Compléments d'algèbre

I - Compléments sur les groupes

1) Sous-groupe engendré par une partie

a) Définition

Soit $(G,*)$ un groupe. Soit A une partie quelconque de G. On va établir le fait qu'il existe un plus petit sous-groupe de G (au sens de l'inclusion) qui contient la partie A.

Il existe au moins un sous-groupe de $(G,*)$ contenant A à savoir G lui-même. Soit alors H l'intersection de tous les sous-groupes de G contenant la partie A. H est un sous-groupe de G en tant qu'intersection de sous-groupe de G et H contient A en tant qu'intersection de parties de G contenant A. Ainsi, H est un sous-groupe de G contenant A. D'autre part, par construction, H est contenu dans tout sous-groupe de G contenant A. Finalement, H est le plus petit (au sens de l'inclusion) sous-groupe de G contenant A. Ceci démontre l'existence d'un tel sous-groupe. Enfin, si H et H' sont deux plus petits sous-groupes de $(G,*)$ contenant A, alors $H \subset H'$ et $H' \subset H$ puis $H' = H$. Ceci démontre l'unicité d'un sous-groupe de $(G,*)$ contenant A.

DÉFINITION 1. Soit $(G,*)$ un groupe. Soit A une partie quelconque de G. Il existe un plus petit sous-groupe de G qui contient la partie A et un seul. Ce sous-groupe s'appelle le **sous-groupe engendré par la partie** A et se note $\mathrm{gr}(A)$.

Commentaire. Nous avons défini le sous-groupe engendré par une partie à partir d'une « approche extérieure » : nous sommes parti de G qui était un sous-groupe de G contenant A puis nous avons diminué la taille de ce sous-groupe au maximum. Cette approche nous a donné rapidement l'existence et l'unicité de $\mathrm{gr}(A)$ mais pas le contenu de $\mathrm{gr}(A)$. C'est ce dont nous allons dorénavant nous préoccuper.

Un premier résultat immédiat est :

Théorème 1. Soit $(G,*)$ un groupe d'élément neutre e. $\mathrm{gr}(\varnothing) = \{e\}$.

Ainsi, dans $(\mathbb{Z},+)$, $\mathrm{gr}(\varnothing) = \{0\}$, dans $(\mathbb{C}^*,\times)$, $\mathrm{gr}(\varnothing) = \{1\}$, dans $(GL(E),\circ)$, $\mathrm{gr}(\varnothing) = \{Id_E\}$ et dans $(GL_n(\mathbb{K},\times)$, $\mathrm{gr}(\varnothing) = \{I_n\}$.

Théorème 2. Soit $(G,*)$ un groupe. Soit A une partie non vide de G. Alors

$$\mathrm{gr}(A) = \{x_1 * \ldots * x_n,\ n \in \mathbb{N}^*,\ x_1 \in A \text{ ou } x_1' \in A,\ \ldots,\ x_n \in A \text{ ou } x_n' \in A\}$$

où x_i' désigne le symétrique de x_i pour $*$ dans G.

Commentaire. Dire que $x_i' \in A$ équivaut à dire que x_i est le symétrique d'un élément de A. Donc, $\mathrm{gr}(A)$ est constitué de tous les produits finis d'éléments de A et de symétriques d'éléments de A. ❑

En notation additive, cela donne : soit $(G,+)$ un groupe et soit A une partie non vide de G.

$$\mathrm{gr}(A) = \{\pm x_1 \pm \ldots \pm x_n,\ n \in \mathbb{N}^*,\ x_1 \in A,\ \ldots,\ x_n \in A\}.$$

En notation multiplicative, cela donne : soit $(G,\times)$ un groupe et soit A une partie non vide de G.

$$\mathrm{gr}(A) = \left\{x_1^{\pm 1} \times \ldots \times x_n^{\pm 1},\ n \in \mathbb{N}^*,\ x_1 \in A,\ \ldots,\ x_n \in A\right\}.$$

Avec la loi $\circ$, cela donne : soit $(G,\circ)$ un groupe de bijections et soit A une partie non vide de G.

$$\mathrm{gr}(A) = \left\{f_1^{\pm 1} \circ \ldots \circ f_n^{\pm 1},\ n \in \mathbb{N}^*,\ f_1 \in A,\ \ldots,\ f_n \in A\right\}.$$

Démonstration du théorème 2. Soit A une partie non vide de G.
Posons $H = \{x_1 * \ldots * x_n,\ n \in \mathbb{N}^*,\ x_1 \in A \text{ ou } x_1' \in A,\ \ldots,\ x_n \in A \text{ ou } x_n' \in A\}$.

- Vérifions que H est un sous-groupe de $(G,*)$ contenant A.
  - A n'est pas vide. Donc, il existe un élément a dans A. H contient alors l'élément $a * a' = e$.
  - un produit de deux produits finis d'éléments de A et de symétriques d'éléments de A est encore un produit fini d'éléments de A et de symétriques d'éléments de A. Donc, H est stable pour $*$.
  - le symétrique d'un produit fini d'éléments de A et de symétriques d'éléments de A est encore un produit fini d'éléments de A et de symétriques d'éléments de A. Donc, H est stable pour le passage au symétrique.

Finalement, H est un sous-groupe du groupe $(G,*)$. D'autre part, H contient les produits de un élément de A ou encore H contient A. Finalement, H est un sous-groupe du groupe $(G,*)$ contenant A.

• D'autre part, un sous-groupe de G contenant A contient nécessairement les produits finis d'éléments de A et de symétriques d'éléments de A . Un tel sous-groupe contient donc H.

On a montré que $H = \text{gr}(a)$.

Exemple 1. Soit $n \in \mathbb{Z}$. Dans $(\mathbb{Z},+)$, $\text{gr}(\{n\}) = \{\pm n \pm n \ldots \pm n\} = \{kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$. En particulier, $\text{gr}(\{1\}) = \mathbb{Z}$ et $\text{gr}(\{0\}) = \{0\}$.

Exemple 2. En général, si $(G,*)$ est un groupe d'élément neutre e, alors $\text{gr}(\{e\}) = \{e\}$.

Exemple 3. On a vu en maths sup que tout automorphisme orthogonal d'un espace vectoriel euclidien de dimension 2 peut s'écrire comme une composée de réflexions. Donc, le groupe $(O(E_2),\circ)$ est engendré par les réflexions.

Exemple 4. On a vu en maths sup que toute permutation de $[\![1,n]\!]$ peut s'écrire comme une composée de transpositions. Donc, le groupe symétrique $(\mathscr{S}_n,\circ)$ est engendré par les transpositions.

b) Groupes monogènes. Groupes cycliques

Définition 2. Soit $(G,*)$ un groupe. $(G,*)$ est **monogène** si et seulement si il existe un élément a de G tel que $G = \text{gr}(\{a\})$.

Notation. Pour alléger la notation ci-dessus, on écrira dorénavant $\text{gr}(a)$ au lieu de $\text{gr}(\{a\})$.

Un groupe monogène est donc un groupe engendré par l'un de ces éléments. Un élément a de G tel que $G = \text{gr}(a)$ est un **générateur** de G. Un tel générateur n'est pas unique et un élément quelconque de G n'est pas nécessairement un générateur de G comme on va le voir plus loin dans quelques exemples.

Décrivons le sous-groupe mogogène engendré par un élément a.

En notation additive : soit $(G,+)$ un groupe. Soit $a \in G$.

$$\text{gr}(a) = \{na,\ n \in \mathbb{Z}\}.$$

En notation multiplicative : soit $(G,\times)$ un groupe. Soit $a \in G$.

$$\text{gr}(a) = \{a^n,\ n \in \mathbb{Z}\}.$$

Avec la loi $\circ$: soit $(G,\circ)$ un groupe de bijections. Soit $f \in G$.

$$\text{gr}(f) = \{f^n,\ n \in \mathbb{Z}\}.$$

Définition 3. Un groupe est dit **cyclique** si et seulement si ce groupe est monogène et fini.

Exemple 1. On a vu que dans $(\mathbb{Z},+)$, $\mathbb{Z} = \text{gr}(1)$. Donc, le groupe $(\mathbb{Z},+)$ est un groupe monogène, non cyclique car $\mathbb{Z}$ est infini. On note que l'on a aussi $\mathbb{Z} = \text{gr}(-1)$ et que tout autre entier que 1 et -1 n'est pas un générateur du groupe $(\mathbb{Z},+)$.

Exemple 2. L'ensemble des racines 4-èmes de l'unité dans $\mathbb{C}$ est $U_4 = \{1,i,-1,-i\}$. U_4 est un sous-groupe fini du groupe $(\mathbb{C}^*,\times)$. $\text{gr}(i) = \{i^n,\ n \in \mathbb{Z}\} = \{i^n,\ 0 \leqslant n \leqslant 3\} = U_4$. Donc, le groupe $(U_4,\times)$ est un groupe cyclique.
Plus généralement, pour $n \geqslant 1$, $U_n = \left\{\omega^k,\ k \in \mathbb{Z}\right\} = \left\{\omega^k,\ 0 \leqslant k \leqslant n-1\right\}$ où $\omega = e^{\frac{2i\pi}{n}}$ et où les ω^k, $0 \leqslant k \leqslant n-1$, sont deux à deux distincts. Donc,

le groupe $(U_n,\times)$ est cyclique d'ordre n (ou de cardinal n).

Théorème 3. Tout groupe monogène est commutatif.

Démonstration. Démontrons le résultat en notation multiplicative. Soit $(G,\times)$ un groupe monogène. Soit $a \in G$ tel que $G = \text{gr}(a)$. Alors, $G = \{a^n,\ n \in \mathbb{Z}\}$.
Soit $(n,m) \in \mathbb{Z}^2$. $a^n \times a^m = a^{n+m} = a^{m+n} = a^m \times a^n$. Ceci montre que le groupe $(G,\times)$ est un groupe commutatif.

Considérons $(\mathscr{S}_3, \circ)$, le groupe symétrique de $[\![1,3]\!]$. On sait que $\mathscr{S}_3 = \{Id, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}, c_1, c_2\}$ où $c_1 = (2 \quad 3 \quad 1)$ et $c_2 = (3 \quad 1 \quad 2)$. On a $\tau_{1,2} \circ \tau_{1,3} = c_2$ et $\tau_{1,3} \circ \tau_{1,2} = c_1$. Donc, $\tau_{1,2} \circ \tau_{1,3} \neq \tau_{1,3} \circ \tau_{1,2}$. Le groupe $(\mathscr{S}_3, \circ)$ n'est donc pas commutatif. On en déduit en particulier que ce groupe n'est pas monogène. De fait, $gr(Id) = \{Id\} \neq S_3$, $gr(\tau_{i,j}) = \{Id, \tau_{i,j}\} \neq S_3$ et $gr(c_i) = \{Id, c_1, c_2\} \neq S_3$. On peut cependant montrer que $S_3 = gr(\tau_{1,2}, c_1)$. ❑

Sinon, on a immédiatement

Théorème 4. Soit $(G, *)$ un groupe. Soit H un sous-groupe du groupe $(G, *)$.

$$\forall x \in G,\ (x \in H \Leftrightarrow gr(x) \subset H.$$

2) Ordre d'un élément dans un groupe

Dans ce qui suit, $(G, *)$ est un groupe d'élément neutre e. Si x est un élément de G, on note x' le symétrique de x pour $*$ puis on pose

$$\forall n \in \mathbb{Z},\ x^n = \begin{cases} \underbrace{x * \ldots * x}_{n \text{ facteurs}} \text{ si } n > 0 \\ e \text{ si } n = 0 \\ \underbrace{x' * \ldots * x'}_{-n \text{ facteurs}} \text{ si } n < 0 \end{cases}.$$

Définition 4. Soit $(G, *)$ un groupe d'élément neutre e. Soit x un élément de G.

• x est **d'ordre fini** si et seulement si il existe $p \in \mathbb{N}^*$ tel que $x^p = e$.
Dans ce cas, l'**ordre de** x est $\text{Min}\{p \in \mathbb{N}^* / \ x^p = e\}$.

• x est **d'ordre infini** si et seulement si $\forall p \in \mathbb{N}^*$ tel que $x^p \neq e$.

