Table des matières

Chapitre 14

Structures Algébriques

Voir Fiche 09

14.1 Lois de Composition interne

14.1.1 Quelques lois

les lois usuelles + et × sont des $\ell.c.i$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

la somme de deux vecteurs défini une $\ell.c.i$ sur $\overrightarrow{\mathcal{P}}$ et sur $\overrightarrow{\mathcal{E}}$

la somme et le produit de fonctions défini deux $\ell.c.i$ sur $\mathcal{F}(I, \mathbb{R})$ ou encore sur $\mathcal{F}(I, \mathbb{C})$

Soit E un ensemble quelconque. $\cap$ et $\cup$ sont des $\ell.c.i$ sur $\mathcal{P}(E)$

$\circ$ est une lci sur l'ensemble des fonctions croissantes de $\mathbb{R}$ dans $\mathbb{R}$. Mais ce n'est pas une lci sur l'ensemble des fonctions décroissantes de $\mathbb{R}$ dans $\mathbb{R}$

14.1.2 Propriétés

Toutes ces lois sont associatives et commutatives.
En revanche le produit vectoriel $\wedge$ sur $\overrightarrow{\mathcal{E}}$ est une $\ell.c.i$ non associative et non commutative.

$$\overrightarrow{i} \wedge \overrightarrow{j} = \overrightarrow{k} \neq -\overrightarrow{k} = \overrightarrow{j} \wedge \overrightarrow{i}$$

Dans $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ la loi $\times$ est distributive sur $+$.

$$x \times (y + z) = x \times y + x \times z$$

L'"autre" distributivité provenant de la commutativité Dans $\mathcal{E}$ la loi $\wedge$ est distributive par rapport à $+$

$$u \wedge (v + w) = u \wedge v + u \wedge w \qquad \text{et} \qquad (v + w) \wedge u = v \wedge u + w \wedge u$$

Dans $\mathcal{P}(E)$ $\cap$ est distributive sur $\cup$ et $\cup$ est distributive sur $\cap$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap B) \qquad \text{et} \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup B)$$

14.1.3 Eléments caractéristiques

0 est l'élément neutre de + dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$
1 est l'élément neutre de × dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$

la fonction constante 0 est l'élément neutre de $(\mathcal{F}(I, \mathbb{R}), +)$
la fonction constante 1 est l'élément neutre de $(\mathcal{F}(I, \mathbb{R}), \times)$

Tout élément de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ admet un opposé dans ce même ensemble, donc un symétrique pour $+$. En revanche 7 n'admet pas de symétrique dans $(\mathbb{N}, +)$.

Tout élément de $\mathbb{Q}^*, \mathbb{R}^*$ ou $\mathbb{C}^*$ admet un inverse dans ce même ensemble, donc un symétrique pour $\times$. En revanche -12 n'admet pas de symétrique dans $(\mathbb{Z}, +)$.

Proposition 14.1.1 *Soit $(E, \top)$ un ensemble muni d'une ℓ.c.i. **associative** $\top$.*
Si l'élément neutre existe, il est unique.
Si x admet un symétrique alors il est unique, on le note $sym(x)$ et on a

$$sym(sym(x)) = x$$

♣

Preuve Soient e_1 et e_2 deux éléments neutres supposés distincts :

$$e_1 = e_1 \top e_2 = e_2$$

Soit x admettant un symétrique y_1, supposons qu'il admet un deuxième symétrique $y_2 \neq y_1$

$$y_2 \top (x \top y_1) = y_2 \top e = y_2 \qquad \text{et} \qquad (y_2 \top x) \top y_1 = e \top y_1$$

D'où par associativité $y_1 = y_2$.

De plus puisque la relation $x \top y = y \top x = e$ est symétrique en x et y on voit bien que $y = sym(x)$ et $x = sym(y)$ •

Exemple: E est l'élément neutre de $(\mathcal{P}(E), \cap)$: $\quad \forall A \subset E, \quad A \cap E = E \cap A = A$
Lorsque $E \neq \emptyset$,seul E admet un symétrique dans$(\mathcal{P}(E), \cap)$:

$$\forall A \subsetneq E, \forall B \subset E \qquad A \cap B \subsetneq E$$

Exemple: Dans $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \times)$ la fonction cos n'admet pas de symétrique.

