Structures algébriques

Olivier Sellès, transcrit par Denis Merigoux

Table des matières

1 Lois internes , monoïdes **2**
1.1 Définition . . . 2
1.2 Vocabulaire . . . 2
1.3 Monoïdes . . . 3
1.4 Éléments inversibles . . . 3
1.5 Éléments réguliers . . . 4
1.6 Itérés d'un élément pour une loi dans un monoïde . . . 4
1.6.1 Définitions . . . 4
1.6.2 Propriétés . . . 4

2 Groupes **6**
2.1 Définitions et exemples . . . 6
2.1.1 Groupe . . . 6
2.1.2 Sous-groupes . . . 7
2.1.3 PGCD et PPCM dans $\mathbb{Z}$ . . . 8
2.1.4 Propriétés des sous-groupes . . . 11
2.2 Morphismes de groupe . . . 12
2.2.1 Définitions . . . 12
2.2.2 Propriété des morphismes . . . 12
2.2.3 Composée de deux morphismes . . . 13

3 Anneaux et corps **14**
3.1 Définitions, règles de calcul, exemples . . . 14
3.1.1 Définitions . . . 14
3.1.2 Règles de calcul dans les anneaux . . . 14
3.1.3 Anneaux intègres . . . 16
3.1.4 Corps . . . 17
3.2 Sous-anneaux, morphismes d'anneaux . . . 17
3.2.1 Sous-anneau . . . 17
3.2.2 Morphisme d'anneaux . . . 18

4 Complément : éléments de torsion dans un groupe **20**

5 Complément : signature d'une décomposition **21**
5.1 Étude préliminaire . . . 21
5.2 Théorème . . . 21
5.3 Application : produit de cycles et ordre . . . 24

6 Complément : corps des fractions d'un anneau intègre **25**
6.1 Introduction . . . 25
6.2 Construction du corps des fractions d'un anneau intègre . . . 26

1 Lois internes , monoïdes

1.1 Définition

Soit E un ensemble non vide. Une loi de composition interne (LCI en abrégé) est une application $\top : E \times E \longrightarrow E$.

On adopte une notation infixe : pour $(x, y) \in E \times E$, on notera $x \top y$ au lieu de $\top(x, y)$. On peut utiliser divers symboles tels que $\top, \times, +, \cdot, \circ, \otimes, \dot{+}$ ...

Exemples
- Opérations usuelles + et × sur les ensembles de nombres
- Produit vectoriel dans $\mathbb{R}^3$
- Si X est un ensemble alors la composition $\circ$ est une loi de composition interne sur $\mathcal{F}(X, X)$
- Soit X un ensemble, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Alors on définit pour $f, g \in \mathcal{F}(X, \mathbb{K})$
  - $f + g$ par $\forall x \in X, (f + g)(x) = f(x) + g(x)$
  - $f \times g$ par $\forall x \in X, (f \times g)(x) = f(x) \times f(x)$

1.2 Vocabulaire

Associativité

$\top$est associative si $\forall a, b, c \in E$

$$(a \top b) \top c = a \top (b \top c)$$

Si c'est le cas on se passe de parenthèses.

Exemple Les exemples de lois de composition interne précédentes sont toutes associatives sauf le produit vectoriel.

Élément neutre

$e \in E$ est élément neutre pour $\top$ si $\forall x \in E$,

$$x \top e = e \top x = x$$

Il ne peut exister qu'un seul neutre : en effet si e_1 et e_2 sont deux éléments neutres pour la loi $\top$, $e_1 = e_1 \top e_2 = e_2$.

Commutativité

Soient $a, b \in E$. On dit que a et b commutent (pour $\top$) si $a \top b = b \top a$.

Ainsi, si $\top$ admet un neutre e, alors e commute avec tout élément de E. $\top$ est dite commutative si $\forall a, b \in E$, a et b commutent.

Exemples
- + et × dans les ensembles usuels sont commutatives
- Sur $E = \mathcal{F}(X, X)$, $\circ$ n'est pas commutative dès que X a au moins deux éléments. En effet supposons que X possède deux éléments a, b avec $a \neq b$. Considérons $f : \begin{array}{ccc} X & \longrightarrow & X \\ t & \mapsto & a \end{array}$ et $g : \begin{array}{ccc} X & \longrightarrow & X \\ t & \mapsto & b \end{array}$: on a $f \circ g(a) = a$ et $g \circ f(a) = b \neq a$. Donc $g \circ f \neq f \circ g$.

1.3 Monoïdes

Un monoïde est un couple $(E, \top)$ où E est un ensemble (non vide) et $\top$ une loi de composition interne associative admettant un neutre sur E.

Exemples

- $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \times)$
- $(\mathcal{F}(X, \mathbb{R}), \circ)$ de neutre Id_X.
- $(\mathcal{F}(X, \mathbb{R}), \times)$ de neutre la fonction constante égale à 1.
- $(\mathcal{F}(X, \mathbb{R}), +)$ de neutre la fonction nulle.

Un monoïde est dit commutatif lorsque $\top$ est commutative. Dans ce cas il est fréquent d'utiliser une notation additive $+$ pour remplacer $\top$. On note généralement 0_E le neutre de $+$ sur E .

1.4 Éléments inversibles

Soit $(E, \top)$ un monoïde, e l'élément neutre de $\top$, et $x \in E$. x est inversible à gauche (respectivement à droite) s'il existe $y \in E$ tel que $y \top x = e$ (respectivement $x \top y = e$). x est inversible si x admet un inverse à gauche et à droite.

Unicité Supposons x inversible. Soient $y, z \in E$ avec $y \top x = x \top z = e$. Alors

$$\begin{aligned} y &= y \top e \\ &= y \top (x \top z) \\ &= (y \top x) \top z \\ &= e \top z \\ &= z \end{aligned}$$

Donc $y = z$. Ceci prouve que si x est inversible ses inverses à gauche et à droite sont égaux. L'unique élément de E tel que $y \top x = x \top y = e$ s'appelle l'inverse de x pour $\top$ et se note x^{-1}.

Remarque Pour une loi additive on parle plutôt d'opposé et on note $-x$ au lieu de x^{-1}.

$$x \text{ est inversible} \Leftrightarrow \exists y \in E, y \top x = x \top y = e$$

Propriétés

- Si x est inversible, x^{-1}aussi et $\left(x^{-1}\right)^{-1} = x$
- Si x et x' sont inversibles alors $x \top x'$ aussi et $(x \top x')^{-1} = x'^{-1} \top x^{-1}$. En effet

$$\begin{aligned} \left(x + x'\right)^{-1} \top \left(x'^{-1} \top x^{-1}\right) &= x \top e \top x^{-1} \\ &= x \top x^{-1} \\ &= e \end{aligned}$$

1.5 Éléments réguliers

$x \in E$ est régulier à gauche si $\forall y, z \in E$,

$$x \top y = x \top z \Rightarrow y = z$$

et $x \in E$ est régulier à droite si $\forall y, z \in E$,

$$y \top x = z \top x \Rightarrow y = z$$

x est régulier si et seulement si x est régulier à droite et à gauche.

Remarque Si x est inversible à gauche (respectivement à droite) alors x est régulier à gauche (respectivement à droite).

En effet, soit x' un inverse de x à gauche, et $y, z \in E$. Alors :

$$\begin{aligned} x \top y = x \top z &\Rightarrow x' \top (x \top y) = x' \top (x \top z) \\ &\Rightarrow \left(x' \top x\right) \top y = \left(x' \top x\right) \top z \\ &\Rightarrow e \top y = e \top z \\ &\Rightarrow y = z \end{aligned}$$

De même, si x est inversible, alors x est régulier.

Piège ! La réciproque est fausse !

- Si l'on considère $(\mathbb{N}, \times)$, tout élément non nul est régulier mais le seul inversible de $(\mathbb{N}, \times)$ est 1.
- Dans $\left(\mathbb{Z}/6\mathbb{Z}, \dot{\times}\right)$, $\overline{2} \neq \overline{0}$ et $\overline{2}$ n'est pas régulier. En effet $\overline{2} \mathbin{\dot{\times}} \overline{3} = \overline{2} \mathbin{\dot{\times}} \overline{0}$ et $\overline{3} \neq \overline{0}$.

1.6 Itérés d'un élément pour une loi dans un monoïde

1.6.1 Définitions

Soit $(E, \top)$ un monoïde de neutre e. On définit pour $n \in \mathbb{N}$, x^n par :
- $x^0 = e$
- $\forall k \in \mathbb{N}$, $x^{k+1} = x^k \top x$

Si $\top$ est commutative et notée de manière additive, on note nx au lieu de x^n, qui se définit alors par $0x = 0_E$ et $\forall k \in \mathbb{N}$, $(k+1)\,x = kx + x$.

1.6.2 Propriétés

(1) $\forall n, m \in \mathbb{N}$, $\forall x \in E$, $x^{m+n} = x^m \top x^n = x^n \top x^m$. En notation additive, $\forall n, m \in \mathbb{N}$, $\forall x \in E$, $(n+m)\,x = nx + mx$.

(2) $\forall m, n \in \mathbb{N}$, $\forall x \in E$, $(x^n)^m = x^{nm}$. En notation additive, ceci donne $\forall x \in E$, $\forall n, m \in \mathbb{N}$, $m\,(nx) = (mn)\,x$.

(3) Soient $x, y \in E$ tels que $x \top y = y \top x$. Alors $\forall p, q \in \mathbb{N}$, $x^p \top y^q = y^q \top x^p$.

(4) Soient $x, y \in E$ tels que $x \top y = y \top x$. Alors $\forall n \in \mathbb{N}$, $(x \top y)^n = x^n \top y^n$.

(5) Soit $x \in E$ inversible pour $\top$. Pour $n \in \mathbb{N}^*$, on pose alors $x^{-n} = \left(x^{-1}\right)^n$. On a les même propriétés : $\forall m, n \in \mathbb{Z}$, $x^{n+m} = x^m \top x^n$ et $x^{nm} = (x^n)^m$. En notation additive, pour $x \in E$ et $n \in \mathbb{N}^*$, $(-n)\,x = (-x)\,n$ et $\forall n, m \in \mathbb{Z}$, $(m+n)\,x = mx + nx$ et $m\,(nx) = (nm)\,x$.

Démonstrations

(1) Soit H_n : « $\forall m \in \mathbb{N}$, $x^{n+m} = x^n \top x^m$ »
- H_0 est vraie : pour $m \in \mathbb{N}$ et $x \in E$, $x^m \top x^0 = x^m \top e = x^m$.
- Supposons H_n vraie pour $n \in \mathbb{N}$ et montrons H_{n+1}. Soient $m \in \mathbb{N}$ et $x \in E$, alors :

$$\begin{aligned} x^{(n+1)+m} &= x^{n+(m+1)} \\ &= x^n \top x^{m+1} \end{aligned}$$

Montrons alors que $\forall m \in \mathbb{N}$, $x^{m+1} = x \top x^m$ [a]. C'est vrai pour $m = 0$ car $x^{0+1} = x \top x^0$. Si c'est vrai pour $m \in \mathbb{N}$, alors

$$\begin{aligned} x^{(m+1)+1} &= x^{m+1} \top x \\ &= (x \top x^m) \top x \\ &= x \top (x^m \top x) \\ &= x \top x^{m+1} \end{aligned}$$

Le résultat est donc vrai, on peut l'appliquer :

$$\begin{aligned} x^{(n+1)+m} &= x^n \top (x \top x^m) \\ &= (x^n \top x) \top x^m \\ &= x^{n+1} \top x^m \end{aligned}$$

(2) Soit H_m : « $\forall n \in \mathbb{N}$, $\forall x \in E$, $(x^n)^m = x^{nm}$ »
- H_0 est vraie : pour $x \in E$ et $n \in \mathbb{N}$, $(x^n)^0 = e$ et $x^{0n} = e$.
- Soit $m \in \mathbb{N}$ tel que H_m est vraie, $x \in E$ et $n \in \mathbb{N}$. Alors :

$$\begin{aligned} (x^n)^{m+1} &= (x^n)^m \top x^n \\ &= x^{nm} \top x^n \\ &= x^{(m+1)n} \end{aligned}$$

(3) Montrons d'abord pour $a, b \in E$ tels que $a \top b = b \top a$, $\forall q \in \mathbb{N}$, $a \top b^q = b^q \top a$; C'est vrai pour $q = 0$ car $a \top e = e \top a$ [b]. Si c'est vrai pour $q \in \mathbb{N}$, alors

$$\begin{aligned} a \top b^{q+1} &= a \top b^q \top b \\ &= b^q \top a \top b \\ &= b^q \top b \top a \\ &= b^{q+1} \top a \end{aligned}$$

Ici, $x \top y = y \top x$ donc $\forall q \in \mathbb{N}$, $x \top y^q = y^q \top x$. En fixant q, on a toujours d'après le lemme $\forall p \in \mathbb{N}$, $x^p \top y^q = y^q \top x^p$.

(4)
- C'est vrai pour $n = 0$, car $e \top e = e$.
- Si c'est vrai pour $n \in \mathbb{N}$, alors :

$$\begin{aligned} (x \top y)^n &= (x \top y)^n \top (x \top y) \\ &= x^n \top y^n \top x \top y \\ &= x^n \top x \top y^n \top y \\ &= x^{n+1} \top y^{n+1} \end{aligned}$$

(5) *« Left to the reader ! »*

a. Le résultat n'est pas trivial : en en effet on ne suppose pas que $\top$ est commutative, et dans la définition les termes sont inversés.

b. *« Une petite dédicace pour nos amis les Basques ! »*

2 Groupes

2.1 Définitions et exemples

2.1.1 Groupe

Un groupe est un monoïde $(G,\cdot)$ tel que tout élément de G admet un inverse pour $\cdot$.
En d'autres termes, un groupe est un couple $(G,\cdot)$ où G est un ensemble non vide, $\cdot$ une loi de composition interne sur G associative, admettant un neutre et telle que tout élément de G admet un inverse pour $\cdot$.