Exemple 1. Dans $(\mathbb{C}^*, \times)$,

- 2 est d'ordre infini car $\forall n \in \mathbb{N}^*$, $2^n \neq 1$.
- 1 est d'ordre 1 car $1^1 = 1$.
- -1 est d'ordre 2 car $(-1)^1 \neq 1$ et $(-1)^2 = 1$.
- i est d'ordre 4 car $i^1 = i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$ et $i^4 = 1$.
- De manière générale, si $z \in \mathbb{C}^*$, z est d'ordre fini si et seulement si il existe $n \in \mathbb{N}^*$ tel que $z^n = 1$. Les éléments d'ordre fini du groupe $(\mathbb{C}^*, \times)$ sont donc les racines n-èmes de l'unité, $n \in \mathbb{N}^*$. ❑

Exemple 2. Dans $(\mathscr{S}_n, \circ)$, $Id_{[\![1,n]\!]}$ est d'ordre 1 et une transposition est d'ordre 2. ❑

Exemple 3. Dans $\left(GL\left(\mathbb{R}^2\right), \circ\right)$, $Id_{\mathbb{R}^2}$ est d'ordre 1, une symétrie distincte de l'identité est d'ordre 2, la rotation d'angle $\frac{2\pi}{3}$ est d'ordre 3 et toute homothétie de rapport non nul est d'ordre infini. ❑

Exemple 4. De manière générale, si $(G, *)$ est un groupe d'élément neutre e, e est un élément de G d'ordre 1 et e est le seul élément de G d'ordre 1. ❑

On donne maintenant la définition de l'ordre d'un élément en notation additive :

Définition 4 bis. Soit $(G, +)$ un groupe d'élément neutre 0. Soit x un élément de G.

• x est **d'ordre fini** si et seulement si il existe $p \in \mathbb{N}^*$ tel que $px = 0$.
Dans ce cas, l'**ordre de** x est $\text{Min}\{p \in \mathbb{N}^* / \ px = 0\}$.

• x est **d'ordre infini** si et seulement si $\forall p \in \mathbb{N}^*$ tel que $px \neq 0$.

Ici, nous sommes face à la difficulté de donner un exemple concret non trivial illustrant cette définition. Dans $(\mathbb{Z}, +)$, 0 et d'ordre 1 et si x est un entier relatif non nul, x est d'ordre infini car $\forall p \in \mathbb{N}^*$, $px \neq 0$ ou encore $\underbrace{x + \ldots + x}_{p \text{ termes}} \neq 0$.

A ce jour, nous ne connaissons pas de situation où un élément est d'ordre 2 ou 3 pour l'addition. Il faudra attendre le paragraphe III (l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$) pour trouver de telles situations.

Théorème 5. L'ordre d'un élément dans un groupe est égal à l'ordre (ou encore le cardinal) du sous-groupe qu'il engendre.

Démonstration. On fait la démonstration en notation multiplicative. Soit $(G, \times)$ un groupe d'élément neutre e. Soit x un élément de G.

1er cas. On suppose que x est d'ordre infini. Montrons que $gr(x)$ est d'ordre infini.

$gr(x) = \{x^n,\ n \in \mathbb{Z}\}$. Montrons que les x^n, $n \in \mathbb{Z}$, sont deux à deux distincts.
Soit n et m deux entiers relatifs tels que $n \geqslant m$. Alors, $n - m \in \mathbb{N}$ puis

$$\begin{aligned} x^n = x^m &\Leftrightarrow x^n \times x^{-m} = e \Leftrightarrow x^{n-m} = e \\ &\Leftrightarrow n - m = 0 \text{ (puisque } n - m > 0 \Rightarrow x^{n-m} \neq e) \\ &\Leftrightarrow n = m. \end{aligned}$$

Ainsi, les x^n, $n \in \mathbb{Z}$, sont deux à deux distincts. On en déduit que $\text{card}(gr(x)) = +\infty$.

2ème cas. On suppose que x est d'ordre fini $n \in \mathbb{N}^*$. Montrons que $gr(x)$ est d'ordre fini n.
Soit $p \in \mathbb{Z}$. La division euclidienne de l'entier p par l'entier non nul n s'écrit $p = nq + r$ où $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$.

$$x^p = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r.$$

Par suite, $gr(x) = \{x^p,\ p \in \mathbb{Z}\} = \left\{x^k,\ k \in [\![0, n-1]\!]\right\}$. Ceci montre déjà que $gr(x)$ est d'ordre fini, inférieur ou égal à n.

Vérifions alors que les x^k, $k \in [\![0, n-1]\!]$, sont deux à deux distincts. Soient k et l deux éléments de $[\![0, n-1]\!]$ tels que $k \geqslant l$. On en déduit que $0 \leqslant k - l \leqslant n - 1$ puis

$$x^k = x^l \Leftrightarrow x^{k-l} = e \Leftrightarrow k - l = 0 \Leftrightarrow k = l$$

(car si $1 \leqslant k - l \leqslant n - 1$, $x^{k-l} \neq e$ par définition de l'ordre n de x.

Ainsi, les x^k, $k \in [\![0, n-1]\!]$, sont deux à deux distincts. On en déduit que $\text{card}(gr(x)) = \text{card}\left\{x^k,\ k \in [\![0, n-1]\!]\right\} = n$.

Dans tous les cas, on a montré que l'ordre de x est égal à l'ordre du sous-groupe qu'engendre x.

Par exemple, dans $(\mathbb{C}^*, \times)$, i est d'ordre 4. Le sous-groupe engendré par i est

$$gr(i) = \{i^n,\ n \in \mathbb{Z}\} = \{i^n,\ 0 \leqslant n \leqslant 3\} = \{1, i, -1, -i\} = U_4$$

et U_4 est constitué de quatre éléments.

Théorème 6. Soit $(G, *)$ un groupe d'élément neutre e. Soit x un élément de G d'ordre fini $n \in \mathbb{N}^*$.

Alors, $\forall p \in \mathbb{Z}$, $x^p = e \Leftrightarrow p \in n\mathbb{Z}$.

Démonstration. Dans la démonstration précédente, on a vu que pour $p \in \mathbb{Z}$, $x^p = x^r$ où r est le reste de la division euclidienne de p par n. Puisque $0 \leqslant r \leqslant n - 1$,

$$x^p = e \Leftrightarrow x^r = e \Leftrightarrow r = 0 \Leftrightarrow p \in n\mathbb{Z}.$$

---

3) Le théorème de Lagrange

Théorème 7 (théorème de Lagrange). Soit $(G, *)$ un groupe **fini**. Soit H un sous-groupe du groupe $(G, *)$.

Le cardinal de H divise le cardinal de G.

Démonstration. Démontrons le résultat en notation multiplicative. Soit $(G, \times)$ un groupe fini d'élément neutre e. Soit H un sous-groupe du groupe $(G, \times)$.

• Sur G, on définit la relation $\mathscr{R}$ par :

$$\forall (x, y) \in G^2,\ \left(x \mathscr{R} y \Leftrightarrow x^{-1} y \in H\right).$$

Vérifions que $\mathscr{R}$ est une relation d'équivalence sur G.

- Soit $x \in G$. $x^{-1}x = e \in H$ car H est un sous-groupe du groupe $(G, \times)$. Donc, $\forall x \in G$, $x \mathscr{R} x$ puis

$\mathscr{R}$ est réflexive.

- Soit $(x, y) \in G^2$ tel que $x \mathscr{R} y$. Alors $x^{-1}y \in H$ puis $y^{-1}x = \left(x^{-1}y\right)^{-1} \in H$ car H est un sous-groupe du groupe $(G, \times)$. Donc, $\forall (x, y) \in G^2$, $(x \mathscr{R} y \Rightarrow y \mathscr{R} x)$ puis

$\mathscr{R}$ est symétrique.

- Soit $(x,y,z) \in G^3$ tel que $x\mathscr{R}y$ et $y\mathscr{R}z$. Alors $x^{-1}y \in H$ et $y^{-1}z \in H$ puis $x^{-1}z = \left(x^{-1}y\right)\left(y^{-1}z\right) \in H$ car H est un sous-groupe du groupe $(G,\times)$. Donc, $\forall (x,y,z) \in G^3$, ($x\mathscr{R}y$ et $y\mathscr{R}z \Rightarrow x\mathscr{R}z$) puis

$$\mathscr{R} \text{ est transitive.}$$

On a montré que $\mathscr{R}$ est une relation d'équivalence.

• Déterminons la classe d'équivalence $\widehat{x}$ d'un élément x de G. Soit $x \in G$.

$$y \in \widehat{x} \Leftrightarrow x\mathscr{R}y \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists h \in H/\ x^{-1}y = h \Leftrightarrow \exists h \in H/\ y = xh \Leftrightarrow y \in xH.$$

Donc, pour tout x de G, $\widehat{x} = xH$. En particulier, $\widehat{e} = eH = \{eh,\ h \in H\} = \{h,\ h \in H\} = H$.

• Montrons que toutes les classes d'équivalence ont le même nombre d'éléments. Soit $x \in G$. Soit $\varphi : \begin{array}{ccc} H & \to & xH \\ h & \mapsto & xh \end{array}$.
Par définition de xH, φ est une application de H vers xH, surjective. D'autre part, pour $(h,h') \in H^2$,

$$\begin{aligned} \varphi(h) = \varphi(h') &\Rightarrow xh = xh' \\ &\Rightarrow h = h' \text{ (car dans un groupe, tout élément est simplifiable).} \end{aligned}$$

Finalement, φ est injective et donc bijective de H sur xH. On en déduit que $\text{card}\,(\widehat{x}) = \text{card}(xH) = \text{card}(H)$.

• Montrons enfin le théorème de Lagrange. On sait que les classes d'équivalence pour la relation $\mathscr{R}$ constituent une partition de G. Si on note p le nombre de classes d'équivalence, puisque toutes les classes ont le même cardinal à savoir le cardinal de H,

$$\text{card}(G) = \underbrace{\text{card}(H) + \ldots + \text{card}(H)}_{p \text{ termes}} = p\ \text{card}(H).$$

Ceci montre que l'entier $\text{card}(H)$ divise l'entier $\text{card}(G)$.

Une conséquence immédiate des théorèmes 5 et 7 est :

Théorème 8. Soit $(G,*)$ un groupe fini. Tout élément de G est d'ordre fini et l'ordre d'un élément de G est un diviseur du cardinal de G.

En particulier, si $\text{card}(G) = n$, alors $\forall a \in G$, $a^n = 1_G$ (où $a^n = \underbrace{a * \ldots * a}_{n \text{ facteurs}}$).

Exemple 1. Le groupe des racines 6-èmes de l'unité dans $\mathbb{C}$ est $U_6 = \left\{1, -j^2, j, -1, j^2, -j\right\}$. U_6 est un groupe fini de cardinal 6. L'ordre d'un élément de U_6 est nécessairement un diviseur de 6 à savoir 1, 2, 3 ou 6. De fait,

- 1 est d'ordre 1 (et engendre le sous-groupe $U_1 = \{1\}$ d'ordre 1),
- -1 est d'ordre 2 (et engendre le sous-groupe $U_2 = \{1, -1\}$ d'ordre 2),
- j et j^2 sont d'ordre 3 (et engendrent l'un ou l'autre le sous-groupe $U_3 = \left\{1, j, j^2\right\}$ d'ordre 3),
- $-j$ et $-j^2$ sont d'ordre 6 (et engendrent l'un ou l'autre le sous-groupe $U_6 = \left\{1, -j^2, j, -1, j^2, -j\right\}$ d'ordre 6).

Le fait que l'on trouve dans U_6 des éléments d'ordre 6 traduit le fait que $(U_6,\times)$ est un groupe cyclique. ❑

Exemple 2. Le groupe $(\mathscr{S}_3,\circ)$ est aussi un groupe d'ordre 6. Il est constitué de $Id_{[\![1,3]\!]}$, des trois transpositions $\tau_{1,2}$, $\tau_{1,3}$ et $\tau_{2,3}$ et des deux cycles de longueur 3 $c_1 = (2\quad 3\quad 1)$ et $c_2 = (3\quad 1\quad 2)$.

- $Id_{[\![1,3]\!]}$ est d'ordre 1 (et engendre le sous-groupe $\left\{Id_{[\![1,3]\!]}\right\}$ d'ordre 1),
- $\tau_{i,j}$ est d'ordre 2 (et engendre le sous-groupe $\left\{Id_{[\![1,3]\!]}, \tau_{i,j}\right\}$ d'ordre 2),
- c_i est d'ordre 3 (et engendre le sous-groupe $\left\{1, c_i, c_i^2\right\}$ d'ordre 3).

On note qu'il n'existe pas d'élément d'ordre 6 et on retrouve le fait que le groupe $(\mathscr{S}_3,\circ)$ n'est pas cyclique.

