Chapitre 14

Structures algébriques classiques

Dans ce dernier chapitre, il s'agit simplement de revenir sur quelques notions algébriques qui peuvent être utiles et qui ont déjà étudiées en cours d'année : les groupes ou les idéaux d'un anneau commutatif... C'est surtout l'occasion de revenir sur quelques exemples et de présenter un cas particulier, celui de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.

Programmes 2022

Pour aller plus loin
Il s'agit simplement de faire quelques rappels en cette fin d'année et on essaiera de retenir la définition de l'anneau $\mathbb{Z}/n\mathbb{Z}$, un anneau de référence pour les exercices d'arithmétique.

1 Compléments sur les groupes

1.1 Rappels sur la structure de groupe

Définition Soit G un ensemble non vide pour lequel on définit $*$ une **loi de composition interne**, c'est à une relation binaire telle que :

$$* : (x, y) \in G \times G \longmapsto x * y \in G$$

On rappelle que $(G, *)$ est un **groupe pour la loi** $*$ si :

1. cette loi est **associative** : $\forall\, x, y, z \in G,\ x * (y * z) = (x * y) * z$
2. cette loi possède un **élément neutre** : $\exists\, e \in G,\ \forall\, x \in G,\ x * e = e * x = x$
3. tout élément admet un **symétrique** par cette loi : $\forall\, x \in G,\ \exists\, sym(x) \in G,\ x * sym(x) = sym(x) * x = e$

Remarques

1. Généralement, on commence par vérifier qu'on a bien une loi de composition interne avant de vérifier ces assertions.
2. Si la loi $*$ est **commutative**, alors on dit que $(G, *)$ est un **groupe commutatif** et dans ce cas, on ne vérifiera les assertions précédentes que pour un côté.

Propriété 1 (unicité des éléments remarquables)**.**

Soit $(G, *)$ un groupe. Alors,

1. l'élément neutre e associé est unique.
2. pour tout élément $x \in G$, le symétrique de x est unique.

▶ *Il suffit de supposer qu'il y en a deux et de prouver l'égalité.*

En première année, on voit les premières structures de groupes : **le groupe des racines n-ièmes de l'unité, le groupe des bijections, le groupe symétrique, le groupe linéaire**... et il nous faudra pas être surpris si on vous interroge dessus !

Par exemple, voici trois exercices assez classiques et indépendants :

Exemple 1 Soit $n \in \mathbb{N}^*$, on se place dans $\mathcal{M}_n(\mathbb{K})$ et on note encore (E_{ij}) les matrices élémentaires qui constituent la base canonique de $\mathcal{M}_n(\mathbb{K})$. On appelle alors :

- **matrice de transvection** toute matrice de la forme :

$$T_{ij}(\lambda) = I_n + \lambda E_{ij} \text{ , avec } \lambda \in \mathbb{K} \text{ et } (i, j) \in [\![1, n]\!]^2,\ i \neq j$$

- **matrice de dilatation** toute matrice de la forme :

$$D_i(\lambda) = I_n + (\lambda - 1)E_{ii} \text{ , avec } \lambda \in \mathbb{K}^* \text{ et } i \in [\![1, n]\!]$$

Soient $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{K})$.

1. Calculer pour tout $\lambda \in \mathbb{K}$ et $(i, j) \in [\![1, n]\!]^2,\ i \neq j$, $T_{ij}(\lambda).A$, puis interpréter votre résultat.
2. Soient $(i, j) \in [\![1, n]\!]^2,\ i \neq j$ et $\lambda, \mu \in \mathbb{K}$. Calculer $T_{ij}(\lambda).T_{ij}(\mu)$. En déduire que les matrices de transvection sont inversibles et préciser leur inverse.
3. Calculer pour tout $\lambda \in \mathbb{K}^*$ et $i \in [\![1, n]\!]$, $D_i(\lambda).A$, puis interpréter votre résultat.
4. Soient $i \in [\![1, n]\!]$ et $\lambda, \mu \in \mathbb{K}^*$. Calculer $D_i(\lambda).D_i(\mu)$. En déduire que les matrices de dilatation sont inversibles et préciser leur inverse.
5. En utilisant votre interprétation en termes d'opérations élémentaires, justifier que le produit suivant revient à échanger les deux lignes L_i et L_j :
$$D_j(-1)T_{ij}(1)T_{ji}(-1)T_{ij}(1).A$$

