Chapitre 1. Compléments d'algèbre

Plan du chapitre

1 Compléments sur les groupes

1.1 Intersection de sous-groupes

On a vu en math sup que, si $(G,*)$ est un groupe, une intersection de deux sous-groupes de G est un sous-groupe de G. Plus généralement :

Théorème 1. Soit $(G,*)$ un groupe. Soient I un ensemble non vide d'indices puis $(H_i)_{i\in I}$ une famille de sous-groupes de $(G,*)$ indexée par I.

Alors, $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G,*)$.

Démonstration. Dans cette démonstration, on note e l'élément neutre du groupe $(G,*)$ et x' le symétrique d'un élément x de G pour $*$.

Soient $(H_i)_{i\in I}$ une famille de sous-groupe du groupe $(G,*)$, indexée par I un ensemble non vide d'indices puis $H=\bigcap_{i\in I} H_i$.

- On sait que pour tout $i\in I$, $e\in H_i$ et donc $e\in H$.
- Soit $(x,y)\in H^2$. Pour tout $i\in I$, $x*y'\in H_i$ et donc $x*y'\in H$.

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

❑

1.2 Sous-groupe engendré par une partie

1.2.1 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 du groupe $(G,*)$ contenant la partie A. H est un sous-groupe du groupe $(G,*)$ en tant qu'intersection de sous-groupe du groupe $(G,*)$ et H contient A en tant qu'intersection de parties de G contenant A. Ainsi, H est un sous-groupe du groupe $(G,*)$ contenant A.
D'autre part, par construction, H est contenu dans tout sous-groupe du groupe $(G,*)$ contenant A. Finalement, H est le plus petit (au sens de l'inclusion) sous-groupe du groupe $(G,*)$ contenant A. Ceci démontre l'existence d'un tel sous-groupe.

Enfin, si H et H' sont deux plus petits sous-groupes du groupe $(G,*)$ contenant A, alors $H\subset H'$ et $H'\subset H$ puis $H'=H$. Ceci démontre l'unicité d'un plus petit sous-groupe du groupe $(G,*)$ 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 partis de G qui était un sous-groupe du groupe $(G,*)$ 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 (en notant e l'élément neutre du groupe $(G,*)$) :

Théorème 2. 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 3. 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, $gr(A)$ 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.

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

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

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

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

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

Démonstration. (du théorème 3) 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 $H = gr(A)$.

❑

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

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

Exemple 3. On a vu en maths sup que toute permutation de $[\![1,n]\!]$ peut s'écrire comme une composée de transpositions. Donc, le groupe symétrique $(\mathcal{S}_n,\circ)$ est engendré par les transpositions.

1.2.2 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 $G = gr(\{a\})$.

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

Un groupe monogène est donc un groupe engendré par l'un de ces éléments. Un élément a de G tel que $G = gr(a)$ 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 $a \in G$.

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

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

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

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

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

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 de cardinal n (on dit aussi d'ordre n).

Théorème 4. 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 $(\mathcal{S}_3,\circ)$, le groupe symétrique de $[\![1,3]\!]$. On sait que $\mathcal{S}_3=\{Id,\tau_{1,2},\tau_{1,3},\tau_{2,3},c_1,c_2\}$ 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 $(\mathcal{S}_3,\circ)$ n'est donc pas commutatif. On en déduit en particulier que ce groupe n'est pas monogène. De fait, $\text{gr}(Id)=\{Id\}\neq\mathcal{S}_3$, $\text{gr}\,(\tau_{i,j})=\{Id,\tau_{i,j}\}\neq\mathcal{S}_3$ et $\text{gr}\,(c_i)=\{Id,c_1,c_2\}\neq\mathcal{S}_3$. On peut cependant montrer que $\mathcal{S}_3=\text{gr}\,(\tau_{1,2},c_1)$. ❑

Sinon, on a immédiatement

Théorème 5. Soit $(G,*)$ un groupe. Soit H un sous-groupe du groupe $(G,*)$.

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

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

Théorème 6. Les sous-groupes du groupe $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, $n\in\mathbb{Z}$.

Démonstration. • Soit $n\in\mathbb{Z}$. $n\mathbb{Z}=\text{gr}(n)$ 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 $\text{gr}(n)\subset H$ 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 6.

Théorème 7.

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 m. On sait que ceci impose $m=\pm n$.

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

Enfin, 2) est une conséquence immédiate de 1) et 3) est une conséquence de 2) et du théorème 6.

❑

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

1.4.1 Définition et propriétés du groupe $(\mathbb{Z}/n\mathbb{Z},+)$

Soit $n\in\mathbb{N}^*$. On sait que la relation de congruence modulo n, définie sur $\mathbb{Z}^2$ par :

$$\forall (a,b)\in\mathbb{Z}^2,\ (a\equiv b\ [n]\Leftrightarrow b-a\in n\mathbb{Z}\Leftrightarrow \exists q\in\mathbb{Z}/\ b=a+nq),$$

et une relation d'équivalence à n classes deux à deux distinctes. Redémontrons-le. Soit $n\in\mathbb{N}$.

- Soit $a\in\mathbb{Z}$. $a=a+0\times a$ avec $0\in\mathbb{Z}$ et donc $a\equiv a\ [n]$. La congruence modulo n est réflexive.
- Soit $(a,b)\in\mathbb{Z}^2$ tel $a\equiv b\ [n]$. Il existe $q\in\mathbb{Z}$ tel que $b=a+nq$. Mais alors $a=b-nq$ ou encore $a=b+nq'$ avec $q'=-q\in\mathbb{Z}$ et donc $b\equiv a\ [n]$. La congruence modulo n est symétrique.
- Soit $(a,b,c)\in\mathbb{Z}^3$ tel $a\equiv b\ [n]$ et $b\equiv c\ [n]$. Il existe $(q,q')\in\mathbb{Z}^2$ tel que $b=a+nq$ et $c=b+nq'$.
  Mais alors $c=b+nq'=a+nq+nq'=a+n(q+q')=a+nq''$ avec $q''=q+q'\in\mathbb{Z}$ et donc $a\equiv c\ [n]$.
  La congruence modulo n est transitive.

Ceci montre que la relation d'équivalence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Vérifions que cette relation a exactement n classes deux à deux distinctes. On note $\widehat{a}$ la classe d'un élément a de $\mathbb{Z}$ (on rappelle que $\widehat{a}$ est constituée des éléments b de $\mathbb{Z}$ qui sont congrus à a modulo n).

Soit $a\in\mathbb{Z}$. La division euclidienne de a par n (on rappelle que $n\neq 0$) s'écrit $a=nq+r$ où $q\in\mathbb{Z}$ et $r\in[\![0,n-1]\!]$. Mais alors, $a\equiv r\ [n]$ puis $\widehat{a}=\widehat{r}$ où cette fois-ci $0\leqslant r\leqslant n-1$. Ceci montre que la congruence modulo n possède au plus n classes d'équivalence, à savoir $\widehat{0}$, $\widehat{1}$, ..., $\widehat{n-1}$. Vérifions maintenant que ces classes sont deux à deux distinctes.