Ainsi, le théorème 8 dit que l'ordre d'un élément dans un groupe divise l'ordre de ce groupe mais il est faux de supposer que tout diviseur de l'ordre du groupe est l'ordre d'un élément de ce groupe. ❑

4) Morphismes de groupes

a) Définition

DÉFINITION 5. Soient $(G,*)$ et $(G',*')$ deux groupes. Un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$ est une application f de G vers G' vérifiant de plus

$$\forall (x,y)\in G^2,\ f(x*y)=f(x)*'f(y).$$

Exemple 1. $(\mathbb{R},+)$ et $(]0,+\infty[,\times)$ sont deux groupes et $\forall (x,y)\in\mathbb{R}^2$, $e^{x+y}=e^x\times e^y$. Donc, l'application
$\begin{array}{rccc}\exp\ :\ & (\mathbb{R},+) & \to & (]0,+\infty[,\times)\\ & x & \mapsto & e^x\end{array}$ est un morphisme de groupes.

Exemple 2. $(GL_n(\mathbb{K}),\times)$ et $(\mathbb{K}^*,\times)$ sont deux groupes et $\forall (A,B)\in (GL_n(\mathbb{R}))^2$, $\det(A\times B)=\det(A)\times\det(B)$. Donc, l'application
$\begin{array}{rccc}\det\ :\ & (GL_n(\mathbb{K}),\times) & \to & (\mathbb{K}^*,\times)\\ & A & \mapsto & \det(A)\end{array}$ est un morphisme de groupes.

Exemple 3. $(\mathscr{S}_n,\circ)$ et $(\{-1,1\},\times)$ sont deux groupes et $\forall (\sigma,\sigma')\in(\mathscr{S}_n)^2$, $\varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\times\varepsilon(\sigma')$ ($\varepsilon(\sigma)$ est la signature de la permutation σ). Donc, l'application
$\begin{array}{rccc}\varepsilon\ :\ & (\mathscr{S}_n,\circ) & \to & (\{-1,1\},\times)\\ & \sigma & \mapsto & \varepsilon(\sigma)\end{array}$ est un morphisme de groupes.

b) Propriétés

Théorème 9. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$.

- L'image par f de l'élément neutre du groupe $(G,*)$ est l'élément neutre du groupe $(G',*')$.
- L'image par f du symétrique d'un élément x du groupe $(G,*)$ est le symétrique de l'élément $f(x)$ du groupe $(G',*')$.

Démonstration. • Notons e et e' les éléments neutres respectifs des groupes $(G,*)$ et $(G',*)$.

$$f(e)*'e'=f(e)=f(e*e)=f(e)*'f(e).$$

Puisque dans le groupe $(G',*)$, tout élément est simplifiable, après simplification par $f(e)$, on obtient $f(e)=e'$.

• Soit x un élément de G de symétrique noté x^{-1}.

$$f(x)*'f\left(x^{-1}\right)=f\left(x*x^{-1}\right)=f(e)=e'$$

et de même, $f\left(x^{-1}\right)*'f(x)=e'$. Donc, le symétrique de $f(x)$ dans G' est $f\left(x^{-1}\right)$ c'est-à-dire l'image par f du symétrique de x dans G.

Pour la fonction exponentielle, cela donne :

- l'image par l'exponentielle de l'élément neutre du groupe $(\mathbb{R},+)$ est l'élément neutre du groupe $(]0,+\infty[,\times)$ ou encore

$$e^0=1,$$

- l'image par l'exponentielle de l'opposé d'un réel est l'inverse du réel strictement positif obtenu ou encore

$$\forall x\in\mathbb{R},\ e^{-x}=\frac{1}{e^x}.$$

Pour le déterminant, cela donne :

- le déterminant de l'élément neutre du groupe $(GL_n(\mathbb{R}),\times)$ est l'élément neutre du groupe $(\mathbb{R}^*,\times)$ ou encore

$$\det(I_n)=1,$$

- le déterminant de l'inverse d'une matrice inversible est l'inverse du déterminant de cette matrice ou encore

$$\forall A\in GL_n(\mathbb{R}),\ \det\left(A^{-1}\right)=\frac{1}{\det(A)}.$$

Théorème 10. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$.

- L'image par f d'un sous-groupe du groupe $(G,*)$ est un sous-groupe du groupe $(G',*')$.
- L'image réciproque par f d'un sous-groupe du groupe $(G',*')$ est un sous-groupe du groupe $(G,*)$.

Démonstration. On note e et e' les éléments neutres respectifs des groupes $(G,*)$ et $(G',*')$. On note x^{-1} le symétrique d'un élément x.

• Soit H un sous-groupe du groupe $(G,*)$. Montrons que $H'=f(H)$ est un sous-groupe du groupe $(G',*')$.

- $e'=f(e)$ est dans H' (d'après le théorème 9).

- Soit $(y_1,y_2)\in(H')^2$. Il existe $(x_1,x_2)\in H^2$ tel que $f(x_1)=y_1$ et $f(x_2)=y_2$ puis $y_1*'y_2^{-1}=f(x_1)*'(f(x_2))^{-1}=f\left(x_1*x_2^{-1}\right)$ (d'après le théorème 9). Puisque H est un sous-groupe du groupe $(G,*)$, $x_1*x_2^{-1}\in H$ et donc $y_1*'y_2^{-1}\in f(H)=H'$.

On a montré que H' est un sous-groupe du groupe $(G',*')$.

• Soit H' un sous-groupe du groupe $(G',*')$. Montrons que $H=f^{-1}(H')$ est un sous-groupe du groupe $(G,*)$.

- $f(e)=e'\in H'$ et donc $e\in f^{-1}(H')=H$.

- Soit $(x_1,x_2)\in H^2$. Alors $f(x_1)\in H'$ et $f(x_2)\in H'$ puis $f\left(x_1*x_2^{-1}\right)=f(x_1)*'(f(x_2))^{-1}\in H'$ car H' est un sous-groupe du groupe $(G',*')$. Mais alors, $x_1*x_2^{-1}\in H$.

On a montré que H est un sous-groupe du groupe $(G,*)$.

---

c) Noyau et image d'un morphisme de groupes

DÉFINITION 6. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$ deux groupes d'éléments neutres respectifs e et e'.

Le **noyau** de f, noté $\mathrm{Ker}(f)$, est l'ensemble des éléments de G dont l'image par f est l'élément neutre du groupe $(G',*')$.

$$\mathrm{Ker}(f)=\{x\in G/\ f(x)=e'\}=f^{-1}\left(\{e'\}\right).$$

L'image de f, notée $\mathrm{Im}(f)$, est l'ensemble des images des éléments de G par f.

$$\mathrm{Im}(f)=\{f(x),\ x\in G\}=\{y\in G'/\ \exists x\in G/\ y=f(x)\}=f(G).$$

Puisque $\{e'\}$ est un sous-groupe du groupe $(G',*')$, le théorème 10 fournit immédiatement

Théorème 11. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$.

$\mathrm{Ker}(f)$ est un sous-groupe du groupe $(G,*)$. $\mathrm{Im}(f)$ est un sous-groupe du groupe $(G',*')$.

Exemple 1. L'application $\exp\ :\ x\mapsto e^x$ est un morphisme du groupe $(\mathbb{R},+)$ vers le groupe $(]0,+\infty[,\times)$. Le noyau de ce morphisme est $\mathrm{Ker}(f)=\{x\in\mathbb{R}/\ e^x=1\}=\{0\}$. De fait, $\{0\}$ est un sous-groupe de $(\mathbb{R},+)$.

Exemple 2. L'application $f\ :\ x\mapsto x^2$ est un morphisme du groupe $(U_4,\times)$ dans lui-même (où $U_4=\{1,i,-1,-i\}$). En effet, pour $(x,y)\in U_4^2$,

$$f(x\times y)=(x\times y)^2=x^2\times y^2.$$

Le noyau de ce morphisme est l'ensemble des éléments de U_4 dont le carré vaut 1. Donc, $\mathrm{Ker}(f)=\{1,-1\}=U_2$. On note que U_2 est effectivement un sous-groupe du groupe $(U_4,\times)$.

Exemple 3. L'application $\det\ :\ A\mapsto\det(A)$ est un morphisme du groupe $(GL_n(\mathbb{K}),\times)$ sur le groupe $(\mathbb{K}^*,\times)$. Le noyau de ce morphisme est l'ensemble des matrices de déterminant 1. C'est un sous-groupe du groupe $(GL_n(\mathbb{K}),\times)$ appelé **groupe spécial linéaire** et noté $SL_n(\mathbb{K})$. L'ensemble des matrices orthogonales de déterminant 1 est un sous-groupe du groupe $(SL_n(\mathbb{R}),\times)$ appelé **groupe spécial orthogonal** et noté $SO_n(\mathbb{R})$ ou $O_n^+(\mathbb{R})$. On peut voir de deux façons que $(SO_n(\mathbb{R}),\times)$ est un groupe : ou bien, $SO_n(\mathbb{R})=SL_n(\mathbb{R})\cap O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ est un sous-groupe de $(GL_n(\mathbb{R}),\times)$ en tant qu'intersection de sous-groupes de $(GL_n(\mathbb{R}),\times)$, ou bien $SO_n(\mathbb{R})$ est le noyau du morphisme de groupes $\begin{array}{rccc}\det\ :&O_n(\mathbb{R})&\to&(\{-1,1\},\times)\\&A&\mapsto&\det(A)\end{array}$.

On a des notions équivalentes dans le groupe $(GL(E),\circ)$, groupe des automorphismes d'un espace de dimension finie E. On définit $SL(E)$ le sous-groupe des automorphismes de déterminant 1. Si de plus E est un espace euclidien, on définit $SO(E)=O^+(E)=O(E)\cap SL(E)$.

Exemple 4. L'application $\varepsilon\ :\ \sigma\mapsto\varepsilon(\sigma)$ est un morphisme du groupe $(\mathscr{S}_n,\circ)$ vers le groupe $(\{-1,1\},\times)$. Le noyau de ce morphisme est l'ensemble des permutations de signature 1. C'est un sous-groupe de $(\mathscr{S}_n,\circ)$ appelé **groupe alterné** et noté $\mathscr{A}_n$. Les permutations de signature 1 sont les **permutations paires** c'est-à-dire les permutations qui sont des composées d'un nombre pair de transpositions.

Théorème 12. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$.

f est injectif si et seulement si $\mathrm{Ker}(f)=\{e\}$. f est surjectif si et seulement si $\mathrm{Im}(f)=G'$.

Démonstration. On note e et e' les éléments neutres respectifs des groupes $(G,*)$ et $(G',*')$.

• Supposons f injectif. Soit $x\in G$. D'après le théorème 9, $f(e)=e'$ et donc

$$f(x)=e' \Leftrightarrow f(x)=f(e) \Leftrightarrow x=e.$$

Ceci montre que $\mathrm{Ker}(f)=\{e\}$.

• Supposons $\mathrm{Ker}(f)=\{e\}$. Soit $(x,y)\in G^2$. En notant y^{-1} le symétrique de y dans G, le théorème 9 fournit

$$\begin{aligned} f(x)=f(y) &\Rightarrow f(x)*'(f(y))^{-1}=e' \Rightarrow f\left(x*y^{-1}\right)=e' \\ &\Rightarrow x*y^{-1}=e \ (\text{car } \mathrm{Ker}(f)=\{e\}) \\ &\Rightarrow x=y. \end{aligned}$$

Ceci montre que f est injectif.

Sinon, il est immédiat que f est surjectif si et seulement si $\mathrm{Im}(f)=G'$.

---

d) Isomorphismes de groupes

DÉFINITION 7. Un **isomorphisme** du groupe $(G,*)$ sur le groupe $(G',*')$ est un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$ qui de plus est une bijection de G sur G'.

Soient $(G,*)$ et $(G',*')$ deux groupes. On dit que $(G,*)$ et $(G',*')$ sont **isomorphes** si et seulement si il existe un isomorphisme de $(G,*)$ sur $(G',*')$.

Par exemple, l'exponentielle est un isomorphisme du groupe $(\mathbb{R},+)$ sur le groupe $(]0,+\infty[,\times)$.

Théorème 13. Soit f un isomorphisme du groupe $(G,*)$ sur le groupe $(G',*')$. Alors, f^{-1} est un morphisme du groupe $(G',*')$ vers le groupe $(G,*)$ (et donc un isomorphisme du groupe $(G',*')$ sur le groupe $(G,*)$).