Toutes les opérations élémentaires sur les lignes reviennent donc à multiplier à gauche par des matrices de diltatation ou de transvection, et de la même façon, on peut montrer que les opérations sur les colonnes reviennent à multiplier à droite par ces matrices. La **méthode du pivot de Gauss** nous permet alors, par opérations élémentaires, d'écrire que pour toute matrice $A \in \mathcal{GL}_n(\mathbb{K})$, il existe $M_1, \dots, M_p,\ N_1, \dots, N_q$ des matrices de ce type telles que $M_p \dots M_1 A N_1 \dots N_q = I_n$.

6. En déduire que $\mathcal{GL}_n(\mathbb{K})$ est engendré par les matrices de diltatation et de transvection.

Exemple 2 Soit $n \in \mathbb{N}^*$, on rappelle que $\mathbb{U}_n$ désigne le groupe des racines n-ièmes de l'unité.

1. Soient $a, b \in \mathbb{N}^*$, montrer plus généralement que :
$$\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_d \text{ , avec } d = pgcd(a,b)$$
2. En déduire la solution du système suivant : $\begin{cases} z^{1346} - 1 = 0 \\ z^{989} - 1 = 0 \end{cases}$.

Exemple 3 Soit $n \in \mathbb{N}, n \geq 2$, on rappelle que S_n désigne le groupe des permutations des entiers $[\![1, n]\!]$.

1. Justifier que $Card(S_n) = n!$, puis établir que S_n est engendré par les transpositions de la forme $(i\ j)$.
2. Montrer que l'ensemble des transpositions de la forme $(1\ i)$, $i \in [\![2, n]\!]$ engendrent S_n.
3. Déterminer alors le centre de S_n. *On pourra distinguer les cas $n = 2$ et $n > 2$.*

Notation Etant donné un groupe, sa loi de composition interne sera souvent notée :

- $+$ si celle-ci est commutative et dans ce cas, $e = 0_G$ et $sym(x) = -x$ appelé **opposé de** x.
- $.$ si on n'a pas d'information sur sa commutativité et dans ce cas, $e = 1_G$ et $sym(x) = x^{-1}$ appelé **inverse de** x.

Définition Soient $(G, *)$ un groupe et $H \subset G$. On dit que H est un **sous-groupe de** G si la loi $*$ induite sur H donne à $(H, *)$ une structure de groupe.

Théorème 2 (caractérisation d'un sous-groupe)**.**

Soit $(G, *)$ un groupe. Alors, on a immédiatement :
$$H \text{ est un sous-groupe de } (G,*) \Leftrightarrow \begin{cases} H \subset G \text{ (inclusion)} \\ e \in H \text{ (élément neutre)} \\ \forall\, x, y \in H,\ x * y \in H \text{ (stabilité pour la loi induite)} \\ \forall\, x \in H,\ sym(x) \in H \text{ (stabilité par passage aux symériques)} \end{cases}$$

Corollaire 3 (cas particulier avec les notations usuelles)**.**

Soit G un groupe. Alors,

- en notation additive, H est un sous-groupe de $(G, +) \Leftrightarrow \begin{cases} H \subset G \\ 0_G \in H \\ \forall\, x, y \in H,\ x + y \in H \\ \forall\, x \in H,\ -x \in H \end{cases}$.
- en notation multiplicative, H est un sous-groupe de $(G, .) \Leftrightarrow \begin{cases} H \subset G \\ 1_G \in H \\ \forall\, x, y \in H,\ x.y \in H \\ \forall\, x \in H,\ x^{-1} \in H \end{cases}$.

