Mathématiques

MPI*

Lycée Champollion

Beanie Hat

2022 - 2023

Pour télécharger le reste de mes cours, suivez le lien ancré dans le code QR en fin de ce document ou allez sur bit.ly/cours-mpi.

Pour toute doléance ou demande, vous pouvez me contacter à beanie[arobase]tuta[point]io.

Fait à CHAMPOLLION.

Table des matières

I

Algèbre

1

Groupes

I. Groupes, sous-groupes et morphismes

1. Groupes

Définition : Groupe
Soit G un ensemble non vide. Soit $*$ une loi de composition interne sur G, c'est-à-dire

$$* : \left| \begin{array}{ccc} G \times G & \to & G \\ (a,b) & \mapsto & a \times b \end{array} \right.$$

On dit que $(G, *)$ est un **groupe** si

- $*$ est associative
- $*$ possède un neutre e_G, c'est-à-dire un élément tel que

$$\forall g \in G, g * e_G = e_g * g = g$$

  En ce cas, e_G est unique. On l'appelle le neutre de $(G, *)$.
- Tout élément de G possède un symétrique pour $*$, c'est-à-dire

$$\forall g \in G, \exists h \in G, g * h = h * g = e_G$$

  De plus, un tel symétrique est unique. On l'appelle le symétrique de G et on le note $h = g^{-1}$.
- On a aussi

$$\forall g_1, g_2 \in G, (g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$$

- Si de plus $*$ est commutative, on dit que $(G, *)$ est un groupe abélien ou commutatif.

Dans le cas où la loi de composition interne est notée $+$, le groupe $(G, +)$ est appelé **groupe additif**. $+$ est en général commutative.
- Le neutre est noté 0 ou 0_G.
- Le symétrique d'un élément $g \in G$ est appelé opposé de g et noté $-g$.
- Pour $n \in \mathbb{N}^*$, l'élément obtenu par n itérations de g est noté $g + \ldots + g = n \cdot g$.
- On note par convention $0 \cdot g = 0_g$.
- Pour $n \in \mathbb{Z} \backslash \mathbb{N}$, on note $n \cdot g = -((-n) \cdot g)$.

Exemple :

$$3 \cdot g = g + g + g$$
$$-2 \cdot g = -(g + g)$$

On a alors $\forall (n,p) \in \mathbb{Z}^2, \forall g \in G$, $(n+p) \cdot g = n \cdot g + p \cdot g$.

Exemple :

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- $(E, +)$ avec E un espace vectoriel.
- $\left(M_{n,p}(\mathbb{K}), +\right)$.
- $\mathbb{K}[X]$.

Dans le cas où la loi de composition interne est notée $\cdot$, le groupe $(G, \cdot)$ est appelé **groupe multiplicatif**.
- Le neutre est noté 1_G.
- Le symétrique de $g \in G$ est appelé l'inverse de g et est noté g^{-1}.
- Pour $n \in \mathbb{N}^*$ et $g \in G$, l'élément obtenu par n itérations de g est noté $g \cdot \ldots \cdot g = g^n$.
- On note $g^0 = 1_G$.
- Pour $n \in \mathbb{Z} \backslash \mathbb{N}$, on note $g^n = (g^{-n})^{-1} = (g^{-1})^{-n}$.
- $\forall n, p \in \mathbb{Z}^2$, $g^{n+p} = g^n \cdot g^p$.

Exemple :

$$g^4 = g \cdot g \cdot g \cdot g$$
$$g^{-3} = g^{-1} \cdot g^{-1} \cdot g^{-1} = (g \cdot g \cdot g)^{-1}$$

Exemple :

- $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, $(\mathbb{R}_+^*, \cdot)$.
- $(1, \cdot)$.
- Pour $n \in \mathbb{N}^*$, $(\mathbb{U}_n, \cdot)$ le groupe des racines $n$ièmes de l'unité
- $(\mathbb{U}, \cdot)$ le groupe des complexes de module 1.
- $(GL_n(\mathbb{K}), \cdot)$ le groupe des matrices carrées inversibles.

Dans le cas générique, la loi de composition interne est notée $*$ ou autrement.

Exemple :

- $(S_n, \circ)$, le groupe symétrique. Pour $g \in S_n$, g est notée sous forme de tableau et est représentée par un graphe.
- Si E est un $\mathbb{K}$-espace vectoriel, $(GL(E), \circ)$ est le groupe des isomorphismes de E.
- Si $E \neq \emptyset$, on définit une loi de composition interne par $\forall A, B \in E, A\Delta B = (A \cup B) \setminus (A \cap B) = (A \backslash B) \cup (B \backslash A)$. On montre que $(P(E), \Delta)$ est un groupe abélien, de neutre $\emptyset$, et pour lequel le symétrique de A est A.

2. Sous-groupes

Définition : Sous-groupe
Soit $(G, *)$ un groupe et $H \subseteq G$ une partie non vide.
On dit que H est un **sous-groupe** de G si $*$ définit une loi de H par laquelle H est un groupe.
On a alors $e_G \in H$ le neutre de $(H, *)$.

Exemple :

- $\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$
- $\{e_G\}$ et G son des sous-groupes de G dits triviaux.

Proposition
Soient $(G, *)$ un groupe et $H \subseteq G$ non vide. Alors H est un sous-groupe de G si et seulement si

- $\forall g, h \in H, g * h \in H$
- $\forall g \in H, g^{-1} \in H$

Preuve : Vue l'an dernier.

Proposition
Soient $(G, *)$ un groupe et $H \subseteq G$ non vide.
Alors H est un sous-groupe de G si et seulement si $\forall g, h \in H, g * h^{-1} \in H$.

Exemple :

- pour $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
- $(\mathbb{U}, \cdot)$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$.

Théorème
Soit I un ensemble non vide, et $(G_i)_{i \in I}$ une famille de sous-groupes de G. Alors

$$\bigcap_{i \in I} G_i = \{g \in G, \forall i \in I, g \in G_i\}$$

est un sous-groupe de G.

Preuve : Notons $H = \bigcap_{i \in I} G_i$. On a $\forall i \in I, e_g \in G_i$ car G_i est un sous-groupe. Donc $e_g \in H$ donc $H \neq \emptyset$.
Soient $g, h \in H$. Montrons que $g * h^{-1} \in H$.
Soit $i \in I$. On a $g, h \in G_i$. Or G_i est un sous-groupe de G. Donc $g * h^{-1} \in G_i$ donc $g * h^{-1} \in H$.
Donc H est un sous-groupe.

(Légèrement hors-programme)
Soient H_1, H_2 des sous-groupes de $(G, *)$. Alors $H_1 \cup H_2$ est un sous-groupe de G si et seulement si $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.

Preuve :

- Si $H_1 \subseteq H_2$, alors $H_1 \cup H_2 = H_2$ est un sous-groupe. De même si $H_2 \subseteq H_1$.
- Par contraposée, si on a $H_1 \not\subseteq H_2$ et $H_2 \not\subseteq H_1$, alors $\exists x \in H_1, x \notin H_2$, et $\exists y \in H_2, y \notin H_1$. On a donc $x, y \in H_1 \cup H_2$.
  Considérons $g = x * y$. On a $x^{-1} * g = y \notin H_1$, donc $g \notin H_1$ car H_1 est un sous-groupe.
  De même, $g \notin H_2$. Donc $g \notin H_1 \cup H_2$. Donc $H_1 \cup H_2$ n'est pas un sous-groupe.

Théorème
Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Preuve :

- Soit $n \in \mathbb{N}$. Considérons $G = n\mathbb{Z}$.
  $G \subseteq \mathbb{Z}$ et $n \cdot 0 \in n\mathbb{Z}$ donc $G \neq \emptyset$.
  Soient $x, y \in G$. $\exists p, q \in \mathbb{Z}, x = np, y = nq$. Donc $x - y = n(p - q) \in \mathbb{Z}$.
  Donc $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
- Réciproquement, soit G un sous-groupe de $\mathbb{Z}$.
  Si $G = \{0\}$, alors $G = 0\mathbb{Z}$.
  Sinon, soit $x_0 \in G$ tel que $x_0 \neq 0$. Alors $x_0 \in G$ car G est un groupe. Donc $|x_0| \in G$.
  Donc $G \cap \mathbb{N}^* \neq \emptyset$.
  Posons $n = \min(G \cap \mathbb{N}^*)$. Montrons que $G = n\mathbb{Z}$.
  - Soit $g \in n\mathbb{Z}$. $\exists p \in \mathbb{Z}, g = p \cdot n$. Or $n \in G$, et $(G, +)$ est un groupe, donc $g \in G$.
    Donc $n\mathbb{Z} \in G$.
  - Soit $g \in G$. Par division euclidienne, $g = nq + r$. Donc $r = g - nq \in G$. Or $r < n$ et $n = \min(G \cap \mathbb{N}^*)$. Donc $r = 0$.
    Donc $g = nq$ donc $G = n\mathbb{Z}$ donc $G \subseteq n\mathbb{Z}$.

Donc $G = n\mathbb{Z}$.

3. Morphismes de groupes

Définition : Morphisme de groupes
Soient $(G, *)$ et $(H, \circ)$ deux groupes, et $\varphi : \left|\begin{array}{ccc} G & \to & H \\ g & \mapsto & \varphi(G) \end{array}\right.$.
On dit que φ est un **morphisme de groupes** si et seulement si

$$\forall g_1, g_2 \in G, \varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$$

Proposition
Avec ces notations, on a :

- $\varphi(e_G) = e_H$
- $\forall g \in G, \varphi(g^{-1}) = (\varphi(g))^{-1}$
- $\forall g \in G, \forall n \in \mathbb{Z}, \varphi(g^n) = (\varphi(g))^n$.