Démonstration. Soit $(y_1,y_2)\in(G')^2$. Soient $x_1=f^{-1}(y_1)$ et $x_2=f^{-1}(y_2)$ de sorte que $f(x_1)=y_1$ et $f(x_2)=y_2$.

$$y_1*'y_2=f(x_1)*'f(x_2)=f(x_1*x_2)=f\left(f^{-1}(y_1)*f^{-1}(y_2)\right)$$

et donc $f^{-1}(y_1*'y_2)=f^{-1}(y_1)*f^{-1}(y_2)$. Ceci montre que f^{-1} est un morphisme du groupe $(G',*')$ vers le groupe $(G,*)$.

Par exemple, l'isomorphisme réciproque de l'isomorphisme $\begin{array}{rccc}\exp : & (\mathbb{R},+) & \to & (]0,+\infty[,\times) \\ & x & \mapsto & e^x\end{array}$ est l'isomorphisme $\begin{array}{rccc}\ln : & (]0,+\infty[,\times) & \to & (\mathbb{R},+) \\ & x & \mapsto & \ln(x)\end{array}$. De fait, on a les formules

$$\forall (x,y)\in]0,+\infty[^2,\ \ln(x\times y)=\ln(x)+\ln(y), \qquad \ln(1)=0, \qquad \forall x>0,\ \ln\left(\frac{1}{x}\right)=-\ln(x).$$

5) Sous-groupes du groupe $(\mathbb{Z},+)$

Théorème 14. Les sous-groupes du groupe $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, $n\in\mathbb{Z}$.

Démonstration. • Soit $n\in\mathbb{Z}$. $n\mathbb{Z}=\mathrm{gr}(n)$ est un sous-groupe du groupe $(\mathbb{Z},+)$.

• Réciproquement, soit H un sous-groupe du groupe $(\mathbb{Z},+)$. Si $H=\{0\}$, alors $H=0\mathbb{Z}$.

Sinon, $H\neq\{0\}$ et donc H contient un certain élément x non nul. Les deux éléments x et $-x$ sont dans H (car H est un sous-groupe) et l'un de ces deux éléments est strictement positif.
L'ensemble $H\cap\mathbb{N}^*$ est alors une partie non vide de $\mathbb{N}$ (et même de $\mathbb{N}^*$). On en déduit que $H\cap\mathbb{N}^*$ admet un plus petit élément que l'on note n. Par définition, n est un entier naturel non nul élément de H.

Puisque H est un sous-groupe de $(\mathbb{Z},+)$ et que $n\in H$, on en déduit que $\mathrm{gr}(n)\subset H$ ou encore $n\mathbb{Z}\subset H$.

Inversement, soit $x \in H$. La division euclidienne de x par n (on rappelle que $n \neq 0$) s'écrit $x = nq + r$ où $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. $r = x - nq$ avec $x \in H$ et $nq \in n\mathbb{Z} \subset H$. Puisque H est un sous-groupe de $(\mathbb{Z}, +)$, on en déduit que $r \in H$. Ainsi, $r \in H \cap [\![0, n-1]\!]$ et donc $r = 0$ par définition de n. Mais alors, $x = nq \in n\mathbb{Z}$. Ceci montre que $H \subset n\mathbb{Z}$ et finalement que $H = n\mathbb{Z}$.

On peut apporter quelques précisions au théorème 14.

Théorème 15.

1) $\forall (n, m) \in \mathbb{Z}^2$, $n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow m = \pm n$.
2) $\forall (n, m) \in \mathbb{N}^2$, $n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow m = n$.
3) Pour tout sous-groupe H du groupe $(\mathbb{Z}, +)$, il existe un entier naturel n et un seul tel que $H = n\mathbb{Z}$.

Démonstration. Soit $(n, m) \in \mathbb{Z}^2$. Supposons que $n\mathbb{Z} = m\mathbb{Z}$. Alors, $m \in m\mathbb{Z} = n\mathbb{Z}$ et donc m est un multiple de n. De même, n est un multiple de n. On sait que ceci impose $m = \pm n$.

Réciproquement, si $m = n$, alors $n\mathbb{Z} = m\mathbb{Z}$ et si $m = -n$, alors $m\mathbb{Z} = \{-kn,\ k \in \mathbb{Z}\} = \{kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$.

Enfin, 2) est une conséquence immédiate de 1) et 3) est une conséquence de 2) et du théorème 14.

Revenons alors sur la notion d'ordre d'un élément dans un groupe. Soit $(G, \times)$ (en notation multiplicative) un groupe d'élément neutre e et x un élément de G. Soit $H = \{p \in \mathbb{Z} / \ x^p = e\}$.
$0 \in H$ et si $(p, q) \in H^2$ alors $p - q \in H$ car $x^{p-q} = x^p \left(x^q\right)^{-1} = e$. Donc, H est un sous-groupe de $(\mathbb{Z}, +)$. Par suite, il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. Le cas $n = 0$ est le cas où x est d'ordre infini et le cas $n \geqslant 1$ est le cas où x est d'ordre fini égal à n. On retrouve ainsi le théorème 6.

II - Compléments sur les anneaux

1) Produit fini d'anneaux

On se donne un nombre fini d'anneaux $(A_1, +_1, *_1)$, ..., $(A_n, +_n, *_n)$. Sur le produit cartésien $A_1 \times \ldots \times A_n$, on définit les lois produit :

$$\forall ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in (A_1 \times \ldots \times A_n)^2,\ (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 +_1 y_1, \ldots, x_n +_n y_n),$$

et

$$\forall ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in (A_1 \times \ldots \times A_n)^2,\ (x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 *_1 y_1, \ldots, x_n *_n y_n).$$

Une vérification fastidieuse mais simple fournit

Théorème 16. $(A_1 \times \ldots \times A_n, +, *)$ est un anneau.

Commentaire. L'élément neutre de $A_1 \times \ldots \times A_n$ pour $+$ est $0 = (0_1, \ldots, 0_n)$ et l'élément neutre pour $\times$ est $1 = (1_1, \ldots, 1_n)$. L'opposé de $x = (x_1, \ldots, x_n)$, c'est-à-dire le symétrique de x pour $+$, est $(-x_1, \ldots, -x_n)$ et l'inverse de $x = (x_1, \ldots, x_n)$, c'est-à-dire le symétrique de x pour $\times$, est $\left(x_1^{-1}, \ldots, x_n^{-1}\right)$.

2) Sous-anneaux

Définition 8. Soit $(A, +, *)$ un anneau d'élément neutre 1_A pour $*$. Soit B une partie de A.

B est un **sous-anneau** de l'anneau $(A, +, *)$ si et seulement si

1) $1_A \in B$,
2) B est stable pour $+$ et $*$,
3) muni des lois induites, B est un anneau.

Théorème 17. Soit $(A, +, *)$ un anneau d'élément neutre 1_A pour $*$. Soit B une partie de A.

B est un sous-anneau de l'anneau $(A, +, *)$ si et seulement si

1) $1_A \in B$,
2) $\forall (x, y) \in B^2,\ x - y \in B$ et $x * y \in B$.

Démonstration. • Il est clair que si B est un sous-anneau de l'anneau $(A, +, *)$, alors les conditions 1) et 2) sont vérifiées.

• Réciproquement, supposons les conditions 1) et 2) vérifiées.

B contient $1_A - 1_A = 0$ et $\forall (x,y) \in B^2$, $x - y \in B$. Donc, B est un sous-groupe du groupe $(A,+)$. En particulier, B est stable pour $+$ et, muni de la loi induite encore notée $+$, B est un groupe commutatif.

B est stable pour la loi $*$. La loi induite est associative (car $*$ est associative dans A), distributive sur la loi induite $+$ (car $*$ est distributive sur $+$ dans A) et enfin $1_A \in B$ est élément neutre pour la loi induite $*$.

Finalement, muni des lois induites, B est un anneau.

Exemple 1. Dans $(\mathbb{Z},+,\times)$, un sous-anneau doit contenir 1 puis $\text{gr}(1) = \mathbb{Z}$. Le seul sous-anneau de l'anneau $(\mathbb{Z},+,\times)$ est $\mathbb{Z}$ lui-même.

Exemple 2. Considérons l'anneau $(\mathscr{P}(E),\Delta,\cap)$ (où Δ est la différence symétrique). Soit F une partie de E distincte de E. $(\mathscr{P}(F),\Delta,\cap)$ est un anneau (d'élément neutre F pour $\cap$) mais $\mathscr{P}(F)$ n'est pas un sous-anneau de $(\mathscr{P}(E),\Delta,\cap)$ car l'élément neutre E pour $\cap$ dans $\mathscr{P}(E)$ n'est pas un élément de $\mathscr{P}(F)$. Dans le cadre du programme officiel, la notion de sous-anneau est très peu riche voire sans intérêt.

Exemple 3. On peut néanmoins signaler le fait que $\mathbb{Z}$ est un sous-anneau de l'anneau $(\mathbb{Q},+,\times)$ (qui est plus précisément un corps). Signalons aussi $\mathbb{Z}[i] = \left\{a+ib,\ (a,b) \in \mathbb{Z}^2\right\}$ qui est un sous-anneau de l'anneau $(\mathbb{C},+,\times)$. $\mathbb{Z}[i]$ est l'**anneau des entiers de Gauss**.

3) Idéal d'un anneau commutatif

Dans ce paragraphe, la deuxième loi d'un anneau sera notée $\times$ car en classe préparatoire, la notion d'idéal d'un anneau ne s'utilise en pratique que dans deux situations : l'anneau $(\mathbb{Z},+,\times)$ et l'anneau $(\mathbb{K}[X],+,\times)$.

a) Définitions et premières propriétés

Définition 9. Soit $(A,+,\times)$ un anneau commutatif. Soit I une partie de A.

I est un **idéal** de l'anneau $(A,+,\times)$ si et seulement si

1) I est un sous-groupe du groupe $(A,+)$
2) $\forall x \in I$, $\forall a \in A$, $ax \in I$.

L'axiome 2) signifie que I contient tout multiple d'élément de I. C'est une propriété plus forte que la stabilité pour le produit (qui sert entre autre dans la définition des sous-anneaux) puisqu'on veut que le produit d'un élément de I par un élément de A (pas forcément dans I) reste un élément de I.

On déterminera plus loin les idéaux de l'anneau $(\mathbb{Z},+,\times)$ et les idéaux de l'anneau $(\mathbb{K}[X],+,\times)$.

Théorème 18. Soit $(A,+,\times)$ un anneau commutatif. Soit $x \in A$. Alors $xA = \{ax,\ a \in A\}$ est un idéal de l'anneau $(A,+,\times)$.

Commentaire. L'ensemble xA est l'ensemble des multiples de x.

Démonstration. Soit x un élément de A. Soit $I = xA$.

• $0 = x \times 0 \in I$.
• Soit $(a,a') \in A^2$. $ax - a'x = (a-a')x \in I$.
• Soit $(a,a') \in A^2$. $(ax)a' = (aa')x \in I$.

Donc, I est un idéal de l'anneau $(A,+,\times)$.

Théorème 19. Soit $(A,+,\times)$ un anneau commutatif.

1) L'intersection de deux idéaux de l'anneau $(A,+,\times)$ est un idéal de cet anneau.
2) La somme de deux idéaux de l'anneau $(A,+,\times)$ est un idéal de cet anneau.

Commentaire. La somme des idéaux I et J est $I+J = \{x+y,\ x \in I,\ y \in J\}$.

Démonstration. Soient I et J deux idéaux d'un anneau $(A,+,\times)$.

1) $I \cap J$ est un sous-groupe du groupe $(A,+)$ en tant qu'intersection de sous-groupe du groupe $(A,+)$. D'autre part, si x est un élément de $I \cap J$ et a est un élément de A, alors $ax \in I$, $ax \in J$ et donc $ax \in I \cap J$.
Ceci montre que $I \cap J$ est un idéal de l'anneau $(A,+,\times)$.

2) $I+J$ est un sous-groupe du groupe $(A,+)$ en tant que somme de sous-groupes du groupe $(A,+)$. D'autre part, si (y,z) est un élément de $I\times J$ et a est un élément de A, alors $a(x+y)=ax+ay\in I+J$.
Ceci montre que $I+J$ est un idéal de l'anneau $(A,+,\times)$.

Théorème 20. Soit $(A,+,\times)$ un anneau commutatif. Soit I un idéal de cet anneau.

$I=A\Leftrightarrow 1_A\in I$.

Démonstration. Si $I=A$, alors $1_A\in I$. Réciproquement, si $1_A\in I$, alors $\forall a\in A$, $a=1_A\times a\in I$ et donc $A=I$.

Ainsi, le seul idéal de l'anneau $(\mathbb{Z},+,\times)$ qui contient l'entier 1 est $\mathbb{Z}$ lui-même.

b) Idéal principal. Anneau principal

On rappelle que si x est un élément de A, l'ensemble xA des multiples de x est un idéal de l'anneau $(A,+,\times)$.