Remarque Pour gagner du temps, on peut aussi remarquer que les deux dernières assertions sont équivalentes à :
$$x - y \in H \text{ ou bien } x.y^{-1} \in H$$
On parle aussi de stabilité par **somme** ou **produit tordu**.

Propriété 4 (intersection de sous-groupes)**.**

Soit $(G, *)$ un groupe et considérons $H_1, \ldots, H_n$ des sous-groupes de G. Alors, $\cap_{i=1}^n H_i$ désigne encore un sous-groupe de G.

▶ *Il suffit de revenir à la caractérisation d'un tel sous-groupe.*

Exemple 4 On note $\mathcal{GL}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$, à coefficients dans $\mathbb{Z}$, qui sont inversibles et dont l'inverse est à coefficients dans $\mathbb{Z}$.

1. On suppose que M est à coefficients dans $\mathbb{Z}$. Montrer que $M \in \mathcal{GL}_n(\mathbb{Z})$ si et seulement si $det(M) = \pm 1$.
2. En déduire que $\mathcal{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$.

1.2 Sous-groupe engendré par une partie

Dans cette partie, on note . la loi du groupe et on adaptera les notations lorsque celle-ci sera additive.

Définition Soient $(G, .)$ un groupe et A une partie non vide de G. On appelle **sous-groupe engendré par** A l'intersection de tous les sous-groupes de G contenant A et il sera noté $< A >$:

$$< A >= \bigcap_{H \text{sous-groupe}, H \supset A} H$$

Propriété 5 (interprétation ensembliste du sous-groupe engendré par une partie A)**.**

Avec les notations de la définitions,

1. $< A >$ désigne le plus petit sous-groupe de G contenant A.
2. $< A >$ peut aussi être vu comme l'ensemble des produits finis :

$$< A > = \{x = x_1 \dots x_n, \text{ avec pour tout } i \in [\![1, n]\!], x_i \text{ ou } x_i^{-1} \in A\}$$

► *On montre d'abord qu'il s'agit d'un sous-groupe de G, avant de justifier que c'est le plus petit d'entre eux contenant A. D'ailleurs, pour le second point, on revient à cette interprétation ensembliste.*

Corollaire 6 (cas particulier des groupes monogènes)**.**

Soit $(G, .)$ un groupe et a un élément de G. Alors, on a immédiatement :

$$< a >= \{a^n,\ n \in \mathbb{Z}\}$$

On dit aussi que $< a >$ est **monogène** et que a désigne un **générateur** de $< a >$.

Remarques

1. On a déjà vu de tels groupes, c'est notamment le cas du groupe $(\mathbb{U}_n, .)$ des racines n-èmes de l'unité :

$$\mathbb{U}_n = \{e^{i2k\pi/n},\ k \in [\![0, n-1]\!]\} = < e^{i2\pi/n} >$$

2. D'ailleurs, on dit aussi qu'un tel groupe est **cylique** s'il est monogène et fini.

1.3 Ordre d'un élément dans un groupe

Définition Soit $(G, .)$ un groupe dont on note encore 1_G l'élément neutre, et considérons $x \in G$. On dit que x est d'**ordre fini** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 1_G$.
De plus, le plus petit entier $n \in \mathbb{N}^*$ satisfaisant cette égalité s'appeller l'ordre de x et sera noté $o(x)$.

Propriété 7 (relation avec l'ordre de x)**.**

Soit $(G, .)$ un groupe dont on note encore 1_G l'élément neutre, et considérons $x \in G$ d'ordre p. Alors, on a :

$$x^n = 1_G \Leftrightarrow p \mid n$$

► *Par double implication : le sens réciproque est immédiat. Pour le sens direct, il suffit de faire la DE de n par p et on montre que le reste est nécessairement nul.*

Propriété 8 (petit théorème de Lagrange)**.**

Soit $(G,.)$ un groupe dont on note encore 1_G l'élément neutre. On suppose de plus que G est un groupe fini commutatif et de cardinal $n \in \mathbb{N}^*$. Alors, on a pour tout $x \in G$,

$$x^n = 1_G$$

En particulier, l'ordre de x divise $card(G)$.