Exemples

- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes commutatifs.
- Pour $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},\dot{+})$ est un groupe (commutatif).
- Soit $(E,\cdot)$ un monoïde, on note $\mathcal{U}(E)$ l'ensemble des éléments inversibles de E par $\cdot$. On a vu que $x,y\in\mathcal{U}(E)\Rightarrow x\cdot y\in\mathcal{U}(E)$. Ainsi, $\cdot$ devient une loi de composition interne sur $\mathcal{U}(E)$ et $(\mathcal{U}(E),\cdot)$ est un groupe :
  - $\cdot$ est associative, admet un neutre. En effet $e\in\mathcal{U}(E)$ car $e\cdot e=e\Rightarrow e^{-1}=e$.
  - Si $x\in\mathcal{U}(E)$, x^{-1} est aussi dans $\mathcal{U}(E)$ donc x est inversible dans $\mathcal{U}(E)$.
- Pour $(\mathbb{Z},\times)$, $\mathcal{U}(\mathbb{Z})=\{\pm1\}$ donc $(\{\pm1\},\times)$ est un groupe.
- Pour $(\mathbb{K},\times)$ avec $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, $\mathcal{U}(\mathbb{K})=\mathbb{K}\backslash\{0\}=\mathbb{K}^*$ donc $(\mathbb{K}^*,\times)$ est un groupe.
- Soit $X\neq\varnothing$, $E=\mathcal{F}(X,X)$ muni de $\circ$. $\mathcal{U}(E)$ est l'ensemble des bijections de X dans X noté $\mathfrak{S}(X)$ et $(\mathfrak{S}(X),\circ)$ est un groupe.
- Si X est fini, on sait que $\mathfrak{S}(X)$ est fini et $\operatorname{Card}\mathfrak{S}(X)=(\operatorname{Card}X)!$. $(\mathfrak{S}(X),\circ)$ n'est pas commutatif dès que X possède trois éléments distincts a,b et c. Pour $x,y\in X$, soit :

$$\begin{array}{rccc}\mathcal{T}_{xy}: & X & \longrightarrow & X\\ & x & \mapsto & y\\ & y & \mapsto & x\\ & t\notin\{x,y\} & \mapsto & t\end{array}$$

  On a donc $\mathcal{T}_{xy}\in\mathfrak{S}(X)$ car $\mathcal{T}_{xy}\circ\mathcal{T}_{xy}=\mathrm{Id}_X$. Or $\mathcal{T}_{ab}\circ\mathcal{T}_{bc}(a)=b$, $\mathcal{T}_{bc}\circ\mathcal{T}_{ab}(a)=c$ et $b\neq c$ donc $\mathcal{T}_{ab}\circ\mathcal{T}_{bc}\neq\mathcal{T}_{bc}\circ\mathcal{T}_{ab}$ donc $(\mathfrak{S}(X),\circ)$ n'est pas commutatif.
- En particulier, pour $n\in\mathbb{N}^*$, on note S_n au lieu de $\mathfrak{S}(\llbracket1,n\rrbracket)$. $(S_n,\circ)$ est appelé le groupe symétrique, non commutatif dès que $n\geqslant3$ et de plus fini. On rappelle $S_2=\{\mathrm{Id},\mathcal{T}_{12}\}$, $S_3=\left\{\mathrm{Id},\mathcal{T}_{12},\mathcal{T}_{23},\mathcal{T}_{31},\begin{pmatrix}1&2&3\end{pmatrix},\begin{pmatrix}1&3&2\end{pmatrix}\right.$
- Soit $n\in\mathbb{N}^*$, $E=\left(\mathbb{Z}/n\mathbb{Z},\dot{\times}\right)$. On a vu que, pour $k\in\mathbb{Z}$, $\overline{k}$ est inversible dans $\left(\mathbb{Z}/n\mathbb{Z},\dot{\times}\right)$ si et seulement si $k\wedge n=1$. Ainsi, $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})=\left\{\overline{k}|k\wedge n=1\right\}$ et $\left(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}),\dot{\times}\right)$ est un groupe commutatif fini. Par exemple, $\mathcal{U}(\mathbb{Z}/12\mathbb{Z})=\left\{\overline{1},\overline{5},\overline{7},\overline{11}\right\}$.

Remarque Soit $(G,\cdot)$ un groupe, $a\in G$. Alors $f_a:x\in G\longrightarrow x\cdot a\in G$ est une permutation de G. Pour $x\in G$:

$$\begin{aligned}f_a\left(f_{a^{-1}}(x)\right)&=a\cdot\left(a^{-1}\cdot x\right)\\&=\left(a\cdot a^{-1}\right)\cdot x\\&=e\cdot x\\&=x\end{aligned}$$

Donc $f_a\circ f_{a^{-1}}=f_{a^{-1}}\circ f_a=\mathrm{Id}_X$.

Application Soit G un groupe fini commutatif, $n=\operatorname{Card}G$. Alors, $\forall x\in G$, $x^n=e$.

En effet, notons $G=\{x_0,x_1,\ldots,x_{n-1}\}$ et soit $p=\prod_{x\in G}x=x_0x_1\cdots x_{n-1}$. Soit $a\in G$, l'ensemble $\{ax_0,ax_1,\ldots,ax_{n-1}\}$ n'est autre que G car $x\longmapsto ax$ est une permutation de G. La loi de G étant commutative, $p=(ax_0)(ax_1)\cdots(ax_{n-1})=a^np$. Or $p\in G$ et p est inversible donc régulier donc $a^n=pp^{-1}=e$.

a. Voir la section 7.4.3.3 du cours complet page 118 pour plus de précisions concernant les cycles et autres permutations.

Ainsi, soit $n \in \mathbb{N}^*$, $\forall x \in \mathbb{Z}/n\mathbb{Z}$ muni de $\dot{+}$, $nx = \overline{0}$. Pour $x \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ muni de $\dot{\times}$, $x^{\mathrm{Card}(\mathbb{Z}/n\mathbb{Z})} = x^{\varphi(n)} = \overline{1}$. En d'autres termes, $\forall k \in \mathbb{Z}/k \wedge n = 1$, $k \equiv 1\ [n]$. En particulier, si n est premier, $\varphi(n) = n-1$ et on retrouve le petit théorème de Fermat : $\forall a \in \mathbb{Z}/n \wedge a = 1 \Leftrightarrow \forall a \in \mathbb{Z}/n \nmid a$, $a^{n-1} \equiv 1\ [n]$.

2.1.2 Sous-groupes

Soit $(G, \cdot)$ un groupe et $H \subset G$. On dit que H est un sous-groupe de G si :
(1) $H \neq \varnothing$
(2) $\forall x, y \in H$, $x \cdot y \in H$
(3) $\forall x \in H$, $x^{-1} \in H$

Remarque Soit $(G, \cdot)$ un groupe de neutre e.
- Si H est un sous groupe de G, alors $e \in H$. En effet, $H \neq \varnothing$ donc pour $x \in H$, $x^{-1} \in H$ puis $x \cdot x^{-1} = e \in H$.
- Soit $H \subset G$, H est un sous groupe de G si et seulement si :

  (1) $e \in H$

  (2) $\forall x, y \in H$, $x^{-1} \cdot y \in H$

  $\Rightarrow$ *« Easy ! »*

  $\Leftarrow$ ∘ $H \neq \varnothing$ car $e \in H$.
  ∘ Soit $x \in H$, alors $x^{-1} = x^{-1} \cdot e \in H$ car $e, x \in H$.
  ∘ Soient $x, y \in H$, $x \cdot y = \left(x^{-1}\right)^{-1} \cdot y \in H$ car $x^{-1}, y \in H$.

- En notation additive, H est un sous groupe de $(G, +)$ si et seulement si :

  (1) $H \neq \varnothing$

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

  (3) $\forall x \in H$, $-x \in H$

Exemples

(1) Soit $(G, \cdot)$ un groupe de neutre e. Alors G et $\{e\}$ sont des sous-groupes de G.

(2) – $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$.
– $\mathbb{Q}$ est un sous-groupe de $(\mathbb{R}, +)$.
– $\mathbb{R}$ est un sous-groupe de $(\mathbb{C}, +)$.
– $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$
– $\forall n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous groupe de $(\mathbb{C}^*, \times)$.

Soit H un groupe fini de $(\mathbb{C}^*, \times)$. On montre [a] que $\exists n \in \mathbb{N}^*$ tel que $H = \mathbb{U}_n$. Plus généralement, si $A \subset \mathbb{C}^*$ est une partie finie et stable par $\times$, alors $\exists n \in \mathbb{N}^*$ tel que $A = \mathbb{U}_n$.

Application aux fonction périodiques On a vu [b] le résultat suivant : si H est un sous-groupe de $(\mathbb{R}, +)$, alors ou bien H est dense dans $\mathbb{R}$, ou bien $\exists \alpha \geqslant 0 \mathrm{Paragraph} H = \alpha\mathbb{Z}$.

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ continue telle que 1 et $\sqrt{2}$ sont deux périodes deux f. Montrons que f est constante.

On rappelle que $T \in \mathbb{R}$ est une période de f si $\forall x \in H$, $f(x+T) = f(x)$. Soit H l'ensemble des périodes de f. H est un sous groupe de $(\mathbb{R}, +)$:
- $0 \in H$.
- Soient $T_1, T_2 \in H$, alors $f(x + T_1 + T_2) = f(x + T_1) = f(x)$ donc $T_1 + T_2 \in H$.
- Si $T \in H$, alors $f(x) = f(x - T + T) = f(x - T)$ donc $-T \in H$.

a. « Left to the reader ! »
b. Voir section 7.1.4.2 du cours complet page 92.

Supposons maintenant que $\exists \alpha \geqslant 0 / H = \alpha\mathbb{Z}$. $1 \in H$ donc $\exists p \in \mathbb{Z}$ tel que $1 = \alpha p$ et $\sqrt{2} \in H$ donc $\exists q \in \mathbb{Z}$ tel que $\sqrt{2} = \alpha q$. Alors

$$\sqrt{2} = \frac{\sqrt{2}}{1} = \frac{q}{p} \in \mathbb{Q}$$

Ce qui est bien évidemment impossible. Donc H est dense dans $\mathbb{R}$. Nous exposerons ici deux méthodes un peu différentes pour arriver au résultat, chacune issue de l'esprit exceptionnellement brillant d'un des élèves de la classe de MPSI2 [a].

B.B.B. Montrons d'abord que H est fermé [b], soit $(T_n)_{n\in\mathbb{N}}$ une suite d'éléments de H qui converge vers $l \in \mathbb{R}$, montrons que $l \in H$. Soit $x \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $f(x) = f(x + T_n)$ donc $f(x + T_n) \underset{n\to+\infty}{\longrightarrow} f(x)$. D'autre part, $x + T_n \underset{n\to+\infty}{\longrightarrow} x + L$ et f est continue en x donc $f(x + T_n) \underset{n\to+\infty}{\longrightarrow} f(x + l)$. Ainsi $f(x) = f(x + l)$ donc $l \in H$. H et fermé donc $H = \mathrm{Adh}(H) = \mathbb{R}$ car H est dense dans $\mathbb{R}$. Si $x \in \mathbb{R}$, $f(x) = f(x + 0) = f(0)$ car x est période de f donc f est constante.

J.G.C. Montrons que f est constante d'une autre manière [c]. Soit $x \in \mathbb{R}$, H est dense dans $\mathbb{R}$ donc $\exists (T_n) \in H^{\mathbb{N}}$ qui converge vers x. Or $\forall n \in \mathbb{N}$, $f(T_n) = f(0)$ donc $f(T_n) \underset{n\to+\infty}{\longrightarrow} f(0)$. Or $T_n \underset{n\to+\infty}{\longrightarrow} x$ et f est continue en x donc $f(T_n) \underset{n\to+\infty}{\longrightarrow} f(x)$ donc $\forall x \in \mathbb{R}$, $f(x) = f(0)$.

On remarque de plus que si f est continue et périodique, alors l'ensemble des périodes de f est de la forme $T\mathbb{Z}$ avec $T > 0$.

Application aux sous-groupes de $\mathbb{Z}$: le retour du PGCD

- Pour $n \in \mathbb{N}$ on note $n\mathbb{Z} = \{np | p \in \mathbb{Z}\}$ l'ensemble des multiples de n dans $\mathbb{Z}$. En effet, $n\mathbb{Z} = (-n)\mathbb{Z}$.
- Si $n \in \mathbb{N}$ alors $n\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$:
  - $0 = n \times 0 \in n\mathbb{Z}$
  - $\forall p, q \in \mathbb{Z}$, $nq - np = n(q - p) \in n\mathbb{Z}$

Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Si $M \neq \{0\}$, soit $x \in H^*$, alors $-x \in H$. H contient donc un entier naturel non nul, c'est-à-dire $H \cap \mathbb{N}^* \neq \varnothing$. Soit donc $n = \min(H \cap \mathbb{N}^*)$, nombre qui existe car toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Montrons que $H = n\mathbb{Z}$.