Exemple :

- Pour ln : $\left|\begin{array}{ccc} (\mathbb{R}_+^*, \cdot) & \to & (\mathbb{R}, +) \\ x & \mapsto & \ln x \end{array}\right.$:
  - $\forall a, b \in \mathbb{R}_+^*, \ln(a, b) = \ln a + \ln b$
  - $\forall a \in \mathbb{R}_+^*, \forall n \in \mathbb{Z}, \ln(a^n) = n \ln a$
- Pour e : $\left|\begin{array}{ccc} (\mathbb{R}, +) & \to & \mathbb{R}_+^* \\ x & \mapsto & e^x \end{array}\right.$:
  - $\forall a, b \in \mathbb{R}, e^{a+b} = e^a e^b$
  - $\forall a \in \mathbb{R}, \forall n \in \mathbb{Z}, e^{na} = (e^a)^n$

Définition : Noyau
Soient $(G, *), (H, \circ)$ des groupes et $\varphi : G \to H$ un morphisme de groupes.
On appelle **noyau** de φ (noté $\ker \varphi$) l'ensemble

$$\ker \varphi = \{g \in G, \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\})$$

THÉORÈME
$\ker \varphi$ est un sous-groupe de G.

Exemple :

- Soit $\varphi : \left| \begin{array}{ccc} \mathbb{C}^* & \to & \mathbb{R}^* \\ z & \mapsto & |z| \end{array} \right.$. Alors $\ker \varphi = \mathbb{U}$.
- Pour $n \in \mathbb{N}^*$, soit $\varphi : \left| \begin{array}{ccc} \mathbb{C}^* & \to & \mathbb{C}^* \\ z & \mapsto & z^n \end{array} \right.$. Alors $\ker \varphi = \mathbb{U}_n$.
- Soit la fonction signature $\varepsilon : \left| \begin{array}{ccc} S_n & \to & \mathbb{U}_2 \\ \sigma & \mapsto & \varepsilon(\sigma) \end{array} \right.$. Alors $\ker \varepsilon = A_n$ est appelé groupe alterné d'ordre n. C'est le groupe des permutations paires.

THÉORÈME
Soit $\varphi : G \to H$ un morphisme de groupes.
Alors φ est injectif si et seulement si $\ker \varphi = \{e_G\}$.

DÉFINITION : IMAGE
Soient $(G, *)$ et $(H, \circ)$ deux groupes, et $\varphi : G \to H$ un morphisme de groupes.
On appelle **image** de φ (notée $\Im\varphi$) l'ensemble

$$\Im\varphi = \{h \in H, \exists g \in G, \varphi(g) = h\} = \varphi(G)$$

THÉORÈME
$\Im\varphi$ est un sous-groupe de H.

DÉFINITION : ISOMORPHISME
Un morphisme de groupes de $(G, *)$ dans $(H, \circ)$ est appelé **isomorphisme** si et seulement si il est bijectif. En ce cas, sa bijection réciproque φ^{-1} est aussi un isomorphisme de groupes.

II. LE GROUPE $\mathbb{Z}/n\mathbb{Z}$

1. DÉFINITIONS

Dans toute cette partie, on prend $n \in \mathbb{N}$ avec $n \geqslant 2$.

DÉFINITION : CONGRUENCE
On considère la relation « **congrue à modulo** n » définie sur $\mathbb{Z}$ par

$$\forall x, y \in \mathbb{Z}, x \equiv y\,[n] \iff n | x - y \iff \exists k \in \mathbb{Z}, x - y = kn$$

PROPOSITION

- La congruence est une relation d'équivalence.
- $\forall x, y \in \mathbb{Z}, x \equiv y[n]$

Preuve :

- Évident.
- Écrivons les deux divisions euclidiennes $x = q_1 n + r_1$ et $y = q_2 n + r_2$.
  - Si $x \equiv y[n]$ alors $\exists k \in \mathbb{Z}$ tel que $x - y = kn$ donc $q_1 n + r_1 - q_2 n - r_2 = kn$ donc $r_1 - r_2 = (k - q_1 + q_2)\, n$ donc $n | r_1 - r_2$ or $-n < r_1 - r_2 < n$ donc $n_1 = n_2$.
  - Si $n_1 = n_2$ alors $x - y = (q_1 - q_2)\, n$ donc $x \equiv y[n]$.

DÉFINITION : $\mathbb{Z}/n\mathbb{Z}$
L'ensemble des classes d'équivalences de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.
Pour $k \in \mathbb{Z}$, sa classe d'équivalence est notée $cl_n(k) = \hat{k}$.

Exemple : Pour $n = 2$, $\mathbb{Z}/2\mathbb{Z} = \{\hat{0}, \hat{1}\}$ où $\hat{0}$ est l'ensemble des entiers pairs et $\hat{1}$ celui des entiers impairs.

Théorème

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

et ces éléments sont deux à deux distincts.
Donc $Card\ \mathbb{Z}/n\mathbb{Z} = n$.

Preuve :

- De droite à gauche : évident car $\forall k \in \{0, ..., n-1\}, \hat{k} \in \mathbb{Z}/n\mathbb{Z}$.
- Inversement, soit $c \in \mathbb{Z}/n\mathbb{Z}$. Soit $x \in c$. Par division euclidienne, $x = qn + r$ donc $x \equiv r[n]$. Donc $c = \hat{r}$ donc $\mathbb{Z}/n\mathbb{Z} \subseteq \left\{\hat{0}, ..., \widehat{n-1}\right\}$
- Soient $k_1, k_2 \in \left\{\hat{0}, ..., \widehat{n-1}\right\}$. Supposons que $\widehat{k_1} = \widehat{k_2}$. Montrons que $k_1 = k_2$. $k_1 \equiv k_2[n]$ donc $\exists q \in \mathbb{Z}, k_1 - k_2 = nq$. Mais $q = 0$, donc $k_1 = k_2$.

2. Structures de groupes

Proposition
Soient $c, d \in \mathbb{Z}/n\mathbb{Z}$. Soient $x \in c$ et $y \in d$.
Alors $\widehat{x+y}$ ne dépend pas du choix de x dans c ni de y dans d.
On peut donc noter cette classe $\widehat{x+y} = c \oplus d$. On a ainsi défini une loi de composition interne $\oplus$ dans $\mathbb{Z}/n\mathbb{Z}$.

Preuve : Soient $x_1, x_2 \in c$ et $y_1, y_2 \in d$.
Alors $\exists p, q \in \mathbb{Z}, x_1 = x_2 + np, y_1 = y_2 + nq$. Donc $x_1 + y_1 = x_2 + y_2[n]$.
Donc $\widehat{x_1 + y_1} = \widehat{x_2 + y_2}$.

Théorème
$(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est un groupe abélien et $\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & \hat{x} \end{array} \right.$ est un morphisme de groupes surjectif de noyau $n\mathbb{Z}$.

Preuve :

- $\oplus$ est une loi de composition interne de $\mathbb{Z}/n\mathbb{Z}$. On prouve aisément qu'elle est associative, commutative, symétrique et que $\hat{0}$ est le neutre. Cela fait donc de $\mathbb{Z}/n\mathbb{Z}$ un groupe.
- Soient $x, y \in \mathbb{Z}$. Alors $\varphi(x+y) = \widehat{x+y} = \hat{x} + \hat{y} = \varphi(x) + \varphi(y)$. Donc φ est un morphisme de groupes.
- Soit $x \in \mathbb{Z}$. $x \in \ker \varphi \iff \hat{x} = \hat{0} \iff x \equiv 0[n] \iff x \in n\mathbb{Z}$.

> φ est appelé le morphisme canonique.

> Dans le groupe de Klein, tout élément est son propre opposé. Ce n'est pas le cas dans $\mathbb{Z}/4\mathbb{Z}$. Donc ces groupes ne sont pas isomorphes.

Exemple : On peut faire des tableaux d'équivalence pour les additions.

3. Isomorphismes

Théorème
L'application

$$\psi : \left| \begin{array}{ccc} (\mathbb{Z}, \oplus) & \to & (\mathbb{U}_n, \cdot) \\ c = \hat{k} & \mapsto & e^{\frac{2ik\pi}{n}} \end{array} \right.$$

est bien définie et est un isomorphisme de groupes, c'est-à-dire que l'image de $c = \hat{k}$ ne dépend pas du choix de k dans c.

Preuve :

- Soient $k_1, k_2 \in c$. Alors $k_1 \equiv k_2 [n]$ donc $\exists p \in \mathbb{Z}, k_1 = k_2 - np$.
Donc $e^{\frac{2ik_1\pi}{n}} = e^{\frac{2ik_2\pi}{n} + 2ip\pi} = e^{\frac{2ik_2\pi}{n}}$ donc ψ est bien définie.
- Soient $c, d \in \mathbb{Z}/n\mathbb{Z}, x \in c, y \in d$. Alors
$\psi(c \oplus d) = \psi(\widehat{x+y}) = e^{2i\pi\frac{x+y}{n}} = e^{\frac{2i\pi x}{n}} \cdot e^{\frac{2i\pi y}{n}} = \psi(c) \cdot \psi(d)$ donc ψ est bien un morphisme de groupes.
- Montrons que ψ est injective. Soit $c \in \ker \psi$ et $k \in c$. Alors $e^{\frac{2ik\pi}{n}} = 1$. Donc $n | k$ donc $c = \hat{0}$. Donc $\ker \psi = \{0\}$ donc ψ est injective. Or, $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$ sont finis et de même cardinal. Donc ψ est bijective.

III. Ordre d'un élément

Dans toute cette section, on a $(G, *)$ un groupe et $a \in G$.