► *On montre d'abord que $\phi : a \longmapsto ax$ est bijective de G sur G de sorte que $\prod_a ax = \prod_a a$ et par commutativité et simplification, il vient $x^n = 1_G$.*

Remarques

1. C'est un résultat assez pratique. Par exemple, si on considère $\mathbb{U}_3$ le groupe des racines 3-èmes de l'unité, il s'agit d'un groupe fini d'ordre 3 et ainsi, on peut affirmer qu'il n'y a pas d'éléments d'ordre 2.
2. Dans le cas particulier où G est cyclique de cardinal n, alors $G =< x >$ et x est nécessairement d'ordre n. En effet, on a d'une part, $o(x)|n$ et si $o(x) < n$, alors G ne pourrait pas contenir n éléments. Et ainsi, $o(x) = n = card(G)$.
3. Pour finir, on peut aussi définir la notion de **morphisme de groupes** : il s'agit d'applications de la forme $\phi : G \longrightarrow H$ compatibles avec les lois données. En particulier, on caractérise encore l'injectivité et la surjectivité à l'aide du noyau et de l'image de ϕ :
$$\begin{cases} \phi \text{ est injective si et seulement si } Ker(\phi) = \{e_G\} \\ \phi \text{ est surjective si et seulement si } Im(\phi) = H \end{cases}$$
Cette dernière notion n'est pas l'essence de ce chapitre, mais il ne faudra pas avoir peur de retrouver ces morphismes dans quelques exercices d'oraux.

Exemple 5 Soit $(G,.)$ un groupe fini et H un sous-groupe de G.

1. Montrer que pour tout $a \in G$, H et $aH = \{ah; h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \emptyset$. En déduire que le cardinal de H divise le cardinal de G.
3. Justifier alors que tout groupe fini de cardinal $p \in \mathcal{P}$ ne possède aucun sous-groupe, à l'exception de G lui-même et $\{e_G\}$.

Remarque En fait ce dernier exemple désigne le **théorème de Lagrange**, et il nous permet de prolonger le résultat précédent sur l'ordre d'un élément : dans un groupe fini G d'ordre n non nécessairement commutatif, le cardinal du sous-groupe $< x >$ engendré par x divise toujours le cardinal de G et on retrouve :

$$x^n = 1_G$$

2 Compléments sur les anneaux

2.1 Rappels sur la structure d'anneau

Définition Soit A un ensemble non vide pour lequel on définit $+$ et $.$ deux **lois de composition interne**.
On rappelle que $(A,+,.)$ est un **anneau pour les lois $+$ et $.$** si :

1. $(A,+)$ est un groupe commutatif, dont on notera désormais 0_A l'élément neutre.
2. la loi $.$ est **associative**: $\forall\, x,y,z \in A,\ x.(y.z) = (x.y).z$
3. cette loi possède un **élément neutre** qu'on notera désormais 1_A: $\forall\, x \in A,\ x * 1_A = 1_A * x = x$
4. cette loi est **distributive** par rapport à $+$: $\forall\, x,y,z \in A,\ x.(y+z) = x.y + x.z$ et $(y+z).x = y.x + z.x$

Remarques

1. Généralement, on commence par vérifier qu'on a bien des lois de composition interne avant de vérifier ces assertions.
2. Si la loi $.$ est **commutative**, on pourra dire que $(A,+,.)$ est un **anneau commutatif** et dans ce cas, on ne vérifiera les assertions précédentes que pour un côté.
3. Attention, les éléments d'un anneau n'ont pas forcément d'inverse par la loi $.$. D'ailleurs, les éléments inversibles d'un anneau pour la loi $.$ constituent un groupe multiplicatif noté $U(A)$, et si $U(A) = A^*$, on dit encore que $(A,+.)$ est un **corps**.
4. Pour finir, on peut aussi définir la notion de **morphisme d'anneaux** : il s'agit d'applications de la forme $\phi : A \longrightarrow B$ compatibles avec les lois données et pour lesquelles $\phi(1_A) = 1_B$.