- $n \in H$ donc $n + n = 2n \in H$ puis, par récurrence, $\forall k \in \mathbb{N}$, $kn \in H$. De même, $-n \in H$ donc $\forall k \in \mathbb{Z}$, $kn \in H$. Ainsi $n\mathbb{Z} \subset H$.
- Soit $m \in H$, $\exists (q, r) \in \mathbb{Z}^2$ tels que $m = nq + r$ et $0 \leqslant r \leqslant n - 1$. $nq \in n\mathbb{Z}$ et $r = m - nq \in H$ car H est un sous-groupe de $(\mathbb{Z}, +)$. Supposons que $r > 0$, $r \in H \cap \mathbb{N}^*$ et $r < n$, ce qui contredit alors la définition de n. Donc $r = 0$ donc $m = nq \in n\mathbb{Z}$ donc $H \subset n\mathbb{Z}$

2.1.3 PGCD et PPCM dans $\mathbb{Z}$

Théorème et définition

Soient $a, b \in \mathbb{Z}$. Alors il existe un unique entier naturel d vérifiant :
(1) $d \mid a$ et $d \mid b$.
(2) $\forall l \in \mathbb{Z}$, $l \mid a$ et $l \mid b \Rightarrow l \mid d$.
Cet entier est appelé le Plus Grand Commun Diviseur de a et b et est noté $a \wedge b$

a. Vous noterez sans doute qu'Aménofis ne figure pas parmi les auteurs de ces solutions. En effet ce dernier a préféré se consacrer entièrement à l'analyse critique du cours de M. Sellès sous forme de questions pertinentes qui ne manquent pas de désarçonner notre professeur par leur caractère direct et leur formulation parfois obscure. Je citerai ici un mot de M. Tancrez, autre figure emblématique de la MPSI2 assurant l'enseignement de physique-chimie ; après une de ces fameuses questions de la part d'Aménofis à laquelle il répondit avec succès, il ne put s'empêcher d'ironiser : *« Tu vois moi aussi je progresse, je te comprends de mieux en mieux. Par contre la prochaine que t'auras une question à poser, lève seulement la main. J'aurai autant d'indications sur le contenu de ta question que si tu parlais. »*

b. Ces initiales ne sont autres que celles de Blayid Ben Belkacem, au sujet duquel M. Sellès eut ce trait d'esprit fort divertissant : *« Il y en a qui sont triple A, lui il est triple B ».*

c. Personnalité phare de la classe (et accessoirement major en maths et major tout court), Julien Grand-Clément montre un certain intérêt pour l'étude des mathématiques. Cela en fait donc un allié de choix pour M. Sellès, qui profite ici de ses facultés de raisonnement.

Démonstration

Unicité : Si d et d' vérifient les conditions (1) et (2) alors $d \mid d'$ (d divise a et b et vérifie 2.) et de même $d' \mid d$. Comme d et d' sont des entiers naturels, $d = d'$.

Existence : Soit $H = a\mathbb{Z} + b\mathbb{Z} = \{ap + bq \mid p, q \in \mathbb{Z}\}$. Alors H est un sous groupe de $\mathbb{Z}$:
- $0 \in H$ car $0 = 0a + 0b$
- soient $p, q, r, s \in \mathbb{Z}$. Alors $(ap + bq) - (ar + bs) = a\underbrace{(p - r)}_{\in\mathbb{Z}} + b\underbrace{(q - s)}_{\in\mathbb{Z}} \in H$

Donc $\forall x, y \in H$, $x - y \in H$. Ainsi $\exists d \in \mathbb{N}$, $H = d\mathbb{Z}$. Montrons que d vérifie les conditions (1) et (2) :
- On a $a \in H$ car $a \times 1 + b \times 0 = a$. Donc $a \in d\mathbb{Z}$ et $d \mid a$. De même, $d \mid b$.
- Soit $l \in \mathbb{Z}$ tel que l divise a et b. $d \in d\mathbb{Z} = H$ donc $\exists u, v \in \mathbb{Z}$, $d = au + bv$. $l \mid a$ donc $l \mid au$. De même $l \mid bv$. Donc $l \mid au + bv = d$.

Remarques
- Avec cette définition, $0 \wedge 0 = 0$ [a].
- Pour $a, b \in \mathbb{Z}$: $a\mathbb{Z} = |a|\,\mathbb{Z}$ et $b\mathbb{Z} = |b|\,\mathbb{Z}$. Donc $a \wedge b = |a| \wedge |b|$ [b].
- Cette nouvelle définition est en accord avec celle du chapitre sur les entiers naturels [c] : en effet soient $a, b \in \mathbb{N}$, non tous deux nuls, $\delta = a \wedge b$ tel que défini dans le cours sur les entiers et $d = a \wedge b$ avec la nouvelle définition. $d \in \mathbb{N}$, $d \mid a$ et $d \mid b$ donc $d \leqslant \delta$ car $\delta = \max(\mathcal{D}(a) \cap \mathcal{D}(b))$. Mais aussi $\delta \mid a$ et $\delta \mid b$ donc $\delta \mid d$ donc $\delta \leqslant d$. Ainsi, $d = \delta$.

Théorèmes de Bézout

(1) $\forall a, b \in \mathbb{Z}$, $d = a \wedge b$, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = d$. En effet, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $d \in d\mathbb{Z}$ d'où le résultat.

(2) $\forall a, b \in \mathbb{Z}$, $a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} / au + bv = 1$.

$\Rightarrow$ *« Djàvu ! »*

$\Leftarrow$ Soit $d = a \wedge b$, $d \in \mathbb{N}$ et $d \mid au + bv = 1$ donc $d = 1$.

Corollaires
- Théorème de Gauss et variantes [d].
- $\forall a, b \in \mathbb{Z}^*$ avec $d = a \wedge b$, on a
$$\frac{a}{d} \wedge \frac{b}{d} = 1$$
En effet, notons $a = da'$ et $b = db'$, d'après le théorème de Bézout, $\exists u, v \in \mathbb{Z}$ tels que
$$\begin{aligned} au + bv = d &\Leftrightarrow d\left(a'u + b'v\right) = d \\ &\Leftrightarrow a'u + b'v = 1 \quad \text{car } d \neq 0 \end{aligned}$$

Exercice Soient $a, b, k \in \mathbb{N}$, alors $(ka) \wedge (kb) = k(a \wedge b)$.
- Si $k = 0$, c'est vrai.
- Si $a = b = 0$, c'est vrai.
- Supposons $k \neq 0$ et $(a, b) \neq (0, 0)$ et soit $d = a \wedge b$, $\delta = ka \wedge kb$. $d \mid a$ et $d \mid b$ donc $kd \mid ka$ et $kd \mid kb$ donc $kd \mid \delta$. De plus, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = d \Rightarrow kau + kbv = kd$ or $\delta \mid kau$ et $\delta \mid kbv$ donc $\delta \mid kd$. Finalement, $\delta = kd$.

Généralisation : PGCD de plusieurs entiers

a. Note d'Alexandre Carton : on notera que lors d'un calcul dans un DM précédent, le magnifique Denis Merigoux, maître des Flambis et disciple Faux-fil, réfléchit quand à la valeur de $0 \wedge 0$, et le superbe, l'impétueux, le terrible, le magnifique, etc. maître du temple des Flambis décréta par anticonformisme que cette valeur était « la tête à toto » . Néanmoins pour simplifier les calculs, on ne tiendra pas compte dans la suite de cette pertinente remarque.

b. Ainsi pour le calcul du PGCD d'entiers relatifs on peut toujours se ramener aux entiers naturels.

c. Voir section 7.3.1.1 du cours complet page 98.

d. Pour les énoncés et démonstrations, se reporter à la section 7.3.2.2 du cours complet page 101.

Théorème et définition Soient $m \geqslant 2$, $a_1, a_2, \ldots, a_m \in \mathbb{Z}$. Alors il existe un unique entier naturel d tel que :

(1) $\forall i \in [\![1, n]\!]$, $d \mid a_i$

(2) $\forall l \in \mathbb{Z}$, si $\exists i \in [\![1, n]\!]$ tel que $l \mid a_i$, alors $l \mid d$.

Démontrons ce résultat :

Unicité : C'est trivial, même démonstration que dans le cas de deux entiers.

Existence : Soit $H = \sum_{i=1}^{n} a_i\mathbb{Z} = \left\{ \sum_{i=1}^{n} a_i\mu_i \middle| (\mu_1, \mu_2, \ldots, \mu_n) \in \mathbb{Z}^n \right\}$. Il est clair que H est un sous-groupe de $(\mathbb{Z}, +)$ donc $\exists d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$, on montre ensuite que d vérifie (1) et (2).

Remarques

- Analogue de Bézout : soient $a_1, a_2, \ldots, a_m \in \mathbb{Z}$ et $d = \bigwedge_{i=1}^{m} a_i$ [a], alors $\exists u_1, u_2, \ldots, u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} a_i u_i = d$.
- On dit que les a_i sont premiers entre eux dans leur ensemble si $\bigwedge_{i=1}^{m} a_i = 1$.
- Corollaire de Bézout : $\bigwedge_{a=1}^{m} a_i = 1 \Leftrightarrow \exists u_1, u_2, \ldots, u_n / \sum_{i=1}^{n} a_i u_i = 1$.
- Soient $a_1, a_2, \ldots, a_m \in \mathbb{Z}$ avec $m \geqslant 2$. S'il existe $i \neq j$ tel que $a_i \wedge a_j = 1$, alors tous les a_iPlait premiers entre eux dans leur ensemble.
  En effet, soit $d = \bigwedge_{k=1}^{m} a_k$. $d \mid a_i$ et $d \mid a_j$ donc $d \mid 1$ donc $d = 1$.
- On en déduit un résultat moins fort : si $\forall i \neq j$, $a_i \wedge a_j = 1$, alors $\bigwedge_{i=1}^{m} a_i = 1$.
  La réciproque est fausse : $a = 6$, $b = 10$ et $c = 15$, soit $d = a \wedge b \wedge c$. Si $d \geqslant 2$, soit p premier divisant d. $p \mid d$ donc $p \mid a$ et $p \mid b$ donc $p \mid a \wedge b = 2$. De même, $p \mid 5$ et $p \mid 3$ donc $p = 1$.

Plus Petit Commun Multiple

Soient $a, b \in \mathbb{Z}$. Alors il existe un et un seul entier naturel m tel que $a \mid m$, $b \mid m$ et $\forall l \in \mathbb{Z}$, si $a \mid l$ et $b \mid l$, alors $m \mid l$.

Unicité : $m_1 \mid m_2$ et $m_2 \mid m_1$ donc $m_1 = m_2$.

Existence : $H = a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ comme intersection de sous-groupes [b] donc $\exists m \in \mathbb{N}$ tel que $H = m\mathbb{Z}$. m vérifie bien (1) et (2).

On remarque les propriétés immédiates suivantes :

- $\forall a, b \in \mathbb{Z}$, $a \vee b = |a| \vee |b|$.
- $\forall a \in \mathbb{Z}$, $a \vee 0 = 0$.

Proposition Pour $a, b \in \mathbb{N}$, $(a \wedge b)(a \vee b) = ab$.

Petit lemme $\forall k, a, b \in \mathbb{N}$, $(ka) \vee (kb) = k(a \vee b)$

- Si $k = 0$, $a = 0$ ou $b = 0$, c'est vrai.
- Supposons $k, a, b \in \mathbb{N}^*$, posons $m = a \vee b$ et $M = (ka) \vee (kb)$. $a \mid m$ donc $ka \mid km$, et de même $kb \mid km$ donc $M \mid km$. De plus, $ka \mid M$ et $kb \mid M$ donc $\exists u, v \in \mathbb{N}$ tels que $M = kau = kbv$ d'où $a \mid \frac{M}{k}$ et $b \mid \frac{M}{k}$ donc $m \mid \frac{M}{k}$ donc $km \mid M$. Ainsi, $km = M$.

a. Ce qui signifie que d est le PGCD de tous les a_i.

b. On admet ici une propriété vue dans la section suivante page 11.

Démonstration
- Si $a = 0$ ou $b = 0$, c'est vrai.
- Supposons $a \neq 0$ et $b \neq 0$.
  - Supposons $a \wedge b = 1$. Soit $m = a \vee b$, $a \mid m$ et $b \mid m$ donc, d'après une variante du théorème de Gauss [a] puisque $a \wedge b = 1$, $ab \mid m$. De plus $a \mid ab$ et $b \mid ab$ donc $m \mid ab$ donc $m = ab$.
  - Revenons au cas général. Soit $d = a \wedge b$, posons $a' = \dfrac{a}{d}$ et $b' = \dfrac{b}{d}$. On a $a \vee b = (da') \vee (db') = d(a' \vee b') = da'b'$ d'après le lemme. En multipliant l'égalité par d, on a $d(a \vee b) = d^2a'b' = ab$ d'où le résultat.

2.1.4 Propriétés des sous-groupes

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

Démonstration $\forall i \in I$, $e \in H_i$ car H_i est un sous-groupe. Soient $x, y \in \bigcap_{i\in I} H_i$, alors pour tout $i \in I$, $x \in H_i$ et $y \in H_i$ donc $x^{-1} \cdot y \in H_i$.

Petite histoire C'est l'histoire d'un sous-groupe engendré par une partie [b]...

Soit $S \subset G$, considérons $\mathcal{F}$ l'ensemble des sous-groupes H tels que $S \subset H$. On note que $\mathcal{F} \neq \varnothing$ car $G \in \mathcal{F}$. Posons $\mathrm{gr}(S) \subset H$ l'intersection de tous les sous-groupes de G que contient $\mathcal{F}$. C'est donc un sous-groupe d'après le théorème.

Si H est un sous groupe de G qui contient S, alors $\mathrm{gr}(S) \subset H$ donc $\mathrm{gr}(S)$ est le plus petit sous-groupe qui contient S. On le nomme sous-groupe de G engendré par S. On dira donc que S engendre G si $\mathrm{gr}(S) = G$.

