints de longueurs  $\ell$  et  $p_r - \ell$ . Donc la signature de  $\sigma \circ \tau$  est  $\prod_{k=1}^{r-1} (-1)^{p_k-1} \times (-1)^{\ell-1} \times (-1)^{p_r-\ell-1} = \prod_{k=1}^r (-1)^{p_k-1} \times (-1) = \varepsilon(\sigma)\varepsilon(\tau)$ ,
- (d) si, au contraire,  $a$  et  $b$  sont deux éléments de deux cycles différents, disons  $\rho_r$  et  $\rho_{r-1}$ , alors  $\rho_{r-1} \circ \rho_r \circ \tau$  est un unique cycle où l'on a recollé les supports de  $\rho_{r-1}$  et  $\rho_r$  en  $a$  et  $b$ . Sa signature est donc  $(-1)^{p_{r-1}+p_r-1}$ , donc

$$\varepsilon(\sigma \circ \tau) = \prod_{k=1}^{r-2} (-1)^{p_k-1} \times (-1)^{p_{r-1}+p_r-1} = (-1)^{p_{r-1}+p_r-1} \times (-1) = \varepsilon(\sigma)\varepsilon(\tau).$$

**(ii) Unicité.** Soit  $\varepsilon'$  une autre application vérifiant les mêmes propriétés que  $\varepsilon$  définie ci-dessus. Soit  $\sigma \in S_n$ ,  $\sigma = \tau_1 \circ \dots \circ \tau_r$  une décomposition de  $\sigma$  en produit de transpositions. Alors par propriété de morphisme,

$$\varepsilon'(\sigma) = \prod_{i=1}^r \varepsilon'(\tau_i) = (-1)^r = \varepsilon(\sigma).$$

Donc  $\varepsilon = \varepsilon'$ , d'où l'unicité !

### Corollaire 66

On a un corollaire amusant : deux décompositions en produits de transpositions ont même parité.

### Point de méthode 67 (À retenir : pour déterminer la signature d'une permutation)

Si  $\sigma$  est une permutation, sa signature vaut :

- $(-1)^{p-1}$  si c'est un  $p$ -cycle,
- $\prod_{i=1}^r (-1)^{p_i-1}$  si  $\sigma$  est le produit de  $r$  cycles chacun de longueur  $p_i$ ,
- $(-1)^s$  si  $\sigma$  est le produit de  $s$  transpositions.

### Exemple 68

Calculer la signature de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 6 & 2 & 1 & 7 \end{pmatrix}$$

On finit le chapitre par définir un sous-groupe de  $S_n$  :

**Définition 69**

Le groupe alterné  $\mathcal{A}_n$  est  $\ker(\varepsilon)$ , i.e.

$$\mathcal{A}_n = \{\sigma \in S_n, \varepsilon(\sigma) = 1\}.$$

**Exemple 70**

(i) Il s'agit clairement d'un sous-groupe de  $S_n$  car c'est le noyau d'un morphisme.

(ii) Décrivons  $\mathcal{A}_3$ .

$\mathcal{A}_3 = \{\sigma \in S_3, \varepsilon(\sigma) = 1\}$ . On sait que  $S_3$  est constitué de  $\text{Id}$ , de trois transpositions (de signature  $-1$ ) et de deux 3-cycles. Donc

$$\mathcal{A}_3 = \{\text{Id}_{[1,3]}, (1 2 3), (1 3 2)\} = \{\rho^0, \rho^1, \rho^2\} = \langle \rho \rangle,$$

si l'on note  $\rho$  le cycle  $(1 2 3)$ .

Ainsi,  $\mathcal{A}_3$  est cyclique : c'est en fait le seul groupe alterné cyclique.

(iii) Déterminer  $\mathcal{A}_4$ ...

**Exercice 71**

Démontrer que  $\mathcal{A}_n$  possède  $\frac{n!}{2}$  éléments.