Soit $(a,b)\in[\![0,n-1]\!]^2$ tel que $\widehat{a}=\widehat{b}$. Puisque $\widehat{a}=\widehat{b}$, on a $a\equiv b\ [n]$. Mais alors, $b-a\in n\mathbb{Z}\cap[\![-(n-1),(n-1)]\!]=\{0\}$ et donc $a=b$. Par contraposition, pour tout $(a,b)\in[\![0,n-1]\!]^2$, $(a\neq b\Rightarrow\widehat{a}\neq\widehat{b})$.
Ceci montre que l'ensemble des classes d'équivalence modulo n est un ensemble constitué d'exactement n éléments. On peut énoncer :

DÉFINITION 4. Soit $n\in\mathbb{N}^*$. L'ensemble des classes d'équivalence de la relation de congruence modulo n se note $\mathbb{Z}/n\mathbb{Z}$. Il est constitué d'exactement n éléments à savoir $\widehat{0}$, $\widehat{1}$, ..., $\widehat{n-1}$.

Ainsi, $\mathbb{Z}/5\mathbb{Z}=\left\{\widehat{0},\widehat{1},\widehat{2},\widehat{3},\widehat{4}\right\}$ où, pour tout $a\in[\![0,4]\!]$, $\widehat{a}=\{a+5q,\ q\in\mathbb{Z}\}$ et donc par exemple,
$\widehat{3}=\{\ldots,-12,-7,-2,3,8,13,\ldots\}$.
On rappelle encore que chaque élément d'une classe peut être choisi comme représentant de cette classe et donc par exemple, dans $\mathbb{Z}/5\mathbb{Z}$, $\widehat{3}=\widehat{8}=\widehat{-2}$ et aussi $\mathbb{Z}/5\mathbb{Z}=\left\{\widehat{-2},\widehat{-1},\widehat{0},\widehat{1},\widehat{2}\right\}$.

On revient au cas général $\mathbb{Z}/n\mathbb{Z}$, $n\in\mathbb{N}^*$. On définit dans $\mathbb{Z}/n\mathbb{Z}$ une addition par :

$$\forall (a,b)\in(\mathbb{Z}/n\mathbb{Z})^2,\ \widehat{a+b}=\widehat{a}+\widehat{b}\quad(*).$$

Théorème 8. Pour tout $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe commutatif, fini de cardinal n.

DÉMONSTRATION. Soit $n\in\mathbb{N}^*$.

• Vérifions d'abord que l'on a bien défini une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$. Il s'agit de vérifier que la définition adoptée de $\widehat{a}+\widehat{b}$ ne dépend pas du choix des représentants respectifs a et b de ces classes.
Soit donc $(a,a',b,b')\in\mathbb{Z}^4$ tel que $\widehat{a}=\widehat{a'}$ et $\widehat{b}=\widehat{b'}$. Montrons alors que $\widehat{a+b}=\widehat{a'+b'}$. Puisque $\widehat{a}=\widehat{a'}$, on a $a\equiv a'\ [n]$ et de même $b\equiv b'\ [n]$. Mais alors, par compatibilité de la congruence avec l'addition, $a+b\equiv a'+b'\ [n]$ puis $\widehat{a+b}=\widehat{a'+b'}$.

Ainsi, $(*)$ définit bien une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.

• Montrons maintenant que $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe commutatif. Il ne s'agit pas de vérifier que $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe d'un groupe déjà connu. $(\mathbb{Z}/n\mathbb{Z},+)$ est un nouveau groupe de référence.

- Soit $(a,b)\in\mathbb{Z}^2$. $\widehat{a}+\widehat{b}=\widehat{a+b}=\widehat{b+a}=\widehat{b}+\widehat{a}$. Donc, $+$ est commutative.
- Soit $(a,b,c)\in\mathbb{Z}^3$. $\left(\widehat{a}+\widehat{b}\right)+\widehat{c}=\widehat{a+b}+\widehat{c}=\widehat{(a+b)+c}=\widehat{a+(b+c)}=\widehat{a}+\widehat{b+c}=\widehat{a}+\left(\widehat{b}+\widehat{c}\right)$. Donc, $+$ est associative.
  On peut donc écrire dorénavant $\widehat{a}+\widehat{b}+\widehat{c}$.
- Soit $a\in\mathbb{Z}$ $\widehat{a}+\widehat{0}=\widehat{a+0}=\widehat{a}$. Donc, $+$ possède un élément neutre, à savoir $\widehat{0}$.
- Soit $a\in\mathbb{Z}$ $\widehat{a}+\widehat{-a}=\widehat{a+(-a)}=\widehat{0}$. Donc, tout élément $\widehat{a}$ de $\mathbb{Z}/n\mathbb{Z}$ admet un opposé pour $+$, à savoir $\widehat{-a}$ (dit autrement $\widehat{-a}=-\widehat{a}$).

On a montré que, pour tout $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe commutatif.

❑

⇛ **Commentaire** . *Nous n'avons pas traité le cas* $n = 0$. *La congruence modulo* 0 *est l'égalité :* $\forall (a,b) \in \mathbb{Z}^2$, $(a \equiv b\ [0] \Leftrightarrow a = b)$. *Dans ce cas, chaque classe d'équivalence est un singleton :* $\forall a \in \mathbb{Z}$, $\widehat{a} = \{a\}$. *On peut alors identifier* $\mathbb{Z}/0\mathbb{Z}$ *et* $\mathbb{Z}$.

Le théorème qui suit précise une règle de calcul dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ (dans le théorème qui suit $\widehat{a}$ désigne donc la classe de a dans $\mathbb{Z}/n\mathbb{Z}$).

Théorème 9. $\forall k \in \mathbb{Z}$, $\forall a \in \mathbb{Z}$, $k\widehat{a} = \widehat{ka}$.

Démonstration . Si $k \in \mathbb{N}^*$. $k\widehat{a} = \underbrace{\widehat{a} + \ldots + \widehat{a}}_{k \text{ termes}} = \widehat{(a + \ldots + a)} = \widehat{ka}$.

Ensuite, $0\,\widehat{a} = \widehat{0} = \widehat{0 \times a}$. Enfin, si $k < 0$, $-k\widehat{a} = \widehat{-ka}$ et donc $k\widehat{a} = --\widehat{ka} = \widehat{ka}$.

❑

Intéressons nous maintenant aux générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Théorème 10.

1) Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique.

2) $\forall n \in \mathbb{N}^*$, $\forall a \in \mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z} = \text{gr}(a) \Leftrightarrow a \wedge n = 1)$.

Démonstration .

1) $\text{gr}(\widehat{1}) = \{k\widehat{1},\ k \in \mathbb{Z}\} = \{\widehat{k},\ k \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$. Donc, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène, fini et donc cyclique. Un générateur de ce groupe est $\widehat{1}$.

2) Soit $a \in \mathbb{Z}$.