On remarque immédiatement que $\mathrm{gr}(\varnothing) = \{e\}$ où e est le neutre de $(G, \cdot)$. Soit $x \in G$, on note $\mathrm{gr}(x)$ le sous-groupe engendré par $\{x\}$. $x \in \mathrm{gr}(x)$ donc $x^2 = x \cdot x \in \mathrm{gr}(x)$ puis, par récurrence, $\forall n \in \mathbb{N}$, $x^n \in \mathrm{gr}(x)$. De la même façon , $x^{-1} \in \mathrm{gr}(x)$ donc $\forall k \in \mathbb{Z}$, $x^k \in \mathrm{gr}(x)$. Ainsi, $L(x) = \left\{x^k | k \in \mathbb{Z}\right\} \subset \mathrm{gr}(x)$.

Mais :

(1) $x \in L(x)$ car $x = x^1$

(2) Pour $n, m \in \mathbb{Z}$, $x^n \cdot x^m = x^{mn}$ puis $\left(x^{-1}\right)^n = x^{-n}$ donc $\forall x, y \in L(x)$, $x^{-1} \cdot y \in L(x)$.

$L(x)$ est un sous-groupe de G qui contient x donc $\mathrm{gr}(x) \subset L(x)$ donc $\mathrm{gr}(x) = L(x) = \left\{x^k | k \in \mathbb{Z}\right\}$.

On dit que G est monogène s'il existe $x \in G$ tel que $G = \mathrm{gr}(x)$. On dit que x est cyclique s'il est monogène et fini.

En notation additive, si $x \in G$ muni de $\cdot$, alors $\mathrm{gr}(x) = \{nx | n \in \mathbb{Z}\}$.

Exemples
- $(\mathbb{Z}, +)$ est monogène car $\mathbb{Z} = \mathrm{gr}(1) = \mathrm{gr}(-1)$.
- $(\mathbb{U}_n, \times)$ est cyclique car $\mathbb{U}_n$ est un sous-groupe muni d'une loi donc un groupe, $\mathbb{U}_n$ est fini de cardinal n et $\mathbb{U}_n = \mathrm{gr}(\omega)$ où $\omega = \mathrm{e}^{\frac{2i\pi}{n}}$.
- $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est cyclique car $\mathbb{Z}/n\mathbb{Z} = \mathrm{gr}\left(\overline{1}\right)$ et $\mathrm{Card}\, \mathbb{Z}/n\mathbb{Z} = n$.

a. Se référer à la section 7.3.2.2 du cours complet page 101.

b. La bienheureuse progéniture de M. Sellès profite bien évidemment des magnifiques petites histoires de celui-ci, qui leur garantissent un sommeil de plomb très rapide.

Conséquences Un groupe monogène est forcément commutatif, donc un groupe non-commutatif ne peut être monogène.

2.2 Morphismes de groupe

2.2.1 Définitions

Soient $(G,\cdot)$ et $(H,\star)$ deux groupes et $f : G \longrightarrow H$. On dit que f est un morphisme de groupes si $\forall x, y \in G$, $f(x \cdot y) = f(x) \star f(y)$.

Exemples
- ln est un morphisme de groupes de $\left(\mathbb{R}_+^*, \times\right)$ dans $(\mathbb{R}, +)$.
- exp est un morphisme de groupes de $(\mathbb{R}, +)$ dans $\left(\mathbb{R}_+^*, \times\right)$.
- Pour $\alpha \in \mathbb{R}$, $x \in \mathbb{R}_+^* \longmapsto x^\alpha$ est un morphisme de groupes de $\left(\mathbb{R}_+^* \times\right)$ dans $\left(\mathbb{R}_+^*, \times\right)$.
- $\varphi : \begin{array}{l} \mathbb{C}^* \longrightarrow \mathbb{R}_+^* \\ z \mapsto |z| \end{array}$ est un morphisme de groupes de $(\mathbb{C}^*, \times)$ dans $\left(\mathbb{R}_+^*, \times\right)$.
- $\psi : \begin{array}{l} \mathbb{C}^* \longrightarrow \mathbb{C}^* \\ z \mapsto \overline{z} \end{array}$ est un morphisme de groupes de $(\mathbb{C}^*, \times)$ dans $(\mathbb{C}^*, \times)$.
- $t \longmapsto \mathrm{e}^{it}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$.

Remarque Soit $(G,\cdot)$ un groupe, H un sous-groupe de G. Alors $\cdot$ devient par restriction une loi de composition interne sur H et $(H,\cdot)$ est un groupe.

Vocabulaire
- Soit $(G,\cdot)$ et $(H,\star)$ deux groupes. Un morphisme de groupes bijectif de G dans H est appelé isomorphisme [a].
- Deux groupes sont isomorphes s'il existe un isomorphisme de l'un dans l'autre.
- Un morphisme de groupes de G dans G est un endomorphisme.
- Un endomorphisme bijectif est un automorphisme.

2.2.2 Propriété des morphismes

Soient $(G,\cdot)$ et $(H,\star)$ deux groupes et $f : G \longrightarrow H$ un morphisme de groupes. Alors :

(1) $f(e_G) = e_H$

(2) Pour $x \in G$:
   (a) $\forall n \in \mathbb{N}$, $f(x^n) = (f(x))^n$
   (b) $f\left(x^{-1}\right) = (f(x))^{-1}$
   (c) $\forall n \in \mathbb{Z}$, $f(x^n) = (f(x))^n$

(3) Soit G_1 un sous-groupe de $(G,\cdot)$. Alors $f(G_1)$ est un sous-groupe de $(H,\star)$.

(4) Soit H_1 un sous-groupe de $(H,\star)$. Alors :
   (a) $f^{-1}(H_1)$ est un sous-groupe de $(G,\cdot)$;
   (b) en particulier, $f^{-1}(\{e_H\}) = \{x \in G | f(x) = e_H\}$ est un sous-groupe de $(G,\cdot)$ appelé noyau de f et noté $\operatorname{Ker} f$;
   (c) f est injective si et seulement si $\operatorname{Ker} f = \{e_G\}$, c'est-à-dire $\forall x \in G$, $f(x) = e_H \Rightarrow x = e_G$.

a. « *Non, ce n'est pas l'isomorphisme végétal d'Yves Rocher. Pire que des chimistes ceux-là !* ». En effet, M Sellès possède un point de vue très hiérarchisé sur les sciences : d'abord les mathématiques, puis les physiciens, enfin les chimistes, qui se vautrent dans les bas-fond de la connaissance. Et les biologistes dans tout cela ? Je ne ferai que citer M. Tancrez : *« Généralement pour faire une régression linéaire il faut au moins une dizaine de points. En dessous c'est pas fiable. À ce propos j'ai vu dans une revue de biologie une régression linéaire faite avec 2 points. Évidemment c'est facile d'aligner deux points, par contre ça fait pas très sérieux. »*.

Démonstrations

(1) On a $f(e_G) = f(e_G \cdot e_G) = f(e_G) \star f(e_G)$. Soit z l'inverse de $f(e_G)$ dans H. Alors $e_H = z \star f(e_G) = \underbrace{z \star f(e_G)}_{e_H} \star f(e_G) = f(e_G)$.

(2) (a) Soit H_n : « $f(x^n) = (f(x))^n$ »
- C'est vrai pour $n = 0$ car $f\left(x^0\right) = f(e_G) = e_H = \left(f\left(x^0\right)\right)^0$.
- Si c'est vrai pour $n \in \mathbb{N}$, alors

$$\begin{aligned} f\left(x^{n+1}\right) &= f(x^n \cdot x) \\ &= f(x^n) \star f(x) \\ &= (f(x))^n \star f(x) \\ &= (f(x))^{n+1} \end{aligned}$$

(b) On a $e_H = f(e_G) = f\left(x \cdot x^{-1}\right) = f(x) \star f\left(x^{-1}\right)$ donc $f\left(x^{-1}\right) = (f(x))^{-1}$.

(c) Pour $n \in \mathbb{N}$, $f(x^{-n}) = f\left(\left(x^{-1}\right)^n\right) = \left(f\left(x^{-1}\right)\right)^n = (f(x))^{-n}$.

(3) – $e_G \in G_1$ donc $e_H = f(e_G) \in G_1$.
– Soient $z, t \in f(G_1)$, montrons que $z^{-1} \star t \in f(G_1)$. On sait que $\exists x, y \in G_1$ tels que $f(x) = z$ et $f(y) = t$. Alors

$$\begin{aligned} z^{-1} \star t &= (f(x))^{-1} \star f(y) \\ &= f\left(x^{-1}\right) \star f(y) \\ &= f\left(x^{-1} \cdot y\right) \end{aligned}$$

Or $x^{-1} \cdot y \in G_1$ car G_1 est un sous-groupe donc $z^{-1} \star t \in f(G_1)$.

(4) (a) Montrons que $f^{-1}(H_1)$ est un sous-groupe :
- $e_G \in f^{-1}(H_1)$ car $f(e_G) = e_H \in H_1$.
- Soient $x, y \in f^{-1}(H_1)$, montrons que $x^{-1} \cdot y \in f^{-1}(H_1)$. $f\left(x^{-1} \cdot y\right) = (f(x))^{-1} \star f(y)$ or $x \in f^{-1}(H_1)$ donc $f(x) \in H_1$ et de même, $f(y) \in H_1$ donc $f(x)^{-1} \star f(y) \in H_1$ car H_1 est un sous-groupe, d'où le résultat.

(b) $\{e_H\}$ est un sous-groupe de $(H, \star)$ donc $\operatorname{Ker} f$ est un sous-groupe de $(G, \cdot)$.

(c) $\Rightarrow$ Si f est injective, montrons que $\operatorname{Ker} f = \{e_G\}$. On a toujours $\{e_G\} \subset \operatorname{Ker} f$. Soit $x \in \operatorname{Ker} f$, montrons que $x = e_G$. $f(x) = e_H = f(e_G)$ car f est un morphisme, et de plus f est injective donc $x = e_G$.

$\Leftarrow$ Supposons que $\operatorname{Ker} f = \{e_G\}$, montrons que f est injective. Soient $x, y \in G$ avec $f(x) = f(y)$, montrons que $x = y$. On a $f(x) \star (f(y))^{-1} = f\left(x^{-1} \cdot y\right) = e_H$ donc $x^{-1} \cdot y \in \operatorname{Ker} f = \{e_G\}$. Ainsi, $x^{-1} \cdot y = e_G \Leftrightarrow x = y$.

2.2.3 Composée de deux morphismes

(1) Soient $(G, \cdot)$, $(H, \star)$ et $(L, \top)$ trois groupes et $f : G \longrightarrow H$ et $g : H \longrightarrow L$ des morphismes de groupes. Alors $g \circ f$ est un morphisme de $(G, \cdot)$ dans $(L, \top)$.

(2) Soient $(G, \cdot)$ et $(H, \star)$ deux groupes et $f : G \longrightarrow H$ un isomorphisme de groupes. Alors f^{-1} est un isomorphisme de $(H, \star)$ dans $(G, \cdot)$.

Démonstrations

(1) Soient $x, y \in G$, alors :

$$\begin{aligned} g \circ f(x \cdot y) &= g(f(x \cdot y)) \\ &= g(f(x) \star f(y)) \\ &= g(f(x)) \top g(f(y)) \\ &= g \circ f(x) \top g \circ f(y) \end{aligned}$$

(2) Soient $z,t\in H$, montrons que $\underbrace{f^{-1}(z\star t)}_{u}=\underbrace{f^{-1}(z)\cdot f^{-1}(t)}_{v}$. On a

$$f(u) = f\left(f^{-1}(z\star t)\right)=z\star t \quad \text{et} \quad f(v)=f\left(f^{-1}(z)\cdot f^{-1}(t)\right)=f\left(f^{-1}(z)\right)\star f\left(f^{-1}(t)\right)=z\star t$$

$f(u)=f(v)$ et f est injective donc $u=v$.

Application Soit $(G,\cdot)$ un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. On a $\mathrm{Aut}(G)\subset\mathfrak{S}(G)$, et de plus :
- $\mathrm{Id}_G\in\mathrm{Aut}(G)$
- $\forall f,g\in\mathrm{Aut}(G)$, $f\circ g\in\mathrm{Aut}(G)$
- $f^{-1}\in\mathrm{Aut}(G)$

Ainsi, $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathfrak{S}(G),\circ)$.

3 Anneaux et corps

3.1 Définitions, règles de calcul, exemples

3.1.1 Définitions

Un anneau est un triplet $(A,+,\times)$ où A est un ensemble non vide, $+$ et $\times$ des lois de composition internes telles que :
(1) $(A,+)$ est un groupe commutatif de neutre O_A (on parle de zéro de A).
(2) $(A,\times)$ est un monoïde de neutre 1_A.
(3) $\times$ est distributive à gauche et à droite par rapport à $+$: $\forall a,b,c\in A$, $(a+b)\times c=a\times c+b\times c$ et $c\times(a+b)=c\times a+c\times b$.

L'anneau $(A,+,\times)$ est commutatif si $\times$ est commutative [a].

Exemples
- $(\mathbb{Z},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$.
- Si X est un ensemble, $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, alors $(\mathcal{F}(X,\mathbb{K}),+,\times)$ est un anneau.
- Pour $n\in\mathbb{N}^*$, $\left(\mathbb{Z}/n\mathbb{Z},\dot{+},\dot{\times}\right)$ est un anneau.

Tous les exemples d'anneaux ci-dessus sont des anneaux commutatifs.