## 4 Anneaux et corps

**Définition 72**

Un ensemble  $A$  muni de deux lois de composition internes  $+$  et  $\times$  est un anneau si les trois conditions suivantes sont vérifiées :

- (i)  $(A, +)$  est un groupe abélien (on notera son élément neutre  $0_A$  et l'inverse d'un élément  $a$ ,  $-a$ ).
- (ii) La loi  $\times$  est associative.
- (iii) La loi  $\times$  possède un élément neutre  $1_A$ .
- (iv) La loi  $\times$  est distributive par rapport à la loi  $+$  :

$$\forall (x, y, z) \in A^3, x \times (y + z) = x \times y + x \times z \text{ et } (y + z) \times x = y \times x + z \times x.$$

Si  $(A, \times)$  est commutatif, on dit que l'anneau est commutatif.

Dans un anneau  $A$ , on note, pour tout entier naturel  $n$ ,

$$na = \underbrace{a + a + \cdots + a}_{n \text{ fois}},$$

$$a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}}.$$

Pour  $n$  négatif, on note  $na = -(-n)a$ .

**Remarque 73**

Tout élément de  $A$  n'admet pas nécessairement d'inverse pour  $\times$ .

**Exemple 74**

- (i)  $(\mathbb{Z}, +, \times)$  est un anneau commutatif.
- (ii)  $(\mathbb{R}^{\mathbb{R}}, +, \times)$  est un anneau commutatif.
- (iii) Si  $E$  est un ensemble,  $(\mathcal{P}(E), \Delta, \cap)$  est un anneau commutatif. Le neutre pour  $\Delta$  est  $\emptyset$  et le neutre pour  $\cap$  est  $E$ .
- (iv) Si  $\mathcal{M}_n(\mathbb{R})$  est l'ensemble des matrices  $n \times n$ ,  $(\mathcal{M}_n(\mathbb{R}), +, \times)$  est un anneau non-commutatif.
- (v)  $(\mathbb{R}, +, \times)$ ,  $(\mathbb{Q}, +, \times)$  et  $(\mathbb{C}, +, \times)$  sont des anneaux commutatifs.

**Proposition 75 (Deux règles de calcul)**

Soit  $(A, +, \times)$  un anneau.

- (i)  $0_A$  est absorbant, c'est-à-dire que pour tout  $a$  de  $A$ ,  $0_A \times a = a \times 0_A = 0_A$ .

Soit  $(x, y) \in A^2$ ,  $n \in \mathbb{N}$ .

- (ii)  $n.(x \times y) = (n.x) \times y = x \times (n.y)$ .

- (iii)  $-(x \times y) = (-x) \times y = x \times (-y)$ .

En particulier,  $(-x) \times (-y) = x \times y$ , et  $(-1_A) \times (-1_A) = 1_A$ .

**Démonstration**

- (i) Soit  $x \in A$ . ALors

$$0_A \times x = (0_A + 0_A) \times x = 0_A \times x + 0_A \times x,$$

donc  $0_A \times x = 0_A$ . Idem pour  $x \times 0_A$ .

- (ii) (distributivité)

■

**Remarque 76**

$0_A$  et  $1_A$  sont-ils différents ?

OUI : si  $0_A = 1_A$ , alors pour tout  $x$  dans  $A$ ,

$$x = 1_A \times x = 0_A \times x = 0_A,$$

donc  $A = \{0_A\}$ . Donc un anneau qui a au moins deux éléments vérifie  $0_A \neq 1_A$ .

**Proposition 77**

Soit  $(A, +, \times)$  un anneau. Soient  $a$  et  $b$  dans  $A$ ,  $n \in \mathbb{N}$ .

- (i) Si  $a \times b = b \times a$ , alors  $(ab)^n = a^n b^n$ .

(ii) (binôme de Newton) Si  $a \times b = b \times a$ , alors

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

(iii) (identité de Bernoulli) Si  $a \times b = b \times a$ , alors

$$a^n - b^n = (a - b) \left( \sum_{k=0}^{n-1} a^k b^{n-1-k} \right)$$

### Démonstration

Toutes les preuves ont été déjà faites, dans ce chapitre ou dans le chapitre 2. ■

#### Définition 78

Soit  $(A, +, \times)$  un anneau, de neutre  $0_A$  pour  $+$ .

(i) On dit que  $A$  est intègre si

$$\forall (x, y) \in A^2, x \times y = 0_A \Rightarrow x = 0_A \text{ ou } y = 0_A.$$

(ii) Si  $A$  n'est pas intègre, deux éléments de  $A$   $x$  et  $y$  tels que  $x \neq 0_A$ ,  $y \neq 0_A$  et  $x \times y = 0_A$  sont appelés diviseurs de 0.