Notation Avec $n \in \mathbb{N}$, on note : $nx = x + \ldots + x$ (n fois), et $x^n = x.\ \ldots\ .x$ (n fois), avec la convention $x^0 = 1_A$.

Propriété 9 (règles de calcul).

On retrouve ici toutes les règles de calculs usuels :

1. 0_A est **absorbant** : $\forall\, x \in A,\ 0_A.x = x.0_A = 0_A$
2. soit $(x, y) \in A^2$ tel que x et y commutent, alors on a toujours la **formule du binôme de Newton** :
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}.y^k$$
3. soit $(x, y) \in A^2$ tel que x et y commutent, alors on a toujours la **formule de factorisation** :
$$x^n - y^n = (x-y).\sum_{k=0}^{n-1} x^k.y^{n-k-1} = \sum_{k=0}^{n-1} x^{n-k-1}.y^k$$

et ainsi,

- $1_A - x^n = (1_A - x).\sum_{k=0}^{n-1} x^k$
- En particulier, si $1_A - x$ est inversible dans A par la loi ., on retrouve : $(1_A - x)^{-1}.(1_A - x^n) = \sum_{k=0}^{n-1} x^k$

Définition Soient $(A, +, .)$ un anneau et $B \subset A$. On dit que B est un **sous-anneau de** A si les lois $+$ et . induites sur B donne à $(B, +, .)$ une structure d'anneau.

Théorème 10 (caractérisation d'un sous-anneau).

Soit A un anneau. Alors,
$$B \text{ est un sous-anneau de } (A,+,.) \Leftrightarrow \begin{cases} B \subset A \\ 1_A \in B \\ \forall\, x, y \in B,\ x - y \in B \\ \forall\, x, y \in B,\ x.y \in B \end{cases}$$

▶ *C'est immédiat : on raisonne simplement par double implication.*

Ainsi, pour démontrer qu'un ensemble donné est un anneau, on pourra ou bien revenir à la définition d'un tel anneau, ou bien le voir comme un sous-anneau d'un anneau donné.

Exemple 6 On note $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss défini par :
$$\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$$
Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, .)$, et déterminer $U(\mathbb{Z}[i])$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}[i]$.

2.2 Cas particulier des idéaux d'un anneau commutatif

Définition Soit $(A, +, .)$ un anneau commutatif. On appelle **idéal** toute partie I non vide de A telle que :

1. I est un sous-groupe de $(A, +)$
2. I est **absorbant** : $\forall\, a \in A,\ \forall\, x \in I,\ a.x \in I$

Propriété 11 (appartenance de l'élément neutre 1_A).

Soient $(A, +, .)$ un anneau commutatif et I un idéal de A.

1. Si $1_A \in I$, alors $I = A$.
2. Plus généralement, si I contient un élément inversible de A, alors $I = A$.

▶ *On utilise à chaque fois le fait que I est absorbant.*

Remarque En fait, la notion d'idéal nous a été très utile cette année et on essaiera de retenir quelques exemples importants : que ce soit la définition du PGCD ou du PPCM dans les structures euclidiennes, ou alors la définition du polynôme minimal d'un endomorphisme en dimension finie.

D'ailleurs, on en rappelle ici les deux résultats principaux qui ont déjà été démontrés :

Propriété 12 (idéaux de l'anneau des entiers relatifs)**.**

On rappelle dans $\mathbb{Z}$ que pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

Et ainsi, on a : I est un idéal de $\mathbb{Z}$ si et seulement s'il existe $n \in I$, $I = n\mathbb{Z}$.
On dit que $\mathbb{Z}$ est un **anneau principal**, car ses idéaux sont engendrés par un seul élément.