Si $\widehat{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, en particulier, $\widehat{1} \in \text{gr}(\widehat{a})$. Il existe donc $u \in \mathbb{Z}$ tel que $\widehat{1} = u\widehat{a} = \widehat{au}$ ou encore $1 \equiv au\ [n]$. Mais alors, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + nv = 1$. D'après le théorème de Bézout, les entiers relatifs a et n sont premiers entre eux.

Réciproquement, supposons les entiers relatifs a et n premiers entre eux. Il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + nv = 1$. Mais alors $\widehat{1} = u\widehat{a} \in \text{gr}(\widehat{a})$. Puisque $(\text{gr}(a), +)$ est un groupe, $\text{gr}(\widehat{a})$ contient encore tous les $k\widehat{1} = \widehat{k}$, $k \in \mathbb{Z}$ et donc $\text{gr}(\widehat{a}) = \mathbb{Z}/n\mathbb{Z}$. Par suite, $\widehat{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

On a montré que pour tout $a \in \mathbb{Z}$, $\widehat{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si les entiers relatifs a et n sont premiers entre eux.

❑

1.4.2 Application aux groupes monogènes

On va voir dans ce paragraphe, qu'il existe un et un seul modèle de groupe monogène infini, à savoir le groupe $(\mathbb{Z}, +)$ et un un et un seul modèle de groupe cyclique de cardinal $n \in \mathbb{N}^*$, à savoir le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Plus précisément,

Théorème 11. Soit $(G, *)$ un groupe monogène.

1) Si G est infini, le groupe $(G, *)$ est isomorphe au groupe $(\mathbb{Z}, +)$.

2) Si G est fini de cardinal $n \in \mathbb{N}^*$, le groupe $(G, *)$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration . On fait la démonstration en notation multiplicative : soit $(G, \times)$ un groupe monogène dont l'élément neutre est noté e. Il existe $a \in G$ tel que $G = \{a^p,\ p \in \mathbb{Z}\}$.

Soit $\varphi : \begin{array}{ccc} (\mathbb{Z}, +) & \to & (G, \times) \\ p & \mapsto & a^p \end{array}$. φ est un morphisme de groupes (car pour tout $(p,q) \in \mathbb{Z}^2$, $a^{p+q} = a^p \times a^q$), surjectif (par définition de a). On sait que $\text{Ker}(\varphi)$ est un sous-groupe de $(\mathbb{Z}, +)$ et donc il existe $n \in \mathbb{N}$ tel que $\text{Ker}(\varphi) = n\mathbb{Z}$ (théorèmes 6 et 7, page 4).

1er cas. Supposons $n = 0$. On a $\text{Ker}(\varphi) = 0\mathbb{Z} = \{0\}$. On sait alors que φ est injectif et donc φ est un isomorphisme du groupe $(\mathbb{Z}, +)$ sur le groupe $(G, \times)$. Dans ce cas, G est nécessairement de cardinal infini.

2ème cas. Supposons $n \in \mathbb{N}^*$. Dans ce cas, $\text{Ker}(\varphi) = n\mathbb{Z} \neq \{0\}$. Pour $(p,q) \in \mathbb{Z}^2$,

$$a^p = a^q \Leftrightarrow a^{p-q} = e \Leftrightarrow p - q \in \text{Ker}(\varphi) = n\mathbb{Z} \Leftrightarrow p \equiv q\ [n].$$

Par suite, $G = \{a^p,\ p \in [\![0, n-1]\!]\}$ où de plus les a^p, $p \in [\![0, n-1]\!]$, sont deux à deux distincts. Dans ce cas, $(G, \times)$ est un groupe fini de cardinal n.

Soit alors $\psi : \begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z},+) & \to & (G,\times) \\ \widehat{p} & \mapsto & a^p\end{array}$.

Vérifions tout d'abord que ψ est bien définie. Soit $(p,q) \in \mathbb{Z}^2$ tel que $\widehat{p} = \widehat{q}$. Alors, $p \equiv q\ [n]$ puis $a^p = a^q$. Ceci montre qu'on a bien défini une application de $\mathbb{Z}/n\mathbb{Z}$ vers G.

ψ ainsi définie est surjective par définition de a. Mais alors, puisque $\text{card}(G) = n = \text{card}(\mathbb{Z}/n\mathbb{Z}) < +\infty$, ψ est une bijection.

Soit enfin $(p,q) \in \mathbb{Z}^2$.

$$\psi(\widehat{p}+\widehat{q}) = \psi\left(\widehat{p+q}\right) = a^{p+q} = a^p \times a_q\psi(\widehat{p}) \times \psi(\widehat{q}).$$

ψ est donc un isomorphisme du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ sur le groupe $(G,\times)$.

❑

Ainsi, par exemple, le groupe $(U_n,\times)$ qui est cyclique de cardinal n, est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Un isomorphisme est $\begin{array}{ccc}(U_n,\times) & \to & (\mathbb{Z}/n\mathbb{Z},+) \\ e^{\frac{2ik\pi}{n}} & \mapsto & \widehat{k}\end{array}$.

Quand $n = 4$, l'isomorphisme s'écrit explicitement

$$\begin{array}{c} 1 \mapsto \widehat{0} \\ i \mapsto \widehat{1} \\ -1 \mapsto \widehat{2} \\ -i \mapsto \widehat{3} \end{array}$$

et par exemple, $-1 \times -i = i$ et $\widehat{2}+\widehat{3} = \widehat{1} = \psi(i)$. A $-1 \times -i$, on a associé $\psi(-1)+\psi(-i)$. « On calcule dans $(U_4,\times)$ comme on calcule dans $(\mathbb{Z}/4\mathbb{Z},+)$ en changeant simplement les notations ».

1.5 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 $*$. On rappelle les notations :

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

ou aussi, en notation additive (en notant $-x$ le symétrique d'un élément x pour $+$),

$$\forall n \in \mathbb{Z},\ nx = \begin{cases} \underbrace{x+\ldots+x}_{n \text{ termes}} \text{ si } n > 0 \\ 0 \text{ si } n = 0 \\ \underbrace{(-x)+\ldots+(-x}_{-n \text{ termes}} \text{ si } n < 0 \end{cases},$$

DÉFINITION 5. 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 $(\mathcal{S}_n,\circ)$, $\text{Id}_{[\![1,n]\!]}$ est d'ordre 1 et une transposition est d'ordre 2. ❑

Exemple 3. Dans $\left(GL\left(\mathbb{R}^2\right),\circ\right)$, $\text{Id}_{\mathbb{R}^2}$ 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, distinct de 1 et -1 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 5 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 $px \neq 0$.

