

# Structures algébriques usuelles

## I Loi de composition interne

On se donne dans cette partie un ensemble non vide  $E$ .

### I.1 Définition, premiers exemples

**Définition.** Une loi de composition interne sur  $E$  est une application  $\varphi$  de  $E \times E$  dans  $E$ .

**Remarque :** En clair, une loi de composition interne (LCI pour les intimes) prend deux éléments de  $E$  et renvoie un élément de  $E$ .

**Notation :** Une loi de composition interne est ce qu'on a appelé jusqu'à présent une « opération ». Par conséquent, une LCI sera plutôt notée de façon opérationnelle plutôt que fonctionnelle. Par exemple, si  $(x, y) \in E^2$ , au lieu de noter  $\varphi(x, y)$  l'image de  $(x, y)$ , on préférera noter cette image  $x + y, x * y, x \top y, x \diamond y$  etc. selon les cas. Dans ce cas, on note la loi  $+, *, \top, \diamond$  etc. selon les cas. Lorsqu'on note la loi  $+$ , on dit que c'est une loi de composition interne lorsque :  $\forall (x, y) \in E^2, x + y \in E$ , et idem lorsqu'on note la loi différemment.

**Exemples :**

- L'addition est une loi interne sur  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$ , ainsi que sur  $\mathbb{R}_+^*$ , sur  $\mathbb{Q}_{+*}$  par exemple, mais pas sur  $\mathbb{R}^*$  car  $-1 + 1 \notin \mathbb{R}^*$ . Une loi est interne lorsqu'on ne peut pas sortir de l'ensemble !
- L'intersection, l'union et la différence symétrique sont des lois internes sur  $\mathcal{P}(E)$ .
- La composition est une loi interne sur  $E^E$ .
- La somme est une loi interne sur  $\mathbb{R}^{\mathbb{N}}$  et sur  $\mathbb{R}^{\mathbb{R}}$  (cf. chapitres 12 et 2).
- La différence est une loi interne sur  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$  mais pas sur  $\mathbb{N}$  ni sur  $\mathbb{R}_+^*$  par exemple.
- Le produit est une loi interne sur  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$ .
- Si  $n \geq 2$ , la somme et le produit sont des lois internes sur  $\mathbb{Z}/n\mathbb{Z}$ .
- Le quotient est une loi interne sur  $\mathbb{Q}^*$ , sur  $\mathbb{R}^*$ , sur  $\mathbb{C}^*$  mais pas sur  $\mathbb{Z}^*$  par exemple (et évidemment ce n'est pas une loi interne sur  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$  car on ne peut pas diviser par 0).
- La puissance (i.e. l'opération  $(a, b) \mapsto a^b$ ) est une loi interne sur  $\mathbb{N}$ .
- Le produit scalaire n'est pas une LCI sur  $\mathbb{R}^2$  ou sur  $\mathbb{R}^3$  puisque le produit scalaire de deux vecteurs du plan ou de l'espace est un réel (donc un élément d'un autre ensemble).
- Une relation d'ordre ou d'équivalence n'est pas une LCI car c'est une partie de  $E \times E$  (et non pas une fonction de  $E \times E$  dans  $E$ ).
- On définit une opération  $\diamond$  par :  $\forall (x, y) \in \mathbb{R}^2, x \diamond y = 0$ . C'est une LCI sur  $\mathbb{R}$  appelée loi interne nulle (mais ne sert pas à grand-chose).

Nous dirons dans le paragraphe I.4 que  $E$  est stable par  $+$ .

**Remarque :** Munir un ensemble d'une LCI (ou de lois externes, cf. chapitre 28) est la base de l'algèbre. Quand on a un ensemble avec des éléments, il est naturel de vouloir définir une opération avec ces éléments, on veut par exemple les sommer, les multiplier etc. C'est plus facile avec certains ensembles qu'avec d'autres : quand on a un ensemble avec des éléments quelconques, il n'est pas du tout évident de les faire interagir entre eux. Par exemple, que vaut la somme « moi + le pape » ? On peut parfois créer des lois « de toute pièces ». Par exemple, on peut munir l'ensemble {chou; banane; carotte} d'une loi  $+$  et d'une loi  $\times$  définies par les tables suivantes :

Une table permet de mieux visualiser une loi. Nous avons donné les tables de l'addition et du produit sur  $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$  et  $\mathbb{Z}/4\mathbb{Z}$  dans le chapitre 16.

+	chou	banane	carotte
chou	chou	banane	carotte
banane	banane	carotte	chou
carotte	carotte	chou	banane

$\times$	chou	banane	carotte
chou	chou	chou	chou
banane	chou	banane	carotte
carotte	chou	carotte	banane

Dans tout le chapitre, quand on donnera la table d'une loi  $*$ , l'élément se trouvant à l'intersection de la ligne  $x$  et de la colonne  $y$  sera  $x * y$ . Ce sera surtout utile quand les lois ne seront pas commutatives.

La question qu'on se pose ensuite est : quand on munit un ensemble de lois, ces lois sont-elles « intéressantes », i.e. vérifient-elles des propriétés qui les rendent « maniables » ? La loi interne nulle, par exemple, n'a aucun intérêt. Mais nous allons voir que la plupart des autres lois vues ci-dessus sont intéressantes (y compris la somme et le produit que l'on a définis sur l'ensemble {chou; banane; carotte} !).

## I.2 Propriétés des LCI

**Définition.** Une loi de composition interne  $*$  sur  $E$  est dite :

- commutative si :  $\forall (a, b) \in E^2, a * b = b * a$ .
- associative si :  $\forall (a, b, c) \in E^3, (a * b) * c = a * (b * c)$ .

**Exemples :**

- L'addition est une loi commutative et associative sur  $\mathbb{N}, \mathbb{Z}, \mathbb{Q} \dots$
- L'intersection, l'union et la différence symétrique sont commutatives et associatives sur  $\mathcal{P}(E)$ .
- La composition est associative sur  $E^E$ , c'est-à-dire que pour toutes fonctions  $f, g, h$  de  $E$  dans  $E$ ,  $f \circ (g \circ h) = (f \circ g) \circ h$ , mais n'est pas commutative en général : cf. chapitre 4.
- La somme est commutative et associative sur  $\mathbb{R}^{\mathbb{N}}$  et  $\mathbb{R}^{\mathbb{R}}$ . En effet, soient  $(u_n)_{n \in \mathbb{N}}, (v_n)_{n \in \mathbb{N}}$  et  $(w_n)_{n \in \mathbb{N}}$  trois suites réelles. Alors

$$\begin{aligned}
 ((u_n)_{n \in \mathbb{N}} + (v_n)_{n \in \mathbb{N}}) + (w_n)_{n \in \mathbb{N}} &= (u_n + v_n)_{n \in \mathbb{N}} + (w_n)_{n \in \mathbb{N}} \\
 &= (u_n + v_n + w_n)_{n \in \mathbb{N}} \\
 &= (u_n)_{n \in \mathbb{N}} + (v_n + w_n)_{n \in \mathbb{N}} \\
 &= (u_n)_{n \in \mathbb{N}} + ((v_n)_{n \in \mathbb{N}} + (w_n)_{n \in \mathbb{N}})
 \end{aligned}$$

Rappelons que si  $u$  et  $v$  sont deux suites réelles, alors  $u + v$  est la suite de terme général  $u_n + v_n$ . En d'autres termes :

$$\begin{aligned}
 (u_n)_{n \in \mathbb{N}} + (v_n)_{n \in \mathbb{N}} &= \\
 (u_n + v_n)_{n \in \mathbb{N}}
 \end{aligned}$$

On utilise sans le dire l'associativité de la somme sur  $\mathbb{R}$ .

Sur  $\mathbb{R}^{\mathbb{R}}$ , c'est la même chose : soient  $f, g, h$  trois fonctions de  $\mathbb{R}$  dans  $\mathbb{R}$ . Alors, pour tout réel  $x$  :

$$\begin{aligned}
 ((f + g) + h)(x) &= (f + g)(x) + h(x) \\
 &= f(x) + g(x) + h(x) \\
 &= f(x) + (g(x) + h(x)) \\
 &= f(x) + (g + h)(x) \\
 &= (f + (g + h))(x)
 \end{aligned}$$

Il en découle que  $(f + g) + h$  et  $f + (g + h)$  coïncident en tout réel  $x$  donc sont égales.

- La différence n'est ni commutative ni associative. Par exemple,  $1 - 2 \neq 2 - 1$  et  $1 - (2 - 3) \neq (1 - 2) - 3$ .
- Si  $n \geq 1$ , la somme et le produit sont des lois associatives et commutatives sur  $\mathbb{Z}/n\mathbb{Z}$  (cf. chapitre 16).

- Le quotient n'est ni commutatif ni associatif.
- Idem pour la puissance :  $a^{(b^c)} \neq (a^b)^c = a^{bc}$  en général.
- On vérifie que la somme et le produit sont des lois commutatives et associatives sur  $\{\text{chou}; \text{banane}; \text{carotte}\}$ . Pour la commutativité, c'est facile : il suffit de voir que les tableaux sont symétriques. Pour l'associativité, il faut le faire à la main... Par exemple,

$$\text{chou} \times (\text{banane} \times \text{carotte}) = \text{chou} \times \text{carotte} = \text{chou}$$

et on a de même  $(\text{chou} \times \text{banane}) \times \text{carotte} = \text{chou}$ .

### Remarques :

- Dire qu'une loi est associative, c'est dire que les parenthèses sont inutiles, c'est-à-dire qu'on peut faire les opérations dans l'ordre qu'on veut, à condition de respecter la position respective des éléments les uns par rapport aux autres. Par exemple, si la loi est associative et si  $(a, b, c, d) \in E^4$ , en posant  $A = a$ ,  $B = b$  et  $C = c * d$ , la propriété  $(A * B) * C = A * (B * C)$  se réécrit  $(a * b) * (c * d) = a * (b * (c * d))$ . On montre de même qu'on peut placer les parenthèses où l'on veut, et on généralise à un nombre quelconque (fini) de termes. En clair, pour une loi associative, on peut se passer de parenthèses. Cependant, lorsque la loi ne l'est pas (ce qui sera rare), il ne faut pas oublier les parenthèses, et idem lorsqu'il y a plusieurs lois sans qu'il y ait d'ordre de priorité entre elles, voir plus bas.
- Dire qu'une loi est commutative, c'est dire qu'on peut changer la position respective des éléments (mais pas faire les opérations dans l'ordre qu'on veut si la loi n'est pas associative). Par exemple, si la loi est commutative et si  $(a, b, c, d) \in E^4$ , alors  $(a * b) * (c * d) = (b * a) * (d * c)$ . De plus, si la loi est associative (ce qui sera le cas en pratique), cette quantité est égale à

$$a * b * c * d = a * c * b * d = c * a * b * d = \dots$$

Plus généralement, on peut permuter les éléments dans l'ordre qu'on veut, les  $4! = 24$  écritures possibles sont égales, et on généralise à un nombre quelconque (fini) de termes. En clair, pour une loi commutative (et associative, ce qui sera le cas en pratique), on se passe de parenthèses et on met les éléments dans l'ordre qu'on veut.

- Comme dit ci-dessus, la plupart des lois seront associatives, les lois non associatives étant très peu maniables. La plupart des lois que nous verrons dans ce chapitre seront associatives, et quand cela nous arrangera, nous n'aurons aucun scrupule à supposer que les lois sont associatives (nous le dirons à chaque fois).
- Sauf cas exceptionnels (par exemple dans certains exercices pour se faire la main), les lois seront notées de deux façons dans la suite : additivement (c'est-à-dire que la loi sera notée  $+$ ) ou multiplicativement ( $\times$  ou  $*$  ou sans rien, c'est-à-dire qu'on écrira  $ab$  le résultat de l'opération combinant  $a$  et  $b$  dans cet ordre). Les lois notées additivement sont forcément commutatives (on aura toujours  $a + b = b + a$ ), les lois notées multiplicativement le seront parfois mais pas toujours (on aura parfois  $ab = ba$  mais pas toujours). Par défaut, on notera une loi multiplicativement, on gardera la notation additive quand on voudra faire une analogie avec l'addition réelle.
- Pour une loi associative notée additivement, on définit la notation  $\sum_{i=1}^n a_i$  de la même façon que dans le chapitre 3, et on définit de même la notation  $\sum_{i \in I} x_i$  lorsque la loi est de plus commutative. De même pour le produit lorsqu'on a une loi notée multiplicativement.
- Soit  $n \geq 1$  et soit  $x \in E$ . Pour une loi associative notée additivement, on note  $nx$  l'élément  $\underbrace{x + \dots + x}_{n \text{ fois}}$ . Attention à ne pas le confondre avec  $n * x$  où  $*$  serait

Tant que le parenthésage reste admissible. Si la loi n'est pas associative, il y a a priori autant de résultats possibles que de façons d'ordonner les parenthèses, et on a vu dans le chapitre précédent qu'il y a  $C_n$  façons d'ordonner  $2n$  parenthèses, où  $C_n$  est le  $n$ -ième nombre de Catalan.

Rappelons qu'il y a  $n!$  permutations dans un ensemble à  $n$  éléments i.e.  $n!$  façons de classer  $n$  éléments.

une LCI notée multiplicativement puisque  $n$  n'est pas un élément de  $E$  ! Ce n'est qu'une notation ! Elle vérifie de plus les propriétés que l'on imagine (par exemple on a  $2x + 3x = 5x$  puisque  $(x + x) + (x + x + x) = x + x + x + x + x$  etc.).

- L'analogie pour une loi notée multiplicativement (associative) est la notation  $x^n$ , c'est-à-dire qu'on pose  $x^n = \underbrace{x \times \cdots \times x}_{n \text{ fois}}$  et cette notation vérifie également les propriétés habituelles des puissances (positives). Cette notation et la précédente décrivent en fait le même objet : l'itéré de  $x$   $n$  fois pour la loi considérée (notée additivement ou multiplicativement). Pour une loi notée différemment, la notation sera introduite par l'énoncé. On trouve par exemple parfois la notation  $f^n$  pour  $\underbrace{f \circ \cdots \circ f}_{n \text{ fois}}$ .

Lorsque l'ensemble est muni de deux lois, on peut se demander comment elles se comportent l'une par rapport à l'autre.

**Définition.** On suppose que  $E$  est muni de deux lois internes  $\star$  et  $\top$ .

- On dit que  $\star$  est distributive à gauche par rapport à  $\top$  si :

$$\forall (a, b, c) \in E^3, a \star (b \top c) = (a \star b) \top (a \star c)$$

- On dit que  $\star$  est distributive à droite par rapport à  $\top$  si :

$$\forall (a, b, c) \in E^3, (b \top c) \star a = (b \star a) \top (c \star a)$$

- On dit que  $\star$  est distributive à par rapport à  $\top$  si elle est distributive à gauche et à droite par rapport à  $\top$ .

Si les lois  $\top$  et  $\star$  sont commutatives, alors la loi  $\top$  est distributive par rapport à  $\star$  si et seulement si elle l'est à droite **ou** à gauche.

**Remarque :** On peut distribuer sur un plus grand nombre d'éléments lorsque la loi  $\top$  est associative (ce qui sera le cas en pratique). Par exemple, pour quatre éléments  $(a, b, c, d)$ ,

$$\begin{aligned} (a \top b \top c) \star d &= (a \top (b \top c)) \star d \\ &= (a \star d) \top ((b \top c) \star d) \\ &= (a \star d) \top ((b \star d) \top (c \star d)) \\ &= (a \star d) \top (b \star d) \top (c \star d) \end{aligned}$$

et on généralise à un nombre quelconque (fini) d'éléments. On peut également distribuer plusieurs éléments à gauche et à droite, par exemple  $(a \top b) \star (c \top d)$ , mais on ne le fera qu'avec des lois notées  $+$  et  $\times$ , et donc il suffit d'être à l'aise sur  $\mathbb{R}$  et le développement de sommes doubles.

**Exemples :**

- Le produit est distributif par rapport à la somme sur  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$ . La remarque ci-dessus devient, lorsqu'on distribue sur  $n$  éléments :

$$\left( \sum_{k=1}^n a_k \right) \times b = \sum_{k=1}^n (a_k \times b)$$

On peut l'écrire avec des flèches si on veut le visualiser. De façon générale, le produit et la somme sont l'archétype d'une loi distributive par rapport à l'autre. Comme dit dans le chapitre 4, on peut parfois écrire au brouillon l'analogie avec les lois  $+$  et  $\times$ , développer puis repasser au propre en reprenant les bonnes lois.

- Sur  $\mathcal{P}(E)$ , l'union et l'intersection sont distributives l'une par rapport à l'autre. La remarque ci-dessus devient donc, lorsqu'on distribue sur  $n$  éléments :

$$\left( \bigcup_{k=1}^n A_k \right) \cap B = \bigcup_{k=1}^n (A_k \cap B) \quad \text{et} \quad \left( \bigcap_{k=1}^n A_k \right) \cup B = \bigcap_{k=1}^n (A_k \cup B)$$

Note pour plus tard : c'est aussi le cas sur  $\mathcal{M}_n(\mathbb{K})$ .

### I.3 Éléments particuliers

On suppose que  $E$  est muni d'une loi interne  $*$ .

**Définition.** Soit  $e \in E$ .

- On dit que  $e$  est un élément neutre à gauche si :  $\forall x \in E, e * x = x$ .
- On dit que  $e$  est un élément neutre à droite si :  $\forall x \in E, x * e = x$ .
- On dit que  $e$  est un élément neutre si  $e$  est un élément neutre à droite et à gauche i.e. :  $\forall x \in E, e * x = x * e = x$ .

**Remarque :** Lorsque la loi  $*$  est commutative, un élément est un élément neutre si et seulement s'il est neutre à gauche ou à droite. Cependant, si la loi  $*$  n'est pas commutative, alors ce n'est pas forcément le cas. Par exemple, pour la loi puissance, i.e.  $a * b = a^b$  sur  $\mathbb{N}$ , 1 est un neutre à droite car pour tout  $a$ ,  $a^1 = a$ , mais 1 n'est pas un élément neutre à gauche donc n'est pas un élément neutre. De plus, si on considère la loi  $*$  définie sur  $\mathbb{R}$  par  $x * y = x$  alors tout réel  $y$  est neutre à droite, mais il n'y a pas de neutre à gauche.

Ces cas de figure sont donnés à titre culturel mais nous ne les rencontrerons pas en pratique. Il faut cependant savoir qu'il ne peut pas y avoir plusieurs éléments neutres :

**Proposition.** Si  $*$  admet un neutre à droite  $e_1$  et un neutre à gauche  $e_2$ , alors  $e_1 = e_2$ . En particulier, si  $*$  admet un élément neutre, celui-ci est unique.

**DÉMONSTRATION.** Par hypothèse, pour tout  $x \in E$ ,  $x * e_1 = x$ . En particulier, si  $x = e_2$ , alors  $e_2 * e_1 = e_1$ . De plus, pour tout  $x \in E$ ,  $e_2 * x = x$ . En particulier, si  $x = e_1$ , alors  $e_2 * e_1 = e_1$  si bien que  $e_1 = e_2$ .

**Exemples :**

- 0 est l'élément neutre pour l'addition sur  $\mathbb{N}, \mathbb{Z}$  etc. De façon générale, lorsqu'on notera une loi additivement, l'élément neutre sera noté  $0_E$  ou 0 si aucune confusion n'est possible : cf. paragraphe II.1.
- 1 est l'élément neutre du produit sur  $\mathbb{N}, \mathbb{Z}$  etc. De même, lorsqu'une loi sera notée multiplicativement, nous noterons parfois le neutre  $1_E$  ou 1 (mais nous utiliserons également souvent la notation  $e$ ).
- La fonction  $\text{Id}_E$  est l'élément neutre pour la composition sur  $E^E$ .
- La suite nulle est l'élément neutre pour la somme sur  $\mathbb{R}^{\mathbb{N}}$  et la fonction nulle est l'élément neutre pour la somme sur  $\mathbb{R}^{\mathbb{R}}$ .
- Si  $n \geq 2$ , alors  $\bar{0}$  est l'élément neutre pour la somme et  $\bar{1}$  est l'élément neutre pour le produit sur  $\mathbb{Z}/n\mathbb{Z}$ .
- On remarque que le chou est l'élément neutre pour l'addition sur  $\{\text{chou}; \text{banane}; \text{carotte}\}$  et que la banane est l'élément neutre pour le produit...
- $2\mathbb{N}$ , muni de la multiplication, n'admet pas d'élément neutre. En effet, il n'existe pas d'élément  $e \in 2\mathbb{N}$  tel que  $2e = 2$ .

**Définition.** On suppose que  $E$  admet un élément neutre  $e$  (pour la loi  $*$ ). Soit  $x \in E$ .

- On dit que  $x$  admet un symétrique à gauche s'il existe  $y \in E$  tel que  $y * x = e$ .
- On dit que  $x$  admet un symétrique à droite s'il existe  $y \in E$  tel que  $x * y = e$ .
- On dit que  $x$  admet un symétrique si  $x$  admet un symétrique à gauche et à droite i.e. s'il existe  $y \in E$  tel que  $x * y = y * x = e$ .

La loi est donc notée multiplicativement, mais on aurait pu la noter additivement ou même de façon quelconque ( $T, \diamond$  etc.).

On pourra donc parler de l'élément neutre (à la place d'un élément neutre), s'il existe évidemment.

S'il n'y a pas d'élément neutre, cela n'a pas de sens de parler d'élément symétrisable. Ainsi, quand on parlera de symétrique, il sera sous-entendu qu'il existe un élément neutre.

**Remarque :** Rappelons que  $\text{Id}_E$  est le neutre sur  $E^E$  muni de la composition. D'après l'exercice 42 du chapitre 4, une fonction  $f : E \rightarrow E$  admet un symétrique à droite si et seulement si  $f$  est surjective, et  $f$  admet un symétrique à gauche si et seulement si  $f$  est injective. Une injection non surjective admet plusieurs symétriques à gauche et une surjection non injective admet plusieurs symétriques à droite.

cf. exercice 9 pour un exemple.

Là aussi, ce genre de cas pathologique est marginal. Cependant, il faut connaître le résultat suivant :

**Proposition.** On suppose que la loi  $*$  est associative. Soit  $x \in E$ . Si  $x$  admet un symétrique à droite  $y_1$  et un symétrique à gauche  $y_2$  alors  $y_1 = y_2$ . En particulier, si  $x$  admet un symétrique, celui-ci est unique.

On fait donc l'hypothèse que  $E$  admet un élément neutre pour la loi  $*$ .

DÉMONSTRATION. D'une part,

$$\begin{aligned} y_2 * (x * y_1) &= y_2 * e \\ &= y_2 \end{aligned}$$

et d'autre part, la loi étant associative,

$$\begin{aligned} y_2 * (x * y_1) &= (y_2 * x) * y_1 \\ &= e * y_1 \\ &= y_1 \end{aligned}$$

□

D'où le résultat.

**Exemples :**

- Sur  $\mathbb{N}$  muni de la somme, seul 0 admet un symétrique : lui-même.
- Sur  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$  munis de la somme, tout élément  $x$  admet un symétrique :  $-x$ . De façon générale, quand la loi est notée additivement, le symétrique de  $x$  est noté  $-x$  et appelé l'opposé de  $x$ .
- Sur  $\mathbb{N}$  muni de la multiplication, seul 1 admet un symétrique : lui-même. Sur  $\mathbb{Z}$  muni de la multiplication, seuls 1 et  $-1$  admettent un symétrique (respectivement 1 et  $-1$ ).
- Sur  $\mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$ , 0 n'admet pas de symétrique (nous généraliserons ce résultat dans le paragraphe V) mais tout élément  $x$  non nul admet un symétrique :  $1/x$ , que l'on note aussi  $x^{-1}$ . De façon générale, quand la loi est notée multiplicativement, le symétrique de  $x$  est noté  $x^{-1}$  et appelé l'inverse de  $x$ .
- Par exemple, sur  $E^E$ , une fonction est symétrisable si et seulement si elle est bijective, et son symétrique est noté  $f^{-1}$  : c'est la bijection réciproque de  $f$ . Bref, dans le doute, sauf quand la loi sera notée additivement, le symétrique d'un élément  $x$  sera toujours noté  $x^{-1}$  et on l'appellera également l'inverse de  $x$ , et on dit aussi que  $x$  est inversible pour dire qu'il est symétrisable.

⚠ Ainsi, si  $x$  admet un symétrique,  $x$  et  $x^{-1}$  peuvent être égaux !

**Proposition.** Si  $x$  admet est inversible (ou symétrisable), alors  $x^{-1}$  l'est aussi, et  $(x^{-1})^{-1} = x$ .

DÉMONSTRATION. Il suffit de voir que  $x^{-1} * x = x * x^{-1} = e$ .

**Proposition.** On suppose que la loi  $*$  est associative. Si  $x$  et  $y$  sont deux éléments inversibles (ou symétrisables), alors  $x * y$  est symétrisable et  $(x * y)^{-1} = y^{-1} * x^{-1}$ .

DÉMONSTRATION. Il suffit de vérifier que  $(x * y) * (y^{-1} * x^{-1}) = (y^{-1} * x^{-1}) * (x * y) = e$ , ce qui découle directement de l'associativité de la loi.

**Remarque :** En d'autres termes, le produit (quand on note la loi multiplicativement, ce qui sera le cas la plupart du temps) de deux éléments inversibles est inversible. Attention, on change l'ordre quand on inverse ! Voir l'analogie avec le trésor dans le chapitre 4.

**Remarque :** Dans le cas où l'ensemble admet un neutre et où un élément est inversible, on peut généraliser la notion de puissance.

**Définition.** On suppose que  $E$  admet un élément neutre  $e$  (pour la loi  $*$ ). Si  $x \in E$ , on pose  $x^0 = e$ . De plus, si  $x$  est symétrisable, on pose, pour tout  $n \in \mathbb{Z}$ ,  $n < 0$ ,  $x^n = (x^{-1})^{-n}$ .

Par exemple, on pose  $x^{-2} = (x^{-1})^2$ .

**Remarques :**

- Ces notations n'ont de sens que lorsque  $E$  admet un élément neutre ou lorsque  $x$  admet un symétrique. Lorsque c'est le cas, les puissances (positives ou négatives) vérifient les mêmes propriétés que sur  $\mathbb{R}$  (mais on fera attention à ne jamais écrire  $1/x$  même lorsque  $x$  est symétrisable).
- De plus, nous avons pris par défaut une loi notée multiplicativement, mais on définit un objet analogue pour les lois notées additivement : s'il y a un neutre (noté  $0_E$ ), alors on pose  $0x = 0_E$  et, si  $n < 0$ , on pose  $nx = (-n)(-x) = \underbrace{-x - \dots - x}_{-n \text{ fois}}$ . Par exemple,  $-2x = -x - x$ . Là aussi, cette notation vérifie les propriétés attendues.

**Remarque :** On peut encore définir d'autres types d'éléments :

- les éléments idempotents i.e. qui vérifient  $x * x = x$ .
- les éléments nilpotents, cf. paragraphe V.2.c.
- les éléments réguliers, cf. paragraphe II.2.

Certains sont relativement classiques et nous les reverrons en temps utile. Les autres seront introduits si besoin dans les exercices.

## I.4 Et sur un ensemble plus petit ?

On se donne dans cette partie un ensemble  $E$  muni d'une loi interne  $*$ .

**Définition.** Soit  $F$  une partie non vide de  $E$ . On dit que  $F$  est stable par  $*$  si :  $\forall (x, y) \in F^2, x * y \in F$ .

**Exemples :**

- $\mathbb{R}_+^*$  est une partie de  $\mathbb{R}$  stable par produit.
- $\mathbb{U}$  est une partie de  $\mathbb{C}$  stable par produit.