DÉFINITION 10. Soit $(A,+,\times)$ un anneau commutatif.

Soit I un idéal de A. L'idéal I est **principal** si et seulement si il existe $x\in A$ tel que $I=xA$. L'idéal xA est appelé **idéal principal engendré par** x.

L'anneau $(A,+,\times)$ est **principal** si et seulement si tout idéal de cet anneau est principal.

Commentaire. Comme dans le cas, des sous-groupes engendrés ou des sous-espaces vectoriels engendrés, l'idéal xA est le plus petit idéal (au sens de l'inclusion) de l'anneau $(A,+,\times)$ contenant l'élément x.

c) Divisibilité dans un anneau commutatif intègre

Les notions d'anneau et d'idéal d'un anneau sont « faites pour » l'arithmétique :

DÉFINITION 11. Soit $(A,+,\times)$ un anneau commutatif intègre.

Soient a et b deux éléments de A tels que $a\neq 0_A$. a **divise** b si et seulement si il existe $q\in A$ tel que $b=aq$. On écrit dans ce cas $a|b$.

Cette notion a été largement détaillée en maths sup dans le cas de l'anneau $(\mathbb{Z},+,\times)$ et de l'anneau $(\mathbb{K}[X],+,\times)$ et ne le sera pas davantage ici. En particulier, on ne s'attardera pas sur l'influence du fait que l'anneau soit supposé intègre (ce qui est le cas des anneaux $(\mathbb{Z},+,\times)$ et $(\mathbb{K}[X],+,\times)$). On peut cependant donner une interprétation de la divisibilité en termes d'idéaux :

Théorème 21. Soit $(A,+,\times)$ un anneau commutatif intègre. Soient a et b deux éléments de A, $a\neq 0_A$.

$$a|b\Leftrightarrow bA\subset aA.$$

Commentaire. Donc, a divise b si et seulement si l'ensemble des multiples de b est contenu dans l'ensemble des multiples de a.

Démonstration. • Supposons que $a|b$. Donc, il existe $q\in A$ tel que $b=qa$ puis

$$bA=\{kb,\ k\in A\}=\{kqa,\ k\in A\}\subset\{k'a,\ k'\in A\}=aA.$$

• Si $bA\subset aA$, alors $b=b\times 1_A\in bA$ et donc $b\in aA$. Par suite, il existe $q\in A$ tel que $b=qa$ et donc $a|b$.

---

4) Morphismes d'anneaux

DÉFINITION 12. Soient $(A,+,*)$ et $(A',+',*')$ deux anneaux. Un morphisme d'anneaux de l'anneau $(A,+,*)$ vers l'anneau $(A',+',*')$ est une application f de A vers A' qui de plus est un morphisme de $(A,+)$ vers $(A',+')$ et de $(A,*)$ vers $(A',*')$ et qui vérifie $f(1_A)=1_{A'}$.

Par exemple, soit $\begin{array}{rccc} f: & (\mathbb{Z}[i],+,\times) & \to & (\mathbb{Z}[i],+,\times) \\ & z & \mapsto & \overline{z}\end{array}$. f est un morphisme d'anneaux car $\overline{1}=1$ et $\forall (z,z')\in(\mathbb{Z}[i])^2$, $\overline{z+z'}=\overline{z}+\overline{z'}$ et $\overline{z\times z'}=\overline{z}\times\overline{z'}$.

DÉFINITION 13. Soit f un morphisme d'anneaux. Le noyau de f est son noyau en tant que morphisme pour l'addition des anneaux $(A,+,*)$ et $(A',+',*')$ qui sont des lois de groupes.

$$\text{Ker}(f)=\{x\in A/\ f(x)=0_{A'}\}.$$

L'image de f est $\text{Im}(f)=f(A)=\{f(x),\ x\in A\}$.

Théorème 22. Soit f un morphisme de l'anneau $(A,+,*)$ vers l'anneau $(A',+',*')$.
Ker(f) est un idéal de l'anneau $(A,+,*)$.

Démonstration. Soit f un morphisme de l'anneau $(A,+,*)$ vers l'anneau $(A',+',*')$. f est en particulier un morphisme du groupe $(A,+)$ vers le groupe $(A',+')$. D'après le théorème 11, Ker(f) est un sous-groupe du groupe $(A,+)$.

Soient $a\in A$ et $x\in\text{Ker}(f)$. $f(a*x)=f(a)*'f(x)=f(a)*'0_{A'}=0_{A'}$ (on sait depuis la maths sup que l'élément neutre pour $+'$ est absorbant pour $*'$). Donc, $ax\in\text{Ker}(f)$.

On a montré que Ker(f) est un idéal de l'anneau $(A,+,*)$.

Sinon, un morphisme d'anneaux étant en particulier un morphisme de groupes, le théorème 12 fournit

Théorème 23. Soit f un morphisme de l'anneau $(A,+,*)$ vers l'anneau $(A',+',*')$.
f est injectif si et seulement si $\text{Ker}(f)=\{0_A\}$. f est surjectif si et seulement si $\text{Im}(f)=A'$.

5) Idéaux de l'anneau $(\mathbb{Z},+,\times)$

a) $(\mathbb{Z},+,\times)$ *est un anneau principal*

Théorème 24. Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont les $n\mathbb{Z}$, $n\in\mathbb{Z}$.
Tout idéal de l'anneau $(\mathbb{Z},+,\times)$ est principal. L'anneau $(\mathbb{Z},+,\times)$ est principal.

Démonstration. On sait déjà d'après le théorème 14 que les sous-groupes du groupe $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, $n\in\mathbb{Z}$. Un idéal de l'anneau $(\mathbb{Z},+,\times)$ est donc nécessairement de cette forme.

Réciproquement, d'après le théorème 18, $n\mathbb{Z}$ est un idéal de l'anneau $(\mathbb{Z},+,\times)$. Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont donc les $n\mathbb{Z}$, $n\in\mathbb{Z}$.

---

b) PGCD et PPCM de deux entiers relatifs non nuls

Le résultat précédent a de nombreuses applications en arithmétique. L'une d'entre elles est la possibilité d'établir rapidement la définition et les premières propriétés du PGCD et du PPCM de deux entiers relatifs non nuls (la notion de PPCM de deux entiers relatifs non nuls n'est pas au programme des classes préparatoires).

• Soient a et b deux entiers relatifs non nuls. $a\mathbb{Z}\cap b\mathbb{Z}$ est un idéal de l'anneau $(\mathbb{Z},+,\times)$ d'après le théorème 19. Il existe donc un entier naturel non nul m tel que

$$a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}\quad(*).$$

$a\mathbb{Z}\cap b\mathbb{Z}$ est l'ensemble des multiples communs à a et à b. L'égalité $(*)$ signifie que m est le plus petit multiple strictement positif commun à a et à b (m est le PPCM de a et b). De plus, l'égalité $(*)$ s'énonce explicitement sous la forme :

les multiples communs à deux entiers relatifs non nuls sont les multiples de leur PPCM.

• Soient a et b deux entiers relatifs non nuls. $a\mathbb{Z}+b\mathbb{Z}$ est un idéal de l'anneau $(\mathbb{Z},+,\times)$ d'après le théorème 19. Il existe donc un entier naturel non nul d tel que

$$a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}\quad(**).$$

Vérifions que le nombre d ainsi défini est un diviseur commun à a et à b puis que d est le plus grand diviseur strictement positif commun à a et à b.

$a\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ et donc d divise a d'après le théorème 21. De même, d divise b et donc d est un diviseur commun à a et à b.
D'autre part, par construction, il existe deux entiers relatifs u et v tels que $d=au+bv$. Donc, si c est un diviseur commun à a et b, c divise $au+bv=d$. On en déduit que d est le plus grand diviseur strictement positif commun à a et à b puis que

les diviseurs communs à deux entiers relatifs non nuls sont les diviseurs de leur PGCD.

On obtient alors très rapidement le théorème de Bézout :

$$\begin{aligned} a \text{ et } b \text{ sont premiers entre eux} &\Leftrightarrow d = 1 \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \\ &\Leftrightarrow 1 \in a\mathbb{Z} + b\mathbb{Z} \text{ (d'après le théorème 20)} \\ &\Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 / \ au + bv = 1. \end{aligned}$$

6) Idéaux de l'anneau $(\mathbb{K}[X], +, \times)$

a) $(\mathbb{K}[X], +, \times)$ *est un anneau principal*

Théorème 25. Les idéaux de l'anneau $(\mathbb{K}[X], +, \times)$ sont les $P \times \mathbb{K}[X] = \{P \times Q, \ Q \in \mathbb{K}[X]\}$ où $P \in \mathbb{K}[X]$.
Tout idéal de l'anneau $(\mathbb{K}[X], +, \times)$ est principal. L'anneau $(\mathbb{K}[X], +, \times)$ est principal.

Démonstration. Soit P un polynôme. D'après le théorème 18, $P \times \mathbb{K}[X]$ est un idéal de l'anneau $(\mathbb{K}[X], +, \times)$ à savoir l'idéal principal engendré par le polynôme P.

Réciproquement, soit I un idéal de l'anneau $(\mathbb{K}[X], +, \times)$. Si $I = \{0\}$, alors $I = 0 \times \mathbb{K}[X]$.
Supposons maintenant $I \neq \{0\}$. On peut considérer $\mathscr{E} = \{\deg(P), \ P \in I \setminus \{0\}\}$. Puisque I n'est pas réduit à 0, $\mathscr{E}$ est une partie non vide de $\mathbb{N}$. $\mathscr{E}$ admet donc un plus petit élément d_0. Soit P_0 un élément de I de degré d_0.

Puisque I est un idéal de l'anneau $(\mathbb{K}[X], +, \times)$, I contient les P_0Q, $Q \in \mathbb{K}[X]$ ou encore $P_0 \times \mathbb{K}[X] \subset I$. Inversement, soit $P \in I$. La division euclidienne de P par P_0 s'écrit $P = P_0 \times Q + R$ où Q et R sont deux polynômes et $\deg(R) < \deg(P_0) = d_0$. $P \in I$ et $P_0 \times Q \in I$ (car $P_0 \times \mathbb{K}[X] \subset I$). Donc, $R = P - P_0 \times Q \in I$ (car I est un sous-groupe de $(\mathbb{K}[X], +)$). Ainsi, R est un élément de I de degré strictement plus petit que d_0. Par définition de d_0, ceci impose $R = 0$ puis $P = P_0 \times Q \in P_0 \times \mathbb{K}[X]$.

On vient de montrer que $I \subset P_0 \times \mathbb{K}[X]$ et finalement $I = P_0 \times \mathbb{K}[X]$. Tout idéal de l'anneau $(\mathbb{K}[X], +, \times)$ est donc principal.

Dans le théorème précédent, le polynôme P n'est pas unique. Par exemple, $X\mathbb{R}[X] = (2X)\mathbb{R}[X]$ (car $2XQ = X(2Q) \in X\mathbb{R}[X]$ et $XQ = (2X)\left(\frac{1}{2}Q\right) \in (2X)\mathbb{R}[X]$). On peut définir le polynôme P de manière unique si on impose en plus au polynôme P d'être unitaire (quand $P \neq 0$ ou encore $I \neq \{0\}$) :

Théorème 26. Soit I un idéal non nul de l'anneau $(\mathbb{K}[X], +, \times)$. Il existe un polynôme unitaire P_0 et un seul tel que $I = P_0 \times \mathbb{K}[X]$.

Démonstration. Soit I un idéal non nul de l'anneau $(\mathbb{K}[X], +, \times)$.

Existence. Soit $P \neq 0$ tel que $I = P \times \mathbb{K}[X]$. Soit $P_0 = \dfrac{1}{\text{dom}(P)}P$. P_0 est un polynôme unitaire élément de I (car multiple de P). De plus, pour tout polynôme Q,

$$P_0 \times Q = P \times \left(\frac{1}{\text{dom}(P)}Q\right) \in P \times \mathbb{K}[X]$$

et

$$P \times Q = P_0 \times (\text{dom}(P)Q) \in P_0 \times \mathbb{K}[X].$$

Donc, $P \times \mathbb{K}[X] = P_0 \times \mathbb{K}[X]$. Ceci montre l'existence de P_0.