⇛ **Commentaire**. *L'égalité* $px = 0$ *ou encore* $\underbrace{x+\ldots+x}_{p \text{ termes}} \neq 0$ *avec* $p \in \mathbb{N}^*$ *peut surprendre. Mais ceci est possible dans les nouveaux groupes* $(\mathbb{Z}/n\mathbb{Z})$. *Par exemple, dans* $(\mathbb{Z}/6\mathbb{Z},+)$, $\widehat{0}$ *est d'ordre* 1, $\widehat{3}$ *est d'ordre* 2 *car* $\widehat{3} \neq 0$, *et* $2.\widehat{3} = \widehat{3}+\widehat{3} = \widehat{0}$, $\widehat{2}$ *et* $\widehat{4}$ *sont d'ordre* 3 *et enfin* $\widehat{1}$ *et* $\widehat{5}$ *sont d'ordre* 6 *:*

$$\widehat{5} \neq \widehat{0},\ \widehat{5}+\widehat{5} = \widehat{4} \neq \widehat{0},\ \widehat{5}+\widehat{5}+\widehat{5} = \widehat{3} \neq \widehat{0},\ \widehat{5}+\widehat{5}+\widehat{5}+\widehat{5} = \widehat{2} \neq \widehat{0},\ \widehat{5}+\widehat{5}+\widehat{5}+\widehat{5}+\widehat{5} = \widehat{1} \neq \widehat{0}$$

et enfin $6.\widehat{5} = \widehat{5}+\widehat{5}+\widehat{5}+\widehat{5}+\widehat{5}+\widehat{5} = \widehat{0}$.

On note que l'ordre d'un élément de $\mathbb{Z}/6\mathbb{Z}$, *à savoir* 1, 2, 3 *ou* 6 *est toujours un diviseur du cardinal de* $\mathbb{Z}/6\mathbb{Z}$, *à savoir* 6 *et que les éléments d'ordre* 6, *à savoir* $\widehat{1}$ *et* $\widehat{5}$, *sont les générateurs du groupe* $(\mathbb{Z}/6\mathbb{Z},+)$ *(d'après le théorème 10, page 6).*

On énoncé maintenant une caractérisation de l'ordre d'un élément.

Théorème 12. Soit $(G,*)$ un groupe dont l'élément neutre est noté e.

1) L'ordre d'un élément x de G est égal à l'ordre (ou encore le cardinal) du sous-groupe qu'il engendre.

2) Si x est un élément de G d'ordre fini $d \in \mathbb{N}^*$, alors : $\forall n \in \mathbb{Z},\ x^n = e \Leftrightarrow d|n$.

DÉMONSTRATION. On fait la démonstration en notation multiplicative. Soit $(G,\times)$ un groupe d'élément neutre e. Soit x un élément de G. Soit $\varphi : \begin{array}{ccc}(\mathbb{Z},+) & \mapsto & (G,\times) \\ n & \mapsto & x^n\end{array}$.
φ est un morphisme de groupes et son noyau, à savoir $\text{Ker}(\varphi) = \{n \in \mathbb{Z} / \ x^n = e\}$ est un sous-groupe du groupe $(\mathbb{Z},+)$. Donc, il existe $d \in \mathbb{N}$ tel que $\text{Ker}(\varphi) = d\mathbb{Z}$.

1er cas. On suppose que $d = 0$ ou encore $\text{Ker}(\varphi) = \{0\}$. Dans ce cas, Pour tout $n \in \mathbb{N}^*$, $x^n \neq e$ et donc x est d'ordre infini. φ est injectif et donc φ induit un isomorphisme $(\mathbb{Z},+)$ sur $(\text{gr}(x),\times)$. En particulier, que $\text{gr}(x)$ est d'ordre infini.

2ème cas. On suppose que $d \in \mathbb{N}^*$. Par définition de d, pour $n \in \mathbb{Z}$,

$$x^n = e \Leftrightarrow n \in \text{Ker}(\varphi) \Leftrightarrow n \in d\mathbb{Z}.$$

Mais alors, x est d'ordre fini égal à d. En posant la division euclidienne de n par d, on obtient le fait que

$$\text{gr}(x) = \{x^n,\ n \in \mathbb{Z}\} = \{x^n,\ n \in [\![0, d-1]\!]\},$$

où cette fois-ci les x^n, $n \in [\![0, d-1]\!]$ sont deux à deux distincts. Ceci montre déjà que $\text{gr}(x)$ est d'ordre fini, égal à d. On note que dans ce cas, $(\text{gr},\times)$ est isomorphe à $(\mathbb{Z}/d\mathbb{Z},+)$.

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

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

et U_4 est effectivement constitué de quatre éléments deux à deux distincts.

1.6 Le théorème de Lagrange

Théorème 13 (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 :

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

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

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

- 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

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

- 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 card(H) divise l'entier card(G). ❑

Théorème 14. Soit $(G,*)$ un groupe fini d'élément neutre e. 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 $\text{card}(G)=n\in\mathbb{N}^*$, alors $\forall a\in G$, $a^n=e$ (où $a^n=\underbrace{a*\ldots*a}_{n \text{ facteurs}}$).

Démonstration. Les théorèmes 12 et 13 donnent immédiatement le résultat. Néanmoins, le théorème de Lagrange n'est pas au programme des classes préparatoires. Le programme officiel demande de démontrer le théorème 14 dans le cas particulier où le groupe $(G,*)$ est commutatif, ce que l'on suppose dorénavant. On note $n\in\mathbb{N}^*$ le cardinal de G et e l'élément neutre de $(G,*)$.

Soit x un élément de G. L'application $\sigma_x : y\mapsto x*y$ est une application de G dans lui-même, injective car pour $(y,y')\in G^2$, $\sigma_x(y)=\sigma_x(y')\Rightarrow xy=xy'\Rightarrow y=y'$ (car dans un groupe tout élément est simplifiable). Puisque G est fini, σ_x est une permutation de G. On en déduit que

$$\prod_{y\in G}y=\prod_{y\in G}\sigma_x(y)=\prod_{y\in G}xy=x^n\prod_{y\in G}y.$$

Après simplification par $\prod_{y\in G}y$ (car dans un groupe, tout élément est simplifiable), on obtient $x^n=e$. D'après le théorème 12, $n=\text{card}(G)$ est un multiple de l'ordre de x.

❑

Exemple 1. Le groupe des racines 6-èmes de l'unité dans $\mathbb{C}$ est $U_6=\left\{1,-j^2,j,-1,j^2,-j\right\}$ (muni de la multiplication). 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 $U_3 = \{1, j, j^2\}$ d'ordre 3),
- $-j$ et $-j^2$ sont d'ordre 6 (et engendrent l'un ou l'autre le sous-groupe $U_6 = \{1, -j^2, j, -1, j^2, -j\}$ 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 $\{Id_{[\![1,3]\!]}\}$ d'ordre 1),
- $\tau_{i,j}$ est d'ordre 2 (et engendre le sous-groupe $\{Id_{[\![1,3]\!]}, \tau_{i,j}\}$ d'ordre 2),
- c_i est d'ordre 3 (et engendre le sous-groupe $\{1, c_i, c_i^2\}$ 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 14 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. ❑

2 Compléments sur les anneaux

2.1 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 15. $(A_1 \times \ldots \times A_n, +, *)$ 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* $*$ *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* $(-x_1, \ldots, -x_n)$.

2.2 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 $(\mathbb{K}[X], +, \times)$.

2.2.1 Définitions et premières propriétés

Définition 6. 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.

• $\{0\}$ et A sont toujours des idéaux de l'anneau $(A, +\times)$.