**Remarque :** Une loi interne est notée sous forme opérationnelle la plupart du temps, mais il ne faut pas oublier la définition, c'est-à-dire qu'une LCI est une application  $\varphi : E^2 \rightarrow E$ . Par conséquent, dire qu'une partie  $F$  de  $E$  est stable par une LCI, c'est dire que la restriction de  $\varphi$  à  $F^2$  est à valeurs dans  $F$ , ou que  $\varphi$  induit une application de  $F^2$  dans  $F$ , cf. chapitre 4. Par conséquent, lorsqu'une partie  $F$  est stable par une LCI  $*$ , on dit que  $*$  induit une loi interne sur  $F$ , et que la loi  $*$  sur  $F$  est la restriction de la loi  $*$  (sur  $E$ ) à  $F$ , ou encore la loi induite par  $*$  sur  $F$ . On la note parfois  $*_F$ , mais en général il n'y a aucune ambiguïté car on sait à quel ensemble appartiennent les éléments que l'on manie.

Ainsi, on trouve parfois les formulations suivantes : montrer que la loi  $*$  induit une loi interne sur  $F$ , ou montrer que la restriction de  $*$  à  $F$  est interne à  $F$ . On demande en fait de prouver que  $F$  est stable par  $*$ , et on peut ensuite considérer  $*$  comme une loi interne comme les autres (sur  $F$ ). Question : quelles propriétés vraies sur  $E$  sont encore vraies sur  $F$  ?

En gros, les propriétés universelles (avec uniquement des  $\forall$ ) sont toujours vraies, et les propriétés existentielles (avec au moins un  $\exists$ ) ne le sont pas forcément. Si on a un doute, on prend les exemples suivants :



- « Tous les Européens peuvent voyager en Europe donc tous les Français peuvent voyager en Europe ». Une chose vraie pour tous les éléments de  $E$  reste vraie pour tous les éléments de  $F$ . Ce serait encore vrai pour deux, trois etc. éléments de  $E$ .
- « Si tous les hommes européens sont mariés à une femme européenne, il n'est pas forcément vrai qu'un homme français est marié à une femme française ». Il y a bien un  $\forall$  mais aussi un  $\exists$  : « pour tous les hommes, il existe une femme etc. » La différence ici est qu'on prend une propriété vraie pour tous les éléments de  $E$  mais elle fait intervenir un autre élément de  $E$  avec un quantificateur existentiel : si le premier appartient à  $F$ , ce n'est pas forcément le cas pour l'autre. Bien retenir ces deux exemples permettra de savoir ce qui est automatique et ce qui ne l'est pas.

### Exemples :

- Si une loi est associative sur  $E$ , alors elle est associative sur  $F$  (si  $F$  est stable par  $*$ ) : en effet, pour tout  $(a, b, c) \in F^3$ ,  $a * (b * c) = (a * b) * c$  car c'est vrai sur  $E$  donc sur  $F$ .
- De même pour commutative.
- Cependant, si un élément admet un symétrique sur  $E$ , ce n'est pas forcément le cas sur  $F$ . En effet, si  $x \in F$ , alors  $x$  admet un symétrique  $y \in E$  mais il n'y a aucune raison que  $y$  appartienne à  $F$ .
- De même, si une loi admet un neutre sur  $E$ , il n'y a aucune raison que le neutre appartienne à  $F$ . Par exemple,  $]0; 1[$  est stable par produit mais le neutre n'appartient pas à  $]0; 1[$ , et l'inverse de tout élément n'appartient pas non plus à  $]0; 1[$ .

## II Groupes

Nous donnerons parfois dans cette partie et les suivantes des résultats au programme de deuxième année ou tout simplement hors programme mais classiques et/ou permettant de s'entraîner avec les outils au programme, ou permettant de mieux visualiser et comprendre certaines notions. Tous ces résultats seront clairement signalés mais les connaître et les revoir vous fera vraiment progresser.

### II.1 Définition et premiers exemples

**Définition.** Un groupe est un ensemble muni d'une loi de composition interne associative, admettant un élément neutre et telle que tout élément admette un symétrique. Si la loi est de plus commutative, le groupe est dit commutatif ou abélien.

#### Remarques :

- Un groupe consiste en un ensemble **et** en une loi. Quand on parle d'un groupe, il faut préciser la loi sinon cela n'a pas de sens. Si l'ensemble est noté  $G$  et la loi  $*$ , on dit que  $(G, *)$  est un groupe ou que  $G$  est un groupe muni de la loi  $*$ . Cependant, parfois, on pourra ne pas expliciter la loi, soit parce qu'on a affaire à un groupe usuel, soit parce que la loi est par défaut notée multiplicativement (voir ci-dessous).
- En poussant un peu, on pourrait même dire que la loi est plus importante que l'ensemble : nous identifierons parfois deux groupes alors que les ensembles sont différents mais les lois « identiques », cf. paragraphe IV.4.a. Cependant, attention : quand on parle de la loi et quand on dit que les lois sont « identiques », on s'intéresse à la façon dont les éléments interagissent entre eux, on s'intéresse à la table de la loi (quand le groupe est fini). Ce n'est pas parce qu'on note deux lois multiplicativement qu'elles sont « identiques ».
- Un groupe additif est un groupe dont la loi est notée additivement et est donc appelée addition. C'est un groupe toujours abélien. L'élément neutre est alors parfois noté  $0_G$  ou  $0$  s'il n'y a aucune ambiguïté.



- Un groupe multiplicatif est un groupe dont la loi est notée multiplicativement et est donc appelée multiplication. C'est un groupe qui est parfois abélien, parfois non. L'élément neutre est alors parfois noté  $1_G$  ou  $1$  s'il n'y a aucune ambiguïté, mais il sera le plus souvent noté  $e$  quand même.
- Par défaut, la loi d'un groupe est notée multiplicativement :  $*$ ,  $\times$  ou rien (i.e. la loi de  $G$  ne sera pas explicitée et on notera souvent  $ab$  le résultat de l'opération combinant  $a$  et  $b$  dans cet ordre). Parfois, on dira « soit  $G$  un groupe », au lieu de dire « soit  $(G, *)$  un groupe », la loi ne sera pas précisée, il sera sous-entendu que la loi est notée multiplicativement.
- Nous noterons donc parfois de la même façon un produit  $h_1 h_2$  dans un groupe  $H$  et un produit  $k_1 k_2$  dans un groupe  $K$ , mais il faudra être conscient du fait que, pour le premier, on utilise la loi de  $H$  et, pour le deuxième, la loi de  $K$ . On pourra se permettre ce raccourci puisqu'en général, il n'y a aucune ambiguïté sur l'ensemble dans lequel on travaille, et qu'il serait fastidieux d'écrire  $h_1 *_H h_2$  et  $k_1 *_K k_2$  (même s'il nous arrivera de le faire, par exemple dans le paragraphe II.3).
- La loi d'un groupe étant associative, les notations  $x^n$  (dans un groupe multiplicatif) et  $nx$  (dans un groupe additif) ont un sens, même pour  $n < 0$  puisqu'un groupe admet un neutre et que tout élément admet un symétrique.

### Exemples :

- $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$  et  $(\mathbb{C}, +)$  sont des groupes. Cependant,  $(\mathbb{N}, +)$  n'en est pas un car les éléments non nuls n'ont pas de symétrique.
- $(\mathbb{Q}^*, +)$ ,  $(\mathbb{R}^*, +)$  et  $(\mathbb{C}^*, +)$  sont des groupes. Cependant,  $(\mathbb{Q}, \times)$ ,  $(\mathbb{R}, \times)$  et  $(\mathbb{C}, \times)$  ne sont pas des groupes car  $0$  n'a pas de symétrique pour la loi  $\times$ . De même,  $(\mathbb{Z}, \times)$  n'est pas un groupe car les entiers différents de  $\pm 1$  n'ont pas de symétrique pour la loi  $\times$ . Ainsi, quand on parlera du groupe  $\mathbb{Z}$ , du groupe  $\mathbb{R}$  etc. il sera sous-entendu qu'on les munit de la loi  $+$ , et quand on parlera de  $\mathbb{R}^*$  etc. il sera sous-entendu qu'on les munit de la loi  $\times$ .
- $\mathbb{Q}_+^*$  et  $\mathbb{R}_+^*$  sont des groupes pour la loi  $\times$ , mais  $\mathbb{Q}_-^*$  et  $\mathbb{R}_-^*$  ne sont pas des groupes car la loi n'est pas interne et car il n'y a pas de neutre (mais la loi est associative et tout élément admet un symétrique).
- Si  $E$  est un ensemble non vide, alors  $\mathcal{P}(E)$  et  $\mathcal{P}_f(E)$  (l'ensemble des parties finies de  $E$ ) sont des groupes, munis de la différence symétrique, cf. exercice 47.
- $(\mathbb{U}, \times)$  est un groupe. En effet, le produit de deux nombres de module 1 est encore de module 1 donc la loi est interne. La multiplication étant associative sur  $\mathbb{C}$ , elle l'est sur  $\mathbb{U}$ . De plus,  $1 \in \mathbb{U}$  : il y a bien un élément neutre. Enfin, si  $z \in \mathbb{U}$ , alors  $1/z \in \mathbb{U}$  : tout élément admet un symétrique/inverse appartenant à l'ensemble.
- L'ensemble à deux éléments  $\{-1; 1\}$  est un groupe muni du produit. Plus généralement, si  $n \geq 1$ , alors  $\mathbb{U}_n$ , l'ensemble des racines  $n$ -ièmes de l'unité, est un groupe pour la multiplication. En effet, si  $z_1$  et  $z_2$  sont deux éléments de  $\mathbb{U}_n$ , alors  $z_1^n = z_2^n = 1$  donc  $(z_1 z_2)^n = z_1^n z_2^n = 1$  c'est-à-dire que  $z_1 z_2 \in \mathbb{U}_n$  : la multiplication est bien interne sur  $\mathbb{U}_n$ . Elle est de plus associative car elle est associative sur  $\mathbb{C}$ . De plus,  $1 \in \mathbb{C}$  : il y a bien un élément neutre. De plus, si  $z_1 \in \mathbb{U}_n$ , alors  $z_1^n = 1$  donc  $z_1 \neq 0$  et  $(1/z_1)^n = 1/z_1^n = 1$  c'est-à-dire que  $1/z_1 \in \mathbb{U}_n$  : tout élément admet bien un inverse appartenant à  $\mathbb{U}_n$ .

Pour tout  $n \geq 1$ ,  $\mathbb{U}_n$  est donc un groupe à  $n$  éléments. Il existe donc des groupes de tout cardinal : ce ne sera pas le cas pour les corps, cf. exercice 56 du chapitre 30.

**Remarque :** On aurait aussi pu le montrer en utilisant la définition équivalente  $\mathbb{U}_n = \{e^{2ik\pi/n} \mid k \in \mathbb{Z}\}$  (exo). C'est un peu plus difficile avec la définition  $\mathbb{U}_n = \{e^{2ik\pi/n} \mid k \in \llbracket 0; n-1 \rrbracket\}$  car, si  $k_1$  et  $k_2$  appartiennent à  $\llbracket 0; n-1 \rrbracket$ , ce n'est pas forcément le cas de leur somme ni de  $-k_1$ , il faut alors trouver un « autre représentant », exo.

**Exemple :** Si  $\theta_1$  et  $\theta_2$  appartiennent à  $[0; 2\pi[$ , on note  $\theta_1 \oplus \theta_2$  l'unique élément de  $[0; 2\pi[$  congru à  $\theta_1 + \theta_2$  modulo  $2\pi$ . Montrons que  $([0; 2\pi[, \oplus)$  est un groupe, c'est-à-dire que  $[0; 2\pi[$  est un groupe pour la somme modulo  $2\pi$ .

On sait que tout intervalle semi-ouvert de longueur  $2\pi$  contient un et un seul élément congru à  $\theta_1 + \theta_2$  modulo  $2\pi$ , cf. chapitre 5.

La loi  $\oplus$  est bien interne (c'est pour cela qu'il faut travailler modulo  $2\pi$  car la somme tout court n'est pas interne!). Soit  $(\theta_1, \theta_2, \theta_3) \in [0; 2\pi[^3$ . Par définition,  $\theta_1 \oplus \theta_2 \equiv \theta_1 + \theta_2 [2\pi]$  donc :

$$\begin{aligned}(\theta_1 \oplus \theta_2) \oplus \theta_3 &\equiv (\theta_1 \oplus \theta_2) + \theta_3 [2\pi] \\ &\equiv (\theta_1 + \theta_2) + \theta_3 [2\pi] \\ &\equiv \theta_1 + (\theta_2 + \theta_3) [2\pi] \\ &\equiv \theta_1 \oplus (\theta_2 \oplus \theta_3) [2\pi]\end{aligned}$$

Car la somme est associative sur  $\mathbb{R}$ .

Or, deux éléments de  $[0; 2\pi[$  congrus l'un à l'autre sont égaux i.e.  $(\theta_1 \oplus \theta_2) \oplus \theta_3 = \theta_1 \oplus (\theta_2 \oplus \theta_3)$  : la loi  $\oplus$  est associative. 0 est évidemment un élément neutre. Enfin, 0 est son propre symétrique/opposé, et si  $\theta \in ]0; 2\pi[$ , alors  $2\pi - \theta$  est l'opposé de  $\theta$  car  $\theta + 2\pi - \theta = 2\pi$  donc  $\theta \oplus (2\pi - \theta) = 0$ . En conclusion,  $([0; 2\pi[, \oplus)$  est bien un groupe.

On parle d'opposé ici car on note la loi additive.

**Rappel (deuxième année) :** Soit  $n \geq 2$ . On note  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble des classes d'équivalence de la congruence modulo  $n$  sur  $\mathbb{Z}$ . Si  $x \in \mathbb{Z}$ , on note  $\bar{x}$  la classe d'équivalence de  $x$ , c'est-à-dire  $\bar{x} = x + n\mathbb{Z}$ . On a alors  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\}$ . De plus, on travaille modulo  $n$ , c'est-à-dire que (par exemple)  $\bar{1} = \overline{n+1}$  et, si  $x \in \mathbb{Z}$ ,  $\overline{-x} = \overline{n-x}$  : l'égalité sur  $\mathbb{Z}/n\mathbb{Z}$  est équivalente à la congruence modulo  $n$  sur  $\mathbb{Z}$ .

$\mathbb{Z}/n\mathbb{Z}$  est muni d'une addition et d'une multiplication définies par :

$$\forall (\bar{x}, \bar{y}) \in (\mathbb{Z}/n\mathbb{Z})^2, \quad \bar{x} + \bar{y} = \overline{x+y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{x \times y}$$

Ci-dessous les tables de l'addition de  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$  et  $\mathbb{Z}/4\mathbb{Z}$  :

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\mathbb{Z}/2\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}/4\mathbb{Z}$

Montrons que  $\mathbb{Z}/n\mathbb{Z}$  est un groupe pour la loi  $+$ . On a vu au chapitre 16 que la loi  $+$  est associative et que  $\bar{0}$  est l'élément neutre. De plus, pour tout  $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ ,  $\bar{x} + \overline{-x} = \bar{0}$  : tout élément admet un opposé. Nous reverrons la représentation cyclique de  $\mathbb{Z}/n\mathbb{Z}$  dans les paragraphes IV.4.c. Cependant,  $\mathbb{Z}/n\mathbb{Z}$  n'est pas un groupe pour la loi  $\times$  car (entre autres)  $\bar{0}$  n'a pas d'inverse : en effet, pour tout  $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ ,  $\bar{0} \times \bar{x} = \bar{0} \neq \bar{1}$  car  $1 \not\equiv 0[n]$ . Attention, il ne suffit pas de dire que  $0 \neq 1$  : par exemple, dans  $\mathbb{Z}/3\mathbb{Z}$ , alors  $\bar{2}$  est inversible car  $\bar{2} \times \bar{2} = \bar{1}$  : ne pas oublier que dans  $\mathbb{Z}/n\mathbb{Z}$ , on travaille modulo  $n$ , et donc les notions de parité n'ont plus tellement de sens. Par exemple, toujours dans  $\mathbb{Z}/3\mathbb{Z}$ ,  $\bar{4} = \bar{1}$ . Nous reparlerons plus en détail de la multiplication dans  $\mathbb{Z}/n\mathbb{Z}$  dans le paragraphe VI.4.

On a donc  $\overline{-x} = \overline{n-x}$  : on parle d'opposé car on note la loi additivement.

**Remarque :** Tous les groupes ci-dessus sont commutatifs, mais on trouve parfois des groupes non commutatifs dans des situations très simples.

#### Définition.

- Si  $E$  est un ensemble non vide, on note  $S_E$  l'ensemble des bijections de  $E$ . On l'appelle aussi l'ensemble des permutations de  $E$ .
- Si  $n \geq 1$ , l'ensemble  $S_{[1; n]}$  des permutations de  $[1; n]$  est noté plus simplement  $S_n$  : on l'appelle le groupe symétrique d'ordre  $n$ .

En particulier,  $S_n$  a  $n!$  éléments. Nous l'étudions plus en détail au chapitre 32.

En effet :

**Proposition.** Si  $E$  est un ensemble non vide,  $S_E$  est un groupe pour la composition. De plus, il est non abélien dès que  $E$  a au moins trois éléments.

DÉMONSTRATION. On sait déjà que la composition est une loi associative et admet comme élément neutre  $\text{Id}_E$  qui est bien bijective donc qui appartient à  $S_E$ . De plus, si  $f \in S_E$ , alors  $f$  est bijective donc  $f$  admet une bijection réciproque  $f^{-1}$  et  $f \circ f^{-1} = f^{-1} \circ f = \text{Id}_E$  donc tout élément de  $S_E$  est inversible :  $(S_E, \circ)$  est bien un groupe.

Supposons que  $E$  admette au moins trois éléments distincts  $i, j, k$ . Notons  $f$  et  $g$  les fonctions de  $E$  dans  $E$  suivantes :

$$f : x \mapsto \begin{cases} x & \text{si } x \neq i, j \\ j & \text{si } x = i \\ i & \text{si } x = j \end{cases} \quad \text{et} \quad g : x \mapsto \begin{cases} x & \text{si } x \neq j, k \\ k & \text{si } x = j \\ j & \text{si } x = k \end{cases}$$

Il est immédiat que  $f$  et  $g$  sont des bijections de  $E$  (soit on le montre à la main, soit on remarque que ce sont des involutions). De plus,

$$\begin{aligned} f \circ g(i) &= f(g(i)) \\ &= f(j) \\ &= i \end{aligned}$$

tandis que

$$\begin{aligned} g \circ f(i) &= g(f(i)) \\ &= g(j) \\ &= k \end{aligned}$$

□

et donc on a  $g \circ f \neq f \circ g$  :  $S_E$  n'est pas abélien.

## II.2 Propriétés

**Proposition.** Un groupe est non vide. De plus, l'élément neutre est unique, ainsi que le symétrique de chaque élément.

DÉMONSTRATION. Un groupe est non vide car contient un élément neutre. L'unicité du neutre et du symétrique de chaque élément découlent du paragraphe I.3.

**Proposition.** Dans un groupe, tout élément est régulier (à gauche et à droite), c'est-à-dire que si  $(G, *)$  est un groupe :

$$\forall (a, b, c) \in G^3, ab = ac \Rightarrow b = c$$

et idem à droite :

$$\forall (a, b, c) \in G^3, ba = ca \Rightarrow b = c$$

DÉMONSTRATION. Soit  $(a, b, c) \in G^3$ . Supposons que  $ab = ac$ . En multipliant par  $a^{-1}$  à gauche,  $a^{-1}(ab) = a^{-1}(ac)$  et la loi est associative donc  $(a^{-1}a)b = (a^{-1}a)c$ . Ainsi,  $e * b = e * c$  donc  $b = c$  car  $e$  est l'élément neutre. De même à droite.

**Remarque :** On dit aussi que tout élément est simplifiable. Mais attention, on ne peut pas simplifier n'importe comment ! On ne peut pas « barrer sauvagement », il faut le faire proprement, i.e. multiplier par  $a^{-1}$  à gauche ou à droite selon les cas. Si on a  $ab = ca$ , alors on ne peut pas simplifier par  $a$ , on n'a pas forcément  $b = c$  ! On a simplement  $aba^{-1} = c$ , on dit alors que les éléments  $b$  et  $c$  sont conjugués.

On peut même montrer que  $S_3$  est le plus petit groupe non abélien, c'est-à-dire que tous les groupes admettant strictement moins de 6 éléments sont abéliens, et en particulier  $S_2$  est abélien, cf. paragraphe IV.

Rappelons que pour montrer que deux fonctions sont distinctes, il suffit d'exhiber **un** élément  $x$  dont les images sont distinctes.

Comme dit plus haut, on omet parfois la loi i.e. on écrit  $ab$  à la place de  $a * b$ .

## II.3 Groupe produit

**Proposition/Définition.** Soient  $(G_1, *_1)$  et  $(G_2, *_2)$  deux groupes. On définit une loi interne  $*$  sur  $G_1 \times G_2$  par :

$$\forall ((g_1, g_2), (h_1, h_2)) \in (G_1 \times G_2)^2, \quad (g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$$

Alors  $(G_1 \times G_2, *)$  est un groupe appelé groupe produit de  $(G_1, *_1)$  et de  $(G_2, *_2)$ .

DÉMONSTRATION. Montrons que la loi est associative. Soient  $(g_1, g_2)$ ,  $(h_1, h_2)$  et  $(i_1, i_2)$  trois éléments de  $G_1 \times G_2$ .

$$\begin{aligned} (g_1, g_2) * ((h_1, h_2) * (i_1, i_2)) &= (g_1, g_2) * (h_1 *_1 i_1, h_2 *_2 i_2) \\ &= (g_1 *_1 (h_1 *_1 i_1), g_2 *_2 (h_2 *_2 i_2)) \\ &= ((g_1 *_1 h_1) *_1 i_1, (g_2 *_2 h_2) *_2 i_2) \\ &= (g_1 *_1 h_1, g_2 *_2 h_2) * (i_1, i_2) \\ &= ((g_1, g_2) * (h_1, h_2)) * (i_1, i_2) \end{aligned}$$

La loi est bien associative. De plus, si on note  $e_1$  le neutre de  $G_1$  et  $e_2$  le neutre de  $G_2$ , alors :

$$\begin{aligned} (g_1, g_2) * (e_1, e_2) &= (g_1 *_1 e_1, g_2 *_2 e_2) \\ &= (g_1, g_2) \end{aligned}$$

□

et on a de même  $(e_1, e_2) * (g_1, g_2) = (g_1, g_2)$  :  $(e_1, e_2)$  est le neutre pour la loi  $*$ . Enfin, si on note  $g_1^{-1}$  l'inverse de  $g_1$  pour la loi  $*_1$  et  $g_2^{-1}$  l'inverse de  $g_2$  pour la loi  $*_2$ , on montre aisément que  $(g_1^{-1}, g_2^{-1})$  est l'inverse de  $(g_1, g_2)$  pour la loi  $*$  (exo, ne pas oublier de le faire des deux côtés).

**Remarque :** Pour faire simple, la première coordonnée est dans  $G_1$ , la seconde dans  $G_2$ , et on définit la loi produit comme la première loi pour la première coordonnée, et la deuxième loi pour la deuxième coordonnée. On fait les opérations idoines coordonnée par coordonnée. La notion de groupe produit permet de « dévisser » un gros groupes en deux groupes plus petits et plus simples, plus faciles à manier et qu'on connaît mieux : cf. paragraphe IV.

**Exemples :**

- Puisque  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$  est un groupe pour la loi  $+$ ,  $\mathbb{K}^n$  est un groupe pour la loi produit que l'on note  $+$  également, et qui consiste simplement à sommer coordonnée par coordonnée (par exemple, dans  $\mathbb{K}^3$ ,  $(1, 2, 3) + (4, 5, 6) = (5, 7, 9)$ ).
- Puisque  $\mathbb{Z}/2\mathbb{Z}$  est un groupe pour la loi  $+$ ,  $(\mathbb{Z}/2\mathbb{Z})^2$  est un groupe pour la loi produit que l'on note  $+$  également. Ci-dessous la table du groupe :

+	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

On généralise aisément à un nombre fini quelconque de groupes. Par exemple, si  $(G, *_G)$  est un groupe et  $n \geq 1$ ,  $G^n$  est un groupe pour la loi produit :

$$\begin{aligned} (g_1, \dots, g_n) * (h_1, \dots, h_n) \\ = (g_1 *_G h_1, \dots, g_n *_G h_n) \end{aligned}$$

Car  $*_1$  et  $*_2$  sont associatives.

- On pourrait donner de même la table de  $(\mathbb{Z}/2\mathbb{Z})^3$  : par exemple  $(\bar{1}, \bar{0}, \bar{1}) + (\bar{1}, \bar{0}, \bar{1}) = (\bar{0}, \bar{0}, \bar{0})$ .
- C'est exactement la même chose pour  $(\mathbb{Z}/2\mathbb{Z})^n$ . En particulier, tout élément de  $(\mathbb{Z}/2\mathbb{Z})^n$  est son propre symétrique/opposé (encore une fois, on parle d'opposé car on note la loi additivement). Les groupes du type  $(\mathbb{Z}/2\mathbb{Z})^n$  sont importants en informatique car on travaille souvent en binaire.
- Donnons la table du groupe produit  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . Attention, la première coordonnée est modulo 2 et la seconde est modulo 3!

On peut même montrer que cette propriété caractérise les groupes du type  $(\mathbb{Z}/2\mathbb{Z})^n$ .

+	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$
$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$

- Il est hors de question de donner la table du groupe  $\mathbb{R}_+^* \times [0; 2\pi[$  car il est infini, mais explicitons tout de même la loi de ce groupe : pour tous  $(r_1, \theta_1)$  et  $(r_2, \theta_2)$  appartenant à  $\mathbb{R}_+^* \times [0; 2\pi[$ , on a  $(r_1, \theta_1) * (r_2, \theta_2) = (r_1 \times r_2, \theta_1 \oplus \theta_2)$  où, comme ci-dessus,  $\theta_1 \oplus \theta_2$  est l'élément de  $[0; 2\pi[$  congru à  $\theta_1 + \theta_2$  modulo  $2\pi$  (la loi  $\oplus$  est la loi dont est muni l'ensemble  $[0; 2\pi[$  et qui en fait un groupe).

### III Sous-groupes

#### III.1 Définition et caractérisation

Ci-dessus, on a vu plusieurs exemples où l'associativité de la loi était automatique car la loi était associative sur un ensemble plus gros. Ce genre de situation est habituel : quand on a un groupe inclus dans un autre, on dit qu'on a un sous-groupe. Plus précisément :

**Définition.** Soit  $(G, *)$  un groupe et soit  $H$  une partie de  $G$ .  $H$  est un sous-groupe de  $G$  si  $H$  est stable par la loi  $*$  et si  $(H, *)$  est un groupe. En d'autres termes, un sous-groupe de  $G$  est un groupe inclus dans  $G$  pour la même loi que  $G$  (restreinte à  $H$ ).

**Remarque :** Comme dit ci-dessus, quand on dit que  $(H, *)$  est un groupe,  $*$  est en fait la loi induite par  $*$  sur  $H$ , la restriction de  $*$  à  $H$ , qu'on note de la même façon que la loi de  $G$  par souci de simplicité et car il n'y aura aucune ambiguïté, on saura à quel ensemble appartiennent les éléments qu'on manipulera.

**Proposition.** Soit  $(G, *)$  un groupe et soit  $H$  un sous-groupe de  $G$ . Alors  $e$  (le neutre de  $G$ ) appartient à  $H$ .

**Remarque :** Il pourrait y avoir une confusion autour du neutre. En effet, on pourrait avoir un élément  $e_H$  neutre pour tous les éléments de  $H$  mais pas pour tous les éléments de  $G$  puisque la condition «  $\forall h \in H, e * h = h * e = h$  » est plus faible que «  $\forall g \in G, e * g = g * e = g$  » puisque  $H$  est inclus dans  $G$ , donc une condition vraie pour tous les éléments de  $G$  est encore vraie pour tous les éléments de  $H$  mais la réciproque n'est pas forcément vraie :  $H$  et  $G$  pourraient ne pas avoir le même neutre.