Unicité. Soient P_0 et P_1 deux polynômes unitaires tels que $P_0 \times \mathbb{K}[X] = P_1 \times \mathbb{K}[X]$. Alors, $P_0 \times \mathbb{K}[X] \subset P_1 \times \mathbb{K}[X]$ puis P_1 divise P_0. De même, P_1 divise P_0. On sait alors qu'il existe $\lambda \in \mathbb{K}$ tel que $P_1 = \lambda P_0$. Puisque P_0 et P_1 sont unitaires, $\lambda = 1$ (en analysant les coefficients dominants) puis $P_1 = P_0$. Ceci montre l'unicité de P_0.

---

b) PGCD et PPCM de deux polynômes non nuls

De la même manière que pour les entiers relatifs, le résultat précédent permet de redéfinir le PGCD (et le PPCM (hors programme)) de deux polynômes non nuls.

Soient A et B deux polynômes non nuls. Il existe un unique polynôme unitaire D tel que

$$(A \times \mathbb{K}[X]) + (B \times \mathbb{K}[X]) = D \times \mathbb{K}[X].$$

D est le polynôme unitaire de plus haut degré qui soit un diviseur commun à A et B et tout diviseur commun à A et B est un diviseur de D. D est le PGCD des polynômes A et B.

De même, il existe un unique polynôme unitaire M tel que

$$(A \times \mathbb{K}[X]) \cap (B \times \mathbb{K}[X]) = M \times \mathbb{K}[X].$$

M est le polynôme non nul, unitaire, de plus bas degré qui soit un multiple commun à A et B et tout multiple commun à A et B est un multiple de M. M est le PPCM des polynômes A et B.

III - Compléments d'arithmétique : l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

1) Définition de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Soit n un entier naturel. Rappelons la définition de la congruence modulo n :

$$\forall (a, b) \in \mathbb{Z}^2,\ (a \equiv b\ [n] \Leftrightarrow b - a \in n\mathbb{Z}).$$

On a vu en maths sup que, quand $n \geqslant 1$, la congruence modulo n est une relation d'équivalence à n classes (la congruence modulo 0 est l'égalité et les classes d'équivalence sont des singletons), à savoir $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$. Par définition, $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble de ces classes.

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

Ainsi, $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$, $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. On sait que l'on n'a pas l'unicité d'un représentant d'une classe d'équivalence et donc on a aussi $\mathbb{Z}/5\mathbb{Z} = \{\overline{-15}, \overline{6}, \overline{-3}, \overline{3}, \overline{19}\}$.

On définit alors dans $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication de la façon suivante :

$$\forall (a, b) \in \mathbb{Z}^2,\ \overline{a+b} = \overline{a} + \overline{b} \text{ et } \overline{a \times b} = \overline{a} \times \overline{b} \quad (*).$$

Ainsi par exemple, dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{2} + \overline{3} = \overline{0}$.

Un problème se pose en raison de la non unicité d'un représentant d'une classe. Pour que les relations $(*)$ définissent effectivement des lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$, il faut se convaincre que la définition de $\overline{a+b}$ et $\overline{a \times b}$ ne dépend pas du choix des représentants a et b de $\overline{a}$ et $\overline{b}$. Par exemple, dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{2} + \overline{3} = \overline{7} + \overline{-12} = \overline{-5} = \overline{0}$.

Soient a, a', b et b' quatre entiers relatifs tels que $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$. Ceci équivaut à $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$. On sait que la relation de congruence modulo n est **compatible** avec l'addition et avec la multiplication. Donc, $a + b \equiv a' + b'\ [n]$ et $a \times b \equiv a' \times b'\ [n]$ ou encore $\overline{a+b} = \overline{a'+b'}$ et $\overline{a \times b} = \overline{a' \times b'}$. Ceci montre que les relations $(*)$ définissent des lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.

Théorème 27. Pour $n \geqslant 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Commentaire. Dans le théorème précédent, on a évité le cas $n = 1$ où $\mathbb{Z}/n\mathbb{Z}$ est réduit à $\{\overline{0}\}$. Dans ce cas, tous les axiomes de la structure d'anneau sont vérifiés avec le défaut qu'un même élément (à savoir $\overline{0}$) est élément neutre pour l'addition et la multiplication. Le programme officiel veut probablement éviter cette situation.

Démonstration. La démonstration de ce théorème est longue et fastidieuse car $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un tout nouvel objet et n'est pas un sous-anneau d'un anneau déjà connu. On doit donc vérifier un à un tous les axiomes de la structure d'anneau. A titre d'exemple, on n'effectuera explicitement que la vérification de la distributivité de la multiplication sur l'addition.

• $+$ est une loi interne, commutative, associative, possède un élément neutre à savoir $\overline{0}$ et enfin, toute classe $\overline{a}$ admet un opposé à savoir $\overline{-a}$.

• $\times$ est une loi interne, commutative, associative, possède un élément neutre à savoir $\overline{1}$ (car $n \geqslant 2$).

• $\times$ est distributive sur $+$. Démontrons-le explicitement. Soit $(a, b, c) \in \mathbb{Z}^3$.

$$\begin{aligned}\left(\overline{a} + \overline{b}\right) \times \overline{c} &= \overline{a+b} \times \overline{c} = \overline{(a+b) \times c} = \overline{a \times c + b \times c} = \overline{a \times c} + \overline{b \times c} \\ &= \overline{a} \times \overline{c} + \overline{b} \times \overline{c}.\end{aligned}$$

Le théorème qui suit est une remarque (conséquence du théorème 21 entre autre) qui mérite d'être énoncée explicitement :

Théorème 28. Soit $n \geqslant 2$. Pour tout entier relatif a,

$$\begin{aligned}\overline{a} = \overline{0} &\Leftrightarrow a \equiv 0\ [n]\\ &\Leftrightarrow a \text{ est multiple de } n\\ &\Leftrightarrow a\mathbb{Z} \subset n\mathbb{Z}\\ &\Leftrightarrow n \text{ divise } a.\end{aligned}$$

On donne maintenant les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On peut noter que les tables d'addition de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ sont similaires : les différentes lignes s'obtiennent par permutation circulaire de la première ligne. Il n'en est pas de même des tables de multiplication. On peut observer que toute classe non nulle de $\mathbb{Z}/5\mathbb{Z}$ a un symétrique pour $\times$ ($\overline{1} \times \overline{1} = \overline{1}$, $\overline{4} \times \overline{4} = \overline{1}$ et $\overline{2} \times \overline{3} = \overline{1}$) ce qui n'est pas le cas dans $\mathbb{Z}/6\mathbb{Z}$. De plus, dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ et $\overline{3}$ sont deux classes distinctes de $\overline{0}$ dont le produit est égal à $\overline{0}$.

Nous allons étudier de manière générale chacun de ces problèmes dans les paragraphes suivants.

2) Inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Théorème 29. Soit $n \geqslant 2$. Soit $a \in \mathbb{Z}$.

$\overline{a}$ est inversible (pour $\times$) dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ si et seulement si les entiers a et n sont premiers entre eux.

Démonstration. Soit $a \in \mathbb{Z}$.

$$\begin{aligned}\overline{a} \text{ inversible} &\Leftrightarrow \exists b \in \mathbb{Z} /\ \overline{a} \times \overline{b} = \overline{1}\\ &\Leftrightarrow \exists b \in \mathbb{Z},\ \exists k \in \mathbb{Z} /\ ab = 1 + kn\\ &\Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 /\ au + vn = 1\\ &\Leftrightarrow a \text{ et } n \text{ sont premiers entre eux (d'après le théorème de BÉZOUT).}\end{aligned}$$

On rappelle que si $(A, +, \times)$ est un anneau, l'ensemble des inversibles (pour $\times$) de cet anneau se note A^* et on rappelle de plus que $(A^*, \times)$ est un groupe. Le théorème 29 affirme que

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a},\ a \in [\![1, n-1]\!],\ a \wedge n = 1\}.$$

Exercice 1. Montrer que $\overline{39}$ est inversible dans l'anneau $(\mathbb{Z}/224\mathbb{Z},+,\times)$ et déterminer son inverse.

Solution 1.

$224 = 2^5 \times 7$ et $39 = 3 \times 13$ sont premiers entre eux car sans facteur premier commun. Donc, $\overline{39}$ est inversible dans l'anneau $(\mathbb{Z}/224\mathbb{Z},+,\times)$.

Déterminons son inverse. L'algorithme d'EUCLIDE s'écrit

$$\begin{array}{l} 224 = 5 \times 39 + 29 \\ 39 = 1 \times 29 + 10 \\ 29 = 2 \times 10 + 9 \\ 10 = 1 \times 9 + 1 \end{array}$$

et fournit

$$\begin{aligned} 1 &= 10 - 9 \\ &= 10 - (29 - 2 \times 10) = 3 \times 10 - 29 \\ &= 3(39 - 29) - 29 = 3 \times 39 - 4 \times 29 \\ &= 3 \times 39 - 4(224 - 5 \times 39) = 23 \times 39 + (-4) \times 224 \end{aligned}$$

et donc $\overline{23} \times \overline{39} = \overline{1}$. L'inverse de $\overline{39}$ dans l'anneau $(\mathbb{Z}/224\mathbb{Z},+,\times)$ est $\overline{23}$.

Une conséquence du théorème 29 est

Théorème 30. Soit $n \geqslant 2$.

L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps si et seulement si n est un nombre premier.

Démonstration. Si n est premier, tout entier k de $[\![1, n-1]\!]$ est premier à n et donc, pour tout $k \in [\![1, n-1]\!]$, $\overline{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ d'après le théorème 29. Ainsi, toute classe non nulle est un inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ et donc l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps.

Si n n'est pas premier (ce qui impose $n \geqslant 4$), n admet au moins un diviseur k dans $[\![2, n-1]\!]$. Puisque $k \in [\![2, n-1]\!]$, $\overline{k} \neq \overline{0}$ et puisque k est un diviseur de n élément de $[\![2, n-1]\!]$, k n'est pas premier à n et donc $\overline{k}$ n'est pas inversible d'après d'après le théorème 29. Ainsi, il existe une classe non nulle qui n'est pas un inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ et donc l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ n'est pas un corps.

---

3) Intégrité de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$

On rappelle qu'un corps commutatif est en particulier un anneau intègre. Redémontrons-le. Soit $(K,+,\times)$ un corps commutatif. Soit $(a,b) \in \mathbb{K}^2$ tel que $a \times b = 0$ et $a \neq 0$. Alors, a est inversible pour $\times$ puis $a^{-1} \times a \times b = a^{-1} \times 0$ puis $b = 0$. Ceci montre que le corps $(K,+,\times)$ est en particulier un anneau intègre.

Ainsi, quand n est un nombre premier, $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps et en particulier un anneau intègre. Vérifions que quand n est un entier supérieur ou égal à 2 non premier, $(\mathbb{Z}/n\mathbb{Z},+,\times)$ n'est pas intègre.

Soit $n \geqslant 2$ non premier (et donc $n \geqslant 4$). Donc n est composé et il existe $(a,b) \in [\![2, n-1]\!]^2$ tel que $n = ab$. Puisque $(a,b) \in [\![2, n-1]\!]^2$, on a $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$ et puisque $n = ab$, on a $\overline{a} \times \overline{b} = \overline{0}$.

On a montré que

Théorème 31. Soit $n \geqslant 2$.

L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est intègre si et seulement si n est un nombre premier.

Exercice 2.

1) Résoudre dans $\mathbb{Z}/13\mathbb{Z}$ l'équation $x^2 = \overline{1}$.

2) Résoudre dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $x^2 = \overline{1}$.

Solution 2. On note $\mathscr{S}$ l'ensemble des solutions de l'équation proposée.

1) 13 est premier. Donc, l'anneau $(\mathbb{Z}/13\mathbb{Z},+,\times)$ est intègre. Par suite, pour $x \in \mathbb{Z}/13\mathbb{Z}$,

$$x^2 = \overline{1} \Leftrightarrow \left(x - \overline{1}\right)\left(x + \overline{1}\right) = \overline{0} \Leftrightarrow x - \overline{1} = \overline{0} \text{ ou } x + \overline{1} = \overline{0}$$
$$\Leftrightarrow x = \overline{1} \text{ ou } x = \overline{12}.$$

$\mathscr{S} = \left\{\overline{1}, \overline{12}\right\}$.