1. Morphisme fondamental

Théorème
L'application $\varphi_a : \left| \begin{array}{ccc} (\mathbb{Z}, +) & \rightarrow & (G, *) \\ k & \mapsto & a^k \end{array} \right.$ est un morphisme de groupes. Son image est un sous-groupe de G, appelé **groupe engendré par** a, et noté

$$\langle a \rangle = \left\{a^k, k \in \mathbb{Z}\right\}$$

Si G est un groupe additif, on a $\langle a \rangle = \{k \cdot a, k \in \mathbb{Z}\}$.

Preuve : Soient $k_1, k_2 \in \mathbb{Z}$. $\varphi_a(k_1 + k_2) = a^{k_1+k_2} = a^{k_1} * a^{k_2} = \varphi_a(k_1) * \varphi_a(k_2)$.

Définition : Ordre d'un élément d'un groupe
Avec ces notations, $ker\varphi_a$ est un sous-groupe de $\mathbb{Z}$, donc $\exists! n \in \mathbb{N}, \ker \varphi_a = n\mathbb{Z}$.

- Si $n > 0$, n est appellé l'**ordre** de a.
- Si $n = 0$, φ_a est injectif. On dit alors que a est d'**ordre infini**.

Exemple :

- Pour $G = \mathbb{U}$ et $a = j$, alors l'ordre de j est 3.
- Pour $G = \mathbb{U}$ et $a = i$, alors l'ordre de i est 4.
- Pour $G = (GL_2(\mathbb{R}), \cdot)$ et $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, alors l'ordre de S est 4.
- Pour $G = \mathbb{Z}$, alors 1 est d'ordre infini.
- Pour $G = (GL_2(\mathbb{R}), \cdot)$ et $T = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$,
on prouve facilement que $\forall k \in \mathbb{Z}, T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Donc φ_T est injective, donc T est d'ordre infini.

2. Éléments d'ordre infini

Proposition
Soit $a \in G$ d'ordre infini. Alors $\widetilde{\varphi_a} : \left| \begin{array}{ccc} \mathbb{Z} & \rightarrow & \langle a \rangle \\ k & \mapsto & a^k \end{array} \right.$ est un isomorphisme de groupes.
En particulier, l'ensemble $\langle a \rangle$ est infini.

Preuve :

- $\widetilde{\varphi_a}$ est surjective par construction.
- $\widetilde{\varphi_a}$ est injective car a est d'ordre infini donc $a^k = e$ si et seulement si $k = 0$.
- $\widetilde{\varphi_a}$ est un mmorphisme de groupes car φ_a en est un.

Exemple :

Dans toute cette section, on prend $a \in G$ d'ordre fini n.

- Pour $(\mathbb{Z}, +)$, $\langle 1 \rangle = \mathbb{Z}$, $\langle 2 \rangle = 2\mathbb{Z}$...
- Pour $(\mathbb{C}^*, \times)$, $\langle 2 \rangle = \left\{2^k, k \in \mathbb{Z}\right\}$.

3. Éléments d'ordre fini

PROPOSITION
Pour $k \in \mathbb{Z}/n\mathbb{Z}$, $a^k = e_G$ si et seulement si $n|k$.

Preuve : En notant $\varphi_a : \left| \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & a^k \end{array} \right.$, on a $\ker \varphi_a = n\mathbb{Z}$. Donc $a^k = e_G$ si et seulement si $k \in \ker \varphi_a$ si et seulement si $k \in n\mathbb{Z}$ si et seulement si $n|k$.

PROPOSITION
On a $n = Card\ \langle a \rangle$, $\langle a \rangle = \{e_G, a, a^2, ..., a^{n-1}\}$ et les éléments sont deux à deux distincts.

Preuve :

- Notons $H = \{a^k, k \in [\![1, n-1]\!]\}$. Alors par définition $H \subseteq \langle a \rangle$.
- Soit $x \in \langle a \rangle$. $\exists k \in \mathbb{Z}, x = a^k$. Par division euclidienne, $k = nq + r$.
  Donc x = $a^{nq+r} = a^n \in H$.
- Soient $k_1, k_2 \in [\![0, n-1]\!]$ tels que $a^{k_1} = a^{k_2}$. Alors $a^{k_1 - k_2} = e_G$ donc $n|k_1 - k_2$ donc $k_1 - k_2 = 0$, soit $k_1 = k_2$. Donc les éléments sont deux à deux distincts et $Card\ \langle a \rangle = n$.

Exemple : Dans $(\mathbb{C}^*, \times)$, les éléments d'ordre fini sont les a tels que $\exists n \geqslant 1$ tel que $a^n = 1$. Ce sont les racines de l'unité.

THÉORÈME
Soit $(G, *)$ un groupe fini et $a \in G$.
Alors a est d'ordre fini et l'ordre de a divise $Card\, G$, que l'on appelle aussi l'ordre de G.
Ainsi, dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe.

Ce théorème est un cas particulier du théorème de Lagrange.

Preuve : Dans le cas où G est commutatif :
Pour N le cardinal de G, on a $\langle a \rangle \subseteq G$, donc a est fini donc a est d'ordre fini n.
Considérons $f : \left| \begin{array}{ccc} G & \to & G \\ x & \mapsto & a * x \end{array} \right.$. f est de bijection réciproque $f^{-1} : \left| \begin{array}{ccc} G & \to & G \\ y & \mapsto & a^{-1} * y \end{array} \right.$.
G étant commutatif, on peut définir $z = \prod_{x \in G} x$. Comme f est bijective, $z = \prod_{x \in G} f(x)$. Donc $\prod_{x \in G} x = \prod_{x \in G} a * x$.
$*$ étant associative et commutative, $z = a^N * z$, donc en multipliant par z^{-1}, $a^n = e_G$.
Donc $n|N$.

THÉORÈME DE LAGRANGE (HORS PROGRAMME)
Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.

Preuve : Dans les grandes lignes : $g_1 \vee g_2 \iff \exists h \in H, g_2 = g_1 H$ est une relation d'équivalence.
On écrit alors G comme union disjointe des classes d'équivalence de $\vee$.
On montre que les classes ont toutes le mème cardinal qui est $Card\, H$.

IV. Groupes monogènes et cycliques

DÉFINITION : GROUPE MONOGÈNE ET MONOGÈNE CYCLIQUE
Soit $(G, *)$ un groupe.
On dit que G est

- **monogène** si et seulement si $\exists a \in G, G = \langle a \rangle$. a est alors appelé un générateur de G.
- **monogène cyclique** si G est de plus fini.

Tout groupe monogène est abélien.

Exemple :

- $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- $\mathbb{U}_6 = \langle -j \rangle = \left\langle -j^2 \right\rangle$.
- $\mathbb{U}_n = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$.
- $\mathbb{Z}/n\mathbb{Z} = \left\langle \hat{1} \right\rangle$.

Théorème
Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.

Preuve : Soit $(G, +)$ un monogène infini, et soit $a \in G$ un générateur.
Alors $G = \langle a \rangle$ infini donc a est d'ordre infini.
Donc $\varphi_a : \left| \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & a^k \end{array} \right.$ est un morphisme de groupes

- surjectif car $G = \langle a \rangle$
- injectif car a est d'ordre infini

Donc φ_a est un isomprhisme.

Théorème
Tout groupe monogène cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Preuve : Soit G d'ordre n monogène, et $a \in G$ tel que $G = \langle a \rangle$.
Considérons $\varphi : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & G \\ C = \hat{k} & \mapsto & a^k \end{array} \right.$. Alors φ est bien défini.
Soient $k_1, k_2 \in C$. Alors $\exists p \in \mathbb{Z}, k_1 = k_2 + np$. Donc $a^{k_1} = a^{k_2 + np} = a^{k_2} * a^{np}$. Or l'ordre de a est égal au cardinal de $\langle a \rangle$, c'est-à-dire n. Donc $a^{np} = e_G$ donc $a^{k_1} = a^{k_2}$ et φ est bien définie.
Soient $C_1, C_2 \in \mathbb{Z}/n\mathbb{Z}$ et $k_1 \in C_1, k_2 \in C_2$.
Alors $k_1 + k_2 \in C_1 \oplus C_2$ donc $\varphi(C_1 \oplus C_2) = a^{k_1 + k_2} = \varphi(C_1) * \varphi(C_2)$. Donc φ est un morphisme.
Soit $C \in \ker \varphi$ et $k \in C$.
On a $a^k = e_G$ donc $n | k$ donc $C = \hat{0}$. Donc φ est injective.
Or $Card\, \mathbb{Z}/n\mathbb{Z} = n = Card\, G$. Donc φ est bijective donc φ est un isomorphisme.

1. Générateurs de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$

Théorème
Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ (respectivement $\mathbb{U}_n$) sont les $\hat{k}$ (respectivement les $e^{\frac{2ik\pi}{n}}$) où $k \in \{1, n-1\}$ vérifie $k \wedge n = PGCD(k, n) = 1$.

Preuve : Dans le cas $\mathbb{Z}/n\mathbb{Z}$ (identique dans $\mathbb{U}_n$ grâce à l'isomorphisme $\hat{k} \mapsto e^{\frac{2ik\pi}{n}}$:

- Soit $C \in \mathbb{Z}/n\mathbb{Z}$ générateur de $\mathbb{Z}/n\mathbb{Z}$. Alors il existe $k \in \{0, \ldots, n-1\}$ tel que $c = \hat{k}$.
  Mais $k \neq 0$ car $\left\langle \hat{0} \right\rangle = \hat{0} \neq \mathbb{Z}/n\mathbb{Z}$ donc $k \in \{1, n-1\}$.
  Et comme $\langle C \rangle = \mathbb{Z}/n\mathbb{Z}$, $\hat{1} \in \langle C \rangle$ et il existe $p \in \mathbb{Z}$ tel que $pc = \hat{1}$, soit $pk \equiv 1[n]$.
  Donc $\exists q \in \mathbb{Z}, pk + nq = 1$.
  Donc par le théorème de Bézout, $PGCD(k, n) = 1$.
- Réciproquement, soit $k \in \{1, \ldots, n-1\}$ tel que $PGCD(k, n) = 1$.
  Montrons que $\left\langle \hat{k} \right\rangle = \mathbb{Z}/n\mathbb{Z}$.
  Par définition, on a $\left\langle \hat{k} \right\rangle \subseteq \mathbb{Z}/n\mathbb{Z}$.
  Soit $C \in \mathbb{Z}/n\mathbb{Z}$ et $x \in C$. Alors $c = \hat{x}$.
  Par le théorème de Bézout, comme $PGCD(k, n) = 1$, $\exists u, v \in \mathbb{Z}, uk + vm = 1$.
  Donc $u\hat{k} = 1$. Donc $xu\hat{k} = \hat{x}$. Donc $C \subseteq \hat{k}$. Donc $\mathbb{Z}/n\mathbb{Z} \subseteq \left\langle \hat{k} \right\rangle$.