14.2 Groupes

14.2.1 Groupes et Sous-groupes

Exemple: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathcal{P}, +), (\mathcal{E}, +)$ sont des groupes $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ aussi

Exemple: Soit E non vide. $(\mathcal{F}(E, E), \circ)$ est un ensemble muni d'une ℓ.c.i associative :
Id_E est l'élément neutre de $(\mathcal{F}(E, E), \circ)$;
On a pour tout $f \in \mathcal{F}(E, E)$

$$f \text{ inversible dans } (\mathcal{F}(E, E), \circ) \iff f \textit{ bijective}$$

Et dans le cas bijectif, le symétrique de f est la fonction réciproque f^{-1}.

Ainsi $(\sigma(E), \circ)$ est un groupe (groupe symétrique de E).

Proposition 14.2.1 *Soient $(F, \top)$ et $(G, \perp)$ deux groupes, alors $(F \times G, \star)$ est un groupe pour la loi produit $\star$* ♣

Preuve Puisque $\top$ et $\perp$ sont des lois de groupes elles sont
- associatives
- e_E et e_F sont leurs éléments neutres
- tout élément admet un inverse

On en déduit pour la loi produit
- elle est associative
- (e_E, e_F) est élément neutre
- tout élément $(x, y) \in E \times F$ admet $(sym(x), sym(y)) \in E \times F$ pour inverse

C'est donc un groupe. •

Exemple: $(R^2, +)$ est le groupe produit de $(\mathbb{R}, +)$ avec lui-même. Il est commutatif.

Exemple: $(\mathbb{R} \times \mathbb{R}^*, \star)$ est un groupe commutatif pour

$$(x, y) \star (u, v) = (x + u, y \times v)$$

Dont l'élément neutre est $(0, 1)$ et (x, y) admet pour inverse

$$(-x, 1/y)$$

Proposition 14.2.2 *Soit $(G, \times)$ un groupe et $H \subset G$* ***non vide****.*

$$H \quad \textit{est un sous-groupe de } (G, \times) \Longleftrightarrow \forall (x, y) \in H^2, \quad x \times y^{-1} \in H$$

♣

Preuve On ne montre que $\Longleftarrow$.

- Puisque H non vide, soit $x \in H$, on a $e = x \times x^{-1} \in H$
- soit $x \in H$, on a puisque $e \in H$ $x^{-1} = e \times x^{-1} \in H$
- Soient a et b dans H, on sait déjà que $b^{-1} \in H$ d'où

$$ab = a(b^{-1})^{-1} \in H$$

•

Exemple: L'ensemble Rot_O des rotations de centre O du plan est un sous-groupe pour la composition de l'ensemble des transformations bijectives du plan.

$$R(a) \circ R(b)^{-1} = R(a) \circ R(-b) = R(a - b)$$

Il en va de même pour les homothéties de centre O

Il en va de même pour les similitudes.

Exemple: $(\mathbb{U}, \times)$ et $(\mathbb{U}_n, \times)$ sont des sous-groupes de $(\mathbb{C}^*, \times)$

$$e^{ia} \times (e^{ib})^{-1} = e^{ia} e^{-ib} = e^{i(a-b)}$$

Exemple: pour $a \in \mathbb{Z}$, on note $a\mathbb{Z} := \{an\ n \in \mathbb{Z}\}$. $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ car non vide ($a \in a\mathbb{Z}$) et

$$\forall (n, m) \in \mathbb{Z}^2, \quad an - am = a(n - m) \in a\mathbb{Z}$$

Donc

$$\forall (x, y) \in (a\mathbb{Z})^2, \quad x - y \in a\mathbb{Z}$$

On dit que a est un générateur du groupe $(a\mathbb{Z}, +)$

Proposition 14.2.3 *Soit G un sous-groupe de $(\mathbb{R}, +)$ alors soit G est dense dans $\mathbb{R}$ soit il existe $a \in \mathbb{R}$ tel que $G = a\mathbb{Z}$.* ♣