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

Théorème 16. Soit $(A, +, \times)$ un anneau commutatif. Soit $x \in A$. Alors $xA = \{ax,\ a \in A\}$ est un idéal de l'anneau $(A, +, \times)$, appelé **idéal principal** (ou monogène) engendré par x.

⇛ **Commentaire**. *L'ensemble* xA *est l'ensemble des multiples de* x. *C'est le plus petit idéal de* A *(au sens de l'inclusion) contenant l'élément* x.

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

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

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

Théorème 17. 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 commutatif $(A, +, \times)$.

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

❑

Théorème 18. Soit $(A, +, \times)$ un anneau commutatif. Soit I un idéal de cet anneau.

$I = A \Leftrightarrow 1_A \in I$ (où 1_A est l'élément neutre de A pour $\times$).

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.

Théorème 19. Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux commutatifs. Soient f un morphisme de l'anneau $(A, +, \times)$ vers l'anneau $(A', +, \times)$.

Alors, $\mathrm{Ker}(f)$ est un idéal de l'anneau $(A, +, \times)$.

On rappelle que le noyau de f est l'ensemble des éléments x de A est $0_{A'}$ (et non pas $1_{A'}$).

Démonstration. f est d'abord un morphisme du groupe $(A, +)$ vers le groupe $(A, +)$ et on sait que $\mathrm{Ker}(f)$ est un sous-groupe du groupe $(A, +)$.
Soient alors $x \in \mathrm{Ker}(f)$ et $a \in A$. $f(xa) = f(x) \times f(a) = 0_{A'} \times f(a) = 0_{A'}$ (on sait que l'élément neutre d'un anneau pour $+$ est toujours absorbant pour $\times$). Donc, $xa \in \mathrm{Ker}(f)$.

On a montré que $\mathrm{Ker}(f)$ est un idéal de l'anneau $(A, +, \times)$.

❑

2.2.2 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 7. 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.

2.2.3 Divisibilité dans un anneau commutatif intègre

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

DÉFINITION 8. 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 20. 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** . *Dit autrement,* 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 $a|b$.

❑

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

2.3.1 $(\mathbb{Z},+,\times)$ est un anneau principal

Théorème 21. 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 6, page 4, 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 16, $n\mathbb{Z}$ est un idéal de l'anneau $(\mathbb{Z},+,\times)$. Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont donc les $n\mathbb{Z}$, $n \in \mathbb{Z}$.

❑

2.3.2 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.

• 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 17. D'après le théorème 21, il existe n entier naturel m, uniquement défini d'après le théorème 7, tel que

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

$a\mathbb{Z} \cap b\mathbb{Z}$ contient ab qui n'est pas nul et donc $m \neq 0$. $a\mathbb{Z} \cap b\mathbb{Z}$ 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 17. Il existe donc un entier naturel d tel que

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

$a\mathbb{Z}+b\mathbb{Z}$ contient $a\neq 0$ et donc $d\neq 0$. 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 20. 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, appelé le PGCD de a et b, puis que

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

On obtient aussi très rapidement le théorème de Bézout :

$$\begin{aligned}a \text{ et } b \text{ sont premiers entre eux} &\Leftrightarrow d=1\Leftrightarrow a\mathbb{Z}+b\mathbb{Z}=\mathbb{Z}\\ &\Leftrightarrow 1\in a\mathbb{Z}+b\mathbb{Z}\ \text{(d'après le théorème 18)}\\ &\Leftrightarrow \exists(u,v)\in\mathbb{Z}^2/\ au+bv=1.\end{aligned}$$

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

Dans cette section, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ comme $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ ou $\left\{a+b\sqrt{2},\ (a,b)\in\mathbb{Q}^2\right\}$ ...
La notion de polynômes a été définie en math sup quand $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$. Elle se généralise à l'identique au cas où $\mathbb{K}$ est un sous-corps quelconque de $\mathbb{C}$.

2.4.1 $(\mathbb{K}[X],+,\times)$ est un anneau principal

Théorème 22. 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 16, $P\times\mathbb{K}[X]$ 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 23. 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 $P_0=\frac{1}{\mathrm{dom}(P)}P$. P_0 est un polynôme unitaire élément de I (car multiple de P). De plus, pour tout polynôme Q,

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

et

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

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_0 divise P_1. 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.

❑

2.4.2 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 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.

On peut généraliser la notion à plus de deux polynômes : soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls. Il existe un et un seul polynôme unitaire D et un et un seul polynôme unitaire M tels que

$$(A_1\mathbb{K}[X]) + \ldots + (A_n\mathbb{K}[X]) = D\mathbb{K}[X]$$

et

$$(A_1\mathbb{K}[X]) \cap \ldots \cap (A_n\mathbb{K}[X]) = M\mathbb{K}[X].$$

On peut montrer que D est le polynôme unitaire de plus haut degré qui soit un diviseur commun à $A_1, \ldots, A_n$ et M est le polynôme unitaire de plus bas degré qui soit un multiple commun à $A_1, \ldots, A_n$. On obtient aussi très rapidement le théorème de Bézout pour n polynômes, $n \geqslant 2$:

$$\mathrm{PGCD}\,(A_1, \ldots, A_n) = 1 \Leftrightarrow \exists\,(U_1, \ldots, U_n) \in (\mathbb{K}[X])^n \,/\, A_1U_1 + \ldots + A_nU_n = 1.$$

En effet,

$$\begin{aligned}\mathrm{PGCD}\,(A_1, \ldots, A_n) = 1 &\Leftrightarrow (A_1\mathbb{K}[X]) + \ldots + (A_n\mathbb{K}[X]) = \mathbb{K}[X]\\ &\Leftrightarrow 1 \in (A_1\mathbb{K}[X]) + \ldots + (A_n\mathbb{K}[X]) \text{ (d'après le théorème 18)}\\ &\Leftrightarrow \exists\,(U_1, \ldots, U_n) \in (\mathbb{K}[X])^n \,/\, A_1U_1 + \ldots + A_nU_n = 1.\end{aligned}$$

2.4.3 Irréductibles de l'anneau $(\mathbb{K}[X], +, \times)$. Décomposition en produit de facteurs irréductibles

On commence par rappeler la définition d'un polynôme irréductible sur $\mathbb{K}$:

Définition 9. Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Soit P un élément de $\mathbb{K}[X]$ de degré supérieur ou égal à 1.

P est **irréductible** sur $\mathbb{K}$ si et seulement si

$$\text{il n'existe pas } (A, B) \in (\mathbb{K}[X])^2 \text{ tel que } P = AB \text{ et } \deg(A) < \deg(P) \text{ et } \deg(B) < \deg(P)$$

ou encore, P est **irréductible** sur $\mathbb{K}$ si et seulement si

$$\forall (A, B) \in (\mathbb{K}[X])^2,\ (P = AB \Rightarrow \deg(A) = \deg(P) \text{ ou } \deg(B) = \deg(P)).$$

⇛ **Commentaire** .