▶ *Cela a déjà été vu et on travaille par double implication : dans le sens direct, une fois le générateur déterminé, on utilisera le théorème de la division euclidienne pour montrer que I est bien de la forme donné ; pour la réciproque, on revient à la définition d'un tel idéal.*

Propriété 13 (idéaux de l'anneau des polynômes)**.**

On rappelle dans $\mathbb{K}[X]$ que pour tout $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$, il existe un unique couple $(Q,R) \in (\mathbb{K}[X])^2$ tel que :

$$\begin{cases} A = BQ + R \\ deg(R) < deg(B) \end{cases}$$

Et ainsi, on a : I est un idéal de $\mathbb{K}[X]$ si et seulement s'il existe $P \in I$, $I = P\mathbb{K}[X]$.
On dit que $\mathbb{K}[X]$ est un **anneau principal**, car ses idéaux sont engendrés par un seul élément.

▶ *Cela a déjà été vu et on travaille par double implication : dans le sens direct, une fois le générateur déterminé, on utilisera le théorème de la division euclidienne pour montrer que I est bien de la forme donné ; pour la réciproque, on revient à la définition d'un tel idéal.*

3 Cas particulier de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$

3.1 Présentation et définition

Définition Soit $n \in \mathbb{N}^*$ et considérons $(x,y) \in \mathbb{Z}^2$. On dit que x est **congru à** y **modulo** n si $y - x \in n\mathbb{Z}$, c'est à dire qu'on note:

$$x \equiv y\ [n] \Leftrightarrow n \mid y - x$$

Remarque Comme pour les autres relations de congruence, il s'agit d'une **relation d'équivalence** dans le sens où cette relation binaire est :

- **réflexive** : pour tout $x \in \mathbb{Z}$, $x \equiv x\ [n]$.
- **symétrique** : pour tout $(x,y) \in \mathbb{Z}^2$, $x \equiv y\ [n] \Rightarrow y \equiv x\ [n]$.
- **transitive** : pour tout $(x,y,z) \in \mathbb{Z}^3$, si $x \equiv y\ [n]$ et $y \equiv z\ [n]$, alors $x \equiv z\ [n]$.

D'ailleurs, on rappelle qu'on peut définir les **classes d'équivalence** associées à une telle relation, et ainsi si $\overline{x}$ désigne la classe de x, alors par définition :

$$\overline{x} = \{y \in \mathbb{Z},\ x \equiv y\ [n]\}$$

et ces classes d'équivalence définissent une partition naturelle de $\mathbb{Z}$. D'ailleurs, si on a besoin de préciser le modulo avec lequel on travaille, on pourra toujours écrire $\overline{x}^{[n]}$: la **classe de** x **modulo** n.

Définition Soit $n \in \mathbb{N}^*$. On appelle **ensemble quotient** $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour la relation de congruence modulo n.
En particulier, on définit l'application surjective $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ par :

$$\pi_n : x \longmapsto \overline{x}$$

Propriété 14 (représentants irréductibles de $\mathbb{Z}/n\mathbb{Z}$).

1. Pour tout $x \in \mathbb{Z}$, il existe un unique $r \in [\![0, n-1]\!]$ tel que $x \equiv r\ [n]$, et ainsi, $\overline{x} = \overline{r}$: on dit que r est un représentant irréductible de $\overline{x}$.
2. En particulier, on en déduit : $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$.

► *Le premier point découle de la division euclidienne dans $\mathbb{Z}$. Le second point est alors immédiat puisque toute classe d'équivalence est de la forme $\overline{r}$.*

Propriété 15 (compatibilité de l'addition et de la multiplication).

Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est compatible avec l'addition et la multiplication, autrement dit pour tout $a, b, c, d \in \mathbb{Z}$, on a :

$$\begin{cases} \overline{a} = \overline{b} \\ \overline{c} = \overline{d} \end{cases} \Rightarrow \begin{cases} \overline{a+c} = \overline{b+d} \\ \overline{ac} = \overline{bd} \end{cases}$$

► *Il suffit de revenir à la relation de congruence et de montrer sous ces hypothèses que n divise la différence.*

Remarque Cette dernière propriété est fondamentale, et elle nous permet de définir des opérations direcement sur $\mathbb{Z}/n\mathbb{Z}$. En effet si on pose pour tout $(\overline{x}, \overline{y}) \in \mathbb{Z}/n\mathbb{Z}^2$,

$$\overline{x} + \overline{y} := \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} := \overline{xy}$$

alors celles-ci sont bien définies sur les classes d'équivalence au sens où **elles ne dépendent pas du choix des représentants**.

Corollaire 16 (structure de l'ensemble quotient).

Soit $n \in \mathbb{N}^*$. On peut montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif dont les éléments neutres pour les lois $+$ et $\times$ sont respectivement $\overline{0}$ et $\overline{1}$.
En particulier, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique de cardinal n et on a pour l'addition :

$$\mathbb{Z}/n\mathbb{Z} = < \overline{1} >$$

Propriété 17 (relation avec les groupes monogènes).

Soit $n \in \mathbb{N}^*$ et on considère $(G, .)$ un groupe monogène dont on note a un générateur.

1. Si G est de cardinal fini n, alors l'application $\phi_a : \overline{k} \in \mathbb{Z}/n\mathbb{Z} \longmapsto a^k \in G$ est bien définie, et elle désigne un isomorphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ sur G.
2. Si par contre G est infini, alors $\phi_a : k \in \mathbb{Z} \longmapsto a^k \in G$ est un isomorphisme de groupes de $\mathbb{Z}$ sur G.

► *Pour chacun de ces points, on revient à la définition d'un isomorphisme de groupes, c'est à dire une application bijective compatible avec les opérations de chaque groupe.*

3.2 Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et corps fini à p éléments

Propriété 18 (caractérisation des éléments inversibles de l'anneau quotient).

Soit $n \in \mathbb{N}^*$ et considérons $U(\mathbb{Z}/n\mathbb{Z})$ le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Alors,

$$\overline{a} \in U(\mathbb{Z}/n\mathbb{Z}) \Leftrightarrow a \wedge n = 1$$

► *On peut procéder par double implication : le théorème de Bézout nous donnera à chaque fois le passage attendu.*

Corollaire 19 (immédiat)**.**

Soit $n \in \mathbb{N}^*$. Alors, on rappelle que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau à n éléments $\overline{0}, \dots, \overline{n-1}$ et ainsi :

$$\mathbb{Z}/n\mathbb{Z} \text{ est un corps } \Leftrightarrow \text{ tous ses éléments non nuls sont inversibles } \Leftrightarrow n \text{ est un nombre premier}$$

Définition Soit $p \in \mathbb{P}$. On appelle **corps fini** à p éléments l'ensemble noté $\mathbb{F}_p$ et défini tout simplement par :

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

3.3 Théorème des restes chinois et fonction indicatrice d'Euler

Théorème 20 (des restes chinois)**.**

Soient $p, q \in \mathbb{N}$, $p, q \geq 2$ qu'on suppose premiers entre eux.

1. Alors, l'application $\phi : \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ telle que :
$$\phi : \overline{a}^{[pq]} \longmapsto (\overline{a}^{[p]}, \overline{a}^{[q]})$$
est bien définie et elle désigne un isomorphisme d'anneaux.
2. En particulier, les ensembles $U(\mathbb{Z}/pq\mathbb{Z})$ et $U(\mathbb{Z}/p\mathbb{Z}) \times U(\mathbb{Z}/q\mathbb{Z})$ sont isomorphes.