Démonstration Soit G un sous-groupe de $(\mathbb{R}, +)$.
Dans le cas $G = \{0\}$ alors $G = 0\mathbb{Z}$, Supposons donc $G \neq \{0\}$.
Soit alors $b \neq 0$ dans G. puisque $-b \in G$, G admet donc un élément > 0.
D'où $G \cap \mathbb{R}_+^*$ est non vide et minoré par 0, soit $a = \inf G \cap \mathbb{R}_+^*$

- 1er Cas : $a > 0$.

Supposons par l'absurde $a \notin G$.
Par définition de la borne inférieure on peut trouver $y \in G \cap \mathbb{R}_+^*$ tel que

$$a \leq y < 2a$$

Et comme $a \notin G$

$$a < y < 2a$$

D'où par définition de la borne inférieure on peut alors trouver $x \in G \cap \mathbb{R}_+^*$ tel que $a < x < y$ D'où

$$y - x \in G \cap \mathbb{R}_+^* \qquad \text{et} \qquad y - x < 2a - a = a$$

D'où la contradiction. Donc $a \in G$, on a alors

$$a\mathbb{Z} \subset G$$

Réciproquement soit $z \in G$,

$$z = ma + r \qquad avec \quad m \in \mathbb{Z}, \quad r \in [0, a[$$

Et donc $r = z - ma \in G \cap [0, a[= \{0\}$.
D'où $z = ma \in a\mathbb{Z}$, soit

$$G \subset a\mathbb{Z}$$

• 2ème Cas $r = 0$.
Soient $(x, y) \in \mathbb{R}^2$ avec $x < y$, montrons que

$$G \cap]x, y[\neq \emptyset$$

Puisque $\inf G \cap \mathbb{R}_+^* = 0$, on peut trouver $z \in G$ tel que $0 < z < y - x$ Notons

$$x = mz + r \qquad avec \quad m \in \mathbb{Z}, \quad r \in [0, z[$$

$0 < (m+1)z - x \leq z < y - x$ Et donc

$$x < (m+1)z < y \qquad \text{et} \qquad (m+1)z \in G$$

•

Remarque: les sous-groupes de $(\mathbb{R}, +)$ de la forme $a\mathbb{Z}$ sont appelés sous-groupes discrets.

Exercice: Montrer que $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$

14.2.2 Morphismes

Exemple: $\omega : x \mapsto e^{ix}$ est un morphisme de groupes entre $(\mathbb{R}, +)$ et $(\mathbb{C}^*, \times)$

Exemple: les seules endomorphismes de $(\mathbb{Z}, +)$ sont de la forme $x \mapsto ax$ avec $a \in \mathbb{Z}$

Exemple: les seuls endomorphismes **continus** (ou **monotones**) de $(\mathbb{R}, +)$ sont de la forme $x \mapsto ax$ avec $a \in \mathbb{R}$ (il s'agit des homothéties de $\mathbb{R}$)

Exemple: toute rotation vectorielle est un isomorphisme de $(\overrightarrow{\mathcal{P}}, +)$

Proposition 14.2.4 *Soit $\varphi : (E, \top) \to (F, \perp)$ un morphisme de groupes.*

$$\varphi \in Isom(E, F) \Longleftrightarrow \varphi \text{ est un morphisme bijectif de } E \text{ dans } F$$

♣

Preuve On ne montre que la réciproque.
Soit φ un morphisme bijectif de E dans F.
Montrons que φ^{-1} est un morphisme de F dans E.
Soient X, Y dans F par surjectivité, $X = \varphi(x)$ et $Y = \varphi(y)$ avec x, y dans E.

$$\varphi^{-1}(X \perp Y) = \varphi^{-1}(\varphi(x) \perp \varphi(y)) = \varphi^{-1}(\varphi(x \top y)) = x \top y = \varphi^{-1}(X) \top \varphi^{-1}(Y)$$