Exercice On définit $M_2(\mathbb{R})$ par l'ensemble des matrices $\begin{pmatrix}a & c\\ b & d\end{pmatrix}$ avec $a,b,c,d\in\mathbb{R}$, et les lois $+$ et $\times$ par : $\forall a,b,c,d,a',b',c',d'\in\mathbb{R}$,

$$\begin{pmatrix}a & c\\ b & d\end{pmatrix}+\begin{pmatrix}a' & c'\\ b' & d'\end{pmatrix}=\begin{pmatrix}a+a' & c+c'\\ b+b' & d+d'\end{pmatrix} \quad \text{et} \quad \begin{pmatrix}a & c\\ b & d\end{pmatrix}\times\begin{pmatrix}a' & c'\\ b' & d'\end{pmatrix}=\begin{pmatrix}aa'+cb' & ac'+cd'\\ ba'+db' & bc'+dd'\end{pmatrix}$$

Vérifier que $(M_2(\mathbb{R}),+,\times)$ est un anneau.

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

Les éléments inversibles s'appellent les unités de A, dont l'ensemble se note $\mathcal{U}(A)$. On sait que $(\mathcal{U}(A),\times)$ est un groupe : le groupe des inversibles du monoïde $(A,\times)$ s'appelle le groupe des unités de A.

Par exemple, pour $\times$, $\mathcal{U}(\mathbb{Z})=\{\pm1\}$, $\mathcal{U}(\mathbb{R})=\mathbb{R}^*$, $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})=\left\{\overline{k}|k\in[\![1,n]\!] \text{ et } k\wedge n=1\right\}$.

3.1.2 Règles de calcul dans les anneaux

Soit $(A,+,\times)$ un anneau de neutre 0_A et 1_A pour $+$ et $\times$ respectivement. Pour $x\in A$, $-x$ est l'opposé de x par $+$.

a. En effet, $+$ est déjà obligatoirement commutative.

Élément absorbant $\forall x \in A$,

$$0_A \times x = x \times 0_A = 0_A$$

Si $1_A \neq 0_A$, ceci montre que 0_A n'est jamais inversible donc $\mathcal{U}(A) \subset A \backslash \{0_A\}$. Si $1_A = 0_A$, alors $\forall x \in A$, $x = x \times 1_A = 0_A$ donc $A = \{0_A\}$. Ce cas trivial sera systématiquement écarté par la suite.

Démonstration On a $0_A = 0_A + 0_A$ donc, pour $x \in A$,

$$\begin{aligned} x \times 0_A &= x \times (0_A + 0_A) \\ &= x \times 0_A + x \times 0_A \end{aligned}$$

D'où :

$$\begin{aligned} 0_A &= x \times 0_A - x \times 0_A \\ &= x \times 0_A + \underbrace{x \times 0_A - x \times 0_A}_{0_A} \\ &= x \times 0_A \end{aligned}$$

Relations entre itération de + et × Fixons $x \in A$, alors $f : y \in A \longrightarrow x \times y$ est un endomorphisme [a] de $(A, +)$. Donc, $\forall y \in A$, $\forall n \in \mathbb{Z}$, $f(ny) = nf(y)$ d'où

$$x \times (ny) = n(x \times y)$$

En particulier, avec $y = 1_A$, $x \times n1_A = n(x \times 1_A) = nx$.psdot[dotstyle=|]$g : y \in A \longrightarrow y \times x$, on a, $\forall y \in A$, $\forall n \in \mathbb{Z}$, $(ny) \times x = n(y \times x)$ d'où $1_A n \times x = nx$. Pour récapituler, $\forall x, y \in A$, $\forall n \in \mathbb{Z}$, on a :

$$x \times (ny) = (nx) \times y = n(x \times y)$$

On a de même, $\forall x \in A$, $-1_A \times x = x \times (-1_A) = -x$.

Règle des signes Soient $x, y \in A$, on a $(-y) \times x = -(x \times y)$ et $x \times (-y) = -(x \times y)$ donc

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

De plus, $(-y) \times (-x) = --(y \times x) = y \times x$.

Distributivité étendue

– Pour $a \in A$, $n \in \mathbb{N}^*$, $b_1, b_2, \ldots, b_n \in A$:

$$a \times \sum_{k=1}^{n} b_k = \sum_{k=1}^{n} a \times b_k \quad \text{et} \quad \left(\sum_{k=1}^{n} b_k\right) \times a = \sum_{k=1}^{n} b_k \times a$$

– Pour $n, m \in \mathbb{N}^*$, $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in A$, alors :

$$\begin{aligned} \underbrace{\left(\sum_{i=1}^{m} a_i\right)}_{a'} \times \left(\sum_{j=1}^{m} b_j\right) &= \sum_{j=1}^{n} a' \times b_j \\ &= \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_i\right) \times b_j \\ &= \sum_{j=1}^{m} \sum_{i=1}^{n} a_i \times b_j \end{aligned}$$

a. Voir section 2.2.1 page 12.

Mais on a aussi :

$$\begin{aligned}\left(\sum_{i=1}^{n} a_i\right) \times \underbrace{\left(\sum_{j=1}^{n} b_j\right)}_{b'} &= \sum_{i=1}^{n} a_i \times b' \\ &= \sum_{i=1}^{n} a_i \times \left(\sum_{j=1}^{m} b_j\right) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i \times b_j\end{aligned}$$

Formule du binôme

Pour $a, b \in A$ tels que $a \times b = b \times a$, $\forall n \in \mathbb{N}$:

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

Piège ! Si $a \times b \neq b \times a$, la formule peut être fausse. Pour $n = 2$, $(a+b)^2 = (a+b) \times (a+b) = a \times (a+b) + b \times (a+b) = a^2 + a \times b + b \times a + b^2$. De plus, $\sum_{k=0}^{2} \binom{2}{k} a^k b^{2-k} = a^2 + 2a \times b + b^2$. Il y a donc égalité si et seulement si $a \times b = b \times a$.

Factorisation De même, pour $a, b \in A$ tels que $a \times b = b \times a$, $\forall n \in \mathbb{N}^*$:

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

En effet, la formule est vraie de manière évidente pour $n = 0$ et $n \geqslant 1$. On pose en effet par convention $\sum_{x \in \varnothing} \cdots = 0_A$. Pour $n \geqslant 1$, on a :

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

Si $ab = ba$ [a], $a^2 - b^2 = (a-b)(a+b)$, mais aussi $a^3 - b^3 = (a-b)\left(a^2 + ab + b^2\right)$ d'où $a^3 + b^3 = (a+b)\left(a^2 - ab + b^2\right)$.

3.1.3 Anneaux intègres

Un anneau $(A, +, \times)$ est intègre si :
(1) $(A, +, \times)$ est commutatif.
(2) $\forall x, y \in A$, $x \times y = 0_A \Rightarrow x = 0_A$ ou $y = 0_A$.
Cette dernière condition est équivalente à $\forall x, y \in A \setminus \{0\}$, $y \times x \neq 0_A$.

a. J'oublie ici volontairement de noter $a \times b$: la multiplication sera désormais implicite lors des calculs.

Exemples
- $(\mathbb{Z}, +, \times)$ est un anneau intègre, ainsi que beaucoup des anneaux usuels. Mais il existe des contre-exemples.
- $\left(\mathbb{Z}/6\mathbb{Z}, \dot{+}, \dot{\times}\right)$ n'est pas intègre : $\overline{2}\dot{\times}\overline{3} = \overline{0}$ mais $\overline{2} \neq \overline{0}$ et $\overline{3} = \overline{0}$.
- Soit $n \in \mathbb{N}^*$, alors $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ est intègre si et seulement si n est premier.

  $\Rightarrow$ Par contraposée : supposons que n n'est pas premier et montrons que $\mathbb{Z}/n\mathbb{Z}$ ne peut être un anneau intègre. Si n n'est pas premier, alors $n = pq$ avec $p, q \in [\![2, n-1]\!]$ d'où :

$$\overline{0} = \overline{n} = \overline{pq} = \overline{p}\dot{\times}\overline{q}$$

  Or $\overline{p} \neq \overline{0}$ et $\overline{q} \neq \overline{0}$ donc $\mathbb{Z}/n\mathbb{Z}$Plain Layoutntègre.

  $\Leftarrow$ Supposons n premier, soient $x, y \in \mathbb{Z}/n\mathbb{Z}$ avec $x\dot{\times}y = \overline{0}$. Alors $\exists k, l \in [\![0, n-1]\!]$ tels que $x = \overline{k}$ et $y = \overline{l}$. Ainsi, $\overline{0} = \overline{kl}$ donc $n \mid kl$. Or n est premier donc $n \mid k$ ou $n \mid l$ donc $\overline{k} = \overline{0}$ ou $\overline{l} = \overline{0}$.

Remarque Soit $(A, +, \times)$ intègre, alors tout élément non nul de A est régulier pour $\times$: si $a \in A \backslash \{0_A\}$, alors $\forall b, c \in A$, $a \times b = a \times c \Rightarrow b = c$.

En effet, $a \times b = a \times c \Rightarrow a \times (b - c) = 0$ donc $a = 0_A$ ou $b - c = 0_A \Leftrightarrow b = c$ or $a \neq 0_A$ donc $b = c$.

3.1.4 Corps

Un anneau commutatif $(\mathbb{K}, +, \times)$ est un corps si tout élément non nul est inversible par $\times$.

Exemples
- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.
- Tout corps est un anneau intègre : soit $(\mathbb{K}, +, \times)$ un corps, $x, y \in \mathbb{K}$ avec $x \times y = 0_{\mathbb{K}}$. Si $x \neq 0_{\mathbb{K}}$, alors x est un inversible donc $x^{-1} \times x \times y = 0_{\mathbb{K}} \Rightarrow y = 0_{\mathbb{K}}$.
- Soit $n \in \mathbb{N}^*$, $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ est un corps si et seulement si n est premier.

  $\Rightarrow$ Si $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ est un corps, c'est un anneau intègre donc n est premier [a].

  $\Leftarrow$ Si n est premier, $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ est un anneau intègre. Montrons que tout élément de $\mathbb{Z}/n\mathbb{Z} \backslash \left\{\overline{0}\right\}$ est inversible. Soit $l \in [[1, n-1]]$, montrons que $\overline{l}$ est inversible. $n \nmid l$ donc $n \wedge l = 1$ car n est premier donc $l \in \mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right)$.

  Si p est un nombre premier, on note en général $\mathbb{F}_p$ au lieu de $\mathbb{Z}/p\mathbb{Z}$.

3.2 Sous-anneaux, morphismes d'anneaux

3.2.1 Sous-anneau

Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un sous-anneau de A si :
(1) B est un sous-groupe de $(A, +)$ [a].
(2) B est stable par $\times$: $\forall x, y \in B$, $x \times y \in B$.
(3) $1_A \in B$.

a. $0_A \in B$ et $\forall x, y \in B$, $x - y \in B$.

Exemples
- $\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$.
- $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$:
  (1) $0 = 0 + i0$ et $\forall a, b, c, d \in \mathbb{Z}[i]$, $a + ib - (c + id) = a - b + i(c - d) \in \mathbb{Z}[i]$.
  (2) $(a + ib)(c + id) = ac - bd + i(ad + bc) \in \mathbb{Z}[i]$.

a. Voir le troisième exemple de la section précédente pour la preuve de ce raisonnement.

(3) $1 = 1 + 0i \in \mathbb{Z}[i]$.

- $\mathbb{Z}$ est l'unique sous-anneau de $\mathbb{Z}$. En effet, si A est un sous-anneau de $\mathbb{Z}$, alors $1 \in A \Rightarrow A = \text{gr}(1) = \mathbb{Z}$.
- $2\mathbb{Z} = \{2m | m \in \mathbb{Z}\}$ vérifie (1) et (2) mais pas (3), ce n'est donc pas un sous-anneau.

Hors-programme Un idéal de $(A, +, \times)$ est une partie I de A telle que :

(1) I est un sous-groupe de $(A, +)$.

(2) $\forall a \in A$, $\forall x \in I$, $x \times a \in I$ et $a \times x \in I$.

Théorème

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

Remarques

- Si B est un sous-anneau de $(A, +, \times)$, alors $(B, +, \times)$ devient un anneau. Si A est intègre, alors B aussi.
- Soit $(L, +, \times)$ un corps et $\mathbb{K} \subset L$. On dit que $\mathbb{K}$ est un sous-corps de L si c'est un sous-anneau de L qui est en fait un corps :

  (1) $\mathbb{K}$ est un sous-anneau de L.

  (2) $\forall x \in \mathbb{K}\backslash\{0\}$, $\dfrac{1}{x} \in \mathbb{K}$.

Application On pose $\mathbb{Q}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} | a, b \in \mathbb{Q}\right\}$. Montrons que $\mathbb{Q}\left[\sqrt{5}\right]$ est un sous-corps de $\mathbb{R}$.

- $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{5}\right]$ car $\forall a \in \mathbb{Q}$, $a = a + 0\sqrt{5} \in \mathbb{Q}\left[\sqrt{5}\right]$.
- $\forall a, b, c, d \in \mathbb{Q}$, $a + b\sqrt{5} + \left(c + \sqrt{5}d\right) = a + b + (c + d)\sqrt{5} \in \mathbb{Q}\left[\sqrt{5}\right]$.
- $\left(a + \sqrt{5}b\right)\left(c + \sqrt{5}d\right) = ac + 5bd + (ad + bc)\sqrt{5} \in \mathbb{Q}\left[\sqrt{5}\right]$.

$\mathbb{Q}\left[\sqrt{5}\right]$ est un donc un sous-anneau de $(\mathbb{R}, +, \times)$.