#### Exemple 79

(i)  $(\mathbb{Z}, +, \times)$  est intègre (de même pour  $\mathbb{R}$ ,  $\mathbb{Q}$  et  $\mathbb{C}$ ).

(ii)  $(\mathbb{R}^\mathbb{R}, +, \times)$  n'est pas intègre. En effet,  $1_{\mathbb{R}_+} \times 1_{\mathbb{R}_-} = 0_{\mathbb{R}^\mathbb{R}}$  mais aucune de ces deux fonctions n'est la fonction nulle.

(iii)  $(\mathcal{P}(E), \Delta, \cap)$  n'est pas intègre (prendre deux parties disjointes de  $E$ )

(iv)  $(\mathcal{M}_n(\mathbb{R}), +, \times)$  n'est pas intègre :  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ .

#### Proposition 80 (et définition)

Soit  $(A, +, \times)$  un anneau. On appelle ensemble des unités de  $A$  l'ensemble des éléments de  $A$  inversibles pour  $\times$ , et on le note  $U(A)$ .

$(U(A), \times)$  est un groupe, que l'on appelle groupe des inversibles de  $A$ .

### Démonstration

On admet que  $(U(A), \times)$  est un groupe. ■

**Remarque 81**

- (i) Si  $x \times y = 0_A$  et  $x \in U(A)$ ,  $y = x^{-1} \times 0_A = 0_A$ , donc  $y = 0_A$ . Ainsi, les diviseurs de zéro ne sont pas inversibles.
- (ii) On peut être intègre et avoir très peu d'éléments inversibles : cf.  $\mathbb{Z}$  par exemple !



**Exemple 82**

- (i) Dans  $(\mathbb{Z}, +, \times)$ , les unités sont  $\{-1, 1\}$ .
- (ii) Dans  $\mathbb{Q}/\mathbb{R}/\mathbb{C}$ , l'ensemble des éléments inversibles est  $\mathbb{Q}^* / \mathbb{R}^* / \mathbb{C}^*$ .
- (iii) Dans  $(\mathbb{R}^\mathbb{R}, +, \times)$ , l'ensemble des inversibles est l'ensemble des fonctions ne s'annulant jamais.
- (iv) Dans  $(\mathcal{P}(E), \Delta, \cap)$ , l'ensemble des inversibles est  $\{E\}$ .

**Définition 83**

Soit  $(A, +, \times)$  un anneau. Une partie  $B$  de  $A$  est un sous-anneau de  $A$  si

- (i)  $B$  est stable par  $\times$  et par  $+$
- (ii)  $(B, +, \times)$  est un anneau avec le même élément neutre que  $A$ .

Comme pour les sous-groupes, il est plus simple de vérifier les propriétés suivante.

**Proposition 84**

Une partie  $B$  d'un anneau  $(A, +, \times)$  est un sous-anneau de  $A$  si, et seulement si

- (i)  $1_A \in B$ ,
- (ii)  $\forall (x, y) \in B^2, x - y \in B$ ,
- (iii)  $\forall (x, y) \in B^2, x \times y \in B$ .

**Exemple 85**

- (i)  $\mathbb{Z}$  est un sous-anneau de  $\mathbb{Q}$  qui est un sous-anneau de  $\mathbb{R}$ , qui est un sous-anneau de  $(\mathbb{C}, +, \times)$ .
- (ii)  $\mathbb{Z}$  est le seul sous-anneau de  $\mathbb{Z}$ .

**Exercice 86**

TD 11, exercice 3.

**Définition 87**

Soient  $(A, +, \times)$  et  $(B, \oplus, \otimes)$  deux anneaux. Un morphisme d'anneaux entre  $A$  et  $B$  est une application  $\varphi : A \rightarrow B$  telle que

- (i)  $\varphi(1_A) = 1_B$ ,
- (ii)  $\forall (x, y) \in A^2, \varphi(x + y) = \varphi(x) \oplus \varphi(y)$ ,
- (iii)  $\forall (x, y) \in A^2, \varphi(x \times y) = \varphi(x) \times \varphi(y)$ .