•

Proposition 14.2.5 *Soit $\varphi : (E, \top) \to (F, \perp)$ un morphisme de groupes.*
$Im(\varphi)$ et $\ker(\varphi)$ sont des sous-groupes de $(F, \perp)$ et $(E, \top)$ respectivement. ♣

Preuve Il est clair que ces deux ensembles contiennent les éléments neutres 0_F et 0_E respectivement. Soient X, Y dans $\operatorname{Im}\varphi$, alors $X = \varphi(x)$ et $Y = \varphi(y)$ avec x, y dans E.

$$X \perp Y^{-1} = \varphi(x) \perp (\varphi(y))^{-1} = \varphi(x) \perp \varphi(y^{-1}) = \varphi(\underbrace{x \top y^{-1}}_{\in E}) \in \operatorname{Im}\varphi$$

Soient a, b dans $\ker\varphi$

$$\varphi(a \top b^{-1}) = \varphi(a) \perp \varphi(b^{-1}) = \varphi(a) \perp (\varphi(b))^{-1} = e_F \perp (e_F)^{-1} = e_F$$

et donc $a \top b^{-1} \in \ker\varphi$ •

Proposition 14.2.6 *Soit $\varphi : (E, \top) \to (F, \perp)$ un morphisme de groupes.*

$$\varphi \text{ est surjective} \iff Im(\varphi) = F$$

$$\varphi \text{ est injective} \iff \ker(\varphi) = \{e_E\}$$

où e_E désigne l'élément neutre de $(E, \top)$ ♣

Démonstration la première implication est évidente.
Soient x, y dans E

$$\varphi(x) = \varphi(y) \Longrightarrow \varphi(x) \perp (\varphi(y))^{-1} = e_F \Longrightarrow \varphi(x) \perp \varphi(y^{-1}) = e_F \Longrightarrow \varphi(x \top y^{-1}) = e_F$$

$$\Longrightarrow x \top y^{-1} \in \ker\varphi = \{e_E\} \Longrightarrow x \top y^{-1} = e_E \Longrightarrow x = y$$

•

Exemple: $\omega : x \mapsto e^{ix}$ est un morphisme de groupes surjectif entre $(\mathbb{R}, +)$ et $(\mathbb{U}, \times)$, mais il n'est pas injectif car $\ker\omega = 2\pi\mathbb{Z}$

14.3 Anneaux

14.3.1 Anneaux et sous-anneaux

Exemple: $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathcal{F}(I, \mathbb{R}), +, \times)$ et $(\mathcal{F}(I, \mathbb{C}), +, \times)$ sont des anneaux commutatifs

Exercice: Trouver un exemple d'anneau pour lequel

$$f \neq 0, \quad g \neq 0 \qquad \text{et} \qquad fg = 0$$

Solution sur $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ prendre $\chi_{\mathbb{R}_+^*}$ et $\chi_{\mathbb{R}_-^*}$

Proposition 14.3.1 *Soient a, b deux éléments d'un anneau $(A, +, \times)$ **commutatif** et $n \in \mathbb{N}$*

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

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

♣

Démonstration Par distributivité et par commutativité

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

D'où

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

Et conclut par un simple changement d'indice.

Montrons la formule du binôme de Newton par récurrence. Soient a et b fixés.

$$\mathcal{P}(n) : "(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k} = \sum_{k=0}^{n} C_n^k a^{n-k} b^k"$$

- $\mathcal{P}(0)$ clair $(1 = 1)$
- Supposons $\mathcal{P}(n)$ vérifié pour un $n \in \mathbb{N}$ quelconque fixé.