Soit $x \in \mathbb{Q}\left[\sqrt{5}\right]\backslash\{0\}$, $x = a + b\sqrt{5}$ avec $(a, b) \neq (0, 0)$. Supposons que $a - b\sqrt{5} = 0$, alors $b\sqrt{5} = a$ donc $\sqrt{5} \in \mathbb{Q}$ ou $b = 0$. Le premier cas est évidemment faux, et le deuxième entraîne $a = 0$, ce qui est également faux. Donc $a - b\sqrt{5} \neq 0$. Ainsi :

$$\begin{aligned}\frac{1}{x} &= \frac{1}{a + b\sqrt{5}} \\ &= \frac{a - b\sqrt{5}}{a^2 + 5b^2} \\ &= \underbrace{\frac{a}{a^2 + 5b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2 + 5b^2}}_{\in\mathbb{Q}}\sqrt{5} \in \mathbb{Q}\left[\sqrt{5}\right]\end{aligned}$$

x est donc inversible et $\dfrac{1}{x} \in \mathbb{Q}\left[\sqrt{5}\right]$.

3.2.2 Morphisme d'anneaux

Soient $(A, +, \times)$ et $\left(B, \dot{+}, \dot{\times}\right)$ deux anneaux. Alors $f : A \longrightarrow B$ un morphisme d'anneau si :

(1) f est un morphisme de groupe de $(A, +)$ dans $(B, \dot{+})$: $\forall x, y \in A$, $f(x + y) = f(x) \dot{+} f(y)$.

(2) $\forall x, y \in A$, $f(x \times y) = f(x) \dot{\times} f(y)$.

(3) $f(1_A) = 1_B$

Exemple $z \in \mathbb{C} \longmapsto \overline{z}$ est un morphisme d'anneau.

Exercice Soit $\mathbb{K} = \mathbb{Q}\left[\sqrt{5}\right]$, déterminons les morphismes d'anneau de $\mathbb{K}$ dans $\mathbb{R}$.

Soit $f : \mathbb{K} \longrightarrow \mathbb{R}$ un tel morphisme d'anneau. On a alors les propriétés suivantes :

(1) $\forall r \in \mathbb{Q} \subset \mathbb{K}$, $f(r) = r$. En effet :
- Pour $n \in \mathbb{Z} \subset \mathbb{K}$, $f(n) = f(n \times 1) = nf(1) = n$ car f est un morphisme d'anneau, il envoie donc 1 en 1.
- Soit $r = \dfrac{p}{q} \in \mathbb{Q} \subset \mathbb{K}$, alors $p = f(p) = f(qr) = qf(r)$ d'où $f(r) = \dfrac{p}{q} = r$.

(2) Si $x \in \mathbb{K}$, alors x s'écrit de manière unique $x = a + b\sqrt{5}$ avec $a, b \in \mathbb{Q}$.
En effet, si $\exists\,(a,b),(c,d) \in \mathbb{Q}^2$ tels que $a + b\sqrt{5} = c + d\sqrt{5}$, alors $a - c = (d-b)\sqrt{5}$. Si $d - b \neq 0$, alors $\sqrt{5} = \dfrac{a-c}{d-b} \in \mathbb{Q}$, ce qui est faux. Donc $d = b$, puis $a = c$ ce qui prouve le résultat.

(3) Soit $(a,b) \in \mathbb{Q}^2$, on a :

$$\begin{aligned} f\left(a + b\sqrt{5}\right) &= f(a) + f\left(b\sqrt{5}\right) \\ &= f(a) + f(b)\, f\left(\sqrt{5}\right) \\ &= a + bf\left(\sqrt{5}\right) \quad \text{car } a, b \in \mathbb{Q} \end{aligned}$$

Il reste donc à connaître $f\left(\sqrt{5}\right)$ pour terminer l'étude de f. On a :

$$\begin{aligned} \left(\sqrt{5}\right)^2 = 5 \;&\Rightarrow\; f\left(\left(\sqrt{5}\right)^2\right) = f(5) = 5 \text{ mais aussi } f\left(\left(\sqrt{5}\right)^2\right) = \left(f\left(\sqrt{5}\right)\right)^2 \\ &\Rightarrow\; \left(f\left(\sqrt{5}\right)\right)^2 = 5 \\ &\Rightarrow\; f\left(\sqrt{5}\right) = \pm\sqrt{5} \end{aligned}$$

- Si $f\left(\sqrt{5}\right) = \sqrt{5}$, alors $\forall a, b \in \mathbb{Q}$, $f\left(a + b\sqrt{5}\right) = a + b\sqrt{5}$ donc f est l'injection canonique [a] $f : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{R} \\ x & \mapsto & x \end{array}$.
Réciproquement, il est clair que cette application est un morphisme d'anneaux.
- Si $f\left(\sqrt{5}\right) = -\sqrt{5}$, alors f est l'application $x = a + b\sqrt{5} \in \mathbb{K} \longmapsto \widetilde{x} = a - b\sqrt{5}$. Montrons que $x \in \mathbb{K} \longmapsto \widetilde{x}$ est un morphisme d'anneau : soient $x, y \in \mathbb{K}$, $x = a + b\sqrt{5}$ et $y = c + d\sqrt{5}$ avec $a, b, c, d \in \mathbb{Q}$:
  - $\widetilde{x+y} = a + c - (b+d)\sqrt{5} = \widetilde{x} + \widetilde{y}$.
  - $\widetilde{1} = 1$
  - $xy = ac + 5bd + (ad + bc)\sqrt{5}$ donc $\widetilde{xy} = ac + 5bd - (ad + bc)\sqrt{5}$. De plus :

$$\begin{aligned} \widetilde{x}\widetilde{y} &= \left(a - b\sqrt{5}\right)\left(c - d\sqrt{5}\right) \\ &= ac + 5(-b)(-d) + (a(-d) + (-b)c)\sqrt{5} \\ &= \widetilde{xy} \end{aligned}$$

Les seuls morphismes d'anneaux de $\mathbb{K}$ dans $\mathbb{R}$ sont donc Id et $x \longmapsto \widetilde{x}$.

Propriétés des morphismes d'anneaux

(1) L'image d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

(2) L'image réciproque d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

(3) La composée de deux morphismes d'anneaux et un morphisme d'anneaux.

(4) L'application d'un isomorphisme d'anneaux [b] est un isomorphisme d'anneaux [c].

a. Selon notre cher M. Sellès, ce terme dénoterait une certaine suffisance chez celui qui le prononce : *« Si vous voulez faire péteux vous dites ça. »*.

b. Morphismes d'anneaux bijectif.

c. Les démonstrations sont laissées au courageux lecteur ! Elles reprennent néanmoins les principes de celles pour les propriétés des morphismes de groupes.

Remarque Soient A et B deux anneaux et f un morphisme d'anneaux injectif de A dans B.

Alors $f(A)$ est un sous-anneau de B isomorphe à A via $f : A \longrightarrow B$, donc B contient via le morphisme f une copie de A. On dit alors que B contient A.

On a de plus la propriété suivante : soit $\mathbb{K}$ un corps, A un anneau et $f : \mathbb{K} \longrightarrow A$ un morphisme d'anneau. Alors f est injective.

En effet, $\operatorname{Ker} f = f^{-1}(\{0_A\})$, montrons que $\operatorname{Ker} f = \{0_\mathbb{K}\}$ [a]. Si $x \in \mathbb{K}\backslash\{0_\mathbb{K}\}$,

$$1_A = f(1_\mathbb{K}) = f\left(x \times \frac{1}{x}\right) = f(x) f\left(\frac{1}{x}\right)$$

donc $f(x) \neq 0_K$ et $x \notin \operatorname{Ker} f$. Ainsi, $\operatorname{Ker} f \subset \{0_\mathbb{K}\}$ et l'inclusion inverse est évidente, d'où le résultat.

4 Complément : éléments de torsion dans un groupe

Soit $(G, \cdot)$ un groupe de neutre e et $x \in G$. On dit que x est un élément de torsion s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$.

Exemples
- e est un élément de torsion car $e^1 = e$.
- Pour $G = (\mathbb{C}^*, \times)$ et $n \in \mathbb{N}^*$, $\omega = \mathrm{e}^{\frac{2i\pi}{n}}$ est un élément de torsion car $\omega^n = 1$.
- Pour $G = (\mathbb{Z}/n\mathbb{Z}, \dot{+})$, tout élément est de torsion car pour $k \in \mathbb{Z}$, $n\overline{k} = \overline{0}$.

Petite histoire Soit $(G, \cdot)$ un groupe et $x \in G$, alors $\operatorname{gr}(x) = \{x^n | n \in \mathbb{Z}\}$. Si x est élément de torsion on peut définir $\delta = \min\{n \in \mathbb{N}^* | x^n = e\}$, alors $\delta \in \mathbb{N}^*$ et $x^\delta = e$. Pour $n \in \mathbb{Z}$, $n = q\delta + r$ avec $r \in [[0, \delta[[$ d'où

$$\begin{aligned} x^n &= x^{q\delta+r} \\ &= \left(x^\delta\right)^q x^r \\ &= e^q x^r \\ &= x^r \end{aligned}$$

Ainsi, $\operatorname{gr}(x) \subset \left\{e, x, x^1, \ldots, x^{\delta-1}\right\}$ et l'inclusion inverse est évidente, d'où $\operatorname{gr}(x) = \left\{e, x, x^2, \ldots, x^{\delta-1}\right\}$. Montrons que tous les éléments de $\operatorname{gr}(x)$ sont distincts.

Soient $0 \leqslant k < l < \delta$, supposons que $x^k = x^l$, alors $e = x^{l-k}$ or $1 \leqslant l - k < \delta$, ce qui contredit la définition de δ. Ainsi $\operatorname{gr}(x) = \left\{e, x, x^1, \ldots, x^{\delta-1}\right\}$ et $\operatorname{Card}\operatorname{gr}(x) = \delta$ donc $\operatorname{gr}(x)$ est fini. On appelle δ l'ordre de x.

Si x n'est pas de torsion, pour $l, k \in \mathbb{Z}$, $k \neq l \Rightarrow x^k \neq x^l$ puisque si $k < l$ et $x^k = x^l$, alors $x^{l-k} = e$ donc x serait de torsion, ce qui est faux. Ainsi, l'application $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \operatorname{gr}(x) \\ n & \mapsto & x^n \end{array}$ est une bijection, $\operatorname{gr}(x)$ est infini.

Finalement :

(1) $x \in G$ est de torsion si et seulement si $\operatorname{gr}(x)$ est fini.

(2) For$x$ est de torsion, son ordre est $\delta = \min\{n \in \mathbb{N}^* | x^n = e\}$. De plus $\operatorname{gr}(x) = \left\{e, x, x^2, \ldots, x^{\delta-1}\right\}$ et $\operatorname{Card}\operatorname{gr}(x) = \delta$.

(3) Sous les même conditions, pour $n \in \mathbb{Z}$, on a $x^n = e \Leftrightarrow \delta \mid n$.

$\Leftarrow$ Si $n = q\delta$, $x^n = x^{q\delta} = (e)^q = e$.

$\Rightarrow$ Si $x^n = e$, $n = q\delta + r$ avec $r \in [\![0, \delta]\!] \setminus \{\delta\}$ donc

$$\begin{aligned} e &= x^n \\ &= x^{q\delta+r} \\ &= x^r \end{aligned}$$

Si $r \neq 0$, alors $r \in \mathbb{N}^*$, $x^r = e$ et $r < \delta$ ce qui contredit la définition de δ donc $r = 0$, d'où le résultat.

[a] Voir la propriété (4) (c) de la section (4)c page 12.

Remarque Soit $(G,\cdot)$ un groupe fini. Alors tout élément est de torsion.
En effet, si $x\in G$, $\mathrm{gr}\,(x)\subset G$ donc il est fini et $\mathrm{Card}\,\mathrm{gr}\,(x)\leqslant \mathrm{Card}\,G$. L'ordre δ vérifie alors $\delta\leqslant \mathrm{Card}\,G$ [a].

5 Complément : signature d'une décomposition

5.1 Étude préliminaire

Dans la suite, $n\in\mathbb{N}$ avec $n\geqslant 2$, on rappelle que $S_n=\mathfrak{S}\left(\llbracket 1,n\rrbracket\right)$ et que $(S_n,\circ)$ est le groupe symétrique.

Définitions Soit $\sigma\in S_n$, posons $C=\left\{(i,j)\in\llbracket 1,n\rrbracket^2\,|i<j\right\}$. On a alors $\mathrm{Card}\,C=\dfrac{n\,(n-1)}{2}$ car C est en bijection avec $\mathcal{P}_2\,(n)$ [b] via $\{\alpha,\beta\}\in\mathcal{P}_2\,(n)\longmapsto(\min(\alpha,\beta),\max(\alpha,\beta))\in C$, et $\mathrm{Card}\,\mathcal{P}_2\,(n)=\binom{n}{2}$. Pour $(i,j)\in C$, on dit que σ présente une inversion en (i,j) si $\sigma(i)>\sigma(j)$.

On note $N(\sigma)$ le nombre d'inversions de σ, c'est-à-dire le nombre de couples $(i,j)\in C$ tels que σ présente une inversion en (i,j). Par exemple, pour $n=7$ et $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\3&4&7&1&2&6&5\end{pmatrix}$: σ présente des inversions en $(1,4)$, $(1,5)$, $(2,4)$, $(2,5)$, $(3,4)$, $(3,5)$, $(3,6)$, $(3,7)$, $(6,7)$ donc $N(\sigma)=9$.