2) 12 n'est pas premier. Donc, l'anneau $(\mathbb{Z}/12\mathbb{Z}, +, \times)$ n'est pas intègre et le raisonnement précédent ne tient plus. L'équation proposée admet bien sûr $\overline{1}$ et $\overline{-1} = \overline{11}$ pour solutions mais il y en a peut -être d'autres :

$\overline{0}^2 = \overline{0} \neq \overline{1}$
$\overline{2}^2 = \overline{4} \neq \overline{1}$
$\overline{3}^2 = \overline{9} \neq \overline{1}$
$\overline{4}^2 = \overline{16} = \overline{4} \neq \overline{1}$
$\overline{5}^2 = \overline{25} = \overline{1}$
$\overline{6}^2 = \overline{36} = \overline{0} \neq \overline{1}$
$\overline{7}^2 = \overline{-5}^2 = \overline{1}$
$\overline{8}^2 = \overline{-4}^2 \neq \overline{1}$
$\overline{9}^2 = \overline{-3}^2 \neq \overline{1}$
$\overline{10}^2 = \overline{-2}^2 \neq \overline{1}$

$\mathscr{S} = \left\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\right\}$. Ainsi, dans l'anneau non intègre $(\mathbb{Z}/12\mathbb{Z}, +, \times)$ admet strictement plus que deux solutions.

Exercice 3 (théorème de Wilson). Soit p un entier supérieur ou égal à 2. Montrer que

$$p \text{ est premier} \Leftrightarrow (p-1)! \equiv -1 \ [p].$$

Solution 3. $p = 2$ est premier et $(2-1)! \equiv -1 \ [2]$. On suppose dorénavant $p \geqslant 3$.

• Supposons que $(p-1)! \equiv -1 \ [p]$ $(*)$. Soit $k \in [\![1, p-1]\!]$. $(*)$ fournit l'existence d'un entier relatif q tel que $(p-1)! = -1 + kp$ ou encore

$$qp + \left(-\prod_{i \neq k} i\right) k = 1.$$

Le théorème de Bézout montre que p et k sont premiers entre eux. Ainsi, le nombre p est premier avec tous les entiers de $[\![1, p-1]\!]$ et donc p est premier.

• Supposons p premier. Donc, l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps et en particulier est un anneau intègre. $\overline{(p-1)!}$ est le produit de toutes les classes non nulles de ce corps ou encore le produit de toutes les classe inversibles.

Déterminons les classes non nulles qui sont leur propre inverse. Ce sont les solutions de l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Puisque l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est intègre, il y en a exactement 2 à savoir $\overline{1}$ et $\overline{-1}$.

Si $p = 3$, $(p-1)! = 2 \equiv -1 \ [3]$. Sinon, $p \geqslant 5$. Dans le produit $\overline{(p-1)!} = \prod_{k=1}^{p-1} \overline{k}$, on isole $\overline{1}$ et $\overline{p-1} = \overline{-1}$ qui sont les seules classes égales à leur inverse. Dans le produit restant, à savoir $\prod_{k=2}^{p-2} \overline{k}$, on regroupe les classes par paires de produit égal à $\overline{1}$ et on obtient

$$\overline{(p-1)!} = \overline{1} \times \overline{-1} \times \prod_{k=2}^{p-2} \overline{k} = \overline{-1} \times 1^{(p-3)/2} = \overline{-1}.$$

Ceci montre que $(p-1)! \equiv -1 \ [p]$.

---

4) Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

a) Générateurs du groupe $(\mathbb{Z}/n\mathbb{Z},+)$

Théorème 32. Soit $n \geqslant 2$. Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique.

Soit $a \in \mathbb{Z}$. $\overline{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ si et seulement si les entiers a et n sont premiers entre eux.

Démonstration. On rappelle que pour $(k,a) \in \mathbb{Z}^2$, le notation $k\,\overline{a}$ signifie $\begin{cases} \underbrace{\overline{a}+\ldots+\overline{a}}_{k \text{ termes}} \text{ si } k>0 \\ \overline{0} \text{ si } k=0 \\ \underbrace{-\overline{a}-\ldots-\overline{a}}_{-k \text{ termes}} \text{ si } k<0 \end{cases}$ et donc $k\,\overline{a}=\overline{ka}$.

• $\text{gr}(\overline{1}) = \left\{k\,\overline{1},\ k\in\mathbb{Z}\right\} = \left\{\overline{k},\ k\in\mathbb{Z}\right\} = \mathbb{Z}/n\mathbb{Z}$. Donc, le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique (et un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est $\overline{1}$).

• Soit $a \in \mathbb{Z}$. Dans le groupe $(\mathbb{Z}/n\mathbb{Z},+)$,

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} = \text{gr}(\overline{a}) &\Leftrightarrow \text{gr}(\overline{a}) = \text{gr}(\overline{1}) \\ &\Leftrightarrow \overline{1}\in\text{gr}(\overline{a}) \text{ et } \overline{a}\in\text{gr}(\overline{1}) \Leftrightarrow \overline{1}\in\text{gr}(\overline{a}) \\ &\Leftrightarrow \exists k\in\mathbb{Z}/\ k\,\overline{a}=\overline{1} \Leftrightarrow \exists k\in\mathbb{Z}/\ \overline{k\times a}=\overline{1} \Leftrightarrow \exists k\in\mathbb{Z}/\ \overline{k}\times\overline{a}=\overline{1} \\ &\Leftrightarrow \overline{a}\in(\mathbb{Z}/n\mathbb{Z})^* \\ &\Leftrightarrow a\wedge n = 1 \text{ (d'après le théorème 29).}\end{aligned}$$

Par exemple, dans $(\mathbb{Z}/6\mathbb{Z},+)$, $\text{gr}(\overline{0})=\{0\}$, $\text{gr}(\overline{1})=\text{gr}(\overline{5})=\mathbb{Z}/6\mathbb{Z}$, $\text{gr}(\overline{2})=\text{gr}(\overline{4})=\{\overline{0},\overline{2},\overline{4}\}$ et $\text{gr}(\overline{4})=\{\overline{0},\overline{3}\}$. Les générateurs du groupe $(\mathbb{Z}/6\mathbb{Z},+)$ sont $\overline{1}$ et $\overline{5}=\overline{-1}$.

b) Application aux groupes monogènes

Théorème 33. Soit $(G,\times)$ un groupe monogène (noté multiplicativement).

Si G est d'ordre infini, le groupe $(G,\times)$ est isomorphe au groupe $(\mathbb{Z},+)$.
Si G est d'ordre fini $n\in\mathbb{N}^*$, le groupe $(G,\times)$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z},+)$.

Démonstration. Soit $(G,\times)$ un groupe monogène d'élément neutre 1_G. Il existe $a\in G$ tel que $G=\left\{a^k,\ k\in\mathbb{Z}\right\}$.

1er cas. On suppose que G est d'ordre infini. D'après le théorème 5, a est d'ordre infini. Soit $\begin{array}{rccc} f: & \mathbb{Z} & \to & G \\ & n & \mapsto & a^n \end{array}$.

• f est bien une application de $\mathbb{Z}$ dans G, surjective par définition de a.
• Pour $(n,m)\in\mathbb{Z}^2$, $f(n+m)=a^{n+m}=a^n\times a^m=f(n)\times f(m)$. Donc, f est un morphisme de groupes.
• Pour $n\in\mathbb{Z}$, $f(n)=1_G\Leftrightarrow a^n=1_G\Leftrightarrow n=0$ (car a est d'ordre infini). Donc, $\text{Ker}(f)=\{0\}$ puis f est injectif.

Finalement, f est un isomorphisme de groupes. On a montré qu'un groupe monogène non cyclique est isomorphe au groupe $(\mathbb{Z},+)$.

2ème cas. On suppose que G est d'ordre fini $n\in\mathbb{N}^*$ (le groupe $(G,\times)$ est donc cyclique). Il existe dans G un élément a tel que $\text{gr}(a)=G$. a est d'ordre n d'après le théorème 5 et $G=\left\{a^k,\ 0\leqslant k\leqslant n-1\right\}$. Soit $\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & G \\ & \overline{k} & \mapsto & a^k \end{array}$.

• Vérifions que f est bien une application de $\mathbb{Z}/n\mathbb{Z}$ dans G. Pour cale, il faut vérifier que si k et k' sont deux représentants d'une même classe dans $\mathbb{Z}/n\mathbb{Z}$, alors $a^k=a^{k'}$.
Soit $(k,k')\in\mathbb{Z}^2$ tel que $\overline{k}=\overline{k'}$. Alors, $k-k'\in n\mathbb{Z}$ puis $a^{k-k'}=1_G$ d'après le théorème 6 et donc $a^k=a^{k'}$.
Ceci montre que f est une application de $\mathbb{Z}/n\mathbb{Z}$ dans G.
• f est surjectif par définition de a.
• Pour $(k,k')\in\mathbb{Z}^2$, $f\left(\overline{k}+\overline{k'}\right)=f\left(\overline{k+k'}\right)=a^{k+k'}=a^k\times a^{k'}=f\left(\overline{k}\right)\times f\left(\overline{k'}\right)$. Donc, f est un morphisme de groupes.
• Soit $k\in\mathbb{Z}$.

$$\begin{aligned} f(\overline{k})=1_G &\Leftrightarrow a^k=1_G \\ &\Leftrightarrow k\in n\mathbb{Z} \text{ (d'après le théorème 6)} \\ &\Leftrightarrow \overline{k}=\overline{0}.\end{aligned}$$

Donc, $\text{Ker}(f)=\{\overline{0}\}$ puis f est injectif.

Finalement, f est un isomorphisme de groupes. On a montré qu'un groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ainsi, le groupe $(U_n, \times)$, qui est cyclique d'ordre n, est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. L'isomorphisme de la démonstration ci-dessus est explicitement $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$. Par exemple, un isomorphisme du groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ sur le groupe $(U_4, \times)$ est $\overline{0} \mapsto 1$, $\overline{1} \mapsto i$, $\overline{2} \mapsto -1$ et $\overline{3} \mapsto -i$.
Par un isomorphisme, « tout est transporté ». Par exemple, $\overline{k}$ est d'ordre p dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $e^{\frac{2ik\pi}{n}}$ est d'ordre p dans le groupe $(U_n, \times)$ et en particulier, $\overline{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $e^{\frac{2ik\pi}{n}}$ est un générateur du groupe $(U_n, \times)$ ce qui équivaut au fait que k et n sont premiers entre eux d'après le théorème 32.
Toute racine n-ème de l'unité qui est de plus un générateur du groupe $(U_n, \times)$ est dite **racine primitive n-ème de l'unité**. Les racine primitive n-ème de l'unité sont les $e^{\frac{2ik\pi}{n}}$ où $0 \leqslant k \leqslant n-1$ et de plus $\text{PGCD}(k, n) = 1$. Les racine primitive n-ème de l'unité sont racines n-èmes de l'unité et « pas moins ».
Les racines primitives quatrièmes de l'unité sont i et $-i$. 1 et -1 sont des racines quatrièmes de l'unité qui sont aussi respectivement racine unième et racine deuxième de l'unité.

5) Le théorème chinois

Théorème 34. Soient m et n deux entiers naturels non nuls et premiers entre eux. On note respectivement $\overline{a}$, $\widehat{a}$ et $\overset{\bullet}{a}$ la classe d'un entier relatif a dans $\mathbb{Z}/nm\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ respectivement.

L'application $\begin{array}{rccc} f : & (\mathbb{Z}/nm\mathbb{Z}, +, \times) & \to & (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times) \\ & \overline{a} & \mapsto & \left(\widehat{a}, \overset{\bullet}{a}\right) \end{array}$ est un isomorphisme d'anneaux.

Démonstration. • Vérifions que f est bien une application.

Soit $(a, a') \in \mathbb{Z}^2$ tel que $\overline{a} = \overline{a'}$. Alors, $a \equiv a' \ [nm]$. En particulier, $a \equiv a' \ [n]$ et $a \equiv a' \ [m]$ ou encore $\widehat{a} = \widehat{a'}$ et $\overset{\bullet}{a} = \overset{\bullet}{a'}$. Ceci montre que f est bien une application de $\mathbb{Z}/nm\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

• Soit $(a, a') \in \mathbb{Z}^2$.

$$\begin{aligned} f\left(\overline{a} + \overline{a'}\right) = f\left(\overline{a+a'}\right) &= \left(\widehat{a+a'}, \overset{\bullet}{(a+a')}\right) = \left(\widehat{a} + \widehat{a'}, \overset{\bullet}{a} + \overset{\bullet}{a'}\right) \\ &= \left(\widehat{a}, \overset{\bullet}{a}\right) + \left(\widehat{a'}, \overset{\bullet}{a'}\right) = f\left(\overline{a}\right) + f\left(\overline{a'}\right) \end{aligned}$$

et

$$\begin{aligned} f\left(\overline{a} \times \overline{a'}\right) = f\left(\overline{a \times a'}\right) &= \left(\widehat{a \times a'}, \overset{\bullet}{(a \times a')}\right) = \left(\widehat{a} \times \widehat{a'}, \overset{\bullet}{a} \times \overset{\bullet}{a'}\right) \\ &= \left(\widehat{a}, \overset{\bullet}{a}\right) \times \left(\widehat{a'}, \overset{\bullet}{a'}\right) = f\left(\overline{a}\right) \times f\left(\overline{a'}\right) \end{aligned}$$

Donc, f est un morphisme pour les deux lois.