$$\begin{aligned}
(a+b)^{n+1} &= (\sum_{k=0}^{n} C_n^k a^k b^{n-k}) \times (a+b) \\
&= \sum_{k=0}^{n} C_n^k a^k b^{n-k} a + \sum_{k=0}^{n} C_n^k a^k b^{n-k+1} \\
&= \sum_{k=0}^{n} C_n^k a^{k+1} b^{n-k} + \sum_{k=0}^{n} C_n^k a^k b^{n-k+1} \\
&= a^{n+1} + \sum_{k=0}^{n-1} C_n^k a^{k+1} b^{n-k} + \sum_{k=1}^{n} C_n^k a^k b^{n-k+1} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} C_n^{k-1} a^k b^{n+1-k} + \sum_{k=1}^{n} C_n^k a^k b^{n-k+1} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \underbrace{(C_n^{k-1} + C_n^k)}_{C_{n+1}^k} a^k b^{n+1-k} + \ + b^{n+1}
\end{aligned}$$

- Conclusion....

La deuxième formule s'obtient par changement d'indice $k \mapsto n-k$ (penser à $C_n^k = C_{n-k}^k$) •

Exemple: $(\mathbb{R}, +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Exemple: $(\mathcal{F}(I, \mathbb{R}), +, \times)$ est un sous-anneau de $(\mathcal{F}(I, \mathbb{C}), +, \times)$.

Exemple: $(C^0(I, \mathbb{R}), +, \times)$ est un sous-anneau de $(\mathcal{F}(I, \mathbb{R}), +, \times)$.

En effet :
- la fonction constante 1 est continue.
- pour f et g continues sur I, $f - g$ est continue sur I
- pour f et g continues sur I, $f \times g$ est continue sur I

Exercice: Montrer que $(C^{n+1}(I, \mathbb{R}), +, \times)$ est un sous-anneau de $(C^n(I, \mathbb{R}), +, \times)$ pour $n \in \mathbb{N}$.

Exemple: Si on note $\mathcal{E}_0$ l'ensemble des suites réelles convergents vers 0. $\mathcal{C}$ l'ensemble des suites convergentes et $\mathcal{B}$ l'ensemble des suites bornées, on a
- $(\mathcal{B}, +, \times)$ est un sous-anneau de $(\mathbb{R}^{\mathbb{N}}, +, \times)$.
- $(\mathcal{C}, +, \times)$ est un sous-anneau de $(\mathcal{B}, +, \times)$.
- $(\mathcal{E}_0, +, \times)$ n'est pas un sous-anneau de $(\mathcal{C}, +, \times)$ $(1 \notin \mathcal{E}_0)$.

14.3.2 Morphismes

Exemple: $Id_{\mathbb{Z}}$ est le seul endomorphismes d'anneaux de $(\mathbb{Z}, +, \times)$

Exemple: $Id_{\mathbb{R}}$ est le seul endomorphismes d'anneaux de $(\mathbb{R}, +, \times)$

14.4 Corps

Exemple: $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ sont des corps.
Ce sont des sous-corps successifs.

Exercice: Montrer que $ab = 0 \iff a = 0 \quad \text{ou} \quad b = 0$

Remarque: On en déduit que $(\mathbb{K} \setminus \{0\}, \times)$ est un groupe.

Exercice: Tout morphisme de corps est injectif.

14.5 Arithmétique dans $\mathbb{Z}$

Proposition 14.5.1 *$(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre, i.e.*

$$\forall (a, b) \in \mathbb{Z}^2, \qquad ab = 0 \Longrightarrow a = 0 \quad ou \quad b = 0$$

Les seuls éléments inversibles sont 1 et -1 ♣

Définition 14.5.1 *Soient a et b deux entiers relatifs.*
On dit que a est un multiple de b ou encore que b divise a (et on note $b \mid a$) lorsque :

$$\exists n \in \mathbb{Z}, \qquad a = nb$$

On dit aussi que b est un diviseur de a ♠

Remarque: En particulier $b \neq 0$ dès que $a \neq 0$.