Donc $\mathbb{Z}/n\mathbb{Z} = \left\langle \hat{k} \right\rangle$.

Exemple : Les générateurs de $(\mathbb{Z}/n\mathbb{Z})$ sont, pour $n =$…

- $2 : \hat{1}$
- $3 : \hat{1}, \hat{2}$
- $4 : \hat{1}, \hat{3}$
- $5 : \hat{1}, \hat{2}, \hat{3}, \hat{4}$
- $6 : \hat{1}, \hat{5}$
- $7 : \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}$
- $8 : \hat{1}, \hat{3}, \hat{5}, \hat{7}$

Les éléments générateurs de $\mathbb{U}_n$ sont appelés racines primitives $n$ièmes de l'unité.

V. Sous-groupe engendré par une partie

Définition : Sous-groupe engendré
Soit $(G, *)$ un groupe et $A \subseteq G$.
On appelle **sous-groupe engendré** par A l'intersection de tous les sous-groupes de G contenant A.
Ce sous-groupe est noté $\langle A \rangle$.

Proposition
Soit $A \in G$.
Alors $\langle A \rangle$ est le plus petit, au sens de l'inclusion, sous-groupe de G contenant A. C'est-à-dire que

- $A \in \langle A \rangle$.
- $\langle A \rangle$ est un sous-groupe de G.
- Si H est un sous-groupe de G contenant A, alors $A \in H$.

Preuve : Notons $(G_i)_{i\in I}$ la famille des sous-groupes de G contenant A. $I \neq \emptyset$ car G est l'un deux. Par définition, $\langle A \rangle = \bigcap_{i\in I} G_i$.

- $\forall i \in I, A \subseteq G_i$, donc $A \subseteq \bigcap_{i\in I} G_i = \langle A \rangle$.
- $\langle A \rangle$ est une intersection de sous-groupes de G, donc un sous-groupe de G.
- Soit H un sous-groupe de G contenant A. Donc il existe $i_0 \in I$ tel que $H = G_{i_0}$ donc $\langle A \rangle = \bigcap_{i\in I} G_i \subseteq G_{i_0} = H$.

Exemple :

- $\langle \emptyset \rangle = \{e_G\}$.
- $\forall a \in G, \langle \{a\} \rangle = \langle a \rangle$.
- $\langle G \rangle = G$
- Si H est un sous-groupe de G, alors $\langle H \rangle = H$.

Définition : Partie génératrice
Soit $A \subseteq G$.
On dit que A est **génératrice** de G si et seulement si $\langle A \rangle = G$.

Théorème
Soit $A \subseteq G$ non vide. Alors

$$\langle A \rangle = \left\{ y \in G \mid \exists n \in \mathbb{N}^*, \exists x_1, \ldots, x_n \in A, \exists k_1, \ldots, k_n \in \mathbb{Z}, y = x_1 k^1 * \ldots * x_n k^n \right\}$$

Preuve : Notons $H = \{y \in G \mid \exists n \in \mathbb{N}, \exists x_1, ..., x_n \in A, \exists k_1, ..., k_n \in \mathbb{Z}, y = x_1 k^1 * ... * x_n k^n\}$.
Montrons que H est un sous-groupe de G contenant A.

- Soit $x \in A$. Alors $x = x^{-1}$ donc $x \in H$ et $A \subseteq H$.
- $A \neq \emptyset$ donc $H \neq \emptyset$.
- Soient $y, z \in H$. $\exists n, p \in \mathbb{N}, \exists x_1, ..., x_n t_1, ..., t_p \in A, \exists k_1, ..., k_n, h_1, ..., h_p \in \mathbb{Z}$,
  $y = x_1^{k_1} * ... * x_n^{k_n}, z = t_1^{k_1} * ... * t_n^{k_n}$.
  Donc $y * z^{-1} = x_1^{k_1} * ... * x_n^{k_n} * t_p^{-h_p} * ... * t_1^{-h_1}$. Donc H est un sous-groupe de G donc $\langle A \rangle \subseteq H$.
- Soit $y \in H$. $\exists n \in \mathbb{N}^*, \exists x_1, ..., x_n \in A, \exists k_1, ..., k_n \in \mathbb{Z}, y = x_1^{k_1} * ... * x_n^{k_n}$.
  $\forall i \in \{1, n\}, x_i \in A$ donc $x_i \in \langle A \rangle$. Or $\langle A \rangle$ est un groupe donc $y \in \langle A \rangle$ donc $H \subseteq \langle A \rangle$.

Exemple : Pour $G = (\mathbb{Z}, +)$, $A = \{k_1, k_2\}$, alors $\langle A \rangle = \{y \in \mathbb{Z}\}, \exists p_1, p_2 \in \mathbb{Z}$,
$y = p_1 k_1 + p_2 k_2 = k_3 \mathbb{Z}$ où $k_3 = PGCD(k_1, k_2)$. En effet,

- Si $y \in \langle A \rangle$ alors $\exists p_1, p_2 \in \mathbb{Z}, y = p_1 k_1 + p_2 k_2$. Or $k_3 \mid k_1$, donc $k_3 \mid y$, donc $\langle A \rangle \subseteq k_3 \mathbb{Z}$.
- Si $y \in k_3 \in \mathbb{Z}, y = q k_3$. Or $\exists u, v \in \mathbb{Z}, k_3 = u k_1 + v k_2$. Donc $y = q u k_1 + q v k_2 \in \langle A \rangle$.

2

Anneaux

I. Anneaux

1. Définition

Définition : Anneau
On appelle **anneau** tout ensemble A non vide muni de deux lois de composition internes notées généralement $+$ et $\cdot$ telles que :

- $(A,+)$ est un groupe abélien de neutre 0_A.
- $\cdot$ est associative et munie d'un neutre noté 1_A.
- $\cdot$ est distributive par rapport à $+$, c'est-à-dire $\forall x,y,z,\in A$,

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

Si, de plus, $\cdot$ est commutative, on dit que A est un **anneau commutatif**.

- Si $A\neq\{0_A\}$ alors $1_A\neq 0_A$.
- $\forall x\in A$, $x\cdot 0_A=0_A\cdot x=0_A$. On dit que 0_A est l'élément absorbant.

Exemple :

- $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$
- Tout corps $\mathbb{K}$
- $M_n(\mathbb{K}),K[X]$
- Si A est un anneau, pour $X\neq\emptyset$, $\mathcal{F}(X,A)$ est un anneau.
- Si E est un $\mathbb{K}$-espace vectoriel, alors $(\mathcal{L}(E),+,\times)$ est un anneau.
- Si $E\neq\emptyset$, $(P(E),\Delta,\wedge)$ est un anneau.

2. Anneau produit

Définition : Anneau produit
Soient $A_1,\dots,A_n$ des anneaux, et $A=A_1\times\dots\times A_n$.
Alors A muni des lois $+$ et $\cdot$ définies par

$$\forall\,(a_1,\dots,a_n,b_1\dots,b_n)\in A,$$
$$(a_1,\dots,a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n)$$
$$(a_1,\dots,a_n)\cdot(b_1,\dots,b_n)=(a_1\cdot b_1,\dots,a_n\cdot b_n)$$

est un anneau appelé **anneau produit**.
Ses neutres sont $(0_A,\dots,0_A)$ et $(1_A,\dots,1_A)$.

Preuve :

- $(A,+)$ est le groupe produit, donc un groupe.
- 1_A est le neutre pour $\cdot$.
- L'associativité et la distributivité se vérifient par le calcul.

3. Sous-anneau

Définition : Sous-anneau
Soit $(A,+)$ un anneau et $B\subset A$ non vide. On dit que B est un **sous-anneau** de A si et seulement si B est un anneau et $1_B=1_A$.

Exemple :

- $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
- Soient E et F non vides tels que $E \subsetneq F$. Alors $(P(E), \Delta, \wedge)$ n'est pas un sous-anneau de $(P(F), \Delta, \wedge)$, car $1_E \neq 1_F$.

Proposition
Soit $(A, +, \cdot)$ un anneau et $B \subset A$ non vide. Alors B est un sous-anneau de A si et seulement si :

- $1_A \in B$
- $\forall x, y \in B, x - y \in B, x \cdot y \in B$.

Preuve :

- Si B est un sous-groupe, alors c'est évident.
- Réciproquement, avec ces hypothèses, B est un sous-groupe de A, $\cdot$ est une loi de composition interne de B, $1_A \in B$ est neutre de $\cdot$ pour B donc 1_B existe et $1_B = 1_A$, et $\cdot$ est associative et distributive dans B car elle l'est dans A.

Proposition
Si B est un sous-anneau de A et C est un sous-anneau de B, alors C est un sous-anneau de A.

Preuve : écoule de la caractérisation du sous-anneau.

Dans toute cette section, soit $(A, +, \cdot)$ un anneau commutatif.