Cette proposition permet de ne se poser aucune question et de travailler avec le neutre sans préciser si c'est le neutre de  $G$  ou le neutre de  $H$  : en effet, le neutre de  $G$  appartient à  $H$  donc, par unicité du neutre, le neutre de  $H$  est le même que le neutre de  $G$ .

Il n'y a par conséquent aucune difficulté pour le symétrique : si  $x \in H$ , le symétrique de  $x$  dans  $G$  vérifie  $x * y_G = y_G * x = e$  et le symétrique dans  $H$  vérifie  $x * y_H = y_H * x = e_H = e$  donc, par unicité de l'inverse,  $y_G = y_H$ .

DÉMONSTRATION. Notons  $e_H$  le neutre de  $H$ . Soit  $h \in H$ . Alors  $e_H * h = h$  mais  $H$  est inclus dans  $G$  donc  $h \in H$  si bien que  $e * h = h$ . Ainsi,  $e * h = e_H * h$  : en multipliant par  $h^{-1}$  à droite (ou car tout élément de  $G$  est régulier), il vient :  $e = e_H$ .

**Remarque :** Ainsi, contenir le neutre est une condition nécessaire pour être un sous-groupe de  $G$ . Par contraposée, si une partie de  $G$  ne contient pas le neutre, alors ce n'est pas un sous-groupe. Par exemple,  $\mathbb{R} \setminus \mathbb{Q}$  ou  $\mathbb{R}^*$  ne sont pas des sous-groupes de  $\mathbb{R}$  (pour la loi  $+$ ) car ne contiennent pas 0. Attention, la réciproque est fautive : une partie de  $G$  qui contient le neutre n'est pas forcément un sous-groupe ! Par exemple,  $\mathbb{R}_+$  n'est pas un sous-groupe de  $\mathbb{R}$  alors qu'il contient 0 car aucun élément non nul n'admet d'opposé dans  $\mathbb{R}_+$ . Pour montrer qu'une partie de  $G$  est un sous-groupe de  $G$ , on a en fait la CNS suivante :

**Proposition.** Soit  $(G, *)$  un groupe. Soit  $H$  une partie de  $G$ . Alors  $H$  est un sous-groupe de  $G$  si et seulement si :

- $H$  est non vide.
- $H$  est stable par  $*$  i.e. :  $\forall (x, y) \in H^2, x * y \in H$ .
- $H$  est stable par inverse i.e. :  $\forall x \in H, x^{-1} \in H$ .

DÉMONSTRATION. Si  $H$  est un sous-groupe de  $G$ , alors  $H$  est stable par  $*$  par définition, non vide car contient le neutre, et  $(H, *)$  est un groupe donc, pour tout  $x \in H$ ,  $x^{-1} \in H$ . Réciproquement, supposons ces trois conditions vérifiées et prouvons que  $H$  est un sous-groupe de  $G$ .

$H$  étant stable par  $*$  par hypothèse, montrons que  $(H, *)$  est un groupe. La loi  $*$  étant associative sur  $G$ , elle l'est sur  $H$ . Tout élément de  $H$  admettant un inverse, il suffit de prouver que  $e \in H$  : en effet,  $e$  étant l'élément neutre de  $G$ ,  $e$  est un élément neutre sur  $H$ . Or,  $H$  est non vide donc il existe  $x \in H$ . Dès lors,  $x^{-1} \in H$  et puisque  $H$  est stable par  $*$ ,  $x * x^{-1} = e \in H$  :  $(H, *)$  est bien un groupe donc  $H$  est un sous-groupe de  $G$ .

**Remarque :** Pour montrer que  $H \neq \emptyset$ , on montre en général que  $e \in H$ . Ainsi, quand on se demande si un ensemble  $H$  est un sous-groupe de  $G$ , on commence par se demander si  $e \in H$ . Si oui, alors  $H$  est non vide et on passe à la suite, sinon alors  $H$  n'est pas un sous-groupe de  $G$ . À tous les coups on gagne ! Attention cependant : ce n'est qu'une condition nécessaire ! Si  $e \in H$ , alors  $H$  n'est pas forcément un sous-groupe de  $E$  !

**Corollaire.** Soit  $(G, *)$  un groupe. Soit  $H$  une partie de  $G$ . Alors  $H$  est un sous-groupe de  $G$  si et seulement si :

- $H$  est non vide.
- $\forall (x, y) \in H^2, x * y^{-1} \in H$ .

DÉMONSTRATION. Supposons que  $H$  soit non vide et que, pour tout  $(x, y) \in H^2, x * y^{-1} \in H$ . Soit  $y \in H$ . Alors  $y * y^{-1} = e \in H$  (on applique l'hypothèse de l'énoncé avec  $y$  à la place de  $x$ , penser à « truc »). Dès lors,  $e * y^{-1} = y^{-1} \in H$  (on applique encore l'hypothèse de l'énoncé avec  $x = e$ ). Enfin, si  $x \in E$ , alors en appliquant l'hypothèse à  $x$  et  $y^{-1}$ , il vient :  $x * y \in H$ . D'après le critère précédent,  $H$  est un sous-groupe de  $G$ . La réciproque est laissée en exo.

Ce ne sera pas forcément le cas sur un anneau, cf. paragraphe V.3.

$h^{-1}$  désigne ici l'inverse de  $h$  dans  $G$  car on ne sait pas encore que les inverses sont les mêmes.

La loi est en général notée multiplicativement. On dira donc parfois que  $H$  est stable par produit au lieu de dire que  $H$  est stable par  $*$  ou par la loi de  $G$ . Lorsque la loi est notée additivement, ces deux conditions deviennent :

$$\forall (x, y) \in H^2, x + y \in H$$

i.e.  $H$  est stable par somme, et :  
 $\forall x \in H, -x \in H$ ,  
 i.e.  $H$  est stable par passage à l'opposé.

Lorsque la loi est notée additivement, cette condition devient :

$$\forall (x, y) \in H^2, x - y \in H$$



**Remarque :** Un sous-groupe est un groupe par définition. Ainsi, pour montrer qu'un ensemble est un groupe, il suffit de prouver que c'est un sous-groupe d'un ensemble dont on sait qu'il est un groupe (pour la même loi). L'avantage de cette méthode est qu'on peut le montrer à l'aide des deux critères précédents qui sont très pratiques car ils ne nécessitent pas la vérification de l'associativité de la loi (étape souvent fastidieuse).

**Exemples :**

- $\mathbb{Q}, \mathbb{Z}$  sont des sous-groupes de  $\mathbb{R}$ . On parlera des sous-groupes de  $\mathbb{R}$  en détail dans le paragraphe III.3.
- $\mathbb{U}$  est un sous-groupe de  $\mathbb{C}^*$  (pour la loi  $\times$ ).
- Soit  $(a, b) \in \mathbb{R}^2$ . Montrons que  $H = a\mathbb{Z} + b\mathbb{Z} = \{an + bp \mid (n, p) \in \mathbb{Z}^2\}$  est un sous-groupe de  $\mathbb{R}$ .

$0 = a \times 0 + b \times 0 \in H$  donc  $H$  est non vide. Soit  $(x_1, x_2) \in H^2$ . Il existe  $(n_1, p_1) \in \mathbb{Z}^2$  et  $(n_2, p_2) \in \mathbb{Z}^2$  tels que  $x_1 = an_1 + bp_1$  et  $x_2 = an_2 + bp_2$  donc  $x_1 + x_2 = a(n_1 + n_2) + b(p_1 + p_2)$ . Or,  $n_1 + n_2 \in \mathbb{Z}$  et  $p_1 + p_2 \in \mathbb{Z}$  si bien que  $x_1 + x_2 \in H$  :  $H$  est stable par somme. Enfin,  $-x_1 = a(-n_1) + b \times (-p_1)$ . Or,  $-n_1$  et  $-p_1$  appartiennent à  $\mathbb{Z}$  donc  $-x_1 \in H$  :  $H$  est stable par passage à l'inverse (ou à l'opposé puisqu'on a un groupe additif) :  $H$  est un sous-groupe de  $\mathbb{R}$ .

On montrera dans l'exercice 37 que  $H$  est dense dans  $\mathbb{R}$  si et seulement si  $a$  et  $b$  sont non nuls et  $a/b$  est irrationnel.

- Si  $\alpha \in \mathbb{R}$ , alors  $\alpha\mathbb{Z}$  est un sous-groupe de  $\mathbb{R}$ , et si  $n \in \mathbb{Z}$ , alors  $n\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$  : voir paragraphes III.2 et III.3.
- Si  $\theta \in \mathbb{R}$ , notons  $r_\theta$  la rotation d'angle  $\theta$  de centre  $O$  dans le plan  $\mathbb{R}^2$  et notons  $R = \{r_\theta \mid \theta \in \mathbb{R}\}$  l'ensemble des rotations de centre  $O$ . Montrons que  $R$  est un sous-groupe de  $(S_{\mathbb{R}^2}, \circ)$  où on rappelle que  $S_{\mathbb{R}^2}$  est l'ensemble des bijections (ou permutations) de  $\mathbb{R}^2$ .

Tout d'abord,  $R$  est inclus dans  $S_{\mathbb{R}^2}$  car une rotation est bien une bijection. On pourrait montrer l'injectivité et la surjectivité, mais il suffit de voir que si  $\theta \in \mathbb{R}$ ,  $r_\theta \circ r_{-\theta} = r_{-\theta} \circ r_\theta = \text{Id}_{\mathbb{R}^2}$  donc  $r_\theta$  est bijective et sa bijection réciproque est  $r_{-\theta}$ . Il en découle de plus que  $R$  est stable par inverse. De plus,  $R$  est évidemment non vide, et stable par composition puisque, pour tout  $(\theta, \theta') \in \mathbb{R}^2$ ,  $r_\theta \circ r_{\theta'} = r_{\theta+\theta'} : R$  est bien un sous-groupe de  $S_{\mathbb{R}^2}$ . On remarque également que  $R$  est commutatif car  $r_\theta \circ r_{\theta'} = r_{\theta+\theta'} = r_{\theta'} \circ r_\theta$  : un groupe non commutatif peut avoir un sous-groupe commutatif différent de  $\{e\}$  !

Si on a  $f \circ g = g \circ f = \text{Id}_E$ , alors  $f$  est bijective et  $g = f^{-1}$ .

**Remarque :** Si  $(G, *)$  est un groupe, alors  $\{e\}$  et  $G$  sont des sous-groupes de  $G$ . Ce sont parfois les seuls, par exemple lorsque le cardinal de  $G$  est premier (cf. paragraphe III.4). En tout cas,  $\{e\}$  est le seul sous-groupe de  $G$  de cardinal 1 : un sous-groupe contient forcément  $e$ , donc si un sous-groupe n'a qu'un élément, il est forcément réduit à  $\{e\}$ .

Certains ensembles émergent assez naturellement et fournissent des exemples assez importants de sous-groupes.

**Exemple :** Si  $G$  est un groupe, on peut se demander s'il est ou non commutatif. Il est alors naturel de s'intéresser à l'ensemble suivant :

$$Z(G) = \{x \in G \mid \forall y \in G, xy = yx\}$$

On l'appelle le centre de  $G$ . En d'autres termes, le centre de  $G$  est l'ensemble des éléments de  $G$  qui commutent avec tous les autres. Montrons que c'est un sous-groupe de  $G$ .

- Tout d'abord,  $Z(G)$  est non vide car  $e \in Z(G)$ . En effet, pour tout  $y \in G$ ,  $y * e = e * y = y$ .
- Soit  $(x_1, x_2) \in Z(G)^2$ . Soit  $y \in G$ .

Et donc  $G$  est commutatif si et seulement si  $Z(G) = G$  : cf. exercice 33 du chapitre 21.



$$\begin{aligned}
(x_1 * x_2) * y &= x_1 * (x_2 * y) \\
&= x_1 * (y * x_2) \\
&= (x_1 * y) * x_2 \\
&= (y * x_1) * x_2 \\
&= y * (x_1 * x_2)
\end{aligned}$$

La loi est associative.

Car  $x_2 \in Z(G)$ .

Car  $x_1 \in Z(G)$ .

En d'autres termes,  $x_1 * x_2 \in Z(G)$  :  $Z(G)$  est stable par produit. En pratique, on pourra aller plus vite car on sait que la loi est associative, on écrira simplement :  $x_1 * x_2 * y = x_1 * y * x_2 = y * x_1 * x_2$ .

- Soit enfin  $x \in Z(G)$ . Soit  $y \in G$ . Puisque  $x \in Z(G)$ , alors  $x$  commute avec tout élément de  $G$  donc également avec  $y^{-1}$ , c'est-à-dire que  $xy^{-1} = y^{-1}x$ . Par conséquent,  $(xy^{-1})^{-1} = (y^{-1}x)^{-1}$  si bien que (on change l'ordre quand on inverse un produit !)  $yx^{-1} = x^{-1}y$  :  $x^{-1} \in Z(G)$ ,  $Z(G)$  est stable par inverse, c'est un sous-groupe de  $G$ .

**Remarque :**  $G$  est commutatif si et seulement si  $Z(G) = G$ . Dans le cas contraire, on peut définir un sous-groupe « intermédiaire ».

**Exemple :** Soit  $G$  un groupe non abélien. Il existe donc deux éléments qui ne commutent pas donc, en particulier, il existe un élément  $x \in G$  qui ne commute pas avec tous les éléments du groupe, et posons  $Z_x = \{y \in G \mid xy = yx\}$  l'ensemble des éléments de  $G$  qui commutent avec  $x$ . Montrons que  $Z_x$  est un sous-groupe de  $G$ .

Ici,  $x$  est fixé.

- Tout d'abord,  $Z_x$  est non vide car  $e \in Z_x$ . En effet,  $x * e = e * x = x$ .
- Soit  $(y_1, y_2) \in Z_x^2$ . En utilisant l'associativité de la loi et le fait que  $y_2$  et  $y_1$  commutent avec  $x$  :

$$\begin{aligned}
y_1 * y_2 * x &= y_1 * x * y_2 \\
&= x * y_1 * y_2
\end{aligned}$$

En d'autres termes,  $y_1 * y_2 \in Z_x$  :  $Z_x$  est stable par produit.

- Soit enfin  $y \in Z_x$ .  $yx = xy$  donc, en multipliant à gauche et à droite par  $y^{-1}$ , il vient  $xy^{-1} = y^{-1}x$ , c'est-à-dire que  $y^{-1} \in Z_x$  :  $Z_x$  est stable par passage à l'inverse.

En conclusion,  $Z_x$  est un sous-groupe de  $G$ . De plus,  $Z(G) \subset Z_x \subset G$  : en effet, les éléments de  $Z(G)$  commutent avec tous les éléments de  $G$  donc en particulier avec  $x$ , d'où l'inclusion de gauche, et par définition  $Z_x \subset G$ .

De plus, les deux inclusions sont strictes. En effet, par choix de  $x$ ,  $x$  ne commute pas avec tous les éléments de  $G$  donc, d'une part,  $Z_x \neq G$ , et d'autre part,  $x \notin Z(G)$ , mais  $x$  commute évidemment avec lui-même donc  $x \in Z_x$ , si bien que  $Z(G) \neq Z_x$ .

**Corollaire.** Soit  $H$  un sous-groupe de  $G$ . Soit  $n \in \mathbb{N}^*$ . Alors  $x^n$  et  $(x^{-1})^n$  appartiennent à  $H$ .

DÉMONSTRATION. Récurrence immédiate.

**Remarques :**

- Puisque  $x^0 = e \in H$ , on en déduit que  $x^n \in H$  pour tout  $n \in \mathbb{Z}$ .
- Si  $x$  et  $y$  sont deux éléments de  $H$ , alors  $x^n * y^p$  appartient à  $H$  pour tous  $n$  et  $p$  et on généralise aisément à un nombre quelconque d'éléments de  $H$  à des puissances quelconques. En clair, les résultats précédents impliquent qu'on ne peut pas « sortir d'un sous-groupe » : c'est normal, il est stable par la loi du groupe et par inverse !
- Si la loi est notée additivement, alors le résultat précédent devient :  $nx \in H$  pour tout  $n \in \mathbb{Z}$ . En particulier :

**Corollaire.** Si  $H$  est un sous-groupe de  $\mathbb{R}$  et si  $\alpha \in H$ , alors  $\alpha\mathbb{Z} \subset H$ .



À savoir démontrer en claquant des doigts ! Voir ci-dessous.

**Proposition.** Soit  $I$  un ensemble non vide et soit  $(H_i)_{i \in I}$  une famille de sous-groupes de  $G$ . Alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ . En d'autres termes, une intersection quelconque de sous-groupes de  $G$  est encore un sous-groupe de  $G$ .

DÉMONSTRATION. Notons  $B$  cette intersection.

- Soit  $i \in I$ .  $H_i$  étant un sous-groupe de  $G$ ,  $e \in H_i$  donc  $e \in B$  :  $B$  est non vide.
- Soit  $(x, y) \in B^2$ . Soit  $i \in I$ .  $x$  et  $y$  appartiennent à  $B$  donc à  $H_i$  qui est un sous-groupe de  $G$  donc  $x * y \in H_i$  si bien que  $x * y \in B$  :  $B$  est stable par  $*$ .
- Soit  $x \in B$ . Soit  $i \in I$ .  $x$  appartient à  $B$  donc à  $H_i$  qui est un sous-groupe de  $G$  donc  $x^{-1} \in H_i$  si bien que  $x^{-1} \in B$  :  $B$  est stable par inverse.

On en déduit que  $B$  est bien un sous-groupe de  $G$ .

**Remarque :** En général, une union de sous-groupes de  $G$  n'est pas un sous-groupe de  $G$ . C'est en fait très rarement le cas : montrons que si  $H_1$  et  $H_2$  sont deux sous-groupes de  $G$ , alors  $H_1 \cup H_2$  est un sous-groupe de  $G$  si et seulement si  $H_1 \subset H_2$  ou  $H_2 \subset H_1$ .

Si  $H_1 \subset H_2$  alors  $H_1 \cup H_2 = H_2$  qui est un sous-groupe de  $G$ . De même si  $H_2 \subset H_1$ .

Réciproquement, supposons que  $H_1 \not\subset H_2$  et  $H_2 \not\subset H_1$  et montrons que  $H_1 \cup H_2$  n'est pas un sous-groupe de  $G$ . Par hypothèse, il existe  $h_1 \in H_1 \setminus H_2$  et  $h_2 \in H_2 \setminus H_1$ . En particulier,  $h_1$  et  $h_2$  appartiennent à  $H_1 \cup H_2$ . Supposons que  $h_1 * h_2 \in H_1 \cup H_2$ . Alors  $h_1 * h_2 \in H_1$  ou  $h_1 * h_2 \in H_2$ .

Si  $h_1 * h_2 \in H_1$  alors,  $h_1^{-1} * h_1 * h_2 = e * h_2 = h_2$ . Il en découle que  $h_2 \in H_1$  : en effet,  $h_1 \in H_1$  et  $H_1$  est un sous-groupe de  $G$  donc  $h_1^{-1} \in H_1$ , et puisque  $h_1 * h_2 \in H_1$  et que  $H_1$  est stable par la loi  $*$ , alors  $h_2 \in H_1$  ce qui est absurde.

Si  $h_1 * h_2 \in H_2$ , on montre de même que c'est absurde en multipliant par  $h_2^{-1}$  à droite et en aboutissant à  $h_1 \in H_2$ .

C'est donc absurde dans tous les cas :  $h_1 * h_2$  n'appartient pas à  $H_1 \cup H_2$  qui n'est donc pas stable par  $*$  : ce n'est pas un sous-groupe de  $G$ .



En d'autres termes, une union de deux sous-groupes est un sous-groupe si et seulement si l'un des deux est inclus dans l'autre.



On utilise sans le dire l'associativité de la loi.

**Proposition/Définition (Deuxième année).** Soit  $A$  une partie de  $G$ . Il existe un unique plus petit sous-groupe de  $G$  qui contient  $A$ . On l'appelle le groupe engendré par  $A$  et on le note  $\langle A \rangle$ ,  $\langle A \rangle$  ou  $\text{gr}(A)$ .

DÉMONSTRATION. Il suffit de voir que

$$B = \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H$$

□

est un sous-groupe de  $G$  d'après ce qui précède car intersection de sous-groupes de  $G$ , et est contenu dans tous les sous-groupes de  $G$  contenant  $A$ . Il y a unicité car si  $C$  est un sous-groupe qui convient, alors  $B \subset C$  car  $C$  est un sous-groupe de  $G$  contenant  $A$ , et  $C \subset B$  pour la même raison donc  $B = C$ .

**Remarques :**

- Dans le cas où  $A = \{x_1; \dots; x_n\}$  est un ensemble fini, on note ce groupe  $\text{gr}(x_1, \dots, x_n)$  au lieu de  $\text{gr}(\{x_1, \dots, x_n\})$ .



Plus petit au sens de l'inclusion, c'est-à-dire que si  $H$  est un sous-groupe qui contient  $A$ , alors  $\text{gr}(A) \subset H$ .

- Dans le cas où  $A$  ne contient qu'un élément, le groupe engendré est très simple. Montrons que  $\text{gr}(x) = \{x^n \mid n \in \mathbb{Z}\}$ . D'après ce qui précède,  $B = \{x^n \mid n \in \mathbb{Z}\}$  est inclus dans chaque sous-groupe de  $G$  contenant  $x$ . Pour conclure, il suffit donc de prouver que c'est un sous-groupe de  $G$ .  $e = x^0 \in B$  donc  $B$  est non vide. Soit  $(x_1, x_2) \in B^2$ . Il existe  $(n_1, n_2) \in \mathbb{Z}^2$  tel que  $x_1 = x^{n_1}$  et  $x_2 = x^{n_2}$  si bien que  $x_1 x_2 = x^{n_1+n_2} \in B$  :  $B$  est stable par produit. Enfin, il est stable par inverse puisque  $x_1^{-1} = x^{-n_1} \in B$ .
- Dans le cas où la loi est notée additivement, on a  $\text{gr}(x) = \{nx \mid n \in \mathbb{Z}\}$ . En particulier, lorsque  $\alpha \in \mathbb{R}$ ,  $\text{gr}(\alpha) = \alpha\mathbb{Z}$ . On retrouve le fait que, si  $H$  est un sous-groupe de  $\mathbb{R}$  contenant  $\alpha$ , alors  $\alpha\mathbb{Z} \subset H$ . Mais puisque ce n'est au programme qu'en deuxième année, il faut savoir le redémontrer ! cf. paragraphes III.2 et III.3. Cependant, il est bon de connaître ce résultat car alors il devient un réflexe, et car l'idée de groupe engendré est assez intuitive et permet de mieux voir ce résultat.
- Cependant, lorsque  $A$  admet au moins deux éléments  $x_1$  et  $x_2$ , ce n'est plus aussi simple. La loi n'étant pas forcément commutative,  $\text{gr}(A)$  contient (au moins) tous les éléments du type  $x_1^{n_1} x_2^{n_2} x_1^{p_1} x_2^{p_2} \dots$ . C'est pour cela qu'on ne cherche plus à expliciter tous les éléments de  $\text{gr}(A)$  mais à le trouver explicitement.

### III.2 Sous-groupes de $\mathbb{Z}$ (deuxième année)

**Proposition.** Les sous-groupes de  $\mathbb{Z}$  sont exactement les  $n\mathbb{Z}$ , pour  $n$  appartenant à  $\mathbb{Z}$ .

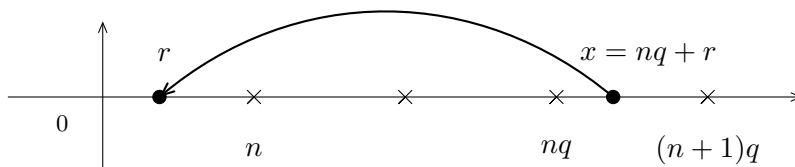
DÉMONSTRATION. Soit  $n \in \mathbb{Z}$ . Montrons que  $n\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ .

Tout d'abord,  $0 \in n\mathbb{Z}$  donc  $n\mathbb{Z}$  est non vide. Soit  $(x, y) \in (n\mathbb{Z})^2$ . Il existe  $(p, k) \in \mathbb{Z}^2$  tel que  $x = np$  et  $y = nk$  si bien que  $x + y = n(p + k)$  et  $-x = n \times (-p)$ . Or,  $p + k$  et  $-p$  appartiennent à  $\mathbb{Z}$  donc  $x + y$  et  $-x$  appartiennent à  $n\mathbb{Z}$  :  $n\mathbb{Z}$  est stable par somme et par passage à l'opposé, c'est bien un sous-groupe de  $\mathbb{Z}$ .

Réciproquement, soit  $H$  un sous-groupe de  $\mathbb{Z}$ . Alors  $0 \in H$  car  $0$  est le neutre de  $\mathbb{Z}$ . Si  $H = \{0\}$  alors  $H = 0\mathbb{Z}$ . Sinon,  $H$  contient un élément  $x$  non nul.  $H$  étant un sous-groupe de  $\mathbb{Z}$ ,  $H$  est stable par passage à l'opposé donc  $-x \in H$ . Puisque soit  $x$  soit  $-x$  est strictement positif, l'ensemble  $H \cap \mathbb{N}^*$  est non vide : c'est une partie non vide de  $\mathbb{N}$  donc admet un plus petit élément noté  $n$ . Montrons que  $H = n\mathbb{Z}$ .

$n \in H$  et  $H$  est un sous-groupe de  $\mathbb{Z}$  donc est stable par somme. Ainsi,  $n + n = 2n \in H$ . De même,  $n + 2n = 3n \in H$ . Par une récurrence immédiate, pour tout  $p \in \mathbb{N}$ ,  $np \in H$ . Enfin, si  $p \in \mathbb{Z}$  et  $p < 0$ , alors  $-p \in \mathbb{N}$  donc  $n \times (-p) \in H$  et  $H$  est stable par opposé donc  $np \in H$ . On en déduit que  $n\mathbb{Z} \subset H$ .

Réciproquement, soit  $x \in H$ . Notons  $x = nq + r$  la division euclidienne de  $x$  par  $n$ . On a donc  $0 \leq r < n$ . Or,  $x \in H$  et  $nq \in H$  car  $n\mathbb{Z} \subset H$  et  $H$  est un sous-groupe de  $\mathbb{Z}$  donc  $r = x - nq \in H$ . Si  $r \neq 0$  alors  $r$  est un élément de  $H$  strictement positif strictement inférieur à  $n$  ce qui est absurde par définition de  $n$ .



Finalement,  $x = nq \in n\mathbb{Z}$ , d'où l'inclusion réciproque, d'où l'égalité.

#### Remarques :

- On a même montré que si  $H$  est un sous-groupe de  $\mathbb{Z}$  non réduit à  $\{0\}$ , alors  $H = n\mathbb{Z}$  où  $n$  est le plus petit élément strictement positif de  $H$ .

Il est sous-entendu : pour la loi  $+$ . De plus, on rappelle que

$$n\mathbb{Z} = \{np \mid p \in \mathbb{Z}\}$$

Puisque le groupe engendré par  $n$  est  $n\mathbb{Z}$  alors  $n\mathbb{Z} \subset H$ , mais on redémontre ce résultat.

$n$  est non nul.

- On a utilisé une méthode qui revient souvent quand on manipule des groupes additifs : se ramener, à l'aide de soustractions, au voisinage de 0 : un groupe additif étant stable par soustraction, ce qui se passe au voisinage d'un point se passe également au voisinage de 0 grâce à des soustractions. Ce sera la même idée pour les sous-groupes de  $\mathbb{R}$  (voir ci-dessous) et aussi pour les noyaux (idem) : ce qui se passe autour du neutre indique ce qui se passe partout dans le groupe.