◇ *Tout élément de $\mathbb{K}[X]$ de degré 1 est par définition irréductible sur $\mathbb{K}$*

◇ *On a déterminé en math sup les irréductibles de $\mathbb{C}[X]$ et les irréductibles de $\mathbb{R}[X]$: les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 (c'est l'une des versions du théorème de d'*Alembert-Gauss*) et les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif. Ainsi, par exemple, le polynôme X^4+X^2+1 n'est pas irréductible sur $\mathbb{R}$, bien que sans racine réelle :*

$$X^4+X^2+1=X^4+2X^2+1-X^2=\left(X^2-X+1\right)\left(X^2+X+1\right).$$

◇ *La notion d'irréductibilité est fonction de $\mathbb{K}$. Par exemple, X^2+1 est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$ car $X^2+1=(X-i)(X+i)$. De même, X^2-2 est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$ ou $\mathbb{C}$ car $X^2-2=\left(X-\sqrt{2}\right)\left(X+\sqrt{2}\right)$.*

On peut montrer qu'il existe des polynômes irréductibles sur $\mathbb{Q}$ de degré aussi grand qu'on veut. L'exercice suivant fournit un polynôme irréductible sur $\mathbb{Q}$ de degré 4.

Exercice 1. Montrer que le polynôme $P=X^4+X^3+X^2+X+1$ est irréductible sur $\mathbb{Q}$.

Solution 1. Les racines dans $\mathbb{C}$ du polynôme $P=\dfrac{X^5-1}{X-1}$ sont les cinq racines 5-èmes de 1 distinctes de 1. Le polynôme P n'a donc pas de racine réelle et en particulier pas de racine rationnelle. Par suite, P n'est pas le produit d'un polynôme de degré 1 et d'un polynôme de degré 3 à coefficients dans $\mathbb{Q}$.

Supposons que P soit le produit de deux polynômes de degré 2 à coefficients dans Q. Quite à mettre en facteur le coefficient dominant d'un des deux polynômes et à le redistribuer dans l'autre, on peut se ramener au cas où les deux polynômes sont unitaires. Donc, il existe trois rationnels a, b et c avec $b\neq 0$ tels que

$$X^4+X^3+X^2+X+1=\left(X^2+aX+b\right)\left(X^2+cX+\frac{1}{b}\right)=X^4+(a+c)X^3+\left(\frac{1}{b}+ac+b\right)X^2+\left(\frac{a}{b}+bc\right)X+1 \quad (*).$$

Il s'agit alors de résoudre dans $\mathbb{Q}$ le système $\left\{\begin{array}{l} a+c=1\\ \dfrac{1}{b}+ac+b=1\\ \dfrac{a}{b}+bc=1\end{array}\right.$ ou encore $\left\{\begin{array}{l} c=1-a\\ b+\dfrac{1}{b}+a(1-a)=1\\ \dfrac{a}{b}+b(1-a)=1\end{array}\right.$.

La dernière équation s'écrit $a\dfrac{1-b^2}{b}=1-b$. Si $b=1$, on obtient $\left\{\begin{array}{l} c=1-a\\ a(1-a)=-1\end{array}\right.$ ou encore $\left\{\begin{array}{l} c=1-a\\ a^2-a-1\end{array}\right.$. La dernière équation admet pour solution les nombres $\dfrac{1\pm\sqrt{5}}{2}$ qui ne sont pas des rationnels (si $a=\dfrac{1\pm\sqrt{5}}{2}$ est rationnel, alors $\sqrt{5}=\pm(2a-1)$ est rationnel, ce qui est faux).
Donc $b\neq 1$ et la dernière équation s'écrit $a(1+b)=b$ puis $a\neq 1$ et $b=\dfrac{a}{1-a}$. La deuxième équation s'écrit alors $\dfrac{a}{1-a}+\dfrac{1-a}{a}+a(1-a)=1$ ou encore $a^4-2a^3+4a^2-3a+1=0$. On sait que si $r=\dfrac{p}{q}$, $(p,q)\in\mathbb{Z}^*\times\mathbb{N}^*$, $p\wedge q=1$ est une solution rationnelle de cette équation, alors $p|1$ et $q|1$ puis $r=\pm 1$. Mais, ni 1, ni -1, ne sont solution de l'équation $a^4-2a^3+4a^2-3a+1=0$ et finalement, le problème $(*)$ n'a pas de solution dans $\mathbb{Q}[X]$.

On a montré que le polynôme $X^4+X^3+X^2+X+1$ est irréductible sur $\mathbb{Q}$.

Autre solution. On peut aussi profiter de la symétrie des coefficients (polynôme réciproque) pour factoriser explicitement le polynôme P dans $\mathbb{R}[X]$:

$$\begin{aligned} X^4+X^3+X^2+X+1&=X^2\left(X^2+\frac{1}{X^2}+X+\frac{1}{X}+1\right)=X^2\left(\left(X+\frac{1}{X}\right)^2+\left(X+\frac{1}{X}\right)-1\right)\\ &=X^2\left(X+\frac{1}{X}-\frac{-1+\sqrt{5}}{2}\right)\left(X+\frac{1}{X}-\frac{-1-\sqrt{5}}{2}\right)\\ &=\left(X^2-\frac{-1+\sqrt{5}}{2}X+1\right)\left(X^2-\frac{-1-\sqrt{5}}{2}+1\right) \quad (**).\end{aligned}$$

(On note que cette décomposition était aussi fournie par la première solution). Maintenant, une factorisation de P en produit de deux polynômes de degré 2 serait aussi une factorisation en produit de facteurs irréductibles dans $\mathbb{R}$. Par unicité d'une telle décomposition, la factorisation $(*)$ est nécessairement la factorisation $(**)$. Comme les nombres $\dfrac{-1\pm\sqrt{5}}{2}$ ne sont pas rationnels, on a de nouveau montré l'impossibilité d'une telle factorisation dans $\mathbb{Q}[X]$.

En math sup, on a donné la décomposition d'un polynôme non constant en produit de facteurs irréductibles dans $\mathbb{C}[X]$ et $\mathbb{C}[X]$. Tout élément P de $\mathbb{C}[X]$ de degré supérieur ou égal à 1, s'écrit de manière unique, à l'ordre près des facteurs, sous la forme

$$P = \lambda \prod_{i=1}^{k} (X - z_i)^{\alpha_i}$$

où $\lambda \in \mathbb{C}^*$, $k \in \mathbb{N}^*$, les z_i sont des complexes deux à deux distincts et les α_i sont des entiers naturels non nuls tels que $\alpha_1 + \ldots + \alpha_k = \deg(P)$.

De même, tout élément P de $\mathbb{R}[X]$ de degré supérieur ou égal à 1, s'écrit de manière unique, à l'ordre près des facteurs, sous la forme

$$P = \lambda \prod_{i=1}^{k} (X - x_i)^{\alpha_i} \prod_{j=1}^{l} \left(X^2 + a_j X + b_j\right)^{\beta_j}$$

où $\lambda \in \mathbb{R}^*$, k et l sont des entiers naturels, l'un des deux au moins étant non nul, les x_i sont des réels deux à deux distincts, les (a_j, b_j) sont des couples deux à deux distincts de réels tels que $a_j^2 - 4b_j < 0$ et les α_i et les β_j sont des entiers naturels non nuls (avec la convention usuelle qu'un produit vide est égal à 1).