▶ *On commence par montrer que ϕ est bien définie, au sens où elle ne dépend pas dureprésentant choisi. Ensuite, on prouve l'injectivité avant de conclure par cardinalité. Par morphisme d'anneaux, on en déduit que les éléments inversibles sont isomorphes.*

Remarques

1. En fait, cela signifie que sous les conditions $p \wedge q = 1$, il existe toujours une solution (modulo pq), à un système de congruence de la forme :
$$\begin{cases} x \equiv a\ [p] \\ x \equiv b\ [q] \end{cases}$$
D'ailleurs, pour résoudre un tel système, on pourra revenir à la résolution d'**équations diophantiennes**.
2. On peut d'ailleurs généraliser l'isomorphisme donné et en notant $p_1, \dots, p_n$ des entiers premiers entre eux deux à deux, alors l'application ϕ définit un isomorphisme de $\mathbb{Z}/\prod_{i=1}^{n} p_i\mathbb{Z}$ sur $Z/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_n\mathbb{Z}$:
$$\phi : \overline{a}^{[p_1 \cdots p_n]} \longmapsto (\overline{a}^{[p_1]}, \dots, \overline{a}^{[p_n]})$$

Exemple 7 Déterminer les solutions dans $\mathbb{Z}$ du système de congruence :

$$\begin{cases} x \equiv 2\ [3] \\ x \equiv 1\ [2] \end{cases}$$

Définition On appelle **fonction indicatrice d'Euler** l'application φ définie sur $\mathbb{N}^*$ par :

$$\varphi(n) = card(\{k \in [\![1, n]\!],\ k \wedge n = 1\}) = card(U(\mathbb{Z}/n\mathbb{Z}))$$

Remarques

1. On a évidemment pour tout $n \geq 2$, $1 \leq \varphi(n) \leq n-1$, et on a même $\varphi(p) = p - 1$ lorsque $p \in \mathbb{P}$.
2. De la même façon, si p est premier, alors :
$$\varphi(p^k) = p^k - p^{k-1}$$
puisqu'on enlève les éléments non premiers avec p^k : tous les multiples de p de la forme $1.p, 2.p, \dots, p^{k-1}.p$.

Théorème 21 (calcul explicite de la fonction indicatrice d'Euler)**.**

1. Soient $p, q \in \mathbb{N}$, $p, q \geq 2$ qu'on suppose premiers entre eux. Alors on a d'après le théorème des restes chinois :
$$\varphi(pq) = \varphi(p)\varphi(q)$$
2. En particulier, si $n \geq 2$ admet pour décomposition primaire $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, il vient :
$$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

▶ *Le premier point est évident cra les éléments inversibles sont isomorphes, donc de même cardinal. Le second point découle du premier et de la remarque précédente.*

Corollaire 22 (théorème d'Euler)**.**

Soit $n \in \mathbb{N}^*$, alors pour tout $a \in \mathbb{Z}$ tel que $a \wedge n = 1$,
$$\overline{a}^{\varphi(n)} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z}, \text{ c'est à dire : } a^{\varphi(n)} \equiv 1 \ [n]$$

▶ *C'est immédiat : si a est premier avec n, il est dans le groupe des éléments inversibles de cardinal $\varphi(n)$ et on invoque le petit théorème de Lagrange.*

Remarques

1. Dans le cas particulier où $p \in \mathbb{P}$, on retrouve le **petit théorème de Fermat** que vous avez démontré en première année :
$$\forall\, a \in \mathbb{Z},\ a^{p-1} \equiv 1 \ [p]$$
2. Ce qui achève l'année... à condition d'aller au bout des ces derniers exemples d'applications :

Exemple 8 Soit $n \in \mathbb{N}^*$. Etablir que :
$$n = \sum_{d|n} \varphi(d)$$
On pourra par exemple introduire les fractions de la forme p/n, $p \in [\![1, n]\!]$ et considérer une partition de cet ensemble.

Exemple 9 Soit $p \in \mathbb{N}, p \geq 2$. Montrer le **théorème de Wilson**, c'est à dire :
$$(p-1)! \equiv -1 \ [p] \ \Leftrightarrow \ p \text{ est premier}$$

Exemple 10 Soit $n \in \mathbb{N},\ n \geq 2$. Déterminer les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.