**Application :** Soient  $a$  et  $b$  deux entiers non nuls. Montrons que tout multiple commun à  $a$  et  $b$  est un multiple de leur PPCM.

L'ensemble des multiples de  $a$  est  $a\mathbb{Z}$  et l'ensemble des multiples de  $b$  est  $b\mathbb{Z}$ , si bien que l'ensemble des multiples communs à  $a$  et  $b$  est  $a\mathbb{Z} \cap b\mathbb{Z}$ . Or, une intersection de sous-groupes de  $\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$  donc  $a\mathbb{Z} \cap b\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ , non réduit à 0 puisqu'il contient  $a \vee b$  (et même  $|ab|$ ). D'après ce qui précède,  $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$  où  $n$  est le plus petit entier strictement positif dans  $a\mathbb{Z} \cap b\mathbb{Z}$ . En d'autres termes,  $n$  est le plus petit entier strictement positif multiple commun à  $a$  et  $b$  donc  $n = a \vee b$  si bien que  $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$ . En d'autres termes, tout multiple commun à  $a$  et  $b$  est divisible par  $a \vee b$ .

Le principe de la démonstration est le même que celle vue dans le chapitre 6. On avait en fait démontré la proposition précédente sans le dire !

### III.3 Sous-groupes de $\mathbb{R}$ (HP)

**Remarque :** Si  $\alpha \in \mathbb{R}$ ,  $\alpha\mathbb{Z}$  est un sous-groupe de  $\mathbb{R}$  (exo). Par exemple,  $2\pi\mathbb{Z}$  est un sous-groupe de  $\mathbb{R}$ . Ici, il n'y a pas de réciproque, mais on peut tout de même affirmer quelque-chose au sujet des sous-groupes de  $\mathbb{R}$ .

$\alpha$  n'est pas forcément un entier !

**Théorème.** Les sous-groupes de  $\mathbb{R}$  sont soit de la forme  $\alpha\mathbb{Z}$ , soit denses.

**Exemple :**  $\mathbb{Q}$  est un sous-groupe de  $\mathbb{R}$  dense dans  $\mathbb{R}$ .

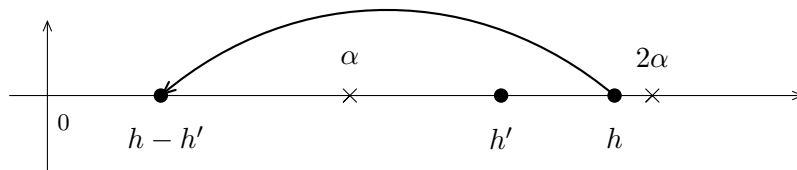
**DÉMONSTRATION.** Le principe de la démonstration est analogue à ci-dessus : l'idée est de tout ramener, par des soustractions successives, au voisinage de 0.

Soit  $H$  un sous-groupe de  $\mathbb{R}$ . Si  $H = \{0\}$  alors  $H = 0\mathbb{Z}$ . Sinon, de même que ci-dessus,  $H$  admet un élément strictement positif. L'ensemble  $H \cap \mathbb{R}_+^*$  est donc une partie non vide minorée (par 0) de  $\mathbb{R}$  donc admet une borne inférieure  $\alpha$ .

Sous-entendu : pour la loi +. Attention, ce théorème ne dit pas qu'une partie dense est forcément un sous-groupe de  $\mathbb{R}$ . Contre-exemple :  $\mathbb{R} \setminus \mathbb{Q}$ .

Contrairement à un plus petit élément,  $\alpha$  n'appartient pas forcément à  $H \cap \mathbb{R}_+^*$  :  $\alpha$  peut être nul ! Cependant,  $\alpha$  est forcément positif (ou nul) puisque 0 est un minorant de  $H \cap \mathbb{R}_+^*$  (et on rappelle que la borne inférieure est le plus grand des minorants).

- Supposons que  $\alpha > 0$ . Montrons que  $H = \alpha\mathbb{Z}$ . Tout d'abord, par caractérisation de la borne inférieure, il existe  $h \in H$  tel que  $\alpha \leq h < 2\alpha$  (possible car  $\alpha > 0$ ). Si  $\alpha < h$  alors, toujours par caractérisation de la borne inférieure, il existe  $h' \in H \cap \mathbb{R}_+^*$  tel que  $\alpha \leq h' < h$ . Puisque  $h$  et  $h'$  appartiennent à  $H$  qui est un groupe,  $h - h' \in H$ . De plus,  $\alpha \leq h' < h < 2\alpha$  donc  $0 < h - h' < \alpha$  ce qui est absurde par définition de  $\alpha$ .



Ainsi,  $h = \alpha$ . En particulier,  $\alpha \in H$ . De même que ci-dessus, on montre que  $\alpha\mathbb{Z} \subset H$ .

Si  $H \neq \alpha\mathbb{Z}$ , il existe  $x \in H \setminus \alpha\mathbb{Z}$ . Soit  $k \in \mathbb{Z}$  tel que  $k\alpha \leq x < (k+1)\alpha$ , et puisque  $x \notin \alpha\mathbb{Z}$ ,  $k\alpha \neq x$  si bien que  $0 < x - k\alpha < \alpha$ . En d'autres termes,  $x - k\alpha$  est un élément de  $H$  (car  $x$  et  $k\alpha$  appartiennent à  $H$  qui est un sous-groupe de  $\mathbb{R}$  donc stable par différence) strictement positif et strictement inférieur à  $\alpha$ , ce qui est absurde. Finalement,  $H = \alpha\mathbb{Z}$ .

$k = \lfloor x/\alpha \rfloor$  pour être précis. Essayez de faire un dessin du même type que ceux ci-dessus.

- Supposons que  $\alpha = 0$ . Soient  $x < y$  deux réels. Par caractérisation de la borne inférieure, il existe un élément  $h \in H \cap \mathbb{R}_+^*$  vérifiant  $0 < h < y - x$ . En particulier,  $h \in H$ . De même que précédemment,  $h\mathbb{Z} \subset H$ . Si on pose  $E = \{k \in \mathbb{Z} \mid hk < y\}$ ,

alors on montre de même que dans la démonstration de la densité de  $\mathbb{Q}$  dans le chapitre 12 que  $E$  admet un plus grand élément  $k_0$  et que  $x < k_0 h < y$ . Finalement,  $k_0 h \in H$  donc il existe un élément de  $H$  dans l'intervalle  $]x; y[$  :  $H$  est dense dans  $\mathbb{R}$  (il rencontre tout intervalle ouvert non vide).


Ce résultat (difficile) est très classique et permet de montrer des résultats qu'il serait compliqué de prouver sans la théorie des groupes. Donnons un exemple (nous en verrons d'autres en TD).


**Activité :** Soit  $f : \mathbb{R} \rightarrow \mathbb{R}$  continue. On suppose que  $f$  est 1-périodique et  $\sqrt{2}$ -périodique. Montrer que  $f$  est constante.

Soit  $T \in \mathbb{R}$ . On rappelle que  $T$  est une période si  $f(x + T) = f(x)$  pour tout  $x$ . Montrons que l'ensemble des périodes de  $f$  (que l'on notera  $H$ ) est un sous-groupe de  $\mathbb{R}$ .

0 est évidemment une période de  $H$  donc  $H$  est non vide. Soit  $(T_1, T_2) \in H^2$ . Soit  $x \in \mathbb{R}$ .

$$\begin{aligned} f(x + T_1 + T_2) &= f(x + T_1) \\ &= f(x) \end{aligned}$$

  $T_2$  est une période.

  $T_1$  est une période.


c'est-à-dire que  $T_1 + T_2$  est une période i.e.  $T_1 + T_2 \in H$  :  $H$  est stable par somme. Enfin,  $T_1$  étant une période,

$$\begin{aligned} f(x - T_1) &= f((x - T_1) + T_1) \\ &= f(x) \end{aligned}$$

donc  $-T_1$  est une période i.e.  $-T_1 \in H$  :  $H$  est stable par différence. Il en découle que  $H$  est un sous-groupe de  $\mathbb{R}$ .

Supposons qu'il existe  $\alpha \in \mathbb{R}$  tel que  $H = \alpha\mathbb{Z}$ . Puisque  $1 \in H$ , il existe  $n \in \mathbb{Z}^*$  tel que  $1 = \alpha n$  donc  $\alpha = 1/n$ . De même, il existe  $p \in \mathbb{Z}^*$  tel que  $\alpha = \sqrt{2}/p$  donc  $\sqrt{2} = p/n \in \mathbb{Q}$  ce qui est absurde.

Finalement,  $H$  est dense dans  $\mathbb{R}$ . Soit  $x \in \mathbb{R}$ .  $H$  étant dense dans  $\mathbb{R}$ , il existe une suite d'éléments de  $H$  notée  $(T_n)_{n \in \mathbb{N}}$  qui converge vers  $x$ . Pour tout  $n \in \mathbb{N}$ ,  $T_n$  est une période de  $f$  donc  $f(T_n) = f(0)$ . Or,  $T_n \xrightarrow{n \rightarrow +\infty} x$  et  $f$  est continue donc  $f(T_n) \xrightarrow{n \rightarrow +\infty} f(x)$ . Or, la suite  $(f(T_n))_{n \in \mathbb{N}}$  est constante égale à  $f(0)$  donc converge vers  $f(0)$ . Par unicité de la limite,  $f(x) = f(0)$  :  $f$  est constante. Le résultat est faux sans la continuité de  $f$ . Par exemple, la fonction indicatrice de  $\mathbb{Z} + \sqrt{2}\mathbb{Z}$  est 1-périodique et  $\sqrt{2}$ -périodique (exo) et n'est pas constante.

 Caractérisation séquentielle de la densité.

### III.4 Théorème de Lagrange (HP)

Dans ce paragraphe, tous les groupes considérés seront finis.

**Théorème (Théorème de Lagrange).** Soit  $G$  un groupe fini. Soit  $H$  un sous-groupe de  $G$ . Alors  $\text{card}(H)$  divise  $\text{card}(G)$ .

DÉMONSTRATION. On définit sur  $G$  la relation  $R$  par :  $xRy \iff xy^{-1} \in H$ . Montrons que  $R$  est une relation d'équivalence.

- Soit  $x \in G$ . Alors  $xx^{-1} = e \in H$  car  $H$  est un sous-groupe de  $G$ . En d'autres termes,  $xRx$  :  $R$  est réflexive.
- Soit  $(x, y) \in G^2$  tel que  $xRy$ . Alors  $xy^{-1} \in H$ .  $H$  étant stable par inverse,  $(xy^{-1})^{-1} = yx^{-1} \in H$  donc  $yRx$  :  $R$  est symétrique.
- Soit  $(x, y, z) \in G^3$  tel que  $xRy$  et  $yRz$ . En d'autres termes,  $xy^{-1}$  et  $yz^{-1}$  appartiennent à  $H$ . De plus,  $H$  est un sous-groupe de  $G$  donc est stable par la loi de  $G$  donc  $xy * yz^{-1} = xz^{-1}$  (la loi est associative). En d'autres termes,  $xRz$  :  $R$  est transitive.

Soit  $x \in G$ . Soit  $y \in G$ . Alors :

$$\begin{aligned} y \in \text{cl}(x) &\iff yx^{-1} \in H \\ &\iff \exists z \in H, yx^{-1} = z \\ &\iff \exists z \in H, y = zx \end{aligned}$$

En d'autres termes,  $\text{cl}(x) = Hx = \{zx \mid z \in H\}$ . Montrons que

$$f : \begin{cases} H & \longrightarrow \text{cl}(x) \\ z & \longmapsto zx \end{cases} \quad \square$$

est une bijection. Elle est surjective d'après ce qui précède. Soient  $z_1$  et  $z_2$  deux éléments de  $H$  et supposons que  $f(z_1) = f(z_2)$ . Ainsi,  $z_1x = z_2x$  et puisque  $x$  est régulier (ou en multipliant à droite par  $x^{-1}$ ), il vient :  $z_1 = z_2$ ,  $f$  est injective.  $f$  est bijective donc  $\text{card}(H) = \text{card}(\text{cl}(x))$ .

Finalement, les classes d'équivalences ont toutes le même cardinal (le cardinal de  $H$ ) et elles forment une partition de  $G$  donc  $\text{card}(G)$  est égal au nombre de classes d'équivalences distinctes multiplié par leur cardinal commun, donc au nombre de classes d'équivalences distinctes multiplié par  $\text{card}(H)$ . En particulier,  $\text{card}(H)$  divise le cardinal de  $G$ .

**Remarque :** On note parfois  $G/H$  l'ensemble des classes de cette relation d'équivalence. Lorsque  $G = \mathbb{Z}$  et  $H = n\mathbb{Z}$ ,  $R$  est la congruence modulo  $n$  donc  $G/H$  est l'ensemble des classes d'équivalence modulo  $n$  : d'où la notation  $\mathbb{Z}/n\mathbb{Z}$  !

**Remarque :** Ce résultat permet de donner certains résultats sur les sous-groupes éventuels d'un groupe fini  $G$ . Par exemple :

- Si  $G$  est un groupe fini de cardinal  $p$  premier, alors  $G$  n'a aucun sous-groupe hormis  $\{e\}$  et lui-même. En effet, si  $H$  est un sous-groupe de  $G$ , alors  $\text{card}(H)$  divise  $\text{card}(G)$  donc  $\text{card}(H) = 1$  et dans ce cas  $H = \{e\}$  ou  $\text{card}(H) = \text{card}(G)$  et dans ce cas  $H = G$ . En particulier, puisqu'une intersection de sous-groupes est un sous-groupe, si  $H_1$  et  $H_2$  sont deux sous-groupes de  $G$  de cardinal  $p$  premier, alors soit  $H_1 \cap H_2$  est triviale (i.e. réduite à  $\{e\}$ ), soit  $H_1 = H_2$ . En effet,  $H_1 \cap H_2$  est un sous-groupe de  $H_1$  et de  $H_2$  et on conclut à l'aide de ce qui précède.
- Attention, la réciproque est fautive : si  $d$  divise  $\text{card}(G)$ , il n'existe pas forcément de sous-groupe de  $G$  de cardinal  $d$ . Il existe par exemple un groupe de cardinal 12 n'ayant aucun sous-groupe de cardinal 4.
- Cependant, ce théorème permet de donner les cardinaux éventuels des sous-groupes de  $G$ . Par exemple, il n'existe aucun sous-groupe de  $G$  dont le cardinal est égal à  $\frac{3}{4} \times \text{card}(G)$ .
- Par exemple, un sous-groupe strict de  $G$  contient au plus  $\text{card}(G)/2$  éléments.
- Donnons une application explicite : soit  $G$  un groupe fini non commutatif. On a vu que, si  $x$  est un élément ne commutant pas avec tous les éléments du groupe, alors  $Z(G) \subset Z_x \subset G$  et ces inclusions sont strictes. Par conséquent,  $Z(G)$  est un sous-groupe strict de  $Z_x$  et  $Z_x$  est un sous-groupe strict de  $G$ . D'après ce qui précède,  $\text{card}(Z_x) \leq \text{card}(G)/2$  et  $\text{card}(Z(G)) \leq \text{card}(Z_x)/2 \leq \text{card}(G)/4$ . En d'autres termes : au plus un quart des éléments commutent avec tous les autres ! Un groupe non commutatif ne peut pas être « trop » commutatif ! Cela permet par exemple de prouver que si  $G$  est un groupe fini non commutatif, la probabilité que deux éléments commutent est inférieure ou égale à  $5/8$  (cf. exercice 74).

On peut voir ça comme une intersection de bateaux à la bataille navale : soit c'est le même bateau, soit ils ne se coupent qu'en un point, le neutre, cf. poly de botanique.



## IV Morphismes de groupes

### IV.1 Définition, premiers exemples

On se donne dans cette partie et la suivante deux groupes  $(G_1, *_1)$  et  $(G_2, *_2)$ . Le but de cette partie est de définir et d'étudier des fonctions allant d'un groupe dans un autre. On a vu que ce qui est important dans un groupe, c'est sa loi : pour qu'une fonction allant de  $G_1$  dans  $G_2$  soit intéressante du point de vue théorie des groupes, il est nécessaire qu'elle « se comporte bien vis à vis des lois de  $G_1$  et de  $G_2$  » ou qu'elle envoie la loi de  $G_1$  sur celle de  $G_2$ . D'où la définition suivante.

**Définition.** Soit  $f : G_1 \rightarrow G_2$ . On dit que  $f$  est un morphisme de groupes si :

$$\forall (x, y) \in G_1^2, \quad f(x *_1 y) = f(x) *_2 f(y)$$

Si  $f$  est de plus bijective, on dit que  $f$  est un isomorphisme, et on dit que les deux groupes  $(G_1, *_1)$  et  $(G_2, *_2)$  sont isomorphes.

Ou plus simplement que  $G_1$  et  $G_2$  sont isomorphes s'il n'y a aucune ambiguïté pour les lois.

#### Remarques :

- En d'autres termes, une fonction est un morphisme de groupes lorsqu'on peut « casser et sortir la loi de  $G_1$  en la changeant en la loi de  $G_2$  ». Encore en d'autres termes, un morphisme de groupes est une fonction qui « transforme la loi de  $G_1$  en la loi de  $G_2$  ».
- On parle parfois plus simplement de morphisme au lieu de morphisme de groupes.
- On parle parfois d'homomorphisme de groupe au lieu de morphisme de groupes (mais c'est plus rare).
- Lorsque  $G_1 = G_2$  (et  $*_1 = *_2$ ), on dit parfois que  $f$  est un endomorphisme (de groupes). Mais on garde en général cette formulation pour l'algèbre linéaire, cf. second semestre.

#### Exemples :

- L'exponentielle est un morphisme de  $(\mathbb{R}, +)$  vers  $(\mathbb{R}_+^*, \times)$ . C'est même un isomorphisme, si bien que  $\mathbb{R}$  et  $\mathbb{R}_+^*$  (munis respectivement de la somme et du produit) sont isomorphes.
- Le  $\ln$  est de même un isomorphisme de  $(\mathbb{R}_+^*, \times)$  vers  $(\mathbb{R}, +)$ . C'est l'isomorphisme réciproque (voir ci-dessous) de l'exponentielle.
- Cependant, l'exponentielle  $z \mapsto e^z$  est un morphisme de groupes de  $(\mathbb{C}, +)$  dans  $(\mathbb{C}^*, \times)$  mais ce n'est pas un isomorphisme car il n'est pas injectif : 0 et  $2i\pi$  ont en effet la même image.
- La fonction  $x \mapsto e^{ix}$  est un morphisme de groupe de  $(\mathbb{R}, +)$  dans  $(\mathbb{U}, \times)$ . Il n'est cependant pas bijectif car il n'est pas injectif (0 et  $2\pi$  ont la même image par exemple).
- Cependant, cette fonction est un isomorphisme entre  $([0; 2\pi[, \oplus)$  (cf. paragraphe II.1) dans  $(\mathbb{U}, \times)$ . En effet, soient  $x, y$  deux éléments de  $[0; 2\pi[$ . Alors  $x \oplus y \equiv x + y[2\pi]$  si bien que

$$\begin{aligned} e^{i(x \oplus y)} &= e^{i(x+y)} \\ &= e^{ix} \times e^{iy} \end{aligned}$$

C'est bien un morphisme de groupes. De plus, on sait que cette fonction est une bijection de  $[0; 2\pi[$  dans  $\mathbb{U}$  : c'est un isomorphisme.

- Montrons que  $(\mathbb{C}^*, \times)$  et le groupe produit  $\mathbb{R}_+^* \times [0; 2\pi[$  muni de la loi produit (cf. paragraphe II.3) sont isomorphes. On sait (cf. chapitre 7) que la fonction  $f : (r, \theta) \mapsto$



$re^{i\theta}$  est une bijection de  $\mathbb{R}_+^* \times [0; 2\pi[$  dans  $\mathbb{C}^*$ . Montrons que c'est un morphisme de groupes. Soient  $(r_1, \theta_1)$  et  $(r_2, \theta_2)$  deux éléments de  $\mathbb{R}_+^* \times [0; 2\pi[$ . Alors

$$\begin{aligned} f((r_1, \theta_1) * (r_2, \theta_2)) &= f(r_1 r_2, \theta_1 \oplus \theta_2) \\ &= r_1 r_2 e^{i(\theta_1 \oplus \theta_2)} \\ &= r_1 r_2 e^{i(\theta_1 + \theta_2)} \\ &= r_1 e^{i\theta_1} \times r_2 e^{i\theta_2} \\ &= f(r_1, \theta_1) \times f(r_2, \theta_2) \end{aligned}$$

Voir ci-dessus.

Pour travailler avec un complexe non nul, il suffit de travailler sur son module et son argument modulo  $2\pi$  : on remarque l'intérêt de la notion de groupe produit. Pour travailler sur le groupe produit, il suffit de travailler sur les deux groupes de base, en général plus simples. Il peut donc être intéressant de « dévisser » un gros groupe en un produit de deux groupes plus simples à manier (mais ce n'est pas toujours possible).

- Enfin,  $([0; 2\pi[, \oplus)$  et  $(R, \circ)$  (où  $R$  est l'ensemble des rotations de centre  $O$ , cf. paragraphe III.1) sont isomorphes par l'application  $f : \theta \mapsto r_\theta$ . Tout d'abord,  $f$  est surjective puisque, pour tout  $x \in \mathbb{R}$ , il existe  $\theta \in [0; 2\pi[$  tel que  $\theta \equiv x[2\pi]$  et on a donc  $r_x = r_\theta = f(\theta)$ .  $f$  est de plus injective car, si  $(\theta_1, \theta_2) \in [0; 2\pi[$ , alors :  $r_{\theta_1} = r_{\theta_2} \iff \theta_1 \equiv \theta_2[2\pi] \iff \theta_1 = \theta_2$ . On montre enfin de même que précédemment que  $f$  est un morphisme de groupe.

## IV.2 Premières propriétés

**Proposition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. Alors  $f(e_1) = e_2$  et, pour tout  $x \in G_1$ ,  $f(x^{-1}) = f(x)^{-1}$ .

**Remarque :** En d'autres termes, un morphisme envoie le neutre sur le neutre et l'inverse sur l'inverse, c'est-à-dire que l'image de l'inverse est l'inverse de l'image. Il est évident que dans l'égalité  $f(x^{-1}) = f(x)^{-1}$ , le premier inverse est pris dans  $G_1$  ( $x^{-1}$  est l'inverse de  $x \in G_1$ ) tandis que le deuxième inverse est pris dans  $G_2$  (c'est l'inverse de  $f(x) \in G_2$ ). On les note de la même façon mais attention à bien voir à quel ensemble appartiennent les éléments.

DÉMONSTRATION.  $f$  étant un morphisme,

$$\begin{aligned} f(e_1) &= f(e_1 *_1 e_1) \\ &= f(e_1) *_2 f(e_1) \end{aligned} \quad \square$$

Or,  $G_2$  est un groupe donc tout élément est régulier, en particulier  $f(e_1)$  donc  $e_2 = f(e_1)$ . Soit  $x \in G_1$ . Alors  $f(x * x^{-1}) = f(x) \times f(x^{-1})$ . Or,  $x * x^{-1} = e_1$  donc, d'après ce qui précède,  $f(x) \times f(x^{-1}) = e_2$  ce qui permet de conclure.

On pouvait aussi, ce qui revient au même, multiplier par  $f(e_1)^{-1}$  à gauche ou à droite.

**Corollaire.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes et soit  $x \in G_1$ . Alors, pour tout  $n \in \mathbb{Z}$ ,  $f(x^n) = f(x)^n$ .

**Remarque :** Idem, il faut bien comprendre que la notation  $a^n$  signifie : l'itéré de  $a$   $n$  fois pour la loi correspondante, à gauche la loi de  $G_1$  et à droite la loi de  $G_2$ . De plus, ce résultat est toujours vrai pour une loi notée additivement en remplaçant la notation  $a^n$  par  $na$ . En particulier, si la loi de  $G_1$  est notée additivement et celle de  $G_2$  multiplicativement, on a  $f(nx) = f(x)^n$ .

DÉMONSTRATION. Par une récurrence immédiate, le résultat est vrai pour tout  $n \in \mathbb{N}$ . On montre également par récurrence que, pour tout  $n \in \mathbb{N}$ ,  $f((x^{-1})^n) = (f(x)^{-1})^n$ , ce qui permet de conclure.

**Proposition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. Si  $f$  est bijective alors  $f^{-1}$  est un morphisme de groupes (de  $G_2$  dans  $G_1$ ).

DÉMONSTRATION. Rappelons que si  $y \in G_2$ , alors  $f^{-1}(y)$  est l'unique antécédent de  $y$  par  $f$ . Soit  $(y_1, y_2) \in G_2^2$ . Notons  $x_1 = f^{-1}(y_1)$  et  $x_2 = f^{-1}(y_2)$ . Par conséquent,  $f$  étant un morphisme,

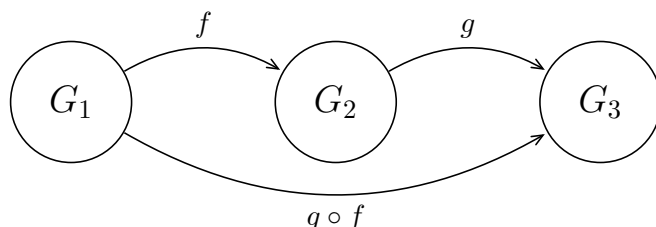
$$\begin{aligned} f(x_1 *_1 x_2) &= f(x_1) *_2 f(x_2) \\ &= y_1 *_2 y_2 \end{aligned}$$

En d'autres termes,  $x_1 *_1 x_2$  est l'unique antécédent de  $y_1 *_2 y_2$  donc

$$\begin{aligned} f^{-1}(y_1 *_2 y_2) &= x_1 *_1 x_2 \\ &= f^{-1}(y_1) *_1 f^{-1}(y_2) \end{aligned}$$

En d'autres termes, la réciproque d'un isomorphisme est aussi un isomorphisme.

**Proposition.** Soient  $(G_1, *_1)$ ,  $(G_2, *_2)$  et  $(G_3, *_3)$  trois groupes, et soient  $f : G_1 \rightarrow G_2$  et  $g : G_2 \rightarrow G_3$  deux morphismes. Alors  $g \circ f$  est un morphisme de groupes de  $G_1$  dans  $G_3$ .



En d'autres termes, quand elle est bien définie, une composée de morphismes est un morphisme.

DÉMONSTRATION. Soit  $(x, y) \in G_1^2$ .  $f$  étant un morphisme,  $f(x *_1 y) = f(x) *_2 f(y)$ .  $g$  étant un morphisme,

$$\begin{aligned} g \circ f(x *_1 y) &= g(f(x *_1 y)) \\ &= g(f(x) *_2 f(y)) \\ &= g(f(x)) *_3 g(f(y)) \\ &= g \circ f(x) *_3 g \circ f(y) \end{aligned}$$

**Corollaire.** La relation « être isomorphe » est une relation d'équivalence.

DÉMONSTRATION.

- Soit  $(G, *)$  un groupe. Alors  $\text{Id}_G$  est un isomorphisme de  $G$  dans lui-même donc  $G$  est isomorphe à lui-même : cette relation est réflexive.
- Soient  $(G_1, *_1)$  et  $(G_2, *_2)$  et supposons que  $G_1$  et  $G_2$  sont isomorphes. Soit  $f : G_1 \rightarrow G_2$  un isomorphisme. On a vu plus haut que  $f^{-1}$  est alors un isomorphisme de  $G_2$  dans  $G_1$  si bien que  $G_2$  et  $G_1$  sont isomorphes : cette relation est symétrique.
- Enfin, soient  $(G_1, *_1)$ ,  $(G_2, *_2)$  et  $(G_3, *_3)$  trois groupes, et on suppose que  $(G_1, *_1)$  et  $(G_2, *_2)$  sont isomorphes, ainsi que  $(G_2, *_2)$  et  $(G_3, *_3)$ . Si  $f$  est un isomorphisme de  $G_1$  dans  $G_2$  et  $g$  un isomorphisme de  $G_2$  dans  $G_3$ , alors  $g \circ f$  est un morphisme de  $G_1$  dans  $G_3$  et il est bijectif car composée de deux bijections, c'est donc un isomorphisme.  $G_1$  et  $G_3$  sont isomorphes : cette relation est transitive.