On admettra plus généralement que

Théorème 24. Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Tout élément P de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 s'écrit de manière unique à l'ordre près des facteurs sous la forme

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i},$$

où $\lambda \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, les P_i sont des polynômes deux à deux distincts irréductibles sur $\mathbb{K}$ et les α_i sont des entiers naturels non nuls tels que $\alpha_1 + \ldots + \alpha_k = \deg(P)$.

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

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

Soit n un entier naturel non nul. On a déjà défini une addition dans $\mathbb{Z}/n\mathbb{Z}$ par :

$$\forall (a, b) \in \mathbb{Z}^2,\ \widehat{a} + \widehat{b} = \widehat{a + b}.$$

et on a vérifié que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif (théorème 8, page 5). On définit de même une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par

$$\forall (a, b) \in \mathbb{Z}^2,\ \widehat{a} \times \widehat{b} = \widehat{ab} \quad (*).$$

Comme pour l'addition, il s'agit de vérifier d'abord que la définition adoptée de $\widehat{a} \times \widehat{b}$ ne dépend pad pas du choix des représentants a et b des classes considérées.

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

Théorème 25. Soit $n \geqslant 2$. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ 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 $\left\{\widehat{0}\right\}$. Dans ce cas, tous les axiomes de la structure d'anneau sont vérifiés avec le défaut qu'un même élément (à savoir $\widehat{0}$) est élément neutre pour l'addition et la multiplication. Le programme officiel veut probablement éviter cette situation.*

Démonstration. On sait déjà que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif et que $\times$ est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.

• Pour $(a, b) \in \mathbb{Z}^2$, $\widehat{a} \times \widehat{b} = \widehat{ab} = \widehat{ba} = \widehat{b} \times \widehat{a}$. Donc, $\times$ est commutative.

• Pour $(a,b,c)\in\mathbb{Z}^3$, $\left(\widehat{a}\times\widehat{b}\right)\times\widehat{c}=\widehat{ab}\times\widehat{c}=\widehat{(ab)c}=\widehat{a(bc)}=\widehat{a}\times\widehat{bc}=\widehat{a}\times\left(\widehat{b}\times\widehat{c}\right)$. Donc, $\times$ est associatative.

• Pour $a\in\mathbb{Z}$, $\widehat{a}\times\widehat{1}=\widehat{a\times 1}=\widehat{a}$. Donc, $\times$ possède un élément neutre à savoir $\widehat{1}$.

• Pour $(a,b,c)\in\mathbb{Z}^3$,

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

Donc, $\times$ est distributive sur $+$.

❑

Le théorème qui suit est une remarque qui mérite d'être énoncée explicitement :

Théorème 26. Soit $n\geqslant 2$. Pour tout entier relatif a,

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

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

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

$\times$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$
$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$
$\widehat{1}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$
$\widehat{2}$	$\widehat{0}$	$\widehat{2}$	$\widehat{4}$	$\widehat{1}$	$\widehat{3}$
$\widehat{3}$	$\widehat{0}$	$\widehat{3}$	$\widehat{1}$	$\widehat{4}$	$\widehat{2}$
$\widehat{4}$	$\widehat{0}$	$\widehat{4}$	$\widehat{3}$	$\widehat{2}$	$\widehat{1}$

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

$+$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$
$\widehat{0}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$
$\widehat{1}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$
$\widehat{2}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$
$\widehat{3}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$
$\widehat{4}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{5}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$

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

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 ($(\mathbb{Z}/5\mathbb{Z},+)$ et $(\mathbb{Z}/6\mathbb{Z},+)$ sont des groupes cycliques). 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 $\times$ ($\widehat{1}\times\widehat{1}=\widehat{1}$, $\widehat{4}\times\widehat{4}=\widehat{1}$ et $\widehat{2}\times\widehat{3}=\widehat{1}$) ce qui n'est pas le cas dans $\mathbb{Z}/6\mathbb{Z}$. De plus, dans $\mathbb{Z}/6\mathbb{Z}$, $\widehat{2}$ et $\widehat{3}$ sont deux classes distinctes de $\widehat{0}$ dont le produit est égal à $\widehat{0}$.

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

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

Théorème 27. Soit $n\geqslant 2$. Soit $a\in\mathbb{Z}$.

$\widehat{a}$ 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 $a \in \mathbb{Z}$.

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

❑

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 26 affirme que

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

Exercice 2. Montrer que $\widehat{39}$ est inversible dans l'anneau $(\mathbb{Z}/224\mathbb{Z},+,\times)$ et déterminer son inverse.

Solution 2.

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

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

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

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

Une conséquence du théorème 26 est

Théorème 28. Soit $n \geqslant 2$.

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

Notation. Soit p un nombre premier. Le corps $(\mathbb{Z}/p\mathbb{Z},+,\times)$ se note $\mathbb{F}_p$.

Démonstration. Si n est premier, tout entier k de $[\![1, n-1]\!]$ est premier à n et donc, pour tout $k \in [\![1, n-1]\!]$, $\widehat{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ d'après le théorème 27. 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 27. 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.

❑

3.3 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 $\widehat{a} \neq \widehat{0}$ et $\widehat{b} \neq \widehat{0}$ et puisque $n = ab$, on a $\widehat{a} \times \widehat{b} = \widehat{ab} = \widehat{0}$.

On a montré que

Théorème 29. Soit $n \geqslant 2$.

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

Exercice 3.

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

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

Solution 3. 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 $x \in \mathbb{Z}/13\mathbb{Z}$,

$$\begin{aligned} x^2 = \widehat{1} &\Leftrightarrow \left(x-\widehat{1}\right)\left(x+\widehat{1}\right) = \widehat{0} \Leftrightarrow x-\widehat{1} = \widehat{0} \text{ ou } x+\widehat{1} = \widehat{0} \\ &\Leftrightarrow x = \widehat{1} \text{ ou } x = \widehat{12}. \end{aligned}$$

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

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 $\widehat{1}$ et $\widehat{-1} = \widehat{11}$ pour solutions mais il y en a peut -être d'autres :

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

$\mathscr{S} = \left\{\widehat{1}, \widehat{5}, \widehat{7}, \widehat{11}\right\}$. Ainsi, dans l'anneau non intègre $(\mathbb{Z}/12\mathbb{Z},+,\times)$, l'équation $x^2 = \widehat{1}$ admet strictement plus que deux solutions.

Exercice 4 (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 4. $p = 2$ 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 $(p-1)! = -1+qp$ 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. $\widehat{(p-1)}!$ est le produit de toutes les classes non nulles de ce corps ou encore le produit de toutes les classes inversibles.

Déterminons les classes non nulles qui sont leur propre inverse. Ce sont les solutions de l'équation $x^2 = \widehat{1}$ 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 $\widehat{1}$ et $\widehat{-1}$.