• Soit $a \in \mathbb{Z}$.

$$\begin{aligned} \overline{a} \in \text{Ker}(f) &\Rightarrow \left(\widehat{a}, \overset{\bullet}{a}\right) = \left(\widehat{0}, \overset{\bullet}{0}\right) \Rightarrow a \equiv 0 \ [n] \text{ et } a \equiv 0 \ [n] \\ &\Rightarrow a \equiv 0 \ [nm] \text{ (car } n \text{ et } m \text{ sont premiers entre eux)} \\ &\Rightarrow \overline{a} = \overline{0}. \end{aligned}$$

Donc, $\text{Ker}(f) = \{\overline{0}\}$ puis f est injectif.

• f est une application injective de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\text{card}(\mathbb{Z}/nm\mathbb{Z}) = nm = \text{card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) < +\infty$. On sait alors que f est bijective.

• $f(\overline{1}) = \left(\widehat{1}, \overset{\bullet}{1}\right)$ et $\left(\widehat{1}, \overset{\bullet}{1}\right)$ est bien l'élément neutre pour $\times$ de l'anneau $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times)$.

Finalement, f est un isomorphisme d'anneaux.

Une première application du théorème 34 est le théorème chinois :

Théorème 35. Soient n_1 et n_2 deux entiers naturels non nuls et premiers entre eux. Soient a_1 et a_2 deux entiers relatifs.
Soit (S) le système de congruences $\begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \end{cases}$ d'inconnue $x \in \mathbb{Z}$.

1) (S) admet au moins une solution x_0 dans $\mathbb{Z}$.
2) Les solutions de (S) dans $\mathbb{Z}$ sont les nombres de la forme $x_0 + kn_1n_2$, $k \in \mathbb{Z}$.

Démonstration. Soit $x \in \mathbb{Z}$. Avec les notations du théorème 34,

$$\begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \end{cases} \Leftrightarrow \begin{cases} \widehat{x} = \widehat{a_1} \\ \overset{\bullet}{x} = \overset{\bullet}{a_2} \end{cases}$$
$$\Leftrightarrow f(\widehat{x}) = \left(\widehat{a_1}, \overset{\bullet}{a_2}\right) \Leftrightarrow \widehat{x} = f^{-1}\left(\left(\widehat{a_1}, \overset{\bullet}{a_2}\right)\right).$$

Enfin, en notant x_0 un représentant de $f^{-1}\left(\left(\widehat{a_1}, \overset{\bullet}{a_2}\right)\right)$ dans $\mathbb{Z}$,

$$\widehat{x} = f^{-1}\left(\left(\widehat{a_1}, \overset{\bullet}{a_2}\right)\right) \Leftrightarrow \widehat{x} = \widehat{x_0} \Leftrightarrow \exists k \in \mathbb{Z},\ x = x_0 + kn_1n_2.$$

*6) L'indicatrice d'*Euler

Définition 14. Pour $n \geqslant 2$, on note $\varphi(n)$ le nombre d'entiers éléments de $[\![1, n]\!]$ qui sont premiers avec l'entier n.

La fonction φ s'appelle l'**indicatrice d'Euler**.

A partir des théorèmes 29 et 32, pour $n \geqslant 2$, on a

$$\begin{aligned} \varphi(n) &= \text{card}\{k \in [\![1, n]\!] / \ \text{PGCD}(k, n) = 1\} \\ &= \text{card}\left\{k \in [\![1, n]\!] / \ \overline{k} \text{ inversible pour } \times \text{ dans } \mathbb{Z}/n\mathbb{Z}\right\} = \text{card}\left((\mathbb{Z}/n\mathbb{Z})^*\right) \\ &= \text{card}\left\{k \in [\![1, n]\!] / \ \overline{k} \text{ générateur de } (\mathbb{Z}/n\mathbb{Z}, +)\right\}. \end{aligned}$$

Ainsi, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, ...

Théorème 36. Soient a et b deux entiers naturels supérieurs ou égaux à 2 et premiers entre eux. Alors,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Démonstration. Soient a et b deux entiers naturels non nuls et premiers entre eux. D'après le théorème 34, les anneaux $(\mathbb{Z}/ab\mathbb{Z}, +, \times)$ et $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +, \times)$ sont isomorphes.
Par l'isomorphisme f de la démonstration du théorème 34, un élément de $\mathbb{Z}/ab\mathbb{Z}$ est un inversible de l'anneau $(\mathbb{Z}/ab\mathbb{Z}, +, \times)$ si et seulement si son image par f est un inversible de l'anneau $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +, \times)$. f induit donc une bijection de $(\mathbb{Z}/ab\mathbb{Z})^*$ sur $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})^*$ et en particulier,

$$\varphi(ab) = \text{card}\left((\mathbb{Z}/ab\mathbb{Z})^*\right) = \text{card}\left((\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})^*\right).$$

Mais les éléments inversibles de l'anneau $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +, \times)$ sont les couples dont la première composante est une classe inversible de l'anneau $(\mathbb{Z}/a\mathbb{Z}, +, \times)$ et la deuxième composante est une classe inversible de l'anneau $(\mathbb{Z}/b\mathbb{Z}, +, \times)$. Donc, $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})^* = (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ puis

$$\varphi(ab) = \text{card}\left((\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*\right) = \varphi(a)\varphi(b).$$

On se propose maintenant de déterminer $\varphi(n)$ à partir de la décomposition primaire de l'entier $n \geqslant 2$.

Théorème 37.

1) Pour tout nombre premier p, $\varphi(p) = p - 1$.
2) Pour tout nombre premier p et tout entier naturel non nul α, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3) Pour tout nombre entier $n \geqslant 2$, $\varphi(n) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$.

Démonstration.

1) Soit p un nombre premier. $\{k \in [\![1, p]\!] / \text{ PGCD}(k, n) = 1\} = [\![1, p-1]\!]$ puis $\varphi(p) = p - 1$.

2) Soient p un nombre premier et α un entier naturel non nul. Pour $k \in [\![1, p^\alpha]\!]$, $\text{PGCD}(k, p^\alpha) = 1$ si et seulement si k n'est pas un multiple de p. Donc,

$$\varphi(p^\alpha) = \text{card}\,[\![1, p^\alpha]\!] - \text{card}\{k \in [\![1, p^\alpha]\!],\ k \text{ multiple de } p\} = p^\alpha - \text{card}\{k \in [\![1, p^\alpha]\!],\ k \text{ multiple de } p\}.$$

Or, k est multiple de p si et seulement si il existe $q \in \mathbb{Z}$ tel que $k = qp$. Donc,

$$\begin{aligned}\text{card}\{k \in [\![1, p^\alpha]\!],\ k \text{ multiple de } p\} &= \text{card}\{q \in \mathbb{Z},\ 1 \leqslant qp \leqslant p^\alpha\} = \text{card}\left\{q \in \mathbb{Z},\ \frac{1}{p} \leqslant q \leqslant p^{\alpha-1}\right\} \\ &= \text{card}\left\{q \in \mathbb{Z},\ 1 \leqslant q \leqslant p^{\alpha-1}\right\} = p^{\alpha-1}.\end{aligned}$$

Finalement, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

3) Soit $n \geqslant 2$. Notons $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la décomposition primaire de l'entier n (ce qui signifie que les p_i sont des nombres premiers deux à deux distincts et que les α_i sont des entiers naturels non nuls). $p_k^{\alpha_k}$ est premier avec $\prod_{i<k} p_i^{\alpha_i}$ et donc, d'après le théorème précédent et le 2),

$$\varphi(n) = \varphi\left(\prod_{i<k} p_i^{\alpha_i}\right) \varphi(p_k^{\alpha_k}) = \varphi\left(\prod_{i<k} p_i^{\alpha_i}\right) \times \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right),$$

puis, par récurrence,

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

ce qui démontre le résultat.

Théorème 38 (théorème d'Euler). Soient $n \geqslant 2$ et $a \in \mathbb{Z}$ tels que $\text{PGCD}(a, n) = 1$.

$$a^{\varphi(n)} \equiv 1\ [n].$$

Démonstration. Soit $n \geqslant 2$, $\varphi(n) = \text{card}\left((\mathbb{Z}/n\mathbb{Z})^*\right)$ et de plus, on sait que $\left((\mathbb{Z}/n\mathbb{Z})^*, \times\right)$ est un groupe. D'après le théorème 8, pour tout élément x de $\left((\mathbb{Z}/n\mathbb{Z})^*, \times\right)$, $x^{\varphi(n)} = \overline{1}$ ou encore, pour tout entier relatif a premier à n, $\overline{a}^{\varphi(n)} = \overline{1}$ ou enfin, pour tout entier relatif a premier à n, $a^{\varphi(n)} \equiv 1\ [n]$.

Remarque. Si n est un nombre premier p, le théorème d'Euler s'écrit :

Soient p un nombre premier et a un entier relatif non divisible par p. Alors,

$$a^{p-1} \equiv 1\ [p].$$

On retrouve ainsi le petit théorème de Fermat.

Exercice 4. Déterminer le reste de la division euclidienne de 4^{291} par 35.

Solution 4. $35 = 5 \times 7$ puis $\varphi(35) = 35\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 4 \times 6 = 24$. Puisque 4 est premier à 35, le théorème d'Euler fournit

$$4^{24} \equiv 1 \ [35]$$

puis

$$4^{291} = \left(4^{24}\right)^{12} \times 4^3 \equiv 4^3 \ [35].$$

Ainsi, $4^{291} \equiv 64$ [35] ou encore $4^{291} \equiv 29$ [35] avec $0 \leqslant 29 < 35$. Le reste de la division euclidienne de 4^{291} par 35 est 29.

Exercice 5. Déterminer le nombre de générateurs du groupe $(U_{12}, \times)$.

Solution 5. Les générateurs du groupe $(U_{12}, \times)$ sont les $e^{\frac{2ik\pi}{12}}$ où $1 \leqslant k \leqslant 12$ et $\text{PGCD}(k, 12) = 1$. Il y en a

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4.$$

Il y a 4 racines primitives 12-èmes de 1 dans $\mathbb{C}$.

Exercice 6. Montrer que pour tout $n \geqslant 1$, $n = \sum_{d|n,\ d>0} \varphi(d)$ (en posant $\varphi(1) = 1$).

Solution 6. Soit $n \geqslant 1$. Pour $d \in [\![1, n]\!]$ diviseur de n donné, notons F_d l'ensemble des entiers $k \in [\![1, n]\!]$ tels que $\text{PGCD}(k, n) = \dfrac{n}{d}$. $(F_d)_{d|n,\ d>0}$ est une partition de $[\![1, n]\!]$ et donc

$$n = \sum_{d|n,\ d>0} \text{card}\,(F_d) \ (*).$$

Soit $d \in [\![1, n]\!]$ un diviseur strictement positif de n. Posons $q = \dfrac{n}{d}$ de sorte que $n = qd$. Soit $k \in [\![1, n]\!]$.

Si $\text{PGCD}(k, n) = q$, alors on peut écrire $k = k'q$ et $n = dq$ où k' est un élément de $[\![1, k]\!] \subset [\![1, n]\!]$ tel que $k' \wedge d = 1$. De plus, $k' = \dfrac{k}{q} \leqslant \dfrac{n}{q} = d$. Donc, si $\text{PGCD}(k, n) = q$, il existe $k' \in [\![1, d]\!]$ tel que $k = k'q$ et $k' \wedge d = 1$
Réciproquement, si il existe $k' \in [\![1, d]\!]$ tel que $k = k'q$ et $k' \wedge d = 1$, alors $1 \leqslant k \leqslant qd = n$ et

$$\text{PGCD}(k, n) = \text{PGCD}(k'q, dq) = q\text{PGCD}(k', d) = q.$$

Donc, $F_d = \{k'q,\ k' \in [\![1, d]\!],\ k' \wedge d = 1\}$ puis

$$\text{card}\,(F_d) = \text{card}\,\{k'q,\ k' \in [\![1, d]\!],\ k' \wedge d = 1\} = \text{card}\,\{k',\ k' \in [\![1, d]\!],\ k' \wedge d = 1\} = \varphi(d).$$

$(*)$ fournit alors

$$n = \sum_{d|n,\ d>0} \varphi(d).$$