## IV.3 Noyau et image

### IV.3.a Image directe et réciproque d'un sous-groupe

**Proposition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupe.

- Si  $H$  est un sous-groupe de  $G_1$  alors  $f(H)$  est un sous-groupe de  $G_2$ , c'est-à-dire que l'image directe d'un sous-groupe de  $G_1$  est un sous-groupe de  $G_2$ .
- Si  $K$  est un sous-groupe de  $G_2$  alors  $f^{-1}(K)$  est un sous-groupe de  $G_1$ , c'est-à-dire que l'image réciproque d'un sous-groupe de  $G_2$  est un sous-groupe de  $G_1$ .

On rappelle que  $f^{-1}(K)$  est bien défini même si  $f$  n'est pas bijective ni injective.

DÉMONSTRATION. Soit  $H$  un sous-groupe de  $G_1$ .

- $e_1 \in H$  car  $H$  est un sous-groupe de  $G_1$  donc  $f(e_1) = e_2 \in f(H)$  :  $f(H)$  est non vide.
- Soit  $(y_1, y_2) \in f(H)^2$ . Il existe donc  $(x_1, x_2) \in H^2$  tel que  $f(x_1) = y_1$  et  $f(x_2) = y_2$ .

$$\begin{aligned} y_1 *_2 y_2 &= f(x_1) *_2 f(x_2) \\ &= f(x_1 *_1 x_2) \end{aligned} \quad \square$$

car  $f$  est un morphisme. Or,  $H$  est un sous-groupe de  $G_1$  donc est stable par la loi de  $G$  donc  $x_1 *_1 x_2 \in H$  si bien que  $y_1 *_2 y_2 \in f(H)$  :  $f(H)$  est stable par la loi de  $G_2$ .

- D'après ce qui précède,  $y_1^{-1} = f(x_1^{-1})$  et  $H$  est un sous-groupe de  $G_1$  donc  $x_1^{-1} \in H$  si bien que  $y_1^{-1} \in f(H)$  :  $f(H)$  est stable par inverse donc est un sous-groupe de  $G_2$ .

Soit à présent  $K$  un sous-groupe de  $G_2$ . Rappelons que  $f^{-1}(K) = \{x \in G_1 \mid f(x) \in K\}$ , c'est-à-dire que :  $x \in f^{-1}(K) \iff f(x) \in K$ .

- $f(e_1) = e_2 \in K$  car  $K$  est un sous-groupe de  $G_2$  donc  $K$  est non vide.
- Soit  $(x_1, x_2) \in f^{-1}(K)^2$ .  $f$  étant un morphisme,  $f(x_1 *_1 x_2) = f(x_1) *_2 f(x_2)$ . Or,  $x_1$  et  $x_2$  appartiennent à  $f^{-1}(K)$  donc  $f(x_1)$  et  $f(x_2)$  appartiennent à  $K$  qui est un sous-groupe de  $G_2$  donc est stable par la loi de  $G_2$ . Finalement,  $f(x_1) *_2 f(x_2) \in K$  donc  $x_1 *_1 x_2 \in f^{-1}(K)$  :  $f^{-1}(K)$  est stable par la loi de  $G_1$ .
- D'après ce qui précède,  $f(x_1^{-1}) = f(x_1)^{-1}$  et  $K$  est un sous-groupe de  $G_2$  donc  $f(x_1)^{-1} \in K$  si bien que  $x_1^{-1} \in f^{-1}(K)$  :  $f^{-1}(K)$  est stable par inverse donc est un sous-groupe de  $G_1$ .

**Remarque :** Un morphisme transporte donc la structure de groupe à l'arrivée ou au départ. Attention,  $f$  n'étant pas forcément bijective,  $f(H)$  n'est pas forcément isomorphe à  $H$  ni  $f^{-1}(K)$ , ce sont des groupes, certes, mais pas forcément « du même modèle » (cf. paragraphe IV.4.a). Par exemple, si  $f : G_1 \rightarrow G_2$  est constant égal à  $e_2$ , alors  $f(H) = \{e_2\}$  qui est bien un sous-groupe de  $G_2$ .

### IV.3.b Image

**Définition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. On note  $\text{Im}(f)$  et on appelle image de  $f$  l'ensemble  $f(G_1)$  i.e.  $\text{Im}(f) = \{f(x) \mid x \in G_1\}$ .

**Remarque :** Avec des quantificateurs,  $y \in \text{Im}(f) \iff \exists x \in G_1, y = f(x)$ .

**Proposition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. Alors  $\text{Im}(f)$  est un sous-groupe de  $G_2$ .

DÉMONSTRATION. Découle de la proposition précédente.

**Remarques :**

- $f$  est surjective si et seulement si  $\text{Im}(f) = G_2$ .
- Si  $f$  est injective, alors  $\text{Im}(f)$  est isomorphe à  $G_1$ .

### IV.3.c Noyau

C'est donc l'ensemble des images des éléments de  $G_1$  ou, ce qui revient au même, l'ensemble des éléments de  $G_2$  atteints par  $f$  ou qui admettent un antécédent par  $f$ .

**Définition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. On appelle noyau de  $f$ , noté  $\ker(f)$ , l'ensemble :

$$\ker(f) = \{x \in G_1 \mid f(x) = e_2\}$$

**Remarque :** En d'autres termes, c'est l'ensemble formé par les antécédents de  $e_2$  c'est-à-dire les éléments qui ont une image par  $f$  égale au neutre (du groupe d'arrivée).

**Proposition.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. Alors  $\ker(f)$  est un sous-groupe de  $G_1$ .

DÉMONSTRATION. Découle de la dernière proposition du paragraphe IV.3.a :  $\ker(f) = f^{-1}(\{e_2\})$  et  $\{e_2\}$  est un sous-groupe de  $G_2$ .

**Exemples :**

- $\ker(\ln) = \{1\}$ .
- Si on considère l'exponentielle comme un morphisme de  $\mathbb{R}$  dans  $\mathbb{R}_+^*$ , alors  $\ker(\exp) = \{0\}$ .
- Si on considère l'exponentielle comme un morphisme de  $\mathbb{C}$  dans  $\mathbb{C}^*$ , alors  $\ker(\exp) = 2i\pi\mathbb{Z}$ .
- Si on note  $f$  le morphisme  $x \mapsto e^{ix}$  de  $\mathbb{R}$  dans  $\mathbb{U}$ , alors  $\ker(f) = 2\pi\mathbb{Z}$ .

On a bien à chaque fois des sous-groupes du groupe de départ (le fait que  $2i\pi\mathbb{Z}$  est un sous-groupe de  $\mathbb{C}$  se démontre de façon analogue au fait que  $n\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$  si  $n \in \mathbb{Z}$  ou que  $\alpha\mathbb{Z}$  est un sous-groupe de  $\mathbb{R}$  si  $\alpha \in \mathbb{R}$ ).

**Théorème.** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes. Alors  $f$  est injective si et seulement si  $\ker(f) = \{e_1\}$ .

**Remarque :** En d'autres termes, un morphisme est injectif si et seulement si son noyau est réduit au neutre (du groupe de départ). Le neutre appartient toujours au noyau (c'est un sous-groupe), et le théorème précédent dit donc que c'est le seul élément du noyau si et seulement si le morphisme est injectif.

On a déjà vu dans des paragraphes précédents que la structure de groupe permettait de se ramener au voisinage du neutre (par exemple dans les paragraphes III.2 et III.3) : il est donc cohérent que la connaissance des antécédents du neutre permette de savoir si le morphisme est injectif ou non.

DÉMONSTRATION. Supposons  $f$  injective.  $e_2$  a donc au plus un antécédent. Or,  $e_1$  est un antécédent de  $e_2$  donc c'est le seul :  $\ker(f) = \{e_1\}$ .

Réciproquement, supposons que  $\ker(f) = \{e_1\}$ . Soit  $(x_1, x_2) \in G_1^2$  tel que  $f(x_1) = f(x_2)$ . Montrons que  $x_1 = x_2$ . On a  $f(x_1) *_2 f(x_2)^{-1} = e_2$ . Or,  $f$  est un morphisme donc  $f(x_1 *_1 x_2^{-1}) = e_2$  donc  $x_1 *_1 x_2^{-1} \in \ker(f) = \{e_1\}$ . Ainsi,  $x_1 *_1 x_2^{-1} = e_1$ . Finalement,  $x_1 = x_2$  donc  $f$  est injective.

**Remarque :** Comme on l'a déjà dit, un noyau est un groupe donc contient toujours le neutre. Ainsi, l'inclusion  $\{e_1\} \subset \ker(f)$  est toujours vraie. Par conséquent, lorsqu'on voudra montrer qu'un morphisme est injectif, on pourra se contenter de prouver que  $\ker(f) \subset \{e_1\}$  c'est-à-dire prendre un élément de  $\ker(f)$  et prouver qu'il est égal à  $e_1$  : l'inclusion réciproque étant toujours vraie, on pourra se dispenser de la prouver.

## IV.4 Bien comprendre la notion d'isomorphisme

### IV.4.a Groupes isomorphes = « mêmes modèles de groupes »

Rappelons les tables de l'addition sur  $\mathbb{Z}/3\mathbb{Z}$  et sur l'ensemble  $\{\text{chou}; \text{banane}; \text{carotte}\}$  :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

+	chou	banane	carotte
chou	chou	banane	carotte
banane	banane	carotte	chou
carotte	carotte	chou	banane

On voit qu'on a en fait la même table :

+	truc 1	truc 2	truc 3
truc 1	truc 1	truc 2	truc 3
truc 2	truc 2	truc 3	truc 1
truc 3	truc 3	truc 1	truc 2

avec, pour  $\mathbb{Z}/3\mathbb{Z}$ , truc 1 =  $\bar{0}$ , truc 2 =  $\bar{1}$  et truc 3 =  $\bar{2}$ , tandis que pour  $\{\text{chou; banane; carotte}\}$ , truc 1 = chou, truc 2 = banane et truc 3 = carotte. Donnons un autre exemple : ci-dessous les tables de  $(\mathbb{U}_4, \times)$  et  $(\mathbb{Z}/4\mathbb{Z}, +)$  :

$\times$	1	$i$	-1	$-i$
1	1	$i$	-1	$-i$
$i$	$i$	-1	$-i$	1
-1	-1	$-i$	1	$i$
$-i$	$-i$	1	$i$	-1

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Là encore, on la même table :

Loi	truc 1	truc 2	truc 3	truc 4
truc 1	truc 1	truc 2	truc 3	truc 4
truc 2	truc 2	truc 3	truc 4	truc 1
truc 3	truc 3	truc 4	truc 1	truc 2
truc 4	truc 4	truc 1	truc 2	truc 3

On peut retrouver cette table dans encore d'autres situations : si  $\theta \in \mathbb{R}$ , rappelons qu'on note  $r_\theta$  la rotation du plan de centre  $O$  d'angle  $\theta$ . Alors  $\{r_0; r_{\pi/2}; r_\pi; r_{3\pi/2}\}$  est stable par composition, et on peut dresser la table de la loi  $\circ$  :

On vérifie à l'aide de cette table que cela donne bien un groupe.

$\circ$	$r_0$	$r_{\pi/2}$	$r_\pi$	$r_{3\pi/2}$
$r_0$	$r_0$	$r_{\pi/2}$	$r_\pi$	$r_{3\pi/2}$
$r_{\pi/2}$	$r_{\pi/2}$	$r_\pi$	$r_{3\pi/2}$	$r_0$
$r_\pi$	$r_\pi$	$r_{3\pi/2}$	$r_0$	$r_{\pi/2}$
$r_{3\pi/2}$	$r_{3\pi/2}$	$r_0$	$r_{\pi/2}$	$r_\pi$

On se dit que ces trois groupes sont « les mêmes » et on cherche une façon rigoureuse de définir le fait que des groupes soient « les mêmes ». On se dit que pour que des groupes  $(G_1, *_1)$  et  $(G_2, *_2)$  soient les mêmes, il suffit qu'il existe une bijection entre  $G_1$  et  $G_2$ , et cela semble coller avec les exemples précédents puisque des ensembles à 3 éléments sont forcément en bijection, ainsi que des ensembles à 4 éléments. Cependant, l'exemple de  $(\mathbb{Z}/2\mathbb{Z})^2$  muni de l'addition nous prouve que cela ne suffit pas :

$+$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

On veut noter truc 1 =  $(\bar{0}, \bar{0})$  (le neutre), mais peu importe qui on note truc 2, truc 3 et truc 4 ici, on n'aura jamais une table comme celle ci-dessus. En effet, on aura toujours truc 2 + truc 2 = truc 1 et pareil pour truc 3 et truc 4. On est en présence ici d'un autre modèle de groupe, différent du modèle des groupes précédents dont on peut donner la table générale ci-dessous :

Loi	truc 1	truc 2	truc 3	truc 4
truc 1	truc 1	truc 2	truc 3	truc 4
truc 2	truc 2	truc 1	truc 4	truc 3
truc 3	truc 3	truc 4	truc 1	truc 2
truc 4	truc 4	truc 3	truc 2	truc 1

On peut montrer que  $\mathbb{Z}/4\mathbb{Z}$  et  $(\mathbb{Z}/2\mathbb{Z})^2$  ne sont pas isomorphes : cf. poly de botanique.

On peut retrouver ce modèle de groupe ailleurs. Par exemple, si on note  $i$  l'identité de  $\mathbb{R}^2$ ,  $s_x$  la symétrie du plan par rapport à l'axe des abscisses,  $s_y$  la symétrie par rapport à l'axe des ordonnées et  $s_O$  la symétrie par rapport à l'origine, alors  $\{i; s_x, s_y; s_O\}$  est stable par composition et on peut dresser la table de la loi  $\circ$

$\circ$	$i$	$s_x$	$s_y$	$s_O$
$i$	$i$	$s_x$	$s_y$	$s_O$
$s_x$	$s_x$	$i$	$s_O$	$s_y$
$s_y$	$s_y$	$s_O$	$i$	$s_x$
$s_O$	$s_O$	$s_y$	$s_x$	$i$

On voit que pour définir le concept de groupes qui sont les « mêmes », il faut tenir compte de la loi, car même avec des ensembles distincts, ce qui fait que des groupes sont « les mêmes », c'est leur loi. En fait, ce ne sont pas tellement les lois mais les tables des lois qui font que des groupes sont « les mêmes ». Il faut donc une bijection (sinon le cardinal n'est pas préservé) qui conserve la loi, ou plutôt la table de la loi, c'est-à-dire qui envoie la loi du premier sur la loi du deuxième : un isomorphisme.

En effet, deux groupes isomorphes ont la même table de loi (même si on ne représente effectivement cette table que lorsque le groupe est fini) :

$$f(x) *_2 f(y) = f(z) \iff f(x *_1 y) = f(z)$$

$$\iff x *_1 y = z$$

car  $f$  est injective. En d'autres termes,  $z$  se trouve à l'intersection de la ligne  $x$  et de la colonne  $y$  si et seulement si on trouve  $f(z)$  à l'intersection de la ligne  $f(x)$  et de la colonne  $f(y)$ . Il en découle que la table de  $G_2$  est obtenue à partir de celle de  $G_1$  en ajoutant  $f(\cdot)$  à toutes les cases : on a donc le même modèle de groupe, la même table (quitte à introduire des « trucs »). Et, réciproquement, deux groupes ayant la même table de loi sont isomorphes, il suffit de prendre la fonction qui envoie chaque élément de la première table sur l'élément correspondant de la deuxième table et on vérifie aisément que c'est un isomorphisme. Par exemple, la fonction  $f : \mathbb{U}_4 \rightarrow \mathbb{Z}/4\mathbb{Z}$  définie par  $f(1) = \bar{0}$ ,  $f(i) = \bar{1}$ ,  $f(-1) = \bar{2}$  et  $f(-i) = \bar{3}$  est bijective et c'est un morphisme car (par exemple) :

$$\begin{aligned} f(i \times -1) &= f(-i) \\ &= \bar{3} \\ &= \bar{1} + \bar{2} \\ &= f(i) + f(-1) \end{aligned}$$

Finalement, deux groupes sont « les mêmes », c'est-à-dire sont des cas particuliers du même modèle de groupe, lorsqu'ils sont isomorphes : les différents exemples du même modèle de groupe sont donc les différents éléments d'une même classe d'équivalence. C'est encore une fois l'idée sous-jacente d'une relation d'équivalence : les éléments d'une même classe d'équivalence ne comptent que pour un seul. Par exemple, quand nous verrons qu'il n'y a que deux classes d'équivalence parmi les groupes à quatre éléments, nous dirons qu'« il n'existe que deux groupes à quatre éléments à isomorphisme près », ou encore qu'il n'y a que deux modèles de groupes à 4 éléments : il suffira ensuite de donner un exemple de chaque modèle i.e. un exemple dans chaque classe d'équivalence.

#### IV.4.b Quelques exemples

**Exemple :** Les trois groupes  $(\mathbb{U}, \times)$ ,  $([0; 2\pi[, \oplus)$  et  $(R, \circ)$  (où  $R$  est l'ensemble des rotations de centre  $O$ ) sont isomorphes. En particulier, on peut les représenter de la même façon à l'aide du cercle unité :

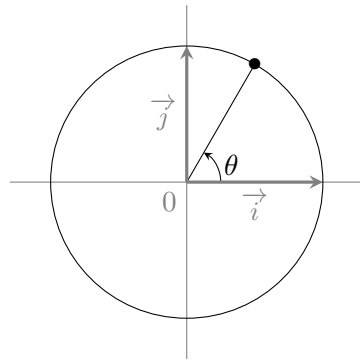
C'est une grande force de la théorie des groupes : ranger sous la même bannière des objets qui n'ont a priori rien à voir.

On vérifie aisément que c'est le cas pour tous  $x$  et  $y$  appartenant à  $\mathbb{U}_4$ .

On rappelle qu'être isomorphe est une relation d'équivalence.

Ou, ce qui revient au même, représenter l'un d'entre eux ou leur modèle de groupe commun.





Pour  $\mathbb{U}$ , on le sait déjà. Mais ça marche aussi pour  $[0; 2\pi[$  et pour  $R$  : une rotation de centre  $O$  est en effet totalement déterminée par la congruence modulo  $2\pi$  de son angle, et puisqu'on travaille modulo  $2\pi$ , on peut représenter  $[0; 2\pi[$  comme un cercle en « collant » les deux réels 0 et  $2\pi$  : si on parcourt  $[0; 2\pi[$ , quand on arrive à  $2\pi$ , on revient en 0 et on recommence, d'où l'intérêt de cette représentation en cercle. On voit bien que des groupes isomorphes sont « le même groupe » !

Donnons à présent quelques groupes non isomorphes. Pour montrer que des groupes  $G_1$  et  $G_2$  sont isomorphes, on donne un isomorphisme explicite (ou on constate qu'ils ont la même table de loi lorsque ce sont des groupes finis de petit cardinal), mais pour prouver qu'ils ne sont pas isomorphes, il n'y a pas unicité de la méthode. En général, on travaille par l'absurde, et on trouve une propriété vérifiée par l'un qui n'est pas vérifiée par l'autre, ce qui est absurde car les deux groupes sont « les mêmes ». À quelles propriétés peut-on s'intéresser ? À toutes celles ayant un rapport avec la structure de groupe. Dans tous les cas ci-dessous, ils ne sont pas isomorphes (la liste ci-dessous est non exhaustive) :

- L'un est commutatif et l'autre non. En effet, si  $G_1$  n'est pas commutatif alors que  $G_2$  l'est, ils ne peuvent pas être isomorphes. S'il existe  $f : G_1 \rightarrow G_2$  est un isomorphisme et si  $x$  et  $y$  sont tels que  $x *_1 y \neq y *_1 x$ , alors

$$\begin{aligned} f(x *_1 y) &= f(x) *_2 f(y) \\ &= f(y) *_2 f(x) \\ &= f(y *_1 x) \end{aligned}$$



$G_2$  est abélien.

et puisque  $f$  est injective, alors  $x *_1 y = y *_1 x$  ce qui est absurde.

- Ils n'ont pas le même cardinal : un isomorphisme étant une bijection, deux groupes isomorphes ont le même cardinal (réciproque fausse, voir ci-dessous).
- L'un a des sous-groupes d'un certain cardinal, et pas l'autre. En effet, s'il existe un isomorphisme  $f : G_1 \rightarrow G_2$  sont isomorphes et si  $H$  est un sous-groupe de  $G_1$ , alors  $f(H)$  est un sous-groupe de  $G_2$  et il a le même cardinal que  $H$ . Par exemple, si  $G_1$  a un sous-groupe de cardinal 12 et pas  $G_2$ , alors ils ne sont pas isomorphes.
- Ils n'ont pas le même nombre de sous-groupes, ou le même nombre de sous-groupes de même cardinal. Par exemple, si  $G_1$  a trois sous-groupes de cardinal 2 et  $G_2$  en a 4, alors ils ne sont pas isomorphes. D'après ce qui précède, s'il existe un isomorphisme  $f$  entre  $G_1$  et  $G_2$ , alors  $f$  envoie les sous-groupes de  $G_1$  à deux éléments sur des sous-groupes de  $G_2$  à deux éléments, et  $f^{-1}$  fait la même chose dans l'autre sens. En d'autres termes,  $f$  envoie exactement les sous-groupes de  $G_1$  à deux éléments sur les sous-groupes de  $G_2$  à deux éléments, et donc il doit y en avoir le même nombre.

Ces exemples se comprennent bien mais se présentent rarement à notre niveau, il y aurait une indication de l'énoncé. L'exemple le plus classique consiste à trouver une équation qui a un certain nombre de solutions dans un groupe et l'équation analogue à un autre nombre dans l'autre groupes. Il faut bien comprendre qu'un morphisme envoie une loi sur l'autre, et donc envoie une équation sur une autre. Si le morphisme est de plus bijectif, les deux équations doivent avoir le même nombre de solutions. Cette méthode générale permet de prouver facilement que certains groupes classiques ne sont pas isomorphes.

Montrons que  $(\mathbb{R}, +)$  et  $(\mathbb{R}^*, \times)$  ne sont pas isomorphes. Cela vient du fait que les deux équations  $2x = 0$  et  $x^2 = 1$  n'ont pas le même nombre de solutions. Il faut bien voir que c'est la même équation :  $x$  itéré deux fois (additivement ou multiplicativement) égal au neutre, et les deux groupes ne peuvent pas être isomorphes car l'une a une solution et l'autre deux. Montrons cela rigoureusement.

Supposons qu'il existe  $f : \mathbb{R} \rightarrow \mathbb{R}^*$  un isomorphisme. Soit  $x \in \mathbb{R}$ .  $f$  étant un isomorphisme,

$$\begin{aligned} 2x = 0 &\iff f(2x) = f(0) \\ &\iff f(x+x) = f(0) \\ &\iff f(x) \times f(x) = 1 \\ &\iff f(x)^2 = 1 \end{aligned}$$

$f$  est un morphisme de groupes.

$f$  étant bijective, il existe  $x_1 \neq x_2$  tels que  $f(x_1) = 1$  et  $f(x_2) = -1$  mais, d'après ce qui précède,  $x_1$  et  $x_2$  sont solutions de l'équation  $2x = 0$  donc  $x_1 = x_2 = 0$  ce qui est absurde : les deux groupes ne sont pas isomorphes.

cf. l'exercice 28 pour d'autres exemples.

## V Anneaux

### V.1 Définition et premiers exemples

**Définition.** Soit  $A$  un ensemble muni de deux lois internes  $+$  et  $\times$ . On dit que  $(A, +, \times)$  est un anneau si :

- $(A, +)$  est un groupe **commutatif**.
- $\times$  est associative et munie d'un élément neutre.
- $\times$  est distributive par rapport à  $+$ .

Si la loi  $\times$  est de plus commutative, l'anneau est dit commutatif.

Un anneau est donc forcément non vide.

On réserve l'adjectif abélien pour les groupes, cela n'a pas de sens de dire qu'un anneau est abélien.

#### Remarques :

- De la même façon qu'un groupe consiste en un ensemble et en une loi, un anneau consiste en un ensemble et en deux lois. Plus précisément, un anneau est un groupe abélien auquel on rajoute une loi (qui doit vérifier certaines propriétés vis-à-vis d'elle-même et de la première loi).
- De même qu'on parle parfois d'un groupe  $G$  en omettant la loi, on parlera parfois d'un anneau  $A$  en omettant les deux lois. Par défaut, la première loi est notée additivement (elle est toujours commutative) et la seconde est notée multiplicativement (elle n'est pas forcément commutative). On peut noter les lois autrement, par exemple on peut noter la première loi  $T$  et la deuxième  $\diamond$  ou le contraire, mais on ne notera jamais la première loi  $\times$  et la seconde  $+$ . L'intérêt de noter ces lois « comme sur  $\mathbb{Z}$  » est justement de travailler avec ces lois comme on le fait sur  $\mathbb{Z}$ .  $\mathbb{Z}$  est en effet l'archétype de l'anneau, même si c'est un anneau « gentil » car toutes les propriétés de  $\mathbb{Z}$  ne sont pas forcément vérifiées sur un anneau quelconque, comme la commutativité ou l'intégrité, voir plus bas.
- De même que pour un groupe multiplicatif, parfois on n'explicitera pas la seconde loi et on notera parfois  $ab$  au lieu de  $a * b$ . De plus, la première loi étant en général notée additivement et la seconde multiplicativement, on pourra dire qu'un ensemble est stable par somme pour dire qu'il est stable par la première loi, et stable par produit pour dire qu'il est stable par la deuxième loi. Nous dirons également que le produit est distributif par rapport à la somme pour dire que la deuxième loi est distributive par rapport à la première etc.
- De plus, les notations  $nx$  et  $x^n$  sont définies comme ci-dessus pour  $n \geq 0$ , la première notation concernant la première loi et la seconde notation la seconde loi.
- La loi  $+$  est par définition commutative mais la loi  $\times$  ne l'est pas forcément. Ainsi, quand nous dirons que deux éléments d'un anneau  $A$  commutent, cela voudra dire :

pour la loi  $\times$ . En d'autres termes, on dit que  $a$  et  $b$  commutent lorsque  $ab = ba$ , et un anneau est commutatif lorsque c'est le cas pour tous  $a$  et  $b$ .

- Dans certains sujets ou livres anciens, l'existence d'un neutre pour la deuxième loi n'apparaît pas dans la définition d'un anneau, et ce que nous appelons un anneau est appelé un anneau « unitaire ». Tout est affaire de convention : dans le programme de MP2I, tous les anneaux sont unitaires, et donc il y a forcément un neutre pour la deuxième loi. C'est comme ça et pas autrement.
- L'élément neutre de la loi  $+$  est en général noté  $0_A$  ou  $0$  s'il n'y a aucune ambiguïté, et l'élément neutre de la seconde loi est noté  $1_A$  ou  $1$  s'il n'y a aucune ambiguïté. Question : peut-on avoir  $0_A = 1_A$  ? Les deux neutres peuvent-ils être égaux ? Commençons par un résultat intermédiaire.

On note également  $A^* = A \setminus \{0_A\}$ .

**Proposition.** Soit  $A$  un anneau. L'élément neutre  $0_A$  pour la somme est absorbant, c'est-à-dire que :  $\forall a \in A, a \times 0_A = 0_A \times a = 0_A$ .