4. Idéal d'un anneau comutatif

Définition : Idéal
Soit $I \subset A$. On dit que I est un **idéal** de A si et seulement si :

- I est un sous-groupe de A.
- $\forall x \in I, \forall a \in A, a \cdot x \in I$.

Si I est un idéal de A tel que $1_A \in I$, alors $A = I$.

Exemple :

- A et $\{0_A\}$ sont des idéaux de A.
- $I = 2\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
- Pour A l'anneau des suites réelles bornées, $I = \left\{(u_n)_{n\in\mathbb{N}} \in A \mid u_n \xrightarrow{n\to+\infty} 0\right\}$ est un idéal de A.
- Pour $A = F(\mathbb{R}, \mathbb{R})$, $I = \{f \in A \mid f(38) = 0\}$ est un idéal de A.

Si A est un corps et I est un idéal de A, alors $I = \{0\}$ ou $I = A$.
En effet, si $I \neq \{0\}$, alors il existe $x \in I \setminus \{0\}$. Or A est un corps, donc $x^{-1} \in A$ existe. Et comme I est un idéal, $x^{-1} \cdot x \in I$, donc $1_A \in I$, donc $I = A$.

Définition
Soit $x \in A$. On définit $xA = \{y \in A, \exists z \in A, y = xz\}$. Alors xA est un idéal de A appelé **idéal engendré** par x.

Un idéal de ce type est appelé **idéal principal**.

Preuve : Montrons que xA est un idéal de A.

- $xA \neq \emptyset$ car $x = x \cdot 1_A \in xA$.
- Soient $z_1, z_2 \in xA$. Alors $\exists y_1, y_2 \in A, z_1 = xy_1, z_2 = xy_2$. Donc $z_1 - z_2 \in xA$. Donc xA est un sous-groupe de $(A, +)$.
- Soit $z \in xA$ et $w \in A$. Alors $\exists y \in A, z = xy$ donc $zw = x(yw) \in A$.

Définition
Si tout idéal de A est principal, on dit que A est un **anneau principal**.

Théorème
$\mathbb{Z}$ est un anneau principal, c'est-à-dire que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Preuve :

- Si $n \in \mathbb{N}$, alors $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
- Si I est un idéal de $\mathbb{Z}$, alors I est un sous-groupe de $(\mathbb{Z}, +)$ donc $\exists n \in \mathbb{N}, I = n\mathbb{Z}$

Proposition
Soient I_1 et I_2 deux idéaux de A. Alors $I_1 + I_2 = \{a \in A, \exists b \in I_1, \exists c \in I_2, a = b + c\}$ et $I_1 \cap I_2$ sont des idéaux de A.
De plus, $I_1 + I_2$ est le plus petit idéal de A contenant I_1 et I_2.

Preuve :

- $I_1 \neq \emptyset, I_2 \neq \emptyset$, donc $I_1 + I_2 \neq \emptyset$. Soient $x, y \in I_1 + I_2$.
  Alors $\exists a_1, b_1 \in I_1, \exists a_2, b_2 \in I_2, x = a_1 + a_2, y = b_1 + b_2$. Alors $x - y \in I_1 + I_2$. Donc $I_1 + I_2$ est un sous-groupe.
  Soit $a \in A$ et $x = a_1 + a_2 \in I_1 + I_2$. Alors $ax = aa_1 + aa_2$. Donc $I_1 + I_2$ est un idéal.
- $I_1 \cap I_2$ est un sous-groupe car intersection de sous-groupes. Soit $a \in A$ et $x \in I_1 \cap I_2$. Alors $ax \in I_1, ax \in I_2$ car ce sont des idéaux, donc $ax \in I_1 \cap I_2$. Donc $I_1 \cap I_2$ est un idéal.

5. Divisibilité

Définition : Diviseur de zéro
Soit $(A, +, \cdot)$ un anneau commutatif. On appelle **diviseur de zéro** de A tout élément $a \in A$ tel que $\exists b \in A, a \neq 0, b \neq 0, a \cdot b = 0$.

Définition : Anneau intègre
Un anneau sans diviseur de zéro est appelé **anneau intègre**.

Proposition
Dans un anneau intègre A, tout élméent non nul est régulier pour la multiplication, c'est-à-dire vérifie

$$\forall x, y \in A, ax = ay \implies x = y.$$

Définition : Diviseur, multiple
Soient $a, b \in A$.
On dit que a divise b, ou que b est un multiple de a, et on note $a|b$, si et seulement si $\exists c \in A, b = ac$.

Pour tous $a \in A$, on a $0 = a \times 0$ donc $a|0$, alors que a n'est pas un diviseur de zéro. La terminologie « diviseur de zéro » est donc ambiguë.

Proposition
Soient $a, b \in A$. Alors :

- $a|b$ si et seulement si $bA \subset aA$.
- $|$ est réflexive et transitive.
- $a|b$ et $b|a$ si et seulement si $\exists c \in A^*$ tel que $b = ac$, où A^* est l'ensemble des éléments inversibles de A. On dit alors que a et b sont **associés**.

Preuve :

- Si $a|b$ alors il existe $c \in A$ tel que $b = ac$. Montrons que $bA \subset cA$.
  Soit $d \in bA$. Alors $\exists e \in A, d = be$. Or $b = ac$ donc $d = ace \in aA$ donc $bA \in aA$.
  Inversement, c'est évident.
- Trivial.
- Avec ces hypothèses, si $b = 0$, alors $c = 1_A$ convient. Sinon, $\exists e, a = eb$, sonc d convient.
  Réciproquement, c'est évident.

Exemple :

- Dans $\mathbb{Z}$, $a|b$ et $b|a$ si et seulement si $b = \pm a$.
- Dans $K[X]$. $P|Q$ et $Q|P$ si et seulement si $\exists \lambda \in K^*, Q = \lambda P$.

6. Morphisme d'anneaux

Définition : Morphisme d'anneaux
Soient a et b deux anneaux et $\varphi : A \to B$. On dit que φ est un **morphisme d'anneaux** si et seulement si $\forall a, b \in A$,

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_A) = 1_B$.

φ est en particulier un morphisme de groupes.

Proposition
$\forall A \in A, \forall n \in \mathbb{Z}, \forall p \in \mathbb{N}^*$,

- $\varphi(na) = n\varphi(a)$
- $\varphi(a^p) = \varphi(a)^p$

Définition : Noyau d'un morphisme d'anneaux
Soit $\varphi : A \to B$ un morphisme d'anneaux. On définit son **noyau** :

$$\ker \varphi = \{a \in A \mid \varphi(a) = 0_B\}$$

C'est aussi le noyau de φ en tant que morphisme de groupes.

Proposition
Soient a et b deux anneaux commutatifs, et $\varphi : A \to B$ un morphisme d'anneaux. Alors $\ker \varphi$ est un idéal de a.

Preuve :

- φ est un morphisme d'anneaux donc de groupes donc $\ker \varphi$ est un sous-groupe de A.
- Soit $a \in \ker \varphi$ et $b \in A$. Il est évident que $ab \in \ker \varphi$.

Image d'un morphisme d'anneaux
Soit $\varphi : A \to B$ un morphisme d'anneaux. Son **image** $\Im\varphi = \{b \in B \mid \exists a \in A, \varphi(a) = b\}$ est un sous-anneau de B.

Preuve :

- $\Im\varphi$ est un sous-groupe de $(B, +)$ car φ est un morphisme de groupes.
- $1_B \in \Im\varphi$.
- Le reste : évident.

Proposition
Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors

- L'image par φ de tout sous-anneau de A est un sous-anneau de B.
- L'image réciproque par φ de tout sous-anneau de B est un sous-anneau de A.

Définition : Isomorphisme d'anneaux
un **isomorphisme d'anneaux** est un morphisme d'anneaux bijectif.

Proposition
Si φ est un isomorphisme d'anneaux, alors φ^{-1} est également un isomorphisme d'anneaux.

7. Éléments inversibles

Définition : Inversible
Soit $a \in A$. On dit que A est **inversible** si et seulement si $\exists b \in A, ab = 1_A$. L'ensemble des éléments inversibles est noté A^*.

Un élément inversible est parfois appelé **unité**.

PROPOSITION
$(A^*, \cdot)$ est inversible.

DÉFINITION : CORPS
On dit que A est un **corps** si et seulement si $A^* = A \setminus \{\}$.

DÉFINITION : SOUS-CORPS
Soient $K \subset L$ deux corps.
Alors K est un sous-anneau de L et on dit que K est un **sous-corps** de L, ou que L est une **extension** de K.

K est un sous-corps de L si et seulement si
- $K \subset L$
- $K \neq \emptyset$
- $\forall x, y \in K, x - y \in K.$
- $\forall x, y \in K^*, xy^{-1} \in K.$

Exemple : $\mathbb{Q}(\sqrt{2})$ est un sous-groupe de $\mathbb{R}$.

On a $xy^{-1} = \frac{x}{y} = y^{-1}x$.

DÉFINITION : CARACTÉRISTIQUE D'UN CORPS (HORS-PROGRAMME)
Soit K un corps.
L'ordre de 1_K dans le groupe $(K, +)$ est défini caractéristique du corps K. Soit

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \rightarrow & \mathbb{K} \\ n & \mapsto & n \cdot 1_K \end{array} \right.$$

Pour $\ker \varphi = p\mathbb{Z}$.

- Si $p = 0$, φ est injective : on dit que K est de caractéristique nulle.
- Sinon on dit que K est de caractéristique p.

Si p est non nul, alors il est premier. En effet, si on avait $p = qr, q, r \in \mathbb{N}^*$, on aurait $0_k = (q_1 k)(r_1 k)$.
Or K est intègre donc $q1_K = 0$ ou $r1_K = 0$. Alors $p|q$ ou $p|r$ donc $p = q$ ou $p = r$ donc p est premier.