Remarque: $b\mathbb{Z}$ est l'ensemble des multiples de b : $\qquad b \mid a \iff a \in b\mathbb{Z} \iff a\mathbb{Z} \subset b\mathbb{Z}$

Proposition 14.5.2 *Pour tout a, b, c dans $\mathbb{Z}$.*

- $a \mid a$
- $a \mid b \quad et \quad b \mid a \Longrightarrow |a| = |b|$
- $a \mid b \quad et \quad b \mid c \Longrightarrow a \mid c$

♣

Démonstration

- $a = 1a$
- Supposons $b = ka \quad$ et $\quad a = k'b$ avec k, k' dans $\mathbb{Z}$

  $$a = kk'a \Longrightarrow (1 - kk')a = 0 \Longrightarrow a = 0 \quad \text{ou} \quad kk' = 1$$

  Si $a = 0$ alors $|b| = |ka| = 0 = |a|$
  Si $kk' = 1$ alors $|k| = |k'| = 1$ (car alors k et k' inversibles) et donc $|b| = |k||a| = |a|$
- Supposons $b = ka \quad$ et $\quad c = k'b$ avec k, k' dans $\mathbb{Z}$

  $$c = kk'a$$

•

Exercice: Montrer que $a\mathbb{Z} = b\mathbb{Z} \Longrightarrow |a| = |b|$

Proposition 14.5.3 *Soient a, b dans $\mathbb{Z}$.*

$$\forall (u, v) \in \mathbb{Z}^2, \quad d \mid a \quad et \quad d \mid b \Longrightarrow d \mid au + bv$$

$$\forall x \in \mathbb{Z}^*, \qquad a \mid b \iff ax \mid bx$$

♣

Exercice: le prouver

Remarque 14.5.1 *Ceci se traduit par :*
$d\mathbb{Z}$ est stable par $\mathbb{Z}$-combinaison linéaire

$$\forall (u, v) \in \mathbb{Z}^2, \quad a \in d\mathbb{Z} \quad et \quad b \in d\mathbb{Z} \Longrightarrow au + bv \in d\mathbb{Z}$$

et par dilatation non nulle

$$\forall x \in \mathbb{Z}^*, \qquad b \in a\mathbb{Z} \iff bx \in ax\mathbb{Z}$$

*

Exercice: Montrer que

$$d \mid a \quad \text{et} \quad d \mid b \Longleftrightarrow a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$$
$$a \mid d \quad \text{et} \quad b \mid d \Longleftrightarrow d\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$$

Théorème 14.5.4 (Division Euclidienne)
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$a = bq + r \quad et \quad 0 \leq r < b$$

Cette décomposition porte le nom de division euclidienne. q est le quotient et r le reste. On note parfois

$$a \equiv r \quad [b]$$

♣

Démonstration
• Existence :
Supposons $a \in \mathbb{N}$.
Soit $A := \{n \in \mathbb{N} \mid \quad nb \leq a\}$, c'est une partie non vide ($0 \in A$) et majorée par a :

$$\forall n \in A, \qquad n \leq nb \leq a$$

Soit q le plus grand élément de A.
Puisque $q \in A$ et $q + 1 \notin A$

$$qb \leq a \qquad \text{et} \qquad (q+1)b > a$$

Posons $r = a - bq$... CQFD **Si** $a \in \mathbb{Z}$, alors en appliquant ce qui précède à $a' = a + |a|b \in \mathbb{N}$ on trouve $(q', r) \in \mathbb{Z} \times \mathbb{N}$

$$a' = a + |a|b = bq' + r' \quad \text{et} \quad 0 \leq r < b$$

On pose alors $q = q' - |a|$ ... CQFD

• Unicité :
Soient (q, r) et (q', r') deux couples distincts donnant la même décomposition.

$$b|q - q'| = |r' - r| < b \quad \text{donc} \quad |q - q'| = 0 \quad \text{d'où} \quad q = q' \quad \text{et} \quad r = r'$$

•

Exemple: $123456 = 270 \times 456 + 336$

Remarque: Le quotient et le reste sont calculés par MAPLE à l'aide des commandes *iquo* et *irem*

Remarque 14.5.2 (Algorithme Naïf)

***Procédure** division(a,b)*
. variables locales : r,q
. $r \leftarrow a$; $q \leftarrow 0$
*. **Tant que** ($r \geq b$) faire : $r \leftarrow r - b$ $q \leftarrow q + 1$ **Fin du Tant que***
Retourne (q, r)
Fin de la procédure

*

Proposition 14.5.5 *Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $a\mathbb{Z}$ avec $a \in \mathbb{Z}$* ♣

Preuve Soit $G \subset$ un sous-groupe de $\mathbb{Z}$, supposons $G \neq \{0\}$ car sinon trivial. Soit alors $b \neq 0$ dans G. puisque $-b \in G$, G admet donc un élément > 0.
D'où $G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$, soit a sont plus petit élément.