DÉMONSTRATION. Soit  $a \in A$ . La loi  $\times$  étant distributive par rapport à la loi  $+$  :

$$(0_A + 0_A) \times a = 0_A \times a + 0_A \times a$$

Or,  $0_A + 0_A = 0_A$  car  $0_A$  est le neutre pour l'addition, si bien que  $(0_A + 0_A) \times a = 0_A \times a$ . Finalement,

$$0_A \times a = 0_A \times a + 0_A \times a \quad \square$$

Tout élément d'un groupe étant régulier (rappelons que  $(A, +)$  est un groupe),  $0_A = 0_A \times a$ . L'autre égalité s'obtient de façon analogue.


**Corollaire.** Soit  $A$  un anneau. Alors  $0_A = 1_A$  si et seulement si  $A$  est un singleton.

DÉMONSTRATION. Si  $A$  est un singleton, tous ses éléments sont égaux donc  $0_A = 1_A$ . Réciproquement, supposons que  $0_A = 1_A$ . Soit  $a \in A$ .  $1_A$  étant le neutre du produit,  $a \times 1_A = a$  et  $0_A$  est absorbant donc  $a \times 0_A = 0_A$ . Or,  $0_A = 1_A$  si bien que  $a = 0_A$ . Finalement,  $A = \{0_A\}$ .

Dans la suite, nous nous donnons un anneau  $A$  dont les deux lois sont notées  $+$  et  $\times$ . Le cas où  $A$  n'a qu'un seul élément étant d'un intérêt limité, nous supposerons que  $A$  a au moins deux éléments, et donc les deux neutres sont distincts, c'est-à-dire que  $0_A \neq 1_A$ .

**Remarques :**

- La première loi étant notée additivement, si  $a \in A$ , le symétrique de  $a$  pour la loi  $+$  (qui existe puisque  $(A, +)$  est un groupe) sera noté  $-a$  et sera appelé l'opposé de  $a$ . Ainsi, on peut définir la notation  $na$  pour  $n < 0$  de la même façon que ci-dessus.
- Attention cependant :  $A$  n'est pas un groupe pour la loi  $\times$ , les éléments de  $A$  ne sont pas forcément inversibles pour la loi  $\times$  et donc la notation  $a^{-1}$  ou, plus généralement,  $a^n$  pour  $n < 0$ , n'ont pas forcément de sens dans un anneau quelconque. Nous parlerons plus longuement des inversibles dans un anneau dans le paragraphe VI.1.
- On sait que tout élément est régulier dans un groupe donc tout élément est régulier dans  $(A, +)$ , et puisque ce groupe est commutatif, on peut « simplifier » par un élément s'il est des deux côtés d'une égalité, même s'il n'est pas aux extrémités. De plus, si un élément  $a$  se trouve d'un côté mais pas de l'autre, en ajoutant  $-a$  des deux côtés, il « disparaît » là où il était et « réapparaît changé en  $-a$  » de l'autre côté. Comme lorsqu'on manie des réels !

- Le produit est distributif par rapport à la somme donc on peut distribuer mais on peut aussi faire le chemin à l'envers i.e. factoriser : par exemple,  $a(b + c) = ab + ac$  par distributivité, mais on peut aussi raisonner à l'envers et écrire :  $ab + ac = a(b + c)$ . En clair : on peut factoriser et développer un élément comme lorsqu'on travaille avec des réels.
-  Attention, quand il y a plusieurs termes, cela ne fonctionne plus aussi bien. Il n'y a aucun problème tant qu'on respecte le sens de la multiplication, par exemple  $(a_1 + a_2) \times (b_1 + b_2) = a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2$  ou plus généralement


$$\left( \sum_{i=1}^n a_i \right) \times \left( \sum_{j=1}^m b_j \right) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} a_i b_j$$

mais il faut faire attention que, lorsque l'anneau n'est pas commutatif, on ne peut pas forcément regrouper certains termes, comme par exemple  $ab$  et  $ba$ , comme on le fait sur  $\mathbb{R}$ . En particulier, les identités remarquables ne sont pas vraies sur un anneau, il faut une condition supplémentaire, cf. paragraphe V.2.b.


- En gros : un anneau est un ensemble dans lequel on peut « sommer », « soustraire » et « multiplier » mais pas forcément diviser ! Ça, ce sera dans un corps (cf. paragraphe VI). C'est pour cela qu'on dit qu'on peut travailler sur un anneau « comme sur  $\mathbb{Z}$  » ou que «  $\mathbb{Z}$  est l'archétype de l'anneau » (encore une fois, même si c'est un anneau « gentil ») alors que  $\mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$  sont aussi des anneaux : on peut diviser sur ces ensembles alors qu'on ne le peut pas sur  $\mathbb{Z}$ , et donc  $\mathbb{Z}$  est un meilleur représentant de la structure d'anneau que  $\mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$ .

### Exemples :

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$  sont des anneaux (commutatifs) munis des lois  $+$  et  $\times$ , mais  $\mathbb{N}$  n'est pas un anneau car  $(\mathbb{N}, +)$  n'est pas un groupe.
- $2\mathbb{Z}$  n'est pas un anneau car il n'a pas de neutre pour le produit.
- $(\mathbb{R}^{\mathbb{R}}, +, \circ)$  n'est pas un anneau car la composition n'est distributive par rapport à la somme qu'à droite. Cependant, quand nous manipulerons des applications linéaires au second semestre, alors on pourra munir  $F^E$  d'une structure d'anneau : cf. chapitre 29.
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$  est un anneau commutatif, tout comme  $(\mathbb{R}^{\mathbb{N}}, +, \times)$  et  $(\mathbb{C}^{\mathbb{N}}, +, \times)$ , les neutres pour la loi  $\times$  étant respectivement la fonction constante égale à 1 et la suite constante égale à 1.
- Plus généralement, si  $X$  est un ensemble quelconque et si  $A$  est un anneau, alors on peut munir  $A^X$  d'une structure d'anneau à l'aide de lois  $+$  et  $\times$  définies de façon analogue.
- Si  $E$  est un ensemble,  $\mathcal{P}(E)$  est un anneau quand on le munit de la différence symétrique et de l'intersection, cf. exercice 47.
- Si  $n \geq 2$ ,  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau : cf. paragraphe VI.4. La structure circulaire de  $\mathbb{Z}/n\mathbb{Z}$  explique le terme « anneau ».

**Remarque :**  Il existe des anneaux non commutatifs. Par exemple,  $\mathbb{H}$ , l'ensemble des quaternions (à ne pas confondre avec  $\mathbb{H}_8$ , cf. poly de botanique, même s'il y a un lien, cf. paragraphe VI.3) est un anneau non commutatif. Celui que nous utiliserons le plus souvent est l'anneau des matrices carrées,  $\mathcal{M}_n(\mathbb{K})$ , que l'on verra dans le chapitre 21. Nous verrons d'autres exemples en TD.

En particulier, si  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$  et si  $X$  est un ensemble, alors  $(\mathbb{K}^X, +)$  est un groupe abélien : cela (ainsi qu'une loi externe) nous permettra de munir  $K^X$  d'une structure de  $\mathbb{K}$ -espace vectoriel : cf. chapitre 28.

 Attention, dans le cas général,  $(A, +)$  n'a aucune raison d'être cyclique ou même monogène (cf. poly de botanique)! Voir les autres exemples ci-contre.

## V.2 Comme sur $\mathbb{Z}$ , vraiment ?

On a dit plus haut qu'on note par convention les lois d'un anneau  $+$  et  $\times$  pour pouvoir pouvoir travailler « comme sur  $\mathbb{Z}$  ». Cependant, dans un anneau quelconque, tout n'est pas toujours aussi simple. Nous allons voir dans ce paragraphe certaines propriétés des anneaux et voir dans quels cas ce qui est vrai sur  $\mathbb{Z}$  est vrai sur  $A$ .

## V.2.a Diviseurs de zéro et intégrité

**Définition.** Soit  $a \in A$ .

- On dit que  $a$  est un diviseur de zéro à gauche si  $a \neq 0$  et s'il existe  $b \neq 0$  tel que  $a \times b = 0$ .
- On dit que  $a$  est un diviseur de zéro à droite si  $a \neq 0$  et s'il existe  $b \neq 0$  tel que  $b \times a = 0$ .
- On dit que  $a$  est un diviseur de zéro si  $a$  est un diviseur de 0 à gauche ou à droite.

On note dans la suite 0 le neutre de  $A$  pour la loi  $+$  c'est-à-dire  $0_A$ .

Un diviseur de zéro (à gauche, à droite ou tout court) est non nul par définition.

**Remarque :** La négation de «  $a$  est un diviseur de zéro à gauche » est :

$$(a = 0) \text{ ou } (\forall b \neq 0, a \times b \neq 0)$$

et de même à droite.

Les diviseurs de zéro seront fréquents quand nous verrons les matrices, mais il existe des situations très simples où on rencontre des diviseurs de zéro.

**Exemples :**

- Sur  $(\mathbb{R}^{\mathbb{R}}, +, \times)$ , les diviseurs de zéro sont exactement les fonctions qui s'annulent (différentes de la fonction nulle). En effet, si  $f$  est une fonction non nulle qui s'annule, alors en posant

$$g : \begin{cases} \mathbb{R} & \longrightarrow \mathbb{R} \\ x & \longmapsto \begin{cases} 0 & \text{si } f(x) \neq 0 \\ 1 & \text{si } f(x) = 0 \end{cases} \end{cases}$$

c'est-à-dire que  $g$  est l'indicatrice de l'ensemble des points où  $f$  ne s'annule pas. Il vient :  $f \times g = 0$  car, pour tout  $x$ , soit  $f(x) = 0$ , soit  $f(x) \neq 0$  mais alors  $g(x) = 0$ . De plus,  $f$  est non nulle et  $g$  également (puisque  $f$  s'annule, il existe  $x$  tel que  $f(x) = 0$  et donc tel que  $g(x) \neq 0$ ) donc  $f$  est bien un diviseur de zéro.

Réciproquement, si  $f$  est une fonction qui ne s'annule pas, soit  $g$  une fonction non nulle. Il existe  $x$  tel que  $g(x) \neq 0$  et  $f$  ne s'annule pas donc  $f(x) \neq 0$  si bien que  $f(x) \times g(x) \neq 0$  :  $f \times g$  n'est pas la fonction nulle,  $f$  n'est pas un diviseur de 0.

- Idem, sur  $(\mathbb{R}^{\mathbb{N}}, +, \times)$ , les diviseurs de zéro sont exactement les suites qui s'annulent (différentes de la suite nulle).
- Dans  $\mathbb{Z}/6\mathbb{Z}$ ,  $\bar{2}$  et  $\bar{3}$  sont des diviseurs de zéro car  $\bar{2} \times \bar{3} = \bar{0}$ . Nous étudierons plus en détail les diviseurs de zéro de  $\mathbb{Z}/n\mathbb{Z}$  dans l'exercice 67.

L'anneau étant ici commutatif, un élément est un diviseur de zéro si et seulement si c'est un diviseur de zéro à gauche ou à droite.

**Morale de l'histoire :** Dans un anneau quelconque, il est faux de dire « un produit de facteurs est nul si et seulement si l'un au moins des facteurs est nul ». En effet, un produit de facteurs non nuls peut être nul s'il existe des diviseurs de 0 ! On voit donc que ce qui est vrai sur  $\mathbb{Z}$  n'est pas vrai sur un anneau quelconque, et l'analogie d'un anneau avec  $\mathbb{Z}$  est à manipuler avec prudence. Les anneaux sur lesquels cette propriété est vraie sont dits intègres. Plus précisément :

**Définition.** Un anneau est intègre s'il n'admet pas de diviseur de 0.

**Remarque :** En d'autres termes,  $A$  est un anneau intègre si le produit de deux éléments non nuls est non nul i.e. :

$$\forall (a, b) \in A^2, (a \neq 0 \text{ et } b \neq 0) \Rightarrow ab \neq 0$$

Ou, ce qui revient au même, par contraposée :

$$\forall (a, b) \in A^2, ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$$

En clair : un anneau est intègre lorsque la phrase « un produit de facteurs est nul si et seulement si l'un au moins des facteurs est nul » est vraie.

**Exemple :**  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$  sont des anneaux intègres,  $\mathcal{P}(E)$  et  $\mathcal{P}_f(E)$  sont aussi intègres (cf. exercice 47) mais, comme on l'a déjà vu,  $\mathbb{R}^{\mathbb{R}}$  et  $\mathbb{R}^{\mathbb{N}}$  ne le sont pas.

**Proposition.** Dans un anneau **intègre**, tout élément différent de 0 est régulier (à gauche et à droite), c'est-à-dire que si  $A$  est un anneau :

$$\forall (a, b, c) \in A^* \times A^2, ab = ac \Rightarrow b = c$$

et idem à droite.

**DÉMONSTRATION.** Soit  $(a, b, c) \in A^* \times A^2$  et supposons que  $ab = ac$ . Alors  $ab - ac = 0$  donc  $a(b - c) = 0$  (rappelons qu'on peut factoriser puisque le produit est distributif par rapport à la somme). Or,  $A$  est intègre et  $a$  est non nul donc  $b - c = 0$ .

**Remarque :** Dans un anneau intègre, seuls les éléments non nuls qui ne sont pas des diviseurs de zéro sont réguliers (démonstration analogue).

**Remarque :** En d'autres termes, cela signifie qu'on peut « simplifier » par tout élément non nul dans un anneau intègre. Attention :

- $A$  n'étant pas forcément commutatif, si on a une égalité du type  $ab = ca$ , on ne peut pas en déduire que  $b = c$ .
- la régularité de  $a$  (non nul) ne provient pas de l'existence d'un inverse par lequel on multiplierait mais du fait que  $A$  est intègre. Par conséquent, pour ne pas risquer de faire apparaître des inverses qui n'existent pas forcément et pour ne pas risquer d'utiliser le caractère commutatif de  $A$  quand ce n'est pas le cas, il est conseillé de refaire la démonstration quand on utilisera ce résultat.

Régulier pour le produit : on sait déjà que tout élément est régulier pour la somme puisque  $(A, +)$  est un groupe, et puisqu'il est commutatif, on peut « barrer sauvagement ».

## V.2.b Identités remarquables et binôme de Newton

On a vu plus haut qu'on pouvait développer et factoriser mais attention, si l'anneau n'est pas commutatif, on ne peut pas intervertir les termes, ce qu'on fait sur  $\mathbb{Z}, \mathbb{R}$  etc. sans même y penser. Par exemple, en général, si  $a$  et  $b$  appartiennent à  $A$ ,  $(ab)^2 \neq a^2b^2$  ! En effet,  $(ab)^2 = abab$  et  $a^2b^2 = aabb$ . Or, si  $a$  et  $b$  ne commutent pas, on n'a pas forcément  $abab = aabb$  ! Plus généralement, on n'a pas forcément  $(ab)^k = a^kb^k$  lorsque  $k \in \mathbb{N}$  ! En effet :

$$(ab)^k = \underbrace{ab \times ab \times \cdots \times ab}_{k \text{ fois}} \quad \text{et} \quad a^kb^k = \underbrace{a \times \cdots \times a}_{k \text{ fois}} \times \underbrace{b \times \cdots \times b}_{k \text{ fois}}$$

et ces deux quantités n'ont aucune raison d'être égales. De la même façon, les identités remarquables ou (ce qui revient au même) la formule du binôme de Newton ou la formule de factorisation de  $a^n - b^n$  ne se généralisent pas sans prendre de gants. Sans hypothèse supplémentaire, tout ce qu'on peut affirmer est que

$$\begin{aligned} (a+b)^2 &= (a+b) \times (a+b) \\ &= a^2 + ab + ba + b^2 \end{aligned}$$

mais  $ab \neq ba$  en général donc on ne peut pas simplifier. De même, sans hypothèse supplémentaire, tout ce qu'on peut affirmer est que

De même,  $(a+b)^3 = (a+b)(a+b)(a+b)$  et, par distributivité du produit sur la somme, on obtient (exo) que  $(a+b)^3 = a^3 + a^2b + aba + ab^2 + ba^2 + bab + b^2a + b^3$  et on ne peut pas faire mieux ! Morale de l'histoire : on peut toujours développer, mais si les éléments ne commutent pas, c'est gore...

$$(a + b) \times (a - b) = a^2 - ab + ba - b^2$$

et on ne peut pas aller plus loin sans hypothèse supplémentaire. En clair : on peut développer  $(a + b)^2$  et plus généralement  $(a + b)^k$  et  $(a - b) \times (a - b)$ , mais on ne peut pas regrouper les termes donc les formules bien connues ne sont pas valables sans une hypothèse supplémentaire : le fait que les éléments commutent.

**Lemme.** Soient  $a$  et  $b$  deux éléments de  $A$  qui commutent. Alors, pour tout  $k \in \mathbb{N}$ ,  $a$  et  $b^k$  commutent.

DÉMONSTRATION. Par récurrence sur  $k$ .

- Pour tout  $k \in \mathbb{N}$ , notons  $H_k$  : «  $ab^k = b^ka$  ».
- $b^0 = 1_A$  et le neutre commute avec tout élément de  $A$  commute avec le neutre donc  $H_0$  est vraie.
- Soit  $k \in \mathbb{N}$ . Supposons  $H_k$  vraie et prouvons que  $H_{k+1}$  est vraie. On a  $ab^{k+1} = ab^kb$ . Par hypothèse de récurrence,  $ab^{k+1} = b^kab$  et, puisque  $a$  et  $b$  commutent,  $ab^{k+1} = b^kba = b^{k+1}a$  :  $H_{k+1}$  est vraie.
- D'après le principe de récurrence,  $H_k$  est vraie pour tout  $k \in \mathbb{N}$ . □

**Remarque :** Plus généralement, toute puissance de  $a$  commute avec toute puissance de  $b$ .

**Proposition.** Soient  $a$  et  $b$  dans  $\mathcal{M}_n(\mathbb{K})$  qui commutent. Alors, pour tout  $k \in \mathbb{N}$ ,  $(ab)^k = a^kb^k$ .

Il suffit d'appliquer ce lemme avec  $\ell \in \mathbb{N}$ ,  $b$  et  $a^\ell$  (au lieu de  $k$ ,  $b$  et  $a$ ).

DÉMONSTRATION.

↔ EXERCICE.

**Proposition (formule du binôme de Newton).** Soient  $a$  et  $b$  deux éléments de  $A$  qui commutent. Alors, pour tout  $n \in \mathbb{N}$ ,

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

Comme dit ci-dessus, l'hypothèse que  $a$  et  $b$  commutent est indispensable.

DÉMONSTRATION. DÉMONSTRATION. Par récurrence sur  $n \in \mathbb{N}$ .

- *Initialisation* : Nous avons :

$$\begin{aligned} \sum_{k=0}^0 \binom{0}{k} a^k b^{0-k} &= 1_A \\ &= (a + b)^0 \end{aligned}$$

donc la formule est vraie au rang 0.

- *Hérédité* : Soit  $n \in \mathbb{N}$ . Supposons que la formule soit vraie au rang  $n$ . Alors,  $(a + b)^{n+1} = (a + b)^n \times (a + b)$  et, par hypothèse de récurrence,

$$\begin{aligned} (a + b)^{n+1} &= \left( \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \right) \times (a + b) \\ &= \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} a + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \end{aligned}$$

Or,  $a$  et  $b$  commutent donc, d'après le lemme ci-dessus,

Par distributivité (à droite) du produit sur la somme.



$$\begin{aligned}
(a+b)^{n+1} &= \sum_{k=0}^n \binom{n}{k} a^k a b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1}
\end{aligned}$$

Le reste de la démonstration est analogue au cas réel (en se souvenant que  $a^0$  et  $b^0$  sont égaux à  $1_A$ ) : exo. □

**Théorème.** Soient  $n \in \mathbb{N}^*$  et  $(a, b) \in A^2$  qui **commutent**. Alors :

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

DÉMONSTRATION. Par distributivité (à gauche) du produit sur la somme,

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

Or,  $a$  et  $b$  commutent : par symétrie des rôles, le lemme permet également d'affirmer que, pour tout  $k$ ,  $b$  et  $a^k$  commutent si bien que

$$\begin{aligned}
(a - b) \times \left( \sum_{k=0}^{n-1} a^k b^{n-1-k} \right) &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b b^{n-1-k} \\
&= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k}
\end{aligned}$$

Le reste de la preuve est analogue au cas réel. □

**Corollaire.** Soient  $n \in \mathbb{N}^*$  et  $a \in A$ . Alors :

$$1_A - a^n = (1_A - a) \times \sum_{k=0}^{n-1} a^k$$

DÉMONSTRATION. Immédiat puisque  $1_A$  et  $a$  commutent.

Nous donnerons une application de ce résultat dans le paragraphe VI.1.

### V.2.c Éléments nilpotents

**Définition.** Soit  $a \in A$ . On dit que  $a$  est nilpotent s'il existe  $n \in \mathbb{N}$  tel que  $a^n = 0_A$ . Le plus petit entier  $n$  qui vérifie cette condition est appelé l'indice de nilpotence de  $a$ .

**Exemple :**  $\bar{2}$  est nilpotent dans  $\mathbb{Z}/4\mathbb{Z}$  car  $\bar{2}^2 = \bar{0}$ . Nous verrons de nombreux exemples d'éléments nilpotents dans le chapitre 21 et au second semestre.

**Remarque :**  $0_A$  est toujours nilpotent (d'indice 1) et, si l'anneau est intègre, c'est le seul. En effet, un élément nilpotent non nul est un diviseur de zéro car, si  $a$  est nilpotent non nul d'indice  $n$ ,  $a \times a^{n-1} = 0_A$  avec  $a$  et  $a^{n-1}$  non nuls donc  $a$  est bien un diviseur de zéro. Attention, la réciproque est fautive : un diviseur de zéro quelconque n'est pas forcément un élément nilpotent. Par exemple,  $\bar{2}$  est un diviseur de zéro dans  $\mathbb{Z}/6\mathbb{Z}$  mais n'est pas un élément nilpotent puisque, pour tout  $k \in \mathbb{N}$ ,  $\bar{2}^k \neq \bar{0}$  puisque  $2^k$  n'est pas divisible par 6.

Ce plus petit entier existe car l'ensemble  $\{k \in \mathbb{N} \mid a^k = 0_A\}$  est une partie non vide (car  $a$  nilpotent) de  $\mathbb{N}$  donc admet un plus petit élément.

**Proposition.** Soit  $a \in A$  nilpotent d'indice  $n$ . Alors :  $\forall k \geq n, a^k = 0_A$ .

DÉMONSTRATION. Soit  $k \geq n$ . Alors

$$\begin{aligned} a^k &= a^n \times a^{k-n} \\ &= 0_A \times a^{k-n} \\ &= 0_A \end{aligned}$$

□

car  $0_A$  est absorbant.

**Proposition.** Soient  $a_1$  et  $a_2$  deux éléments de  $A$  nilpotents qui **commutent**. Alors  $a_1 \times a_2$  est nilpotent.

DÉMONSTRATION. Notons  $n_1$  l'indice de nilpotence de  $a_1$  et  $n_2$  celui de  $a_2$ . Soit  $n = \min(n_1, n_2)$ . Puisque  $a_1$  et  $a_2$  commutent, alors :  $(a_1 \times a_2)^n = a_1^n \times a_2^n$ . Or,  $n = n_1$  ou  $n = n_2$  donc  $a_1^n = 0$  ou  $a_2^n = 0$  donc  $(a_1 \times a_2)^n = 0$ .

On note 0 au lieu de  $0_A$  car il n'y a aucune ambiguïté.

**Remarque :** ⚠ C'est faux si les deux éléments ne commutent pas ! Nous verrons un contre-exemple dans le chapitre 21.

**Proposition.** Soient  $a_1$  et  $a_2$  deux éléments de  $A$  nilpotents qui **commutent**. Alors  $a_1 + a_2$  est nilpotent.

DÉMONSTRATION. Notons  $n_1$  l'indice de nilpotence de  $a_1$  et  $n_2$  celui de  $a_2$ . Montrons que  $(a_1 + a_2)^{n_1+n_2-1} = 0$ .  $a_1$  et  $a_2$  commutent donc, d'après le binôme de Newton :

$$(a_1 + a_2)^{n_1+n_2-1} = \sum_{k=0}^{n_1+n_2-1} \binom{n_1+n_2-1}{k} a_1^k \times a_2^{n_1+n_2-1-k}$$

□

Résultat classique mais HP : à savoir redémontrer !

Soit  $k \in \llbracket 0; n_1 + n_2 - 1 \rrbracket$ .

- Si  $k \geq n_1$  alors  $a_1^k = 0$ .
- Si  $k < n_1$  alors  $n_1 + n_2 - 1 - k > n_2 - 1$  donc  $n_1 + n_2 - 1 - k \geq n_2$ . En particulier,  $a_2^{n_1+n_2-1-k} = 0$ .

Finalement, tous les termes de la somme sont nuls :  $(a_1 + a_2)^{n_1+n_2-1} = 0$ ,  $a_1 + a_2$  est bien nilpotent.

**Remarque :** ⚠ C'est faux si les deux éléments ne commutent pas ! Nous verrons encore un contre-exemple dans le chapitre 21.

### V.3 Sous-anneaux

**Définition.** Soit  $B$  une partie de  $A$ .  $B$  est un sous-anneau de  $A$  si

- $B$  est stable par les lois  $+$  et  $\times$ .
- ⚠  $1_A \in B$ .
- $(B, +, \times)$  est un anneau.

En d'autres termes, un sous-anneau de  $A$  est un anneau inclus dans  $A$  pour les mêmes lois et les mêmes neutres que  $A$ .

**Remarques :**

- ⚠ Disons-le tout de suite : il est possible que  $B$  admette un élément neutre  $1_B$  pour la loi  $\times$  différent de  $1_A$  et tel que  $(B, +, \times)$  soit un anneau inclus dans  $A$ , mais alors  $B$  n'est pas un sous-anneau de  $A$ . Par exemple,  $\{0_A\}$  est un anneau inclus dans  $A$  mais n'est pas un sous-anneau de  $A$ .

La raison profonde est qu'être le neutre pour tous les éléments de  $B$ , c'est-à-dire

$$\forall b \in B, e \times b = b \times e = b$$

est une condition plus faible qu'être le neutre pour tous les éléments de  $A$  : il peut donc y avoir un neutre différent (mais ce n'est pas le cas si  $1_A \in B$  par unicité du neutre).

- Donnons un exemple moins trivial : notons  $B$  l'ensemble des fonctions de  $\mathbb{R}$  dans  $\mathbb{R}$  nulles sur  $\mathbb{R}_+^*$ . Alors on montre facilement que  $B$  est stable par somme et par produit et que  $(B, +, \times)$  est un anneau mais que le neutre pour le produit est la fonction indicatrice de  $\mathbb{R}_-$  c'est-à-dire la fonction nulle sur  $\mathbb{R}_+^*$  et égale à 1 sur  $\mathbb{R}_-$  : on a un ensemble inclus dans un autre qui est un anneau pour les mêmes lois, mais le neutre pour le produit n'est pas le même donc  $B$  n'est pas un sous-anneau de  $\mathbb{R}^{\mathbb{R}}$ . L'appartenance du neutre pour la deuxième loi n'est pas automatique !
- Par contre, si  $B$  est un sous-anneau de  $A$ , alors en particulier  $B$  est un sous-groupe de  $(A, +)$  donc  $0_A \in B$  et est le neutre de  $B$ . Ainsi, c'est au neutre de la multiplication qu'il faut faire attention, le neutre de l'addition est automatiquement le neutre de  $B$ .
- La définition est en fait analogue à la définition de sous-groupe et peut être généralisée à encore d'autres structures : si  $E$  est muni d'une structure de truc, une partie  $F$  de  $E$  est munie d'une structure de sous-truc si  $F$  est stable par toutes les lois qui font de  $E$  un truc et si  $F$ , muni des mêmes lois **et des mêmes neutres** que  $E$ , a aussi une structure de truc. L'appartenance du neutre ne figure pas dans la définition d'un sous-groupe car elle est automatique, mais ce n'est pas le cas pour un sous-anneau, d'où le fait qu'elle figure dans la définition ici. Ce sera la même chose avec les sous-corps, cf. paragraphe VI.2.