On a toujours $N(\sigma)\in\left\llbracket 0,\dfrac{n\,(n-1)}{2}\right\rrbracket$: en effet, $I(\mathrm{Id})=0$ et pour $\sigma=\begin{pmatrix}1&2&\cdots&n\\n&n-1&\cdots&1\end{pmatrix}$, $N(\sigma)=\dfrac{n\,(n-1)}{2}$. Par définition, pour $\sigma\in S_n$, la signature de σ est :

$$\varepsilon(\sigma)=(-1)^{N(\sigma)}=\begin{cases}1 & \text{si } N(\sigma) \text{ est pair}\\ -1 & \text{si } N(\sigma) \text{ est impair}\end{cases}$$

Exemples
- Soit $(i,j)\in C$, alors $\varepsilon(\mathcal{T}_{ij})=-1$. En effet, on écrit :

$$\mathcal{T}_{ij}=\begin{pmatrix}1&2&\cdots&i&i+1&\cdots&j-1&j&\cdots&n\\1&2&\cdots&j&i+1&\cdots&j-1&i&\cdots&n\end{pmatrix}$$

  $\mathcal{T}_{ij}$ présente des inversions en $(i,i+1)$, $(i,i+2)$,..., (i,j) et en $(i+1,j)$, $(i+2,j)$,..., $(j-1,j)$. Soit au total

$$\begin{aligned}N(\mathcal{T}_{ij}) &= j-(i+1)+1+(j-1-(i+1)+1)\\ &= j-i+j-i-1\\ &= 2(j-i)-1\end{aligned}$$

  ainsi$N(\mathcal{T}_{ij})$ est impair d'où le résultat.
- Soit $p\in\llbracket 2,n\rrbracket$, γ le p-cycle $\gamma=\begin{pmatrix}1&2&\cdots&p\end{pmatrix}$. On écrit :

$$\gamma=\begin{pmatrix}1&2&3&\cdots&p-1&p&p+1&\cdots&n\\2&3&4&\cdots&p&1&p+1&\cdots&n\end{pmatrix}$$

  Il y a donc $p-1$ inversions : $(1,p)$, $(2,p)$,..., $(p-1,p)$ donc $N(\sigma)=p-1$ donc $\varepsilon(\sigma)=(-1)^{p-1}$.

5.2 Théorème

Pour $\sigma,\sigma'\in S_n$, $\varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\,\varepsilon(\sigma')$. La signature ε est un morphisme de groupes de $(S_n,\circ)$ dans $(\{\pm1\},\times)$.

a. En fait, on a même $\delta\mid\mathrm{Card}\,G$.
b. Ensemble des parties à deux éléments de $\llbracket 1,n\rrbracket$.

Lemme : étude d'une loi Soit $X = \mathcal{F}(\mathbb{R}^n, \mathbb{R})$, pour $f, g \in X$, on sait définir αf et $f + g$ pour $\alpha \in \mathbb{R}$. Pour $\sigma \in S_n$ et $f \in X$, on définit $\sigma \star f$ par $\forall (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$,

$$(\sigma \star f)((x_1, x_2, \ldots, x_n)) = f\left(\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right)\right)$$

Par exemple, pour $n = 3$, $f(x_1, x_2, x_3) = x_1 + x_2 x_3$ et $\sigma = \mathcal{T}_{12}$, alors :

$$\begin{aligned}(\mathcal{T}_{12} \star f)((x_1, x_2, x_3)) &= f(x_2, x_1, x_3)\\ &= x_2 + x_1 x_3\end{aligned}$$

Maintenant, soient $\sigma, \sigma' \in S_n$, *quid* de $\sigma' \star (\sigma \star f)$? Soient $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, alors :

$$\begin{aligned}\sigma' \star (\sigma \star f) &= \sigma' \star f\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right)\\ &= \sigma' \star f(y_1, y_2, \ldots, y_n)\\ &= f\left(y_{\sigma'(1)}, y_{\sigma'(2)}, \ldots, y_{\sigma'(n)}\right)\\ &= f\left(x_{\sigma' \circ \sigma(1)}, x_{\sigma' \circ \sigma(2)}, \ldots, x_{\sigma' \circ \sigma(n)}\right)\\ &= \left(\sigma' \circ \sigma\right) \star f\end{aligned}$$

D'autre part, pour $f, g \in X$:
- $\sigma \star (\alpha f) = \alpha \sigma \star f$
- $\sigma \star (f + g) = \sigma \star f + \sigma \star g$
- $\sigma \star (fg) = (\sigma \star f)(\sigma \star g)$

Démonstration On rappelle que $C = \left\{(i, j) \in [\![1, n]\!]^2 \,|\, i < j\right\}$. Soit l'application :

$$\begin{aligned}\psi : \mathbb{R}^n &\longrightarrow \mathbb{R}\\ (x_1, x_2, \ldots, x_n) &\mapsto \prod_{(i,j) \in C} (x_j - x_i)\end{aligned}$$

Par exemple, pour $n = 3$, $\psi(x_1, x_2, x_3) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$. Montrons maintenant que $\sigma \star \psi = \varepsilon(\sigma)\psi$. On a pour $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$:

$$\psi(x_1, x_2, \ldots, x_n) = \prod_{A \in \mathcal{P}_2(n)} \underbrace{\left(x_{\max A} - x_{\min A}\right)}_{f_A(x_1, x_2, \ldots, x_n)}$$

Avec $\mathcal{P}_2(n)$ l'ensemble des paires $\{\alpha, \beta\}$ avec $\alpha, \beta \in [\![1, n]\!]$ et $\alpha \neq \beta$. Pour $\sigma \in S_n$,

$$\begin{aligned}\sigma \star \psi &= \sigma \star \left(\prod_{A \in \mathcal{P}_2(n)} f_A\right)\\ &= \prod_{A \in \mathcal{P}_2(n)} \sigma \star f_A\end{aligned}$$

Posons $A = \{\alpha, \beta\}$ avec $\alpha < \beta$, ainsi $\sigma(A) = \{\sigma(\alpha), \sigma(\beta)\}$ et :

$$\begin{aligned}(\sigma \star f)(x_1, x_2, \ldots, x_n) &= f_A\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right)\\ &= x_{\sigma(\beta)} - x_{\sigma(\alpha)}\end{aligned}$$

- Si σ n'a pas d'inversions en (α, β), alors $\sigma \star f_A = +\left|f_{\sigma(A)}\right|$.
- Si σ présente une inversion en (α, β), alors $\sigma \star f = -\left|f_{\sigma(A)}\right|$.

On a ainsi :

$$\begin{aligned}\sigma\star\psi &= \prod_{A\in\mathcal{P}_2(n)}\sigma\star f_A\\ &= (-1)^{N(\sigma)}\prod_{A\in\mathcal{P}_2(n)}f_{\sigma(A)}\end{aligned}$$

Or lorsque A décrit $\mathcal{P}_2(n)$, $\sigma(A)$ décrit aussi $\mathcal{P}_2(n)$ donc :

$$(-1)^{N(\sigma)}\psi=\sigma\star\psi$$

Or $(-1)^{N(\sigma)}=\varepsilon(\sigma)$, d'où $\sigma\star\psi=\varepsilon(\sigma)\psi$. Pour $\sigma,\sigma'\in S_n$:

$$\begin{aligned}\left(\sigma\circ\sigma'\right)\star\psi &= \varepsilon\left(\sigma\circ\sigma'\right)\psi\\ &= \sigma\star\left(\sigma'\star\psi\right)\\ &= \varepsilon\left(\sigma'\right)\sigma\star\psi\\ &= \varepsilon\left(\sigma'\right)\varepsilon(\sigma)\psi\end{aligned}$$

En particulier, $\varepsilon(\sigma\circ\sigma')\psi(1,2,\ldots,n)=\varepsilon(\sigma)\varepsilon(\sigma')\psi(1,2,\ldots,n)\Rightarrow\varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$.

Remarque

$$\varepsilon(\sigma)=\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}$$

En effet, $(\sigma\star\psi)(1,2,\ldots,n)=\varepsilon(\sigma)\psi(1,2,\ldots,n)$, or $(\sigma\star\psi)(1,2,\ldots,n)=\prod_{i<j}(\sigma(j)-\sigma(i))$ et $\psi(1,2,\ldots,n)=\prod_{i<j}(i-j)$ d'où le résultat.

Conséquences

(1) Soit $\sigma\in S_n$, on sait que σ s'écrit comme un produit de transposition donc $\sigma=\mathcal{T}_1\circ\mathcal{T}_2\circ\cdots\circ\mathcal{T}_r$ avec $r\in\mathbb{N}$ et $\forall i\in[\![1,n]\!]$, $\mathcal{T}_i$ est une transposition. Alors $\varepsilon(\sigma)=\varepsilon(\mathcal{T}_1)\varepsilon(\mathcal{T}_2)\cdots\varepsilon(\mathcal{T}_r)=(-1)^r$.
- Si $\varepsilon(\sigma)=1$, on dit que c'est une permutation paire, et σ ne peut s'écrire que comme produit d'un nombre pair de transpositions.
- Si $\varepsilon(\sigma)=-1$, on dit que c'est une permutation impaire, et σ ne peut s'écrire que comme produit d'un nombre impair de transpositions.

(2) Soit $p\in[\![1,n]\!]$, γ un p-cycle. On note γ_1 le p-cycle $\gamma_1=\begin{pmatrix}1&2&\cdots&p\end{pmatrix}$, on a vu que $\varepsilon(\gamma_1)=(-1)^{p-1}$. Notons $\gamma=\begin{pmatrix}x_1&x_2&\cdots&x_p\end{pmatrix}$, $\forall i\in[\![1,p-1]\!]$, $\gamma(x_i)=x_{i+1}$, $\gamma(p)=x_1$ et pour $k\notin\{x_1,x_2,\ldots,x_p\}$, $\gamma(k)=k$. Soit maintenant $\sigma\in S_n$ telle que $\forall k\in[\![1,p]\!]$, $\sigma(k)=x_k$. Il y a alors $(n-p)!$ telles permutations, et on a $\gamma=\sigma\circ\gamma_1\circ\sigma^{-1}$. En effet, soit $y\in[[1,n]]$:
- Si $y\notin\{x_1,x_2,\ldots,x_p\}$, alors $\sigma^{-1}(y)\notin\{1,2,\ldots,p\}$ donc $\gamma_1\left(\sigma^{-1}(y)\right)=\sigma^{-1}(y)$ d'où $\sigma\circ\gamma_1\circ\sigma^{-1}(y)=y$.
- Si $y\in\{x_1,x_2,\ldots,x_p\}$, $\forall k\in[\![1,p]\!]$, $\sigma^{-1}(x_k)=k$ donc

$$\gamma\left(\sigma^{-1}(k)\right)=\gamma_1(x_k)=\begin{cases}k+1 & \text{si } k<p\\ 1 & \text{si } k=p\end{cases}$$

Ainsi, on a bien en composant à droite par σ que $\sigma\circ\gamma\circ\sigma^{-1}(y)=\gamma(y)$.
D'où :

$$\begin{aligned}\sigma(\gamma) &= \varepsilon\left(\sigma^{-1}\circ\gamma_1\circ\sigma\right)\\ &= \frac{1}{\varepsilon(\sigma)}\varepsilon(\gamma_1)\varepsilon(\sigma)\\ &= \varepsilon(\gamma_1)\end{aligned}$$

La signature d'un p-cycle quelconque est donc $(-1)^{p-1}$.

(3) Si $\sigma \in S_n$, l'écriture de σ comme produit de cycles donne la signature de σ. par exemple, pour $n = 9$:

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

D'où $\varepsilon(\sigma) = (-1)^{1+3+2} = 1$, ce qui concorde avec $N(\sigma) = 26$.

(4) On rappelle que $\varepsilon : (S_n, \circ) \longrightarrow (\{\pm 1\}, \times)$. On note A_n l'ensemble des permutations paires, et $B_n = S_n \backslash A_n$ l'ensemble des permutations impaires. Alors $\sigma \in A_n \Leftrightarrow \varepsilon(\sigma) = 1$, donc $\sigma \in \operatorname{Ker} \varepsilon$ [a]. On a donc $A_n = \operatorname{Ker} \varepsilon$, et A_n est un sous-groupe de $(S_n, \circ)$. $(A_n, \circ)$ s'appelle le groupe alterné.

Supposons $n \geqslant 2$, et $\mathcal{T}$ une transposition, alors $\varepsilon(\mathcal{T}) = -1$. Si $\sigma \in A_n$, alors $\varepsilon(\mathcal{T} \circ \sigma) = \varepsilon(\mathcal{T})\varepsilon(\sigma) = -1$ donc $(\mathcal{T} \circ \sigma) \in B_n$.Si $\sigma \in B_n$, alors $\mathcal{T} \circ \sigma \in A_n$. On a donc les applications suivantes :

$$f : \begin{array}{l} A_n \longrightarrow B_n \\ \sigma \mapsto \mathcal{T} \circ \sigma \end{array} \quad \text{et} \quad g : \begin{array}{l} B_n \longrightarrow A_n \\ \sigma \mapsto \mathcal{T} \circ \sigma \end{array}$$

Pour $\sigma \in A_n$, $g \circ f(\sigma) = \sigma$ et pour $\sigma \in B_n$, $f \circ g(\sigma) = \sigma$ donc f et g sont des bijections réciproques l'une de l'autre donc $\operatorname{Card} A_n = \operatorname{Card} B_n$. D'autre part, $A_n \cap B_n = \varnothing$ et $S_n = A_n \cup B_n$ donc $n! = \operatorname{Card} S_n = \operatorname{Card} A_n + \operatorname{Card} B_n = 2 \operatorname{Card} A_n$ d'où

$$\operatorname{Card} A_n = \frac{n!}{2}$$

5.3 Application : produit de cycles et ordre

Soit $\sigma \in S_n$, alors $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r$ ou $\forall i \in [\![1, r]\!]$, γ_i est un cycle de support A_i avec $p_i = \operatorname{Card} A_i$. On a de plus $A_i \cap A_j = \varnothing$ pour $i \neq j$ [b]. Alors l'ordre [c] δ de σ au sens de la composition [d] est $\operatorname{PPCM}(p_1, p_2, \ldots, p_r)$.