II. L'ANNEAU $\mathbb{Z}$

1. ARITHMÉTIQUE DANS $\mathbb{Z}$

DÉFINITION : PGCD
Soient $a, b \in \mathbb{Z}$.
Alors il existe un unique $c \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$.
De plus, c est l'unique naturel tel que

- $c|a$
- $c|b$
- $\forall d \in \mathbb{N}, (d|a) \wedge (d|b) \implies d|c$

Donc $c = PGCD(a, b)$.

Preuve :

- Soient $a, b \in \mathbb{Z}$. Alors $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Donc $\exists! c \in \mathbb{N}, a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$.
- On a $0 \in b\mathbb{Z}$ donc $a\mathbb{Z} \subset c\mathbb{Z}$. Donc $c|a$. De même, $c|b$.
  Soit $d \in \mathbb{N}$ tel que $d|a$ et $d|b$. On a $c \in c\mathbb{Z}$ donc $c \in a\mathbb{Z} + b\mathbb{Z}$. Donc $\exists u, v \in \mathbb{Z}, c = au + bv$.
  Donc $d|c$. Et si il existe un autre c' qui vérifie la même propriété, alors $c'|a$, $c'|b$, et donc $c'|c$, donc $c' = c$.

Corollaire
Si $a, b \in \mathbb{Z}$ et $c = PGCD(a, b)$, alors $\exists u, v \in \mathbb{Z}, au + bv = c$.

Preuve : $c \in c\mathbb{Z}$ donc $c \in a\mathbb{Z} + b\mathbb{Z}$.

DÉFINITION : PPCM
Soient $a, b \in \mathbb{Z}$.
Alors il existe un unique $c \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$.
De plus, c est l'unique naturel tel que

- $a|c$
- $b|c$
- $\forall d \in \mathbb{N}, (a|d) \wedge (b|d) \implies c|d$

Donc $c = PPCM(a, b)$.

Preuve :

- Soient $a, b \in \mathbb{Z}$. Alors $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Donc $\exists! c \in \mathbb{N}, a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$.
- On a $c \in a\mathbb{Z}$. Donc $a|c$. De même, $b|c$.
  Soit $d \in \mathbb{N}$ tel que $a|d$ et $b|d$. On a $m \in a\mathbb{Z} \cap b\mathbb{Z}$ donc $d \in a\mathbb{Z} + b\mathbb{Z}$. Donc $d \in c\mathbb{Z}$. Donc $c|d$. Et si il existe un autre c' qui vérifie la même propriété, alors $a|c'$, $b|c'$, et donc $c|c'$, donc $c' = c$.

2. Algorithme d'Euclide

But : trouver une relation de Bézout entre $a, b \in \mathbb{N}$.
- $a \times 1 + b \times 0 = a$
- $a \times 0 + b \times 1 = b$
- $a - bq = r$
- $\vdots$
- $au + bv = PGCD(a, b)$

Exemple :

- $37 \times 1 + 15 \times 0 = 37$.
- $37 \times 0 + 15 \times 1 = 15$.
- $37 - 2 \times 15 = 7$.
- $-2 \times 37 + 5 \times 15 = 1$.

3. Nombres premiers

Définition : Nombre premier
Soit $p \in \mathbb{N}^* \setminus \{1\}$. On dit que p est un **nombre premier** si et seulement si les seuls diviseurs naturels de p sont 1 et p.

Définition : Ensemble des nombres premiers
On note $\mathcal{P}$ l'**ensemble des nombres premiers**.

Proposition
$\mathcal{P}$ est infini.

Théorème de décomposition
Tout relatif $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ peut se décomposer de manière unique (à l'ordre près des facteurs) sous la forme

$$a = \varepsilon \prod_{i=1}^{n} p_i^{\alpha_i}$$

où $\varepsilon \in \mathbb{Z}^* = \mathbb{U}_2, p_1, \dots, p_n \in \mathcal{P}$, et $a_i \in \mathbb{N}^*$.

Proposition
Soient $a, b \in \mathbb{Z} \setminus \{0, 1, -1\}$ tels que $a = \varepsilon \prod_{i=1}^{n} p_i^{\alpha_i}$ et $a = \varepsilon' \prod_{i=1}^{n} p_i^{\beta_i}$ avec $p_1, \dots, p_n \in \mathcal{P}, \alpha_i, \beta_i \in \mathbb{N}, \varepsilon, \varepsilon'$. Alors

$$PGCD(a, b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$$

$$PPCM(a, b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

On déduit $|ab| = PGCD(a, b) \times PPCM(a, b)$.

4. Compléments hors-programme

Pour $x \in \mathbb{R}^+$, on pose $\Pi(x) = Card \{p \in \mathcal{P} \mid p \leqslant x\}$

Théorème des nombres premiers de Hadamard et de la Vallée Poussin

$$\Pi(x) \sim \frac{x}{\ln(x)}$$

Définition : Fonction logarithme intégral
On définit la fonction **logarithme intégral** :

$$li(x) = \int_2^x \frac{dt}{\ln t} + li(2)$$

avec $li(2) \approx 1,04$.

Conjecture

$$\Pi(x) - li(x) = O\left(\sqrt{x}\ln x\right)$$

On montre que pour x « petit »,

$$\Pi(x) \leqslant li(x)$$

Définition : Nombres premiers jumeaux
$p, q \in \mathcal{P}$ sont dits **jumeaux** si et seulement si $|p-q| = 2$.

Exemple : 3 et 5 ou 5 et 7 ou 11 et 13.

Conjecture des nombres premiers
On ne sait pas s'il existe une infinité de nombres premiers.

Conjecture de Goldbach
Tout entier pair supérieur à 3 peut s'écrire comme la somme de deux nombres premiers.

Théorème de la progression arithmétique de Dirichlet
Si $a \wedge b = 1$ alors $\{a + bn, n \in \mathbb{N}\} \cap \mathcal{P}$ est infini.

Théorème de Green et de Tao
$\forall k \geqslant 1$, il existe une suite de k nombres premiers en progression arithmétique.

III. L'anneau $\mathbb{Z}/n\mathbb{Z}$

1. Structure

Théorème
Soient $c, d \in \mathbb{Z}/n\mathbb{Z}$. Soit $x \in c, y \in d$.
Alors $\widehat{x \cdot y}$ ne dépend pas du choix de y.
On peut donc la noter $\widehat{x \cdot y} = c \odot d$.
On définit ainsi une loi de composition interne dans $\mathbb{Z}/n\mathbb{Z}$. Et alors $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$ est un anneau commutatif et

$$\left|\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & \hat{x} \end{array}\right.$$

est un morphisme d'anneaux surjectif de noyau $n\mathbb{Z}$.

Preuve :

- Soient $x, x' \in c, y.y' \in d$. Alors $\exists k, l \in \mathbb{Z}, x = x' + kn, y = y' + ln$.
  Donc $xy = x'y' + n(lx' + ky' + kln)$. Donc $\widehat{xy} = \widehat{x'y'}$.
- $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est un groupe abélien.
  Soient $c, d, e \in \mathbb{Z}/n\mathbb{Z}, x \in c, y \in d, z \in e$. Alors $d \odot c = \hat{x} \odot \hat{y} = \widehat{xy} = \hat{y} \odot \hat{x} = d.c$ donc $\odot$ est commutative.
  $c \odot (d \odot e) = (c \odot d) \odot e$ de la même manière donc $\odot$ est transitive.
  $\hat{1} \odot c = \widehat{1 \cdot x} = c = c \odot 1$ donc $\hat{1}$ est l'élément neutre.
  Enfin $c \odot (d \oplus e) = c \odot d + c \odot e$.
  Donc c'est un anneau commutatif.
- On sait que $\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & \hat{x} \end{array} \right.$ est un morphisme de groupes commutatif de noyau $n\mathbb{Z}$.
  Soient $x, y \in \mathbb{Z}$. Alors $\varphi(xy) = \widehat{xy} = \hat{x} \odot \hat{y} = \varphi(x)\varphi(y)$. Enfin, $\varphi(1) = \hat{1}$.

$\mathbb{Z}/n\mathbb{Z}$ est donc un anneau commutatif par les lois $+ : (\hat{x}, \hat{y}) \mapsto \hat{x} + \hat{y} = \widehat{x+y}$ et $\times : (\hat{x}, \hat{y}) \mapsto \hat{x} \times \hat{y} = \widehat{x \times y}$, d'éléments neutres $\hat{0}$ et $\hat{1}$.

Éléments de $\mathbb{Z}/n\mathbb{Z}$
Pour $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments :

$$\mathbb{Z}/n\mathbb{Z} = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$$

2. Éléments inversibles

Théorème
Soit $c \in \mathbb{Z}/n\mathbb{Z}$ tel que $c \neq \hat{0}$ et $x \in c$. Alors les assertions suivantes sont équivalentes :

- c est inversible.
- c n'est pas un diviseur de zéro.
- $PGCD(x, n) = 1$.

Preuve :

- 1 vers 2. Un diviseur de zéro n'est jamais inversible.
- 2 vers 3. Supposons que $d = PGCD(x, n) \neq 1$. Alors soient $x = dx', n = dn'$, de telle sorte que $PGCD(x', n') = 1$.
- Alors $xn' = dx'n' = x'n$ donc $\widehat{xn'} = \hat{0}$ donc $c \odot \widehat{n'} = 0$. Or $d > 1$ donc $0 < n' < n$. Donc $\widehat{n'} \neq \hat{0}$ donc c est un diviseur de zéro.
- 3 vers 1. Par le théorème de Bézout, il existe $u, v \in \mathbb{Z}, xu + nv = 1$. Donc $\widehat{xu} = \hat{1}$ donc $c \odot \hat{u} = \hat{1}$. Donc c est inversible et $c^{-1} = \hat{u}$.