### Exemples :

- $\mathbb{Z}$  est un sous-anneau de  $\mathbb{Q}$  qui est lui-même un sous-anneau de  $\mathbb{R}$  qui est lui-même un sous-anneau de  $\mathbb{C}$ .
- Comme dit ci-dessus, un sous anneau de  $A$  est un sous-groupe de  $(A, +)$  mais la réciproque est fautive. Par exemple,  $\mathbb{Z}$  est le seul sous-anneau de  $\mathbb{Z}$  : les seuls sous-groupes de  $\mathbb{Z}$  sont les  $n\mathbb{Z}$  mais le seul  $n\mathbb{Z}$  contenant 1 est  $\mathbb{Z}$  lui-même. En d'autres termes,  $\mathbb{Z}$  est le seul sous-anneau éventuel de  $\mathbb{Z}$ , et c'est évidemment un sous-anneau de  $\mathbb{Z}$ , d'où le résultat.

Plus généralement,  $A$  est toujours un sous-anneau de  $A$ .

**Proposition.** Soit  $B$  une partie de  $A$ .  $B$  est un sous-anneau de  $A$  si et seulement si :

- $B$  est un sous-groupe de  $A$ .
- $1_A \in B$ .
- $B$  est stable par produit.

**Remarque :** On peut utiliser la caractérisation des sous-groupes vue dans le paragraphe II.3. Par conséquent, on peut remplacer la première condition par «  $B$  est stable par comme et par passage à l'opposé », c'est-à-dire :

$$\forall (a, b) \in B^2, a + b \in B \quad \text{et} \quad \forall a \in B, -a \in B$$

ou «  $B$  est stable par différence », c'est-à-dire :

$$\forall (a, b) \in B^2, a - b \in B$$

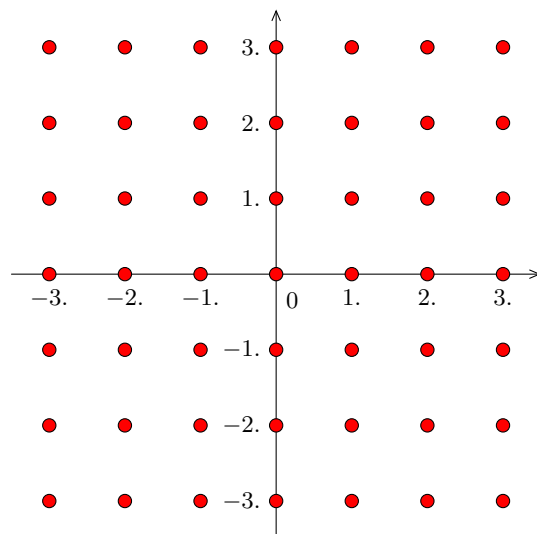
**DÉMONSTRATION.** Le sens direct est immédiat. Pour la réciproque, il ne manque que l'associativité de la loi  $\times$  et la distributivité de la loi  $\times$  par rapport à la loi  $+$ , qui sont automatiques car ces propriétés sont vraies sur  $A$ .

### Exemples :

- Notons  $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$ . Montrons que  $\mathbb{Z}[i]$  est un sous-anneau de  $\mathbb{C}$ .
  - ★ Soit  $(z_1, z_2) \in \mathbb{Z}[i]^2$ . Il existe alors  $(a_1, b_1, a_2, b_2) \in \mathbb{Z}^4$  tel que  $z_1 = a_1 + ib_1$  et  $z_2 = a_2 + ib_2$  si bien que  $z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2)$  et  $-z_1 = -a_1 + i(-b_1)$ . Or,  $a_1 + a_2, b_1 + b_2, -a_1$  et  $-b_1$  appartiennent à  $\mathbb{Z}$  donc  $z_1 + z_2$  et  $-z_1$  appartiennent à  $\mathbb{Z}[i]$  qui est donc stable par somme et par passage à l'opposé.

★  $1 = 1 + 0 \times i \in \mathbb{Z}[i]$ .

★ Enfin,  $z_1 \times z_2 = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$  et  $a_1a_2 - b_1b_2$  et  $a_1b_2 + a_2b_1$  appartiennent à  $\mathbb{Z}$  donc  $z_1 \times z_2$  appartient à  $\mathbb{Z}[i]$  qui est donc stable par produit : c'est bien un sous-anneau de  $\mathbb{C}$ , c'est l'ensemble des complexes ayant une abscisse et une ordonnée entières, qu'on a représenté ci-dessous.



- Montrons que  $\mathcal{C}(\mathbb{R}, \mathbb{R})$  est un sous-anneau de  $\mathbb{R}^{\mathbb{R}}$ .


La fonction constante égale à 1 appartient à  $\mathcal{C}(\mathbb{R}, \mathbb{R})$  et cet ensemble est stable par différence et par produit car une différence et un produit de fonctions continues sont continus donc  $\mathcal{C}(\mathbb{R}, \mathbb{R})$  est bien un sous-anneau de  $\mathbb{R}^{\mathbb{R}}$ .

## V.4 Morphismes d'anneaux

On se donne dans ce paragraphe deux anneaux  $(A_1, +_1, \times_1)$  et  $(A_2, +_2, \times_2)$ .

### V.4.a Définition et propriétés

**Définition.** Soit  $f : A_1 \rightarrow A_2$ . On dit que  $f$  est un morphisme d'anneaux si :

- $\forall (a, b) \in A_1^2, f(a +_1 b) = f(a) +_2 f(b)$ .
- $\forall (a, b) \in A_1^2, f(a \times_1 b) = f(a) \times_2 f(b)$ .
-   $f(1_{A_1}) = 1_{A_2}$ .

Si  $f$  est de plus bijective, on dit que  $f$  est un isomorphisme (d'anneaux) et on dit que les anneaux  $A_1$  et  $A_2$  sont isomorphes.

#### Remarques :

- En d'autres termes, un morphisme d'anneau est une fonction compatible avec les deux lois (i.e. on peut « casser et sortir les lois de  $A_1$  en les changeant en les lois correspondantes de  $A_2$  ») et qui envoie le neutre de la deuxième loi de  $A_1$  sur le neutre de la deuxième loi de  $A_2$ .
- En effet, contrairement au cas d'un morphisme de groupes, ce n'est pas automatique. Par exemple, la fonction constante  $a \mapsto 0_{A_2}$  est compatible avec les lois mais n'envoie pas  $1_{A_1}$  sur  $1_{A_2}$ . Il est donc indispensable de rajouter cette condition.
- Comme pour les sous-anneaux, cette définition peut être généralisée à d'autres structures : si  $E_1$  et  $E_2$  sont munis d'une structure de truc, une fonction  $f : E_1 \rightarrow E_2$  est appelée un morphisme de trucs si  $f$  est compatible pour toutes les lois et si  $f$  envoie tous les neutres de  $E_1$  sur les neutres correspondants de  $E_2$ . La condition concernant le neutre ne figure pas dans la définition de morphisme de groupe car elle est automatique, ce qui n'est pas le cas pour un morphisme d'anneau, d'où le fait qu'elle figure dans la définition ici.

- Un morphisme d'anneaux est un morphisme de groupes entre  $(A_1, +_1)$  et  $(A_2, +_2)$ . Les propriétés suivantes découlent donc directement du paragraphe IV.2.

**Proposition.** Soit  $f : A_1 \rightarrow A_2$  un morphisme d'anneaux.




- $f(0_{A_1}) = 0_{A_2}$ .
- $\forall a \in A, \forall n \in \mathbb{Z}, f(na) = nf(a)$ .
- $\ker(f)$  (dont on rappelle qu'il est défini par :  $\ker(f) = \{a \in A \mid f(a) = 0_{A_2}\}$ ) est un sous-groupe de  $(A_1, +)$ .
- $f$  est injective si et seulement si  $\ker(f) = \{0_{A_1}\}$ .

Les propriétés suivantes sont, elles, relatives à la structure d'anneau de  $A_1$  et de  $A_2$  et se démontrent de façon analogue aux propriétés des morphismes de groupes : exo.

**Proposition.** Soit  $f : A_1 \rightarrow A_2$  un morphisme d'anneaux.

- $\forall a \in A, \forall n \in \mathbb{N}, f(a^n) = f(a)^n$ .
- Si  $f$  est bijective alors  $f^{-1}$  est un morphisme d'anneaux.
- Lorsqu'elle est bien définie, une composée de morphismes d'anneaux est un morphisme d'anneaux.
- La relation « être isomorphe » est une relation d'équivalence.
- L'image directe d'un sous-anneau de  $A_1$  par  $f$  est un sous-anneau de  $A_2$ .
- L'image réciproque d'un sous-anneau de  $A_2$  par  $f$  (même si  $f$  n'est pas bijective) est un sous-anneau de  $A_1$ .
- L'image de  $f$  (toujours définie par  $\text{Im}(f) = f(A_1)$ ) est donc un sous-anneau de  $A_2$ .

**Remarques :**

-  Les éléments de  $A$  ne sont pas forcément inversibles pour la loi  $\times$ , cela n'a donc pas de sens d'écrire  $a^n$  avec  $n < 0$ . Cependant, lorsque  $a$  est inversible, alors l'égalité  $f(a^n) = f(a)^n$  est vraie même lorsque  $n$  est négatif, cf. paragraphe VI.1.
-   $\ker(f)$  n'est pas forcément un sous-anneau de  $A_1$  ! En effet,  $\{0_{A_2}\}$  n'est pas un sous-anneau de  $A_2$  donc le noyau de  $f$ , son image réciproque, n'a aucune raison d'en être un : cf. paragraphe suivant.
-  Il faut bien comprendre que, même si un morphisme d'anneaux est un morphisme de groupes, un morphisme d'anneaux vérifie deux conditions supplémentaires. Ainsi, une application  $f : A_1 \rightarrow A_2$  peut être un isomorphisme de groupes, i.e. un morphisme bijectif entre les groupes  $(A_1, +_1)$  et  $(A_2, +_2)$ , sans être un isomorphisme d'anneaux car l'une des deux autres propriétés n'est pas vérifiées. En d'autres termes, deux anneaux peuvent être isomorphes en tant que groupes sans l'être en tant qu'anneaux (par exemple lorsque l'un est commutatif et pas l'autre), mais ce cas de figure est assez rare en pratique.

Plus fort : ce n'est **jamais** un sous-anneau de  $A_1$  dès que  $A_2$  a au moins deux éléments, cf. exercice 48. Le noyau d'un morphisme d'anneaux a tout de même une structure plus riche qu'une structure de groupe : c'est ce qu'on appelle un idéal, cf. exercice 64.

## V.4.b Exemples

**Exemples :**

- Si  $A$  est un anneau, alors  $\text{Id}_A$  est un isomorphisme d'anneaux.
- Si  $A$  est un anneau et  $B$  un sous-anneau de  $A$ , alors l'injection canonique est un morphisme d'anneau injectif de  $B$  dans  $A$ .
- La conjugaison est un isomorphisme d'anneaux de  $\mathbb{C}$  dans lui-même. C'est même un isomorphisme de corps (cf. paragraphe VI.2).
- La fonction

Rappelons que l'injection canonique de  $B$  dans  $A$  est la fonction

$$i : \begin{cases} B & \longrightarrow A \\ x & \longmapsto x \end{cases}$$

$$\varphi : \begin{cases} \mathbb{R}^{\mathbb{R}} & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(0) \end{cases}$$

est un morphisme d'anneaux appelé morphisme d'évaluation en 0. Il est surjectif (car, pour tout  $a \in \mathbb{R}$ ,  $a = \varphi(\tilde{a})$  où  $\tilde{a}$  est la fonction constante égale à  $a$ ) non injectif car  $\ker(\varphi)$  est l'ensemble des fonctions nulles en 0 : on voit bien que ce n'est pas un sous-anneau de  $\mathbb{R}^{\mathbb{R}}$  !

On peut bien sûr évaluer en n'importe quel réel et pas forcément en 0.

- Soit  $n \geq 2$ . La fonction

$$\varphi : \begin{cases} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \bar{k} \end{cases}$$

est un morphisme d'anneaux (car, pour tous  $k_1$  et  $k_2$ ,  $\overline{k_1 + k_2} = \overline{k_1} + \overline{k_2}$  et idem pour le produit, et on a bien  $\varphi(1) = \bar{1}$ ) surjectif de noyau  $n\mathbb{Z}$ .

- Soit  $A$  un anneau quelconque. La fonction

$$f : \begin{cases} \mathbb{Z} & \longrightarrow & A \\ n & \longmapsto & n.1_A \end{cases}$$

est un morphisme d'anneaux. De plus, son noyau est de la forme  $n\mathbb{Z}$  car est un sous-groupe de  $\mathbb{Z}$ . Supposons que  $f$  ne soit pas injective et que  $A$  soit un anneau intègre. Montrons que  $n$  est alors un nombre premier.

$f$  n'étant pas injective,  $n$  est non nul car  $\ker(f) \neq \{0\}$ . Supposons que  $n$  ne soit pas premier. Alors il existe  $2 \leq a, b \leq n-1$  tels que  $n = ab$ . Or,  $n = ab \in \ker(f)$  donc  $f(ab) = f(a) * f(b) = 0_A$ . Enfin,  $A$  étant intègre,  $f(a) = f(b) = 0_A$  donc  $a$  ou  $b$  appartient à  $\ker(f) = n\mathbb{Z}$  ce qui est absurde. Ce résultat permet de prouver qu'un corps fini a un cardinal qui est une puissance d'un nombre premier, cf. chapitre exercice 56 du 30.

Rappelons que  $0.1_A = 0_A$ , que si  $n > 0$ , alors

$$n.1_A = \underbrace{1_A + \dots + 1_A}_{n \text{ fois}}$$

et enfin que, si  $n < 0$ ,

$$n.1_A = \underbrace{-1_A - \dots - 1_A}_{-n \text{ fois}}$$

où  $-1_A$  est l'opposé de  $1_A$  pour la loi  $+$ , cf. paragraphe I.3.

- Soit  $p$  un nombre premier. Montrons que la fonction

$$f : \begin{cases} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ x & \longmapsto & x^p \end{cases}$$

est un isomorphisme d'anneaux. On a évidemment  $f(\bar{1}) = \bar{1}$  et, pour tout  $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ ,

$$\begin{aligned} f(a \times b) &= (a \times b)^p \\ &= a^p \times b^p \\ &= f(a) \times f(b) \end{aligned}$$

On est dans un anneau commutatif.

Enfin, donnons-nous  $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ . L'anneau étant commutatif, on peut appliquer le binôme de Newton :

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

Or (cf. chapitre 6),  $p$  est premier donc, pour tout  $k \in \llbracket 1; p-1 \rrbracket$ ,  $p$  divise  $\binom{p}{k}$  donc, dans  $\mathbb{Z}/p\mathbb{Z}$ ,  $\binom{p}{k} a^k b^{p-k} = \bar{0}$  si bien que

$$\begin{aligned}
f(a+b) &= (a+b)^p \\
&= b^p + a^p \\
&= f(b) + f(a) \\
&= f(a) + f(b)
\end{aligned}$$

C'est donc bien un morphisme d'anneaux. Soit  $x \in \ker(f)$ . Alors  $x^p = \bar{0}$ . Soit  $k \in \mathbb{Z}$  tel que  $x = \bar{k}$  si bien que  $\bar{k}^p = \bar{0}$ , c'est-à-dire que  $p$  divise  $k^p$ . Or,  $p$  est premier donc  $p$  divise  $k$  (on peut le montrer en étudiant la décomposition en facteurs premiers de  $k$  ou, ce qui revient au même, sa valuation  $p$ -adique et le fait que  $v_p(k^p) = pv_p(k)$ , ou encore à l'aide du théorème de Fermat) donc  $x = \bar{k} = \bar{0} : \ker(f) = \{\bar{0}\}$  donc  $f$  est injective. Or,  $f$  va d'un ensemble fini dans lui-même : en particulier,  $f$  va d'un ensemble fini dans un ensemble fini de même cardinal donc est une bijection, c'est donc un isomorphisme, appelé isomorphisme de Frobenius.

La somme est toujours commutative dans un anneau, même non commutatif.

## VI Corps

On rappelle qu'un anneau  $(A, +, \times)$  est un groupe pour la loi  $+$  et donc que tout élément est symétrisable pour cette loi. De plus, cette loi étant notée la plupart du temps additivement, on parle plutôt d'opposé que de symétrique ou d'inverse. Par conséquent, quand on parlera d'inverse ou d'élément inversible, il sera sous-entendu : pour la loi  $\times$  i.e. la seconde loi de l'anneau.

### VI.1 Éléments inversibles dans un anneau

On se donne dans ce paragraphe un anneau  $(A, +, \times)$  (pas forcément commutatif) contenant au moins deux éléments (et donc on a  $0_A \neq 1_A$ ).

**Proposition.**  $0_A$  n'est pas inversible.

DÉMONSTRATION.  $0_A$  est absorbant donc, pour tout  $a \in A$ ,  $a \times 0_A = 0_A \neq 1_A$  : il n'existe donc pas d'élément  $a \in A$  tel que  $a \times 0_A = 0_A \times a = 1_A$ ,  $0_A$  n'est pas inversible.

**Proposition.** Un diviseur de zéro n'est pas inversible.

DÉMONSTRATION. Soit  $a$  un diviseur de 0. Il existe donc  $b \neq 0$  tel que  $ab = 0$  ou  $ba = 0$ . Sans perte de généralité, supposons que  $ba = 0$ . Si  $a$  est inversible alors, en multipliant par  $a^{-1}$  à droite, il vient  $b \times 1_A = 0_A \times a^{-1}$  si bien que  $b = 0_A$  ce qui est absurde.

**Remarque :** En particulier, un élément nilpotent (nul ou non) n'est pas inversible. Cependant, on a tout de même le résultat suivant :

**Proposition (HP).** Soit  $a \in A$  nilpotent d'indice  $n$ . Alors  $1_A - a$  est inversible et :

$$(1_A - a)^{-1} = \sum_{k=0}^{n-1} a^k$$

DÉMONSTRATION.  $1_A$  et  $a$  commutent donc (théorème de factorisation de  $a^n - b^n$  lorsque  $a$  et  $b$  commutent) :

$$1_A^n - a^n = (1_A - a) \times \sum_{k=0}^{n-1} a^k$$

Le résultat en découle puisque  $1_A^n = 1_A$  et  $a^n = 0$ . □

Attention, la réciproque est fautive : un élément non inversible n'est pas forcément un diviseur de zéro (par exemple, dans  $\mathbb{Z}$ , 2 n'est pas inversible alors que ce n'est pas un diviseur de zéro).

Moyen mnémotechnique : cela ressemble à la somme des termes d'une suite géométrique. Attention, ce n'est qu'un moyen mnémotechnique !



**Proposition/Définition.** On note  $U(A)$  ou  $A^\times$  l'ensemble des inversibles de  $A$ . Alors  $(U(A), \times)$  est un groupe.

**Remarque :** Un inversible est parfois appelé une unité, d'où la notation  $U(A)$ .

**DÉMONSTRATION.**  $U(A)$  est non vide car  $1_A$  est inversible (et est son propre inverse). De plus, la loi  $\times$  est interne car un produit d'éléments inversibles est inversible (cf. paragraphe I.3) et associative puisque  $(A, +, \times)$  est un anneau. Enfin,  $1_A \in U(A)$  donc  $U(A)$  admet un élément neutre, et si  $x \in U(A)$ , alors  $x$  admet un inverse par définition, et  $x^{-1}$  est aussi inversible (cf. I.3) donc  $x^{-1} \in U(A)$ , d'où le résultat.



Ne pas confondre  $A^\times$  avec  $A^*$ , l'ensemble des éléments non nuls de  $A$ .  $A^\times$  est inclus dans  $A^*$  d'après ce qui précède mais ces deux ensembles ne sont pas égaux en général (voir ci-dessous). C'est pour cela qu'on utilisera surtout la notation  $U(A)$ .

**Exemples :**

- $U(\mathbb{Z}) = \{\pm 1\}$ .
- $U(\mathbb{Z}/4\mathbb{Z}) = \{\bar{1}; \bar{3}\}$ .

**Remarque :** On peut parfois être amené à utiliser une fonction « multiplicative » pour donner les inversibles d'un anneau (mais il y aurait une indication de l'énoncé).

**Exemple :** Donnons les inversibles de  $\mathbb{Z}[i]$ .

Introduisons pour cela la fonction  $N$  (comme norme) définie par :

$$N : \begin{cases} \mathbb{Z}[i] & \longrightarrow & \mathbb{Z} \\ a + ib & \longmapsto & a^2 + b^2 \end{cases}$$

Si  $z_1 \in \mathbb{Z}[i]$ ,  $N(z_1) = |z_1|^2$ . Il en découle que  $N$  est multiplicative, c'est-à-dire que pour tous  $z_1$  et  $z_2$  dans  $\mathbb{Z}[i]$ ,  $N(z_1 \times z_2) = N(z_1) \times N(z_2)$ . Ainsi, si  $z_1$  est inversible, il existe  $z_2$  tel que  $z_1 z_2 = 1$  donc en particulier  $N(z_1 z_2) = N(z_1) \times N(z_2) = N(1) = 1$ . En particulier,  $N(z_1)$  est un inversible de  $\mathbb{Z}$  donc  $N(z_1) = 1$  (puisque  $N(z_1) \geq 0$ ). Or,  $a^2 + b^2 = 1$  si et seulement si  $(a = \pm 1 \text{ et } b = 0)$  ou  $(a = 0 \text{ et } b = \pm 1)$  si bien que les seuls inversibles « éventuels » de  $\mathbb{Z}[i]$  sont  $\pm 1$  et  $\pm i$ , et on montre facilement qu'ils sont effectivement inversibles. Finalement,  $U(\mathbb{Z}[i]) = \{\pm 1; \pm i\}$ .

**Remarque :** On peut se demander l'intérêt d'introduire une nouvelle fonction  $N$  puisque celle-ci est juste égale au module au carré. Cette méthode peut en fait se généraliser à des anneaux plus généraux, cf. exercice 49.

**Proposition.** Soient  $A_1$  et  $A_2$  deux anneaux et soit  $f : A_1 \rightarrow A_2$  un morphisme d'anneaux. Soit  $a \in A_1$ . Si  $a$  est inversible alors  $f(a)$  est inversible et, pour tout  $n \in \mathbb{Z}$ ,  $f(a^n) = f(a)^n$ . En particulier,  $f(a^{-1}) = f(a)^{-1}$ .

**DÉMONSTRATION.** Par hypothèse, il existe  $b \in A_1$  tel que  $a \times_1 b = b \times_1 a = 1_{A_1}$ .  $f$  étant un morphisme d'anneaux,

$$f(a \times_1 b) = f(a) \times_2 f(b) = f(b) \times_2 f(a) = f(1_{A_1}) = 1_{A_2}$$

c'est-à-dire que  $f(a)$  est inversible (d'inverse  $f(b)$ ). En particulier,  $f(U(A_1))$  est inclus dans  $U(A_2)$ .  $f$  induit donc un morphisme de groupes de  $U(A_1)$  dans  $U(A_2)$  ce qui permet de conclure d'après le paragraphe IV.2.  $\square$

## VI.2 Corps

**Définition.** Soit  $(K, +, \times)$  un anneau. On dit que  $K$  est un corps si  $K$  est commutatif et si tout élément de  $K$  distinct du neutre de l'addition est inversible.



C'est-à-dire si tout élément distinct de  $0_K$  est inversible.

**Remarques :**

- Attention, il est bien précisé « tout élément distinct du neutre de l'addition » c'est-à-dire de  $0_K$ . En effet, celui-ci n'est jamais inversible dès que  $K$  a au moins deux éléments (voir ci-dessus), ce qu'on supposera dans la suite car, comme pour les anneaux, le cas des corps à un élément est assez peu intéressant... En d'autres termes, dans la suite, quand nous parlerons d'anneaux ou de corps, il sera sous-entendu qu'ils ont au moins deux éléments (et donc  $0 \neq 1$ ).
- Un corps est commutatif par définition. Certains livres ou certains anciens sujets ne demandent pas la commutativité et parlent donc de corps non commutatif. Tout dépend en fait des conventions : en prépa, un corps est commutatif, c'est comme ça et pas autrement. S'il ne manque que la commutativité (c'est-à-dire si  $K$  est un anneau non commutatif dont tout élément non nul est inversible), on parle plutôt « d'algèbre à division » ou de « corps gauche ». Cependant, ces appellations ne sont pas universelles (alors qu'en anglais on parle de « division ring » lorsque ce n'est pas commutatif et de « field » lorsque ça l'est), il nous arrivera donc parfois (rarement) de parler de corps non commutatif, surtout pour bien nous faire comprendre. Mais qu'on se souvienne qu'un corps est commutatif par définition !
- Un corps étant commutatif, un élément est inversible si et seulement s'il est inversible à gauche ou à droite. Ainsi, si on veut prouver qu'un anneau commutatif est un corps, il suffit de prouver que tout élément est inversible à gauche ou à droite.
- Enfin, puisqu'un corps est commutatif, si on a un élément non nul  $a$  des deux côtés d'une équation (par exemple  $ab = ca$ ), alors on peut s'arranger pour mettre  $a$  du même côté (dans notre exemple  $ab = ac$ ) puis multiplier par  $a^{-1}$  et donc faire « disparaître »  $a$  (dans notre exemple,  $b = c$ ). Morale de l'histoire : dans un corps, on peut simplifier comme on veut, il n'est pas nécessaire que l'élément par lequel on veut simplifier « soit à la même extrémité des deux côtés de l'égalité ».
- En clair, un corps est un anneau (commutatif) auquel on a rajouté la division (pour les éléments non nuls : on ne peut pas diviser par 0!). C'est ce qui manquait dans un anneau. Par exemple,  $\mathbb{Z}$  est un anneau mais pas un corps car on ne peut pas diviser dans  $\mathbb{Z}$ .

### Exemples :

- $\mathbb{Z}$  n'est pas un corps car les seuls inversibles de  $\mathbb{Z}$  sont  $\pm 1$ . Cependant,  $\mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$  sont des corps.
- $\mathbb{Q}$  est même le plus petit corps (au sens de l'inclusion) contenant 1. En effet, soit  $K$  un corps contenant 1 (le 1 réel). Puisque  $K$  est un groupe (pour l'addition), il est stable par somme donc contient  $1 + 1 = 2, 2 + 1 = 3$  etc. donc tous les entiers  $n \in \mathbb{N}$  par une récurrence immédiate. Il est également stable par opposé donc contient aussi tous les entiers négatifs donc contient  $\mathbb{Z}$  (on pouvait directement dire qu'il contient  $\text{gr}(1) = \mathbb{Z}$ ). De plus, tout élément non nul étant inversible,  $K$  contient tous les  $1/q$  avec  $q$  non nul, et il est stable par produit donc contient tous les éléments de la forme  $p \times \frac{1}{q}$  donc contient tous les rationnels.

Voir ci-dessous pour d'autres exemples.

⚠ Un corps peut être fini ! cf. paragraphe VI.4.

**Proposition.** Un corps est un anneau intègre.

DÉMONSTRATION. Soit  $(a, b) \in K^2$  tel que  $ab = 0_K$ . Si  $a \neq 0_K$  alors, en multipliant par  $a^{-1}$  (à gauche mais ça n'a aucune importance car  $K$  est commutatif), il vient  $1_K \times b = a^{-1} \times 0_K$  si bien que  $b = 0_K$  ( $0_K$  est absorbant). Il en découle que  $a = 0_K$  ou que  $b = 0_K$  :  $K$  est bien intègre.

**Remarque :** ⚠ La réciproque est (très) fausse ! Un anneau intègre n'a aucune raison d'être un corps ! Par exemple,  $\mathbb{Z}$  est un anneau intègre mais n'est pas un corps. Il en découle qu'un corps ne contient aucun diviseur de zéro ni aucun élément nilpotent non nul. Dans le cas d'un ensemble fini, on a cependant la réciproque :

$\mathbb{K}[X]$  est aussi un anneau intègre qui n'est pas un corps, cf. chapitre 19.