$a \in G$, et donc

$$a\mathbb{Z} \subset G$$

Réciproquement Soit $x \in G$, par division euclidienne par rapport à a,

$$x = na + r \qquad \text{avec} \quad n \in \mathbb{Z} \quad \text{et} \quad r \in [\![0, a-1]\!]$$

On a

$$x - na = r \in G \cap [\![0, a-1]\!] = \{0\}$$

D'où $x = na \in a\mathbb{Z}$... CQFD •

Remarque 14.5.3 *Dans $a\mathbb{Z}$, a est ce qu'on appelle un générateur du groupe $a\mathbb{Z}$, il est unique au signe près.* ∗

Exemple: Soient a, b dans $\mathbb{Z}$, d'après ce qui précède, on peut trouver α et β uniques au signe près tels que

$$a\mathbb{Z} + b\mathbb{Z} = \alpha\mathbb{Z} \qquad \text{et} \qquad a\mathbb{Z} \cap b\mathbb{Z} = \beta\mathbb{Z}$$

En effet il s'agit de sous-groupes :

- $0 \in a\mathbb{Z} + b\mathbb{Z}$ $\qquad (resp.\ 0 \in a\mathbb{Z} \cap b\mathbb{Z})$

• Pour x et y quelconques dans $a\mathbb{Z} + b\mathbb{Z}$ $\quad (resp.\ a\mathbb{Z} \cap b\mathbb{Z})$

$$x = au + bv \quad \text{et} \quad y = am + bn \qquad (resp. \quad x = ka = k'b \quad \text{et} \quad y = la = l'b)$$

$$x - y = a(m-u) + b(v-n) \in a\mathbb{Z} + b\mathbb{Z} \qquad (resp. \quad x - y = (k-l)a = (k'-l')b \in a\mathbb{Z} \cap b\mathbb{Z})$$

α et β sont au signe près le pgcd et ppcm de a et b respectivement.
Ces dénominations s'expliquent grâce aux inclusions (d'où le mot petit, grand relativement à la relation d'ordre "$\supset$") :

$$d \text{ divise } a \text{ et } b \iff a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$$

$$d \text{ multiple de } \ a \text{ et } b \iff d\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$$

voir les commandes *igcd* et *ilcm* dans MAPLE

Définition 14.5.2 *Un entier $p \in \mathbb{N}$ est dit premier lorsqu'il admet exactement 2 diviseurs*

$$1 \qquad et \qquad p$$

On note $\mathcal{P}$ l'ensemble des nombres premiers ♠

Remarque: $-1, 0, 1$ ne sont pas premiers

Remarque: voir le type *prime* dans MAPLE

Proposition 14.5.6 *Tout entier $a \in \mathbb{Z}^*$ non nul admet une décomposition en facteurs premiers*

$$n = \varepsilon \prod_{i \in I} p_i^{\alpha_i}$$

avec $\varepsilon \in \{-1, 1\}$, $(p_i)_{i \in I}$ est une famille finie (éventuellement vide) de nombres premiers et $(\alpha_i)_{i \in I}$ est une famille finie (éventuellement vide) d'entiers.
Cette décompostion est unique à l'ordre des facteurs près.
Ainsi dans la décomposition ci-dessus α_i porte le nom de valuation p_i-adique de n ♣

Exemple:

$$123456789 = 3^2 \times 3803 \times 3607$$

Remarque: MAPLE décompose tout entier à l'aide de la commande $ifactor$