On définit de même les notions d'endomorphisme, d'isomorphisme, d'automorphisme d'anneaux.

#### Remarque 88

- (i) En déduire que  $\forall (x, y) \in A^2, \varphi(x - y) = \varphi(x) \oplus (-\varphi(y))$ .
- (ii) Quels sont les endomorphismes d'anneaux de  $(\mathbb{Z}, +, \times)$  ?

#### Définition 89

Soit  $K$  un ensemble muni de deux lois de composition internes  $+$  et  $\times$ , de neutres respectifs  $0_K$  et  $1_K$ . On dit que  $(K, +, \times)$  est un corps si

- (i)  $(K, +, \times)$  est un anneau commutatif,
- (ii)  $\forall x \in K \setminus \{0_K\}$ ,  $x$  est inversible (pour  $\times$ )

#### Remarque 90

On note souvent  $K^* = K \setminus \{0_K\}$ .

#### Exemple 91

- (i)  $(\mathbb{Q}, +, \times)$  est un corps. C'est d'ailleurs le plus petit corps contenant  $\mathbb{Z}$  : on l'appelle corps des fractions de  $\mathbb{Z}$ .
- (ii)  $(\mathbb{R}, +, \times)$  et  $(\mathbb{C}, +, \times)$  sont des corps.

#### Exercice 92

Démontrer que tout anneau fini intègre est un corps.

#### Définition 93

Soit  $(K, +, \times)$  un corps,  $L \subset K$ . On dit que  $L$  est un sous-corps de  $K$  si

- (i)  $L$  est stable par  $+$  et  $\times$ ,
- (ii)  $(L, +, \times)$  est un corps.

#### Proposition 94

Soit  $(K, +, \times)$  un corps de neutre  $1_K$  pour  $\times$ . Soit  $L \subset K$ . Alors  $L$  est un sous-corps de  $K$  si et seulement si

- (i)  $1_K \in L$ ,
- (ii)  $\forall (x, y) \in L^2, x - y \in L$ ,
- (iii)  $\forall (x, y) \in L^2, x \times y \in L$ ,
- (iv)  $\forall x \in L \setminus \{0_K\}, x^{-1} \in L$ .

**Exemple 95**

$\mathbb{Q}$  est un sous corps de  $\mathbb{R}$  qui est un sous-corps de  $\mathbb{C}$ .

**Exercice 96**

- (i) Démontrer que  $\mathbb{Q}$  est le seul sous-corps de  $\mathbb{Q}$ .
- (ii) TD11, ex. 4.

**Définition 97**

Soient  $(\mathbb{K}, +, \times)$  et  $(\mathbb{L}, \oplus, \otimes)$  deux corps. Un morphisme de corps entre  $\mathbb{K}$  et  $\mathbb{L}$  est une application  $\varphi : \mathbb{K} \rightarrow \mathbb{L}$  telle que

- (i)  $\varphi(1_{\mathbb{K}}) = 1_{\mathbb{L}}$ ,
- (ii)  $\forall (x, y) \in \mathbb{K}^2, \varphi(x + y) = \varphi(x) \oplus \varphi(y)$ ,
- (iii)  $\forall (x, y) \in \mathbb{K}^2, \varphi(x \times y) = \varphi(x) \times \varphi(y)$ .

On définit de même les notions d'endomorphisme, d'isomorphisme, d'automorphisme de corps.

**Remarque 98**

- (i) Que vaut alors  $\varphi(x^{-1})$  ?
- (ii) (exo) Démontrer que tout morphisme de corps est injectif.

**Remarque 99**

Nous avons peu développé la théorie des anneaux et des corps :

- la théorie des anneaux trouve tout son intérêt lorsqu'on développe la théorie des **idéaux**. Cette théorie vous servira (en MP/MP\*) lorsque vous ferez de la réduction.
- la théorie des corps trouve toute sa saveur lorsque l'on s'intéresse aux **extensions de corps**, notamment aux parties  $L$  de  $\mathbb{R}$  telles que  $\mathbb{Q}$  est un sous-corps de  $L$ . Combinée à de l'algèbre linéaire, cette théorie permet de mieux comprendre les nombres dits algébriques.