**Proposition.** Un anneau commutatif intègre **fini** est un corps.

DÉMONSTRATION. Soit  $K$  un anneau intègre commutatif fini. Soit  $a \neq 0_K$  et soit

$$f_a : \begin{cases} K & \longrightarrow & K \\ b & \longmapsto & ab \end{cases}$$

Soit  $(b_1, b_2) \in K^2$ . Alors

$$\begin{aligned} f_a(b_1 + b_2) &= a(b_1 + b_2) \\ &= ab_1 + ab_2 \\ &= f_a(b_1) + f_a(b_2) \end{aligned}$$

Ce résultat n'est pas explicitement au programme : il faut donc savoir le redémontrer !

Distributivité du produit sur la somme.

$f_a$  est donc un morphisme de groupes de  $(A, +)$  dans lui-même. . Soit  $b \in \ker(f)$ . Alors  $f(a) = ab = 0$  mais  $a \neq 0$  et  $A$  est intègre si bien que  $b = 0 : \ker(f) = \{0\}$ ,  $f_a$  est injective. Or,  $f_a$  est une injection d'un ensemble fini dans lui-même donc entre deux ensembles finis de même cardinal donc est une bijection. En particulier,  $1_K$  est atteint : il existe  $b \in K$  tel que  $ab = 1$  donc  $a$  admet un inverse (à droite mais  $K$  est commutatif donc c'est un inverse tout court). Tout élément non nul admet un inverse,  $K$  est un corps.

$f_a$  n'est pas un morphisme d'anneaux !

**Remarque :** Si  $A$  est un anneau intègre, on peut définir ce qu'on appelle son corps des fractions : sans rentrer dans les détails (c'est un ensemble quotient, cf. chapitre 16), disons simplement qu'on peut construire un corps dont les éléments sont notés  $a/b$  avec  $a$  et  $b$  dans  $A$  avec  $b \neq 0$ , et avec la convention que deux fractions  $a/b$  et  $c/d$  sont égales si  $ad = bc$ . C'est d'ailleurs comme ça qu'on construit  $\mathbb{Q}$  (cf. chapitre 16) et  $\mathbb{K}(X)$  (cf. chapitre 20) puisque ce sont les corps des fractions de  $\mathbb{Z}$  et  $\mathbb{K}[X]$  respectivement. En clair : de la même façon qu'on construit  $\mathbb{Q}$  comme ensemble des fractions d'éléments de  $\mathbb{Z}$  et que  $\mathbb{Z}$  est inclus dans  $\mathbb{Q}$ , on peut définir un corps  $\mathbb{K}$  à partir de n'importe quel anneau intègre  $A$ , comme ensemble des fractions d'éléments de  $A$  et ce corps est appelé corps des fractions de  $A$ , et on peut considérer que  $A$  est inclus dans  $\mathbb{K}$ . Si vous rencontrez ça dans un sujet (par exemple ENS MPI 2023), pas de panique : retenez juste que ça marche comme  $\mathbb{Z}$  et  $\mathbb{Q}$ .

Le fait que tout anneau intègre soit inclus dans un corps permet de prouver sur des anneaux intègres des résultats valables uniquement sur des corps, cf. chapitre 33.

**Proposition.** Soit  $K$  un anneau commutatif. Alors  $K$  est un corps si et seulement si  $K^*$  est un groupe (pour la loi  $\times$ ).

DÉMONSTRATION. Si  $K$  est un corps, alors  $K$  est intègre donc la multiplication est une loi interne sur  $K^*$  (un produit d'éléments non nuls reste non nul). Puisque la loi  $\times$  est associative et admet un élément neutre par définition, il ne manque que l'existence d'un inverse pour tout élément de  $K^*$ , ce qui est le cas puisque  $K$  est un corps :  $(K^*, \times)$  est bien un groupe. La réciproque est immédiate.

Rappelons que  $K^*$  est  $K$  privé de  $0_K$ , à ne pas confondre avec  $K^\times$  qui, lui, est toujours un groupe (cf. paragraphe VI.1).

On se donne dans la suite un corps (commutatif et non réduit à un élément)  $(K, +, \times)$ .

**Définition.** Soit  $L$  une partie de  $A$ .  $L$  est un sous-corps de  $K$  si

- $L$  est stable par les lois  $+$  et  $\times$ .
- $1_K \in L$ .
- $(L, +, \times)$  est un corps.

En d'autres termes, un sous-corps de  $K$  est un corps inclus dans  $K$  pour les mêmes lois et les mêmes neutres que  $K$ .

On dit que  $K$  est un sur-corps ou une extension de corps de  $K$ .

**Remarques :**

- Là aussi, c'est un cas particulier de la définition de sous-truc vue dans le paragraphe V.3.
- Si  $L$  est un sous-corps de  $K$ , alors  $L^*$  est un sous-groupe de  $K^*$ . Il en découle que  $L^*$  est également stable par inverse. On en déduit également la caractérisation suivante (même s'il suffit de prouver que  $L$  est un sous-anneau puis que tout élément non nul de  $L$  est inversible) :

**Proposition.** Soit  $L$  une partie de  $K$ .  $L$  est un sous-corps de  $K$  si et seulement si :

- $L$  est un sous-groupe de  $K$ .
- $1_K \in L$ .
- $L$  est stable par produit.
- $L^*$  est stable par inverse.

**Exemple :** Soit  $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$ . Montrons que  $\mathbb{Q}[\sqrt{2}]$  est un corps.

Il suffit donc de montrer que c'est un sous-corps de  $\mathbb{R}$ .

- $0 = 0 + 0 \times \sqrt{2}$  et  $0 \in \mathbb{Q}$  donc  $0 \in \mathbb{Q}[\sqrt{2}]$  qui est donc non vide.
- Soit  $(x_1, x_2) \in \mathbb{Q}[\sqrt{2}]^2$ . Il existe  $(a_1, b_1, a_2, b_2) \in \mathbb{Q}^4$  tel que  $x_1 = a_1 + b_1\sqrt{2}$  et  $x_2 = a_2 + b_2\sqrt{2}$  si bien que  $x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$ . Or, une somme de rationnels est un rationnel donc  $a_1 + a_2$  et  $b_1 + b_2$  appartiennent à  $\mathbb{Q}$  si bien que  $x_1 + x_2 \in \mathbb{Q}[\sqrt{2}]$  :  $\mathbb{Q}[\sqrt{2}]$  est stable par somme.
- $-x_1 = -a_1 + (-b_1) \times \sqrt{2}$ .  $-a_1$  et  $-b_1$  sont rationnels donc  $-x_1 \in \mathbb{Q}[\sqrt{2}]$  qui est stable par opposé : c'est un sous-groupe de  $\mathbb{R}$ .
- $1 = 1 + 0 \times \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ .
- $x_1 \times x_2 = (a_1a_2 + 2b_1b_2) + \sqrt{2} \times (a_1b_2 + a_2b_1)$ . Or, une somme et un produit de rationnels sont des rationnels si bien que  $a_1a_2 + 2b_1b_2$  et  $a_1b_2 + a_2b_1$  appartiennent à  $\mathbb{Q}$ . En d'autres termes,  $x_1x_2 \in \mathbb{Q}[\sqrt{2}]$  qui est donc stable par produit : c'est donc un sous-anneau de  $\mathbb{R}$ . En particulier c'est un anneau.
- Supposons que  $x_2$  soit non nul. Alors

$$\frac{1}{x_2} = \frac{1}{a_2 + b_2\sqrt{2}}$$

Utilisons la méthode de l'expression conjuguée. Montrons que  $a_2 - b_2\sqrt{2} \neq 0$ . Si  $a_2 - b_2\sqrt{2} = 0$  alors  $b_2\sqrt{2} = a_2$ . Si  $b_2 \neq 0$  alors  $\sqrt{2} = a_2/b_2 \in \mathbb{Q}$  ce qui est absurde donc  $b_2 = 0$  et donc  $a_2 = 0$  donc  $x_2 = 0$  ce qui est exclu. On a bien  $a_2 - b_2\sqrt{2} \neq 0$  si bien que

$$\begin{aligned} \frac{1}{x_2} &= \frac{1}{a_2 + b_2\sqrt{2}} \times \frac{a_2 - b_2\sqrt{2}}{a_2 - b_2\sqrt{2}} \\ &= \frac{a_2 - b_2\sqrt{2}}{a_2^2 + b_2^2} \end{aligned}$$

et puisque  $\frac{a_2}{a_2^2 + b_2^2}$  et  $\frac{-b_2}{a_2^2 + b_2^2}$  sont des rationnels,  $1/x_2 \in \mathbb{Q}[\sqrt{2}]$ ,  $\mathbb{Q}[\sqrt{2}]$  est stable par inverse : c'est donc un sous-corps de  $\mathbb{R}$  et donc un corps.

On montrerait de même que  $\mathbb{Q}[i] = \{a + ib \mid (a, b) \in \mathbb{Q}^2\}$  est un corps (exo).

**Définition.** Un morphisme de corps est un morphisme d'anneaux entre deux corps. Si, de plus, ce morphisme est bijectif, on dit que c'est un isomorphisme de corps.

**Remarque :** D'après la dernière proposition du paragraphe VI.1, un morphisme d'anneaux est aussi compatible avec l'inverse lorsque les éléments sont inversibles, et en particulier dans un corps, pour tous les éléments non nuls. C'est la raison pour laquelle il n'est pas nécessaire de donner une définition impliquant cette condition : elle est automatique. On en revient à la définition de morphisme de truc : il suffit d'être compatible avec les lois et d'envoyer les neutres sur les neutres, le passage à l'inverse ou à l'opposé est alors automatique ! Il en découle qu'un morphisme de corps n'est rien d'autre qu'un morphisme d'anneaux, mais entre deux corps. Attention cependant : la structure de corps étant plus riche que celle d'anneaux, un morphisme de corps vérifie des propriétés que ne vérifie pas forcément un morphisme d'anneaux. Par exemple, un morphisme de corps est forcément injectif (si  $K_2$  n'est pas réduit à un élément), cf. exercice 64, alors que ce n'est pas du tout le cas pour un morphisme d'anneaux !

**Exemple :**

- On a vu dans l'exercice 12 du chapitre 12 que l'identité est le seul morphisme de corps de  $\mathbb{R}$ .
- Donnons tous les morphismes de corps de  $\mathbb{C}$  dans  $\mathbb{C}$  qui fixent tous les éléments de  $\mathbb{R}$  (i.e. tels que la restriction de  $\varphi$  à  $\mathbb{R}$  soit l'identité).

Soit  $\varphi$  un tel morphisme. Alors  $\varphi(i^2) = \varphi(i)^2$  si bien que  $\varphi(i)^2 = \varphi(-1) = -1$  puisque  $\varphi$  fixe  $\mathbb{R}$ . En d'autres termes,  $\varphi(i) = i$  ou  $\varphi(i) = -i$ .

Si  $\varphi(i) = -i$  alors, pour tout  $(a, b) \in \mathbb{R}^2$ ,  $\varphi$  étant un morphisme de corps qui fixe tous les éléments de  $\mathbb{R}$ ,

$$\begin{aligned}\varphi(a + ib) &= \varphi(a) + \varphi(i) \times \varphi(b) \\ &= a - ib\end{aligned}$$

En d'autres termes, pour tout  $z \in \mathbb{C}$ ,  $\varphi(z) = \bar{z}$ , c'est-à-dire que  $\varphi$  est la conjugaison. Si  $\varphi(i) = i$  alors on montre de même que  $\varphi$  est l'identité, c'est-à-dire que l'identité et la conjugaison sont les deux seules solutions **éventuelles** (encore une fois, on a fait sans le dire une analyse synthèse), et on vérifie aisément qu'elles sont effectivement solutions, c'est-à-dire que ce sont des morphismes de corps fixant tous les éléments de  $\mathbb{R}$ . Ainsi, les seuls morphismes de corps de  $\mathbb{C}$  dans  $\mathbb{C}$  fixant tous les éléments de  $\mathbb{R}$  sont la conjugaison et l'identité.

### VI.3 Construction de $\mathbb{C}$

Nous sommes à présent en mesure de prouver l'existence de  $\mathbb{C}$  que nous avons admise dans le chapitre 7. Nous la prouverons une nouvelle fois dans l'exercice 20 du chapitre 21.

On munit  $\mathbb{R}^2$  des deux lois internes  $+$  et  $\times$  définies par :

$$\forall ((x_1, y_1), (x_2, y_2)) \in (\mathbb{R}^2)^2, \quad \left\{ \begin{array}{l} (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \\ \text{et} \\ (x_1, y_1) \times (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \end{array} \right.$$

Ces deux lois sont bien internes par construction. Montrons que  $(\mathbb{R}^2, +, \times)$  est un corps.

- On montre aisément que la loi  $+$  est associative, commutative, que  $(0, 0)$  est son élément neutre et que, pour tout  $(x, y) \in \mathbb{R}^2$ ,  $(-x, -y)$  est le symétrique de  $(x, y)$  pour la loi  $+$ . En d'autres termes,  $(\mathbb{R}^2, +)$  est un groupe abélien.
- Montrons que la loi  $\times$  est associative et distributive par rapport à la loi  $+$ . Soient donc  $(x_1, y_1)$ ,  $(x_2, y_2)$  et  $(x_3, y_3)$  trois éléments de  $\mathbb{R}^2$ . D'une part :

$$\begin{aligned}(x_1, y_1) \times ((x_2, y_2) \times (x_3, y_3)) &= (x_1, y_1) \times (x_2 x_3 - y_2 y_3, x_2 y_3 + x_3 y_2) \\ &= (x_1 x_2 x_3 - x_1 y_2 y_3 - y_1 x_2 y_3 - y_1 x_3 y_2, x_1 x_2 y_3 + x_1 x_3 y_2 + y_1 x_2 x_3 - y_1 y_2 y_3)\end{aligned}$$

et d'autre part :

$$\begin{aligned} ((x_1, y_1) \times (x_2, y_2)) \times (x_3, y_3) &= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \times (x_3, y_3) \\ &= (x_1x_2x_3 - x_3y_1y_2 - y_3x_1y_2 - y_3x_2y_1, x_1x_2y_3 - y_1y_2y_3 + x_3x_1y_2 + x_3x_2y_1) \end{aligned}$$

On obtient la même chose : la loi est bien associative. On montre de façon analogue qu'elle est distributive à gauche par rapport à la somme, i.e.

$$(x_1, y_1) \times ((x_2, y_2) + (x_3, y_3)) = (x_1, y_1) \times (x_2, y_2) + (x_1, y_1) \times (x_3, y_3)$$

Les réels  $x_1$  et  $x_2$ ,  $y_1$  et  $y_2$  jouant le même rôle dans l'expression de  $(x_1, y_1) \times (x_2, y_2)$ , la loi est commutative : elle est donc distributive par rapport à la somme.

- Enfin,  $(1, 0) \times (x_1, y_1) = (x_1, y_1)$  donc (la loi est commutative donc un neutre à gauche est l'élément neutre) le neutre de la loi  $\times$  est  $(1, 0)$ . Finalement,  $(\mathbb{R}^2, +, \times)$  est bien un anneau commutatif.
- Soit  $(x, y) \neq (0, 0)$  et montrons que  $(x, y)$  est inversible. Soit  $(a, b) \in \mathbb{R}^2$  et résolvons l'équation (E) :  $(x, y) \times (a, b) = (1, 0)$ .

$$\begin{aligned} (E) &\iff (ax - by, ay + bx) = (1, 0) \\ &\iff \begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases} \end{aligned}$$

**Premier cas :** supposons que  $x = 0$ . Alors  $y \neq 0$  car  $x$  et  $y$  sont non tous nuls si bien que :

$$\begin{aligned} (E) &\iff \begin{cases} -by = 1 \\ ay = 0 \end{cases} \\ &\iff \begin{cases} b = -1/y \\ a = 0 \end{cases} \end{aligned}$$

Il en découle que  $(0, -1/y)$  est l'unique inverse à gauche donc l'unique inverse (la loi est commutative) de  $(x, y)$ .

**Deuxième cas :** supposons que  $x \neq 0$ . Alors :


$$(E) \iff \begin{cases} a - \frac{by}{x} = \frac{1}{x} \\ ay + bx = 0 \end{cases}$$


$$\iff \begin{cases} a - \frac{by}{x} = \frac{1}{x} \\ b \left( x + \frac{y^2}{x} \right) = -\frac{y}{x} \end{cases}$$

$$\iff \begin{cases} a - \frac{by}{x} = \frac{1}{x} \\ b \times \frac{x^2 + y^2}{x} = -\frac{y}{x} \end{cases}$$

$$\iff \begin{cases} a = \frac{-y^2}{x(x^2 + y^2)} + \frac{1}{x} \\ b = \frac{-y}{x^2 + y^2} \end{cases}$$

$$\iff \begin{cases} a = \frac{x}{x^2 + y^2} \\ b = \frac{-y}{x^2 + y^2} \end{cases}$$

  $L_2 \leftarrow L_2 - yL_1.$

  $x$  et  $y$  sont non tous nuls donc  $x^2 + y^2 \neq 0$ .

On en déduit dans tous les cas que  $(x, y)$  est inversible d'inverse  $\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$  (cette expression étant aussi valable dans le cas où  $x = 0$ ). Finalement, tout élément différent de  $(0, 0)$  est inversible :  $(\mathbb{R}^2, +, \times)$  est bien un corps.

Notons  $\mathbb{C}$  l'ensemble  $\mathbb{R}^2$ , qu'on munit de ces deux lois. Montrons que  $\mathbb{C}$  vérifie les propriétés admises dans le chapitre 7 :

- Soit

$$f : \begin{cases} \mathbb{R} & \longrightarrow & \mathbb{R}^2 \\ x & \longmapsto & (x, 0) \end{cases}$$

On montre facilement que  $f$  est un morphisme de corps injectif. Par conséquent,  $\mathbb{R}$  est isomorphe à  $\text{Im}(f)$  : on identifie donc  $\mathbb{R}$  à son image. Par conséquent,  $\mathbb{C}$  contient une copie conforme de  $\mathbb{R}$  que l'on identifie à  $\mathbb{R}$ , on peut donc dire par abus de langage que  $\mathbb{C}$  contient  $\mathbb{R}$ , et, si  $x \in \mathbb{R}$ , on identifie le réel  $x$  à l'élément  $(x, 0)$  de  $\mathbb{C}$ .

- Posons  $i = (0, 1)$ . Alors  $i \times i = (-1, 0)$ . Or, on identifie  $(-1, 0)$  et le réel  $-1$  : il existe bien un élément  $i \in \mathbb{C}$  vérifiant  $i^2 = -1$ .
- Les lois  $+$  et  $\times$  prolongent celles de  $\mathbb{R}$  : en effet, si  $x_1$  et  $x_2$  sont deux réels, on les identifie à  $(x_1, 0)$  et  $(x_2, 0)$  et  $(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0)$ . La somme (au sens de la loi  $+$  définie sur  $\mathbb{C}$  vue plus haut) de  $x_1$  et de  $x_2$  donne la somme  $x_1 + x_2$  au sens réel, et idem pour le produit. En d'autres termes, les opérations  $+$  et  $\times$  donnent les mêmes résultats que la somme et le produit lorsqu'on les applique à des réels : ces nouvelles opérations prolongent donc celles de  $\mathbb{R}$ .
- Enfin, soit  $z = (x, y) \in \mathbb{R}^2$ . Alors  $z = (x, 0) + (y, 0) \times (0, 1) = x + iy$ . De plus, si  $z = a + ib$ , alors  $z = (a, 0) + (0, b) \times (0, 1) = (a, b)$  d'où  $x = a$  et  $y = b$ . Tout complexe  $z$  s'écrit de façon unique sous la forme  $x + iy$ .

Nous avons donc enfin prouvé l'existence de  $\mathbb{C}$  et qu'il vérifie bien les propriétés admises dans le chapitre 7. Il est donc naturel de se poser la question suivante : est-il possible d'aller encore plus loin ? Est-il possible de définir un corps encore plus gros ? Peut-on définir de la même façon un surcorps de  $\mathbb{R}$  de dimension 3 i.e. faire comme ci-dessus et munir  $\mathbb{R}^3$  d'une structure de corps ?

La réponse est non : il est impossible de définir un surcorps de  $\mathbb{R}$  de dimension 3 i.e. munir  $\mathbb{R}^3$  d'une structure de corps (théorème de Frobenius, 1877) mais on peut montrer qu'il est possible de définir un surcorps de  $\mathbb{R}$  de dimension 4 i.e. munir  $\mathbb{R}^4$  d'une structure de corps (non commutatif). Il existe en effet un ensemble  $\mathbb{H}$  contenant  $\mathbb{C}$  dont tous les éléments s'écrivent de façon unique sous la forme

$$h = a + bi + cj + dk$$

où  $(a, b, c, d)$  sont quatre réels et où  $i$  est le complexe habituel et où  $j$  et  $k$  sont deux nouveaux éléments vérifiant  $i^2 = j^2 = k^2 = -1$  et où  $ij = k$ ,  $ji = -k$  etc. c'est-à-dire que  $i, j, k$  vérifient la table du dernier paragraphe du poly de botanique.  $\mathbb{H}$  est appelé corps (non commutatif) des quaternions et donc le groupe  $\mathbb{H}_8 = \{\pm 1; \pm i; \pm j; \pm k\}$  est appelé groupe des quaternions.

En fait, on définit  $\mathbb{H}$  de la même façon que ci-dessus c'est-à-dire qu'on définit  $\mathbb{H}$  comme  $\mathbb{R}^4$  muni de deux lois  $+$  et  $\times$  qui font bien ce qu'elles sont censées faire (distributivité etc.) et on pose (entre autres)  $i = (0, 1, 0, 0)$  etc. mais je vous laisse imaginer les réjouissances... Un moyen simple de le faire est d'utiliser les matrices, cf. exercice 21 du chapitre 21.

Enfin, on peut montrer que cette chaîne infernale s'arrête là : les seuls corps (commutatifs ou non) de dimension finie sur  $\mathbb{R}$  sont (à isomorphisme près)  $\mathbb{C}$  et  $\mathbb{H}$ .

## VI.4 Retour sur les $\mathbb{Z}/n\mathbb{Z}$

On se donne dans ce paragraphe un entier  $n \geq 2$ . On renvoie au chapitre 16 et au paragraphe II.1 pour les rappels sur  $\mathbb{Z}/n\mathbb{Z}$  et les lois  $+$  et  $\times$  qu'on définit sur cet ensemble.

On montre facilement que l'image d'un morphisme de corps est un corps. Ainsi,  $\mathbb{R}$  et  $\text{Im}(f)$  sont deux corps isomorphes. Puisque ces deux corps sont isomorphes, comme pour les groupes, ils représentent « le même corps ».


$\mathbb{C}$  est en fait le plan que l'on munit de deux lois qui font bien ce qu'elles sont censées faire. Ce n'est pas très étonnant puisqu'on identifie tout le temps  $\mathbb{C}$  au plan complexe !

$j$  n'est pas le complexe  $e^{2i\pi/3}$ .



**Proposition.**  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau commutatif.

DÉMONSTRATION. On sait déjà que  $(\mathbb{Z}/n\mathbb{Z}, +)$  est un groupe commutatif. De plus, on a vu dans le chapitre 16 que la loi  $\times$  est associative, distributive par rapport à la somme et que  $\bar{1}$  est l'élément neutre du produit.  $\mathbb{Z}/n\mathbb{Z}$  est donc un anneau, et il est commutatif car le produit est commutatif.

**Remarque :**  Ce n'est pas forcément un anneau intègre (donc ce n'est pas forcément un corps) ! En effet, par exemple  $\bar{4} \times \bar{3} = \bar{0}$  dans  $\mathbb{Z}/6\mathbb{Z}$  et dans  $\mathbb{Z}/12\mathbb{Z}$ .

**Proposition.** Soit  $k \in \mathbb{Z}$ . Alors :  $\bar{k} \in U(\mathbb{Z}/n\mathbb{Z}) \iff k \wedge n = 1$ . En d'autres termes,  $\bar{k}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$  si et seulement si  $k$  est premier avec  $n$ .

DÉMONSTRATION.  $\bar{k}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$  si et seulement s'il existe  $\bar{u} \in \mathbb{Z}/n\mathbb{Z}$  tel que  $\bar{k} \times \bar{u} = \bar{1}$  donc si et seulement s'il existe  $u \in \mathbb{Z}$  tel que  $ku \equiv 1[n]$  donc si et seulement s'il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $ku + nv = 1$ . On conclut à l'aide du théorème de Bézout.

**Corollaire.**  $\mathbb{Z}/n\mathbb{Z}$  est un corps si et seulement si  $n$  est premier.

DÉMONSTRATION. Si  $n$  est premier, alors  $1, 2, \dots, n-1$  sont premiers avec  $n$  donc les éléments  $\bar{1}, \bar{2}, \dots, \overline{n-1}$  sont inversibles :  $\mathbb{Z}/n\mathbb{Z}$  est un corps.

Réciproquement, supposons que  $n$  ne soit pas premier. Il existe donc  $2 \leq a, b \leq n-1$  tels que  $n = ab$  si bien que  $\bar{a} \times \bar{b} = \bar{n} = \bar{0}$ . Or,  $a$  et  $b$  appartiennent à  $\llbracket 2; n-1 \rrbracket$  si bien que  $\bar{a}$  et  $\bar{b}$  sont non nuls :  $\mathbb{Z}/n\mathbb{Z}$  n'est pas un anneau intègre, ce n'est pas un corps.

**Remarques :**

- Les  $\mathbb{Z}/p\mathbb{Z}$  (pour  $p$  premier) sont donc des exemples de corps finis. Par exemple,  $\mathbb{Z}/2\mathbb{Z}$  et  $\mathbb{Z}/3\mathbb{Z}$  sont des corps mais  $\mathbb{Z}/4\mathbb{Z}$  n'en est pas un.
- Plus généralement, on montrera dans l'exercice 56 du chapitre 30 qu'un corps fini a forcément un cardinal qui est une puissance d'un nombre premier. Par exemple, il n'existe pas de corps à 10 éléments.
- Si  $q = p^n$  est la puissance d'un nombre premier, on peut montrer qu'il existe (à isomorphisme près) un unique corps à  $q$  éléments qu'on note  $\mathbb{F}_q$ , mais ce n'est pas facile. En tout cas, ce n'est pas  $\mathbb{Z}/p^n\mathbb{Z}$  (ce n'est pas un corps si  $n \geq 2$  d'après ce qui précède) ni même  $(\mathbb{Z}/p\mathbb{Z})^n$  (qu'on peut munir d'une structure d'anneau produit de la même façon que pour la structure de groupe produit). Par exemple, dans  $(\mathbb{Z}/2\mathbb{Z})^2$ ,  $(\bar{0}, \bar{1})$  est un élément non nul qui n'est pas inversible pour la loi produit  $\times$  donc ce n'est pas un corps. On zappe...
- Cette structure de corps (ou la structure d'anneau de  $\mathbb{Z}/n\mathbb{Z}$  dans le cas général) permet de prouver des résultats plus simplement qu'en travaillant sur  $\mathbb{Z}$  avec des congruences. On verra des exemples en TD.

On montrera dans l'exercice 67 que  $\bar{k}$  est un diviseur de zéro dans  $\mathbb{Z}/n\mathbb{Z}$  si et seulement si  $k$  n'est pas un multiple de  $n$  et n'est pas premier avec  $n$ .

Un corps étant intègre, on a montré au passage que  $\mathbb{Z}/n\mathbb{Z}$  est intègre si et seulement si  $n$  est premier.

Et oui, un corps n'est pas forcément infini !

Par exemple il existe un unique corps à 4 ou à 8 éléments.