Exemple : Dans $\mathbb{Z}/36\mathbb{Z}, \hat{7}$ est inversible car $7 \wedge 36 = 1$. Or $36 - 5 \times 7 = 1$. Donc $-5 \times 7 \equiv 1[36]$. Donc $\left(\hat{7}\right)^{-1} = \widehat{-5} = \widehat{31}$.

Définition : Groupe des inversibles
Le **groupe des inversibles** est le groupe

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\hat{x} \mid x \in \{1, \ldots, n-1\}, PGCD(x, n) = 1\}.$$

Exemple :

- $(\mathbb{Z}/4\mathbb{Z})^* = \{\hat{1}, \hat{3}\}$
- $(\mathbb{Z}/6\mathbb{Z})^* = \{\hat{1}, \hat{5}\}$

Proposition
Soit $n \geqslant 2$.
Alors les trois assertions sont équivalentes :

- $\mathbb{Z}/n\mathbb{Z}$ est un corps
- $\mathbb{Z}/n\mathbb{Z}$ est intègre
- n est premier

Ainsi, pour p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps noté $\mathbb{F}_p$.

Preuve : $\mathbb{Z}/n\mathbb{Z}$ est un corps
$\iff$ tout élément non nul est inversible
$\iff$ aucun élément non nul n'est un diviseur de zéro

$\Longleftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est intègre
$\Longleftrightarrow$ $\forall k \in \{1, ..., n-1\}, \hat{k}$ est inversible
$\Longleftrightarrow$ $\forall k \in \{1, ..., n-1\}, PGCD(k, n) = 1$
$\Longleftrightarrow$ n est premier.

Exemple : $\mathbb{F}_2 = \{\hat{0}, \hat{1}\}$

3. Compléments hors-programme

Recherche de l'inverse
Soit $k \in \{1, ..., n-1\}$ tel que $PGCD(k, n) = 1$.
Alors $\hat{k} \in (\mathbb{Z}/n\mathbb{Z})^*$, et $\left(\hat{k}\right)^{-1} = \hat{u}$ où $uk + vn = 1$.

Structure de $(\mathbb{Z}/p\mathbb{Z})$
Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})^* = \{\hat{1}, ..., \widehat{p-1}\}$ est un groupe cyclique.
Un générateur de ce groupe est appelé élément primitif.

Exemple : Pour $p = 7$, $\hat{3}$ est un élément primitif.

4. Théorème chinois

Théorème chinois
Soient $n, p \in \mathbb{N}^* \backslash [1]$ tels que $PGCD(n, p) = 1$. Alors l'application

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z}/np\mathbb{Z} & \to & (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \\ c = \hat{k} & \mapsto & \left(\hat{k}, \hat{k}\right) \end{array} \right.$$

(avec les $\hat{k}$ les classes d'équivalence dans les ensembles correspondants) est bien définie et est un morphisme d'anneaux.

Preuve :

- Soit $c \in \mathbb{Z}/np\mathbb{Z}$ et $k_1, k_2 \in c$. Alors $\exists u, v \in \mathbb{Z}, k_1 = k_2 + unp$ donc $k_1 \equiv k_2[n]$ et $\widehat{k_1} = \widehat{k_2}$, de même pour $\mathbb{Z}/p\mathbb{Z}$, donc φ est bien définie.

- Soient $c_1, c_2 \in \mathbb{Z}/n\mathbb{Z}, k_1 \in c_1, k_2 \in c_2$.
Alors on a rapidement que $\varphi(c_1 + c_2) = \varphi(c_1) + \varphi(c_2)$, et de même pour $\cdot$. Enfin, $\varphi\left(\hat{1}\right) = \left(\hat{1}, \hat{1}\right)$. Donc φ est bien un morphisme d'anneaux.

- Soit $c \in \ker \varphi$ et $k \in c$. Alors $\varphi(c) = \left(\hat{0}, \hat{0}\right)$ donc $n|k$ et $p|k$. Or $PGCD(n, p) = 1$ donc $np|k$ donc $\hat{k} = \hat{0}$ donc φ est injective.

- Enfin, $Card\, \mathbb{Z}/np\mathbb{Z} = mp = Card\, \mathbb{Z}/n\mathbb{Z} \times Card\, \mathbb{Z}/p\mathbb{Z}$,

Extension du théorème chinois
Soit $k \geqslant 2$ et $n_1, ..., n_k \in \mathbb{N}^* \backslash \{1\}$ deux à deux premiers entre eux. Alors

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z}/(n_1 ... n_k)\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z} \\ c = \hat{x} & \mapsto & \left(cl_{n_1}(x), ..., cl_{n_k}(x)\right) \end{array} \right.$$

est bien définie et est un morphisme d'anneaux.

Preuve : Identique au cas précédent.

Systèmes de congruences

Soient $n_1, \ldots, n_k$ des entiers supérieurs à 2 premiers entre eux, et soient $a_1, \ldots, a_k \in \mathbb{Z}$. Alors l'ensemble des solutions du système $x \equiv a_1[n_1], \ldots, x \equiv a_k[n_k]$ est une certaine classe $c \in \mathbb{Z}/(n_1 \ldots n_k)\mathbb{Z}$.
De plus, $c = \hat{b}$ avec

$$b = \sum_{i=1}^{k} a_i v_i \left(\prod_{\substack{j=1 \\ j \neq i}} n_j \right)$$

où on a pour tout $i \in \{1, \ldots, k\}$,

$$u_i n_i + v_i \prod_{\substack{j=1 \\ j \neq i}} n_j = 1$$

est une relation de Bézout entre n_i et $\prod_{\substack{j=1 \\ j \neq i}} n_j$.
Ainsi, x est solution du système si et seulement si $x \equiv b[n_1 \ldots n_k]$.

Preuve : Considérons φ le morphisme chinois.
x est solution du système si et seulement si $\left(cl_{n_1}(x), \ldots, cl_{n_k}(x)\right) = \left(cl_{n_1}(a_1), cl_{n_k}(a_k)\right)$. Par φ^{-1}, x l'est si et seulement si $cl_{n_1 \ldots n_k}(x) = \varphi^{-1}\left(cl_{n_1}(a_1), \ldots, cl_{n_k}(a_k)\right) = c$.
Pour tout $i \in \{1, \ldots, k\}$, n_i et $\prod_{\substack{j=1 \\ j \neq i}} n_j$ sont premiers entre eux.
Donc on peut trouver une relation de Bézout : $u_i n_i + v_i \prod_{\substack{j=1 \\ j \neq i}} n_j = 1$.

Posons $b = \sum_{i=1}^{k} a_i v_i \left(\prod_{\substack{j=1 \\ j \neq i}} n_j \right)$.
Alors pour $l \in [1, \ldots, k]$,

$$\begin{aligned} b &\equiv a_l v_l \prod_{\substack{j=1 \\ j \neq i}} n_j [nl] \\ &\equiv al\,(1 - u_l n_l)\,[nl] \end{aligned}$$

Donc $b \equiv al[nl]$ donc b est solution donc $c = \hat{b}$.

Exemple : Pour $x \equiv 1[5], x \equiv 4[7], x \equiv 2[11]$.
Alors $x \equiv b[385]$ avec b comme solution particulière. On a
$31 \times 5 - 2 \times 77 = 1, 8 \times 7 - 55 = 1, 16 \times 11 - 5 \times 35 = 1$.
Posons $b = 1(-2 \times 77) + 4(-55) + 2(-5 \times 35) = -724 \equiv 46[385]$.
Donc $x \equiv 46[385]$.

5. Indicatrice d'Euler et petit théorème de Fermat

Définition : Indicatrice d'Euler

On appelle **indicatrice d'Euler** l'application

$$\varphi : \left| \begin{array}{ccc} \mathbb{N}^* \setminus \{1\} & \to & \mathbb{N} \\ n & \mapsto & \varphi(n) \end{array} \right.$$

où $\varphi(n) = Card\,\{k \in \{1, \ldots, n-1\} \mid PGCD(k, n) = 1\} = Card\,(\mathbb{Z}/n\mathbb{Z})^*$.

Théorème

Si $n, p \in \mathbb{N}^*$ sont premiers entre eux, alors $\varphi(np) = \varphi(n)\varphi(p)$.
On dit que φ est une fonction multiplicative.

Preuve : Soient n et p premiers entre eux.
Considérons le morphisme chinois $\psi : \mathbb{Z}/np\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Soient $c \in (\mathbb{Z}/np\mathbb{Z})^*$ et $x \in c$. Alors $\psi(c) = \psi(cl_{np}(x) = (cl_n(x), cl_p(x))$.
Et comme $PGCD(x,np) = 1$, on a $PGCD(x,n) = 1$ donc $cl_n(x) \in (\mathbb{Z}/n\mathbb{Z})^*$. De même, $cl_p(x) \in (\mathbb{Z}/p\mathbb{Z})^*$.

On peut donc définir $\widetilde{\psi}$: $\left| \begin{array}{ccc} (\mathbb{Z}/np\mathbb{Z})^* & \to & (\mathbb{Z}/n\mathbb{Z})^*, (\mathbb{Z}/p\mathbb{Z})^* \\ c = cl_{np}(x) & \mapsto & \left(cl_n(x), cl_p(x)\right) \end{array} \right.$.

- ψ étant un morphisme d'anneaux, $\widetilde{\psi}$ est un morphisme de groupes.
- $\ker \widetilde{\psi} = \left\{cl_{np}(1)\right\}$ car ψ est bijective. Donc $\widehat{\psi}$ est injective.