Si $p = 3$, $(p-1)! = 2 \equiv -1$ [3]. Sinon, $p \geqslant 5$. Dans le produit $\widehat{(p-1)!} = \prod_{k=1}^{p-1} \widehat{k}$, on isole $\widehat{1}$ et $\widehat{p-1} = \widehat{-1}$ 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 $\widehat{1}$ et on obtient

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

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

3.4 Le théorème chinois

Théorème 30. 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 $a \in \mathbb{Z}$.

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

Donc, $\mathrm{Ker}(f) = \{\overline{0}\}$ 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 $\mathrm{card}(\mathbb{Z}/nm\mathbb{Z}) = nm = \mathrm{card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) < +\infty$. 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 30 est le théorème chinois :

Théorème 31. 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 30,

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

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

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

❑

Le théorème 31 se généralise par récurrence à un système de p équations, $p \geqslant 2$, où « les modulo » sont deux à deux premiers entre eux.

3.5 L'indicatrice d'Euler

Définition 10. 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 10 et 27, pour $n \geqslant 2$, on a

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

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

Théorème 32. 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 30, 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 29, 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 33.

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),

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

puis, par récurrence sur k,

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

ce qui démontre le résultat.

❑

Théorème 34 (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 $n \geqslant 2$, $\varphi(n) = \text{card}\,((\mathbb{Z}/n\mathbb{Z})^*)$ et de plus, on sait que $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe de cardinal $\varphi(n)$. On sait que l'ordre d'un élément d'un groupe divise l'ordre de ce groupe et donc, pour tout élément x de $((\mathbb{Z}/n\mathbb{Z})^*, \times)$, $x^{\varphi(n)} = \overline{1}$ 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 5. Déterminer le reste de la division euclidienne de 4^{291} par 35.

Solution 5. $35 = 5 \times 7$ 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 6. Déterminer le nombre de générateurs du groupe $(U_{12}, \times)$.

Solution 6. Le groupe groupe $(U_{12}, \times)$ est isomorphe au groupe $(\mathbb{Z}/12\mathbb{Z}, +)$.
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 générateurs du groupe $(U_{12}, \times)$ ou encore il y a 4 racines primitives 12-èmes de 1 dans $\mathbb{C}$.

Exercice 7. Montrer que pour tout $n \geqslant 1$, $n = \sum_{d|n,\ d>0} \varphi(d)$ (en posant $\varphi(1) = 1$).

Solution 7. 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

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

---

4 Algèbres

4.1 Définition d'une algèbre

Dans cette section, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ comme $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Définition 11. Soit $\mathscr{A}$ un ensemble non vide muni de deux lois de composition interne notées $+$ et $*$ et d'une loi de composition externe de domaine $\mathbb{K}$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) notée ..

$(\mathscr{A}, +, ., *)$ est une **$\mathbb{K}$-algèbre** si et seulement si

- $(\mathscr{A}, +, .)$ est un $\mathbb{K}$-espace vectoriel,
- $(\mathscr{A}, +, *)$ est un anneau,
- $\forall (x, y) \in \mathscr{A}^2$, $\lambda.(x * y) = (\lambda.x) * y = x * (\lambda.y)$.

La dimension de l'algèbre $(\mathscr{A}, +, ., *)$ est la dimension de l'espace vectoriel $(\mathscr{A}, +, .)$.
L'algèbre $(\mathscr{A}, +, ., *)$ est dite **commutative** si et seulement si $*$ est commutative.

L'algèbre $(\mathscr{A}, +, ., *)$ est dite **intègre** si et seulement si l'anneau $(\mathscr{A}, +, *)$ est un anneau intègre ce qui équivaut à

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

Exemples fondamentaux. Il est fastidieux mais facile de montrer que :

- $(\mathbb{C}, +, ., \times)$ est une $\mathbb{R}$-algèbre commutative et intègre.
- $(\mathbb{K}[X], +, ., \times)$ est une $\mathbb{K}$-algèbre commutative et intègre.
- $(\mathscr{L}(E), +, ., \circ)$ est une $\mathbb{K}$-algèbre, non commutative et non intègre dès que $\dim(E) \geqslant 2$.
- $(\mathscr{M}_n(\mathbb{K}), +, ., \times)$ est une $\mathbb{K}$-algèbre, non commutative et non intègre dès que $n \geqslant 2$.
- Si X est un ensemble non vide quelconque, $(\mathbb{K}^X, +, ., \times)$ est une $\mathbb{K}$-algèbre commutative, non intègre si $\text{card}(X) \geqslant 2$.

On doit aussi avoir conscience que $(\mathbb{K}_n[X], +, ., \times)$ n'est pas une $\mathbb{K}$-algèbre car $\mathbb{K}_n[X]$ n'est pas stable pour le produit

4.2 Sous-algèbres

Définition 12. Soit $(\mathscr{A}, +, ., *)$ est $\mathbb{K}$-algèbre. Soit B une partie de $\mathscr{A}$.

B est une sous-algèbre de l'algèbre $(\mathscr{A}, +, ., *)$ si et seulement si B est non vide, stable pour $+$, $.$ et $*$ et B muni des lois induites est une $\mathbb{K}$-algèbre.

Le théorème suivant est facile à démontrer :

Théorème 35. Soit $(\mathscr{A}, +, ., *)$ est $\mathbb{K}$-algèbre. Soit B une partie de $\mathscr{A}$.

B est une sous-algèbre de l'algèbre $(\mathscr{A}, +, ., *)$
$\Leftrightarrow 1_{\mathscr{A}} \in B$ et B est stable pour $+$, $.$ et $\times$
$\Leftrightarrow 1_{\mathscr{A}} \in B$ et $\forall (x, y) \in B^2$, $x + y \in B$ et $\forall (\lambda, x) \in \mathbb{K} \times B$, $\lambda x \in B$ et $\forall (x, y) \in B^2$, $x * y \in B$
$\Leftrightarrow 1_{\mathscr{A}} \in B$ et $\forall (x, y) \in B^2$, $\forall (\lambda, \mu) \in \mathbb{K}^2$, $\lambda x + \mu y \in B$ et $\forall (x, y) \in B^2$, $x * y \in B$.

4.3 Morphismes d'algèbres

Définition 13. Soient $(\mathscr{A}, +, ., *)$ et $(\mathscr{B}, +, ., *)$ deux $\mathbb{K}$-algèbres. Soit f une application de $\mathscr{A}$ vers $\mathscr{B}$.

f est un morphisme d'algèbre si et seulement si

$$\begin{array}{l} \forall (x, y) \in \mathscr{A}^2,\ f(x + y) = f(x) + f(y) \\ \forall (\lambda, x) \in \mathbb{K} \times \mathscr{A},\ f(\lambda x) = \lambda f(x) \\ \forall (x, y) \in \mathscr{A}^2,\ f(x * y) = f(x) * f(y) \\ f(1_{\mathscr{A}}) = 1_{\mathscr{B}}. \end{array}$$

Par exemple, l'application $z \mapsto \overline{z}$ est un morphisme d'algèbres, de la $\mathbb{R}$-algèbre $(\mathbb{C}, +, ., \times)$ sur elle-même.