Lemme L'ordre d'un p-cycle est p.

Soit γ un p-cycle de S_n, d'ordre $\delta(\gamma) = p$. Notons $\gamma = \begin{pmatrix} x_1 & x_2 & \cdots & x_p \end{pmatrix}$, on a pour $i \in [\![1, p-1]\!]$, $\gamma^i(x_1) = x_{i+1}$ donc $\gamma^i \neq \mathrm{Id}$. Or $\gamma^p(x_1) = x_1$ donc pour $2 \leqslant k \leqslant p$:

$$\begin{aligned}\gamma^p(x_k) &= \gamma^p \circ \gamma^{k-1}(x_1) \\ &= \gamma^{k-1} \circ \gamma^p(x_1) \\ &= \gamma^{k-1}(x_1) \\ &= x_k\end{aligned}$$

De plus, pour $x \notin \{x_1, x_2, \ldots, x_p\}$, $\gamma(x) = x$ donc $\forall n \in \mathbb{N}$, $\gamma^n(x) = x$ donc $p = \min\{m \in \mathbb{N}^* | \gamma^m = \mathrm{Id}\}$.

Démonstration Pour $i, j \in [\![1, r]\!]$, γ_i et γ_j sont des cycles à supports disjoints donc $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$. Soit $m = \operatorname{PPCM}(p_1, p_2, \ldots, p_r)$ et δ l'ordre de σ dans S_n.

On a

$$\begin{aligned}\sigma^m &= (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r)^m \\ &= \gamma_1^m \circ \gamma_2^m \circ \cdots \circ \gamma_r^m\end{aligned}$$

Ceci est vrai car les γ_i commutent. Or $\forall i \in [\![1, r]\!]$, $p_i \mid m$ et p est l'ordre de γ_i donc $\gamma_i^m = \mathrm{Id}$ donc $\sigma^m = \mathrm{Id}$. On en déduit que $\delta \mid m$ [e].

D'autre part, $\mathrm{Id} = \sigma^\delta = \gamma_1^\delta \circ \gamma_2^\delta \circ \cdots \circ \gamma_r^\delta$. Montrons que $\gamma_r^\delta = \mathrm{Id}$.

a. Voir la section 2.2.2 page 12 pour un rappel de la définition de Ker.
b. Voir la fin de la section 7.4.3.3 du cours complet page 118.
c. Voir l'annexe 4 page 20.
d. C'est à dire que n est l'ordre de σ si $\underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{n \text{ fois}} = \mathrm{Id}$
e. Voir la propriété (3) page 20.

– Si $x \in A_r$, alors $\gamma_r(x) \in A_r$ donc $\gamma_r^\delta(x) \in A_r$. Or, $x = \gamma_1^\delta \circ \gamma_2^\delta \circ \cdots \circ \gamma_r^\delta(x)$ et pour $i \neq j$, $A_i \cap A_j = \varnothing$ donc si $y \in A_r$, $\forall i \in [\![1, r-1]\!]$, $\gamma_i(y) = y$ donc $\gamma_i^\delta(y) = y$. Ainsi, $\gamma_1^\delta \circ \gamma_2^\delta \circ \cdots \circ \gamma_{r-1}^\delta(y) = y$ donc $x = \gamma_1^\delta \circ \gamma_2^\delta \circ \cdots \circ \gamma_{r-1}^\delta\left(\gamma_r^\delta(x)\right) = \gamma_r^\delta(x)$
– Si $x \notin A_r$, alors $\gamma_r(x) = x$ donc $\gamma_r^\delta(x) = x$.

En réitérant le processus pour $k \in [\![1, r-1]\!]$, on montre que $\gamma_r^\delta = \gamma_{r-1}^\delta = \cdots = \gamma_1^\delta = \mathrm{Id}$.

Ainsi, $\forall i \in [\![1, r]\!]$, $p_i \mid \delta$ donc $m \mid \delta$, d'où $m = \delta$.

Application Quels sont les ordres possibles de S_4 ($\mathrm{Card}\, S_4 = 4! = 24$) ?

Soit $\sigma \in S_4$.

– Si $\sigma = \mathrm{Id}$, alors $\delta(\sigma) = 1$.
– Si $\sigma \neq \mathrm{Id}$, alors σ s'écrit comme un produit de cycles à supports disjoints. Plusieurs possibilités se présentent alors :
  ◦ Si $\sigma = \mathcal{T} \circ \mathcal{T}'$, avec $\mathcal{T}$ et $\mathcal{T}'$ des transpositions à supports disjoints, alors $\delta(\sigma) = 2$.
  ◦ Si $\sigma = \mathcal{T}$ est une transposition, alors $\delta(\sigma) = 2$.
  ◦ Si σ est un 3-cycle, alors $\delta(\sigma) = 3$.
  ◦ Si σ est un 4-cycle, alors $\delta(\sigma) = 4$.

  Toutes les possibilités ont été envisagées. En effet, les cycles étant à support disjoints, un cycle de support de cardinal 2 ne laissera qu'un seul cycle de support de cardinal 2 lui aussi (c'est le cas des deux transpositions), par exemple. On ne considère pas les cycles triviaux de support de cardinal 1 qui correspondent en fait à l'identité.

Ainsi, les ordres possibles de S_4 sont 1, 2, 3 et 4.

6 Complément : corps des fractions d'un anneau intègre

6.1 Introduction

Soit $\mathbb{L}$ un corps, A un sous-anneau de $\mathbb{L}$ [a]. On cherche à décrire le plus petit sous-corps de L qui contient A [b]. Notons $\mathbb{K}$ ce sous-corps, alors $\forall a \in A$, $a \in \mathbb{K}$ et $\forall b \in A\backslash\{0\}$, $b \in \mathbb{K}\backslash\{0\}$ donc $\dfrac{1}{b} \in \mathbb{K}$ [c]. Dans ce cas, $\forall (a,b) \in A \times A\backslash\{0\}$, $\dfrac{a}{b} = a \times \dfrac{1}{b} \in \mathbb{K}$ donc $\Lambda = \left\{\frac{a}{b} \middle| (a,b) \in A \times A\backslash\{0\}\right\} \subset \mathbb{K}$.

D'autre part, $A \subset \Lambda$. En effet, si $a \in A$, $a = \dfrac{a}{1}$ et $1 \in A\backslash\{0\}$ donc $a \in \Lambda$. On a aussi $0, 1 \in \Lambda$. Soient $x, y \in \Lambda$, $\exists (a,b), (c,d) \in A \times A\backslash\{0\}$ tels que $x = \dfrac{a}{b}$ et $y = \dfrac{c}{d}$, donc :

$$\begin{aligned} x + y &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad}{bd} + \frac{bc}{bd} \\ &= \frac{ad + bc}{bd} \end{aligned}$$

On a bien $bd \in A\backslash\{0\}$ car A est intègre et $ad + bc \in A$ donc $x + y \in \Lambda$. De plus,

$$xy = \frac{ab}{cd}$$

Donc $xy \in \Lambda$ car $ab \in A$ et $cd \in A\backslash\{0\}$ car A est intègre.

Si $x = \dfrac{a}{b} \in \Lambda\backslash\{0\}$, alors $a \in A\backslash\{0\}$ et $x \times \dfrac{b}{a} = 1$ donc $\dfrac{b}{a} \in \Lambda$. Ainsi, Λ est bien un sous-corps de $\mathbb{L}$ qui contient A donc $\Lambda \supset \mathbb{K}$.

Ainsi, $\Lambda = \mathbb{K}$.

a. A est donc nécessairement intègre.
b. Ce plus petit sous-corps est l'intersection de tous les sous-corps qui contiennent A.
c. $\dfrac{1}{b}$ étant la notation de l'inverse de b dans le corps $\mathbb{K}$ par la multiplication.

Remarque Pour $(a,b),(c,d) \in A \times A\backslash\{0\}$,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

$\Rightarrow$ $\frac{a}{b} = \frac{c}{d}$ d'où $db\frac{a}{b} = bd\frac{c}{d} \Rightarrow ad = bc$.
$\Leftarrow$ Si $ad = bc$, $\frac{1}{bd}ad = \frac{1}{bd}bc \Rightarrow \frac{a}{b} = \frac{c}{d}$.

6.2 Construction du corps des fractions d'un anneau intègre

Soit A un anneau, on cherche à rendre inversibles les éléments de $A\backslash\{0\}$, c'est-à-dire un corps $\mathbb{L}$ tel que A soit isomorphe à $\mathbb{L}$. Si un tel corps $\mathbb{L}$ existe, alors A apparaît comme un sous-anneau d'un anneau intègre donc doit lui-même est intègre.

On supposera désormais que A est intègre. Soit $X = A \times A\backslash\{0\}$, on définit une relation binaire R sur A par $\forall (a,b),(c,d) \in X$, $(a,b)\,R\,(c,d) \Leftrightarrow ad = bc$. Montrons que R est une relation d'équivalence :

(1) R est réflexive :$\forall (a,b) \in X$, $ab = ba$ car A est commutatif.
(2) R est symétrique : si $(a,b)\,R\,(c,d)$, alors $ad = bc \Rightarrow cb = da$ donc $(c,d)\,R\,(a,b)$.
(3) R est transitive : si $(a,b)\,R\,(c,d)$ et $(c,d)\,R\,(e,f)$, alors $ad = bc$ et $cf = de$ d'où $adf = bcf \Rightarrow adf = bde$ or $d \neq 0$ et A est intègre donc $af = be$ donc $(a,b)\,R\,(e,f)$.

On note $\mathbb{K} = {}^{X}/_{R} = \{\mathrm{cl}_R(a,b) \,|\, (a,b) \in X\}$. Les classes d'équivalence de R s'appellent les *fractions* et pour $(a,b) \in X$, on note $\frac{a}{b}$ la classe de (a,b).

Lois de composition interne sur $\mathbb{K}$

Addition Soient $(a,b),(a',b'),(c,d),(c',d') \in X$ avec $\frac{a}{b} = \frac{a'}{b'}$ et $\frac{c}{d} = \frac{c'}{d'}$. Ainsi, $(a,b)\,R\,(a',b') \Leftrightarrow ab' = a'b$, montrons que :

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \Leftrightarrow (ad+bc)\,b'd' = \left(a'd'+b'c'\right)bd$$

On sait que $ab' = a'b$ et $cd' = c'd$ donc :

$$\begin{aligned}(ad+bc)\,b'd' &= adb'd' + bcb'd' \\ &= ab'dd' + cd'bb' \\ &= bd\left(a'd'+b'c'\right)\end{aligned}$$

Il devient donc cohérent de poser, pour $x,y \in \mathbb{K}$:

$$x + y = \frac{ad+bc}{bd}$$

où (a,b) est n'importe quel représentant de x et (c,d) n'importe quel représentant de y.

$+$ est associative, commutative, admet comme neutre $0_{\mathbb{K}} = \frac{0_A}{1_A}$ et tout élément de $x \in K$ admet un opposé ($-\frac{a}{b} = \frac{-a}{b}$).

Multiplication Pour $(a,b),(a',b'),(c,d),(c',d') \in X$, on a $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ et on pose alors, pour $x,y \in \mathbb{K}$,

$$xy = \frac{ac}{bd}$$

avec (a,b) n'importe quel représentant de x une(x,d) n'importe quel représentant de y.

Le produit est associatif, commutatif, admet comme neutre $1_{\mathbb{K}} = \frac{1_A}{1_A}$, est distributif par rapport à $+$. De plus, si $x \in \mathbb{K}\backslash\{0_{\mathbb{K}}\}$, $x = \frac{a}{b}$ avec $(a,b) \in (A\backslash\{0_A\})^2$ car si $a = 0_A$, $\frac{a}{b} = 0_{\mathbb{K}}$. Posons $y = \frac{b}{a}$, alors $xy = yx = 1_{\mathbb{K}}$ donc x est inversible. Ainsi, $\mathbb{K}$ est un corps.

Identification de A dans $\mathbb{K}$ Soit $\varphi : \begin{array}{ccc} A & \longrightarrow & \mathbb{K} \\ a & \mapsto & \dfrac{a}{1_A} \end{array}$, φ est un morphisme d'anneaux de A dans K car :

- $\varphi(1_A) = \dfrac{1_A}{1_A} = 1_{\mathbb{K}}$.
- Pour $a, b \in A$, $\varphi(a+b) = \dfrac{a+b}{1_A} = \dfrac{a}{1_A} + \dfrac{b}{1_A} = \varphi(a) + \varphi(b)$ et $\varphi(ab) = \dfrac{ab}{1_A} = \dfrac{a}{1_A}\dfrac{b}{1_A} = \varphi(a)\varphi(b)$.

φ est de plus injective. En effet, soit $a \in \operatorname{Ker}\varphi$, montrons que $a = 0_A$. $\varphi(a) = 0_{\mathbb{K}}$ donc

$$\begin{aligned} \varphi(a) = 0_{\mathbb{K}} &\Rightarrow \frac{a}{1_A} = \frac{0_A}{1_A} \\ &\Rightarrow 0_A 1_A = a 1_A \\ &\Rightarrow a = 0_A \end{aligned}$$

On identifie donc $a \in A$ à $\dfrac{a}{1_A} \in \mathbb{K}$, A apparaît comme un sous-anneau de $\mathbb{K}$.

Le corps $\mathbb{K}$ ainsi construit s'appelle le corps des fractions de A et se note $\operatorname{Frac}(A)$. Par exemple, $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$.

Exercice Si L est un corps qui contient A [a], alors L contient $\operatorname{Frac}(A)$.

a. C'est-à-dire s'il existe un morphisme d'anneaux injectif $\psi : A \longrightarrow L$.