- Soient $c_1, c_2 \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$. Posons $c = \psi^{-1}(c_1, c_2)$ et $x \in c$.
  On a $PGCD(x,n) = 1$ et $PGCD(x,p) = 1$. Or n et p sont premiers entre eux donc $PGCD(X,np) = 1$. Donc $c \in (\mathbb{Z}/n\mathbb{Z})^*$. Donc $\widetilde{\psi}(c) = (c_1, c_2)$ donc $\widetilde{\psi}$ est surjective donc bijective.

Donc $Card(\mathbb{Z}/np\mathbb{Z})^* = Card(\mathbb{Z}/n\mathbb{Z})^* \times Card\,(\mathbb{Z}/p\mathbb{Z})^*$ et $\varphi(np) = \varphi(n)\varphi(p)$.

Lemme

Soit p premier et $\alpha \geqslant 1$, alors $\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1}$

Preuve : Soit $k \in \{1, ..., p^\alpha\}$. k n'est pas premier avec p^α si et seulement si k et p^α ont un diviseur commun si et seulement si $p|k$ si et seulement si $k \in \left\{p, 2p, ..., p^{\alpha-1}\right\}$. Donc $Card\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^* = p^\alpha - p^{\alpha-1}$.

Décomposition d'un entier par l'indicatrice d'Euler

Soit $n \geqslant 2$. Décomposons n en

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

avec p_i des premiers distincts.
Comme φ est multiplicative,

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

THÉORÈME D'EULER
Soit $n \geqslant 2$ et $a \in \mathbb{Z}$ tel que $a \wedge 1 = 1$.
Alors $a^{\varphi(n)} \equiv 1[n]$.

Preuve : $\hat{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Donc l'ordre de $\hat{a}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ divise l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$. Or ce dernier vaut $\varphi(n)$. Donc $\hat{a}^{\varphi(n)} = \hat{1}$. Donc $a^{\varphi(n)} \equiv 1[n]$.

PETIT THÉORÈME DE FERMAT
Soient p un entier premier et $a \in \mathbb{Z}$ tels que $p \nmid a$. Alors $a^{p-1} \equiv 1[p]$.

Preuve : $a \wedge p = 1$ donc $a^{\varphi(p)} \equiv 1[p]$ donc $a^{p-1} \equiv 1[p]$.

IV. COMPLÉMENTS HORS-PROGRAMME

PROPOSITION
Soit $p \geqslant 3$ impair.

- Si $2^{p-1} \not\equiv 1[p]$ alors p n'est pas premier (par contraposée)
- Si $2^{p-1} \equiv 1[p]$ alors
  - Soit p est premier
  - Soit p n'est pas premier. On dit alors que p est 2-pseudo-premier.

Hélas, il existe des entiers qui ne sont pas premiers mais qui sont a-pseudos premiers pour tout a. On les appelle nombres de Carmichaël. Il y en a une infinité, et le premier est 561.

V. L'anneau $\mathbb{K}[X]$

Dans toute cette partie, soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$.

1. Idéaux de $\mathbb{K}[X]$

Idéaux de $\mathbb{K}[X]$

Les idéaux de $\mathbb{K}[X]$ sont du type $P_0 \cdot \mathbb{K}[X]$ avec P_0 nul ou unitaire. Dans ce cas, P_0 est unique. On l'appelle **générateur** nul ou unitaire de l'idéal.
Ainsi, $\mathbb{K}[X]$ est un anneau principal.

Preuve :

- Soit $I = \{0\}$ l'idéal nul. Alors $I = 0\mathbb{K}[X]$.
- Pour $P_0 \in \mathbb{K}[X]$, on sait que $P_0 \cdot \mathbb{K}[X]$ est un idéal.
- Réciproquement, soit I un idéal non nul de $\mathbb{K}[X]$. Considérons $A = \{\deg P, \mid P \in I \setminus \{0\}\}$.
  On a $A \subset \mathbb{N}, A \neq 0$, car $I \neq \{0\}$. On a donc l'existence de $d_0 = \min A$
  Or $d_0 \in A$ donc il existe $P_1 \in I$ tel que $\deg P_1 = d_0$.
  $P_1 \neq 0$ donc notons α son coefficient dominant, et posons $P_0 = \frac{P_1}{\alpha}$. Alors $P_0 \in I$ (car I est idéal), P_0 est unitaire, et $\deg P_0 = d_0$.
  Montrons que $I = P_0 \cdot \mathbb{K}[X]$.
  - $P_0 \in I$ et I est idéal donc $P_0\mathbb{K}[X] \subset I$.
  - Soit $P \in I$. Par division euclidienne, P s'écrit $P_0Q + R$ avec $Q, R \in \mathbb{K}[X]$ et $\deg R < \deg P_0$.
    $P \in I$, $P_0Q \in I$, donc $R = P - P_0Q \in I$. Or $\deg R < d_0$ donc $R = 0$. Donc $P \in P_0\mathbb{K}[X]$. Donc $I \subset P_0\mathbb{K}[X]$.

  Donc $I = P_0\mathbb{K}[X]$.
- Montrons que P_0 est unique. Soit I un idéal non nul qui vérifie $I = P_0\mathbb{K}[X] = P_2\mathbb{K}[X]$, avec P_0 et P_2 unitaires.
  Or $P_0 \in I$ donc $P_2 | P_0$. De même, $P_0 | P_2$.
  Donc P_0 et P_2 sont associés. Et comme ils sont unitaires, $P_0 = P_2$.

> - Soit I un idéal non nul de $K[X]$. Alors le polynôme P_0 est l'unique générateur unitaire de I et est appelé polynôme minimal de I.
> - Si A est une matrice carrée, et $P \in \mathbb{K}[X]$, on définit la matrice $P(A)$.
>   On montre que
> $$\left| \begin{array}{ccc} \mathbb{K}[X] & \to & M_n(\mathbb{K}) \\ P & \mapsto & P(A) \end{array} \right.$$
>   est un morphisme d'anneaux.
> $\{P \in \mathbb{K}[X] \mid P(A) = 0\}$, son noyau, est donc un idéal de $\mathbb{K}[X]$. On montre qu'il est non nul.
>   L'unique polynôme unitaire tel que $\ker \varphi = P_0\mathbb{K}[X]$ est appelé polynôme minimal de la matrice A.

2. Arithmétique dans $\mathbb{K}[X]$

Définition : PGCD

Soient $P, Q \in \mathbb{K}[X]$. Alors il existe un unique polynôme $D \in \mathbb{K}[X]$ unitaire non nul tel que

$$P\mathbb{K}[X] + Q\mathbb{K}[X] = D\mathbb{K}[X].$$

De plus, D est l'unique poynôme non nul tel que

- $D|P$
- $D|Q$
- $\forall R \in \mathbb{K}[X], (R|P) \wedge (R|Q) \implies R|D$

On appelle D le **PGCD** de P et Q.

Preuve : La preuve est la même que dans $\mathbb{Z}$.

Définition : PPCM

Soient $P, Q \in \mathbb{K}[X]$. Alors il existe un unique polynôme $M \in \mathbb{K}[X]$ unitaire non nul tel que

$$P\mathbb{K}[X] \cap Q\mathbb{K}[X] = M\mathbb{K}[X].$$

De plus, M est l'unique poynôme non nul tel que

- $P|M$
- $Q|M$
- $\forall R \in \mathbb{K}[X], (P|R) \wedge (Q|R) \implies M|R$

On appelle M le **PPCM** de P et Q.

Preuve : La preuve est la même que dans $\mathbb{Z}$.

3. Irréductibles de $\mathbb{K}[X]$

Définition : Irréductible
Soit $P \in \mathbb{K}[X]$ de degré supérieur à 1.
On dit que P est **irréductible** si et seulement si ses seuls diviseurs sont les polynômes constants non nuls et ses polynômes associés.
C'est-à-dire si et seulement si si $P = P_1P_2$ alors $\deg P_1 = 0$ ou $\deg P_2 = 0$, soit $P_1 \in \mathbb{K}^*$ ou $P_2 \in \mathbb{K}^*$.

Exemple : Tout polynôme de degré 1 est irréductible.

Proposition
Un polynôme inversible de degré supérieur ou égal à 2 n'a pas de racine dans $\mathbb{K}$.

Preuve : Si P a une racine λ, $P = (X - \lambda)Q$ donc P n'est pas irréductible.

Exemple : $X^2 + 1$ dans $\mathbb{R}$.

Théorème de décomposition
Soit $P \in \mathbb{K}[X]$ tel que $\deg P \geqslant 1$.
Alors P se décompose de manière unique (à l'ordre près) sous la forme

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

où

- $\lambda \in \mathbb{K}^*$
- $n \geqslant 1$
- $P_1, \ldots, P_n$ sont des polynômes irréductibles unitaires.
- $\alpha_i \geqslant 1$

Preuve : Vue l'an dernier.

De manière analogue à $\mathbb{Z}$, cette décomposition permet de calculer les PGCD et les PPCM.

Exemple : Dans $\mathbb{R}[X]$, $X^3 - 1 = (X - 1)(X^2 + X + 1)$.

Théorème de d'Alembert-Gauss
$\mathbb{C}$ est algébriquement clos.
C'est-à-dire que tout polynôme sur $\mathbb{C}$ est scindé.
C'est-à-dire que tout polynôme de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

Irréductibles dans $\mathbb{C}[X]$
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Irréductibles dans $\mathbb{R}[X]$
Les irréductibles dans $\mathbb{R}[X]$ sont :

- Les polynômes de degré 1
- Les polynômes de degré 2 sans racine réelle

Exemple : $X - 38$ et $X^2 + X + 1$ sont des irréductibles de $\mathbb{R}[X]$.

VI. Algèbres

Définition : Algèbre
Soit A un ensemble non vide muni de deux lois de composition internes $+$ et $\cdot_{int}$ et d'une loi de composition externe à opérateurs dans un corps $\mathbb{K}$, $\cdot_{ext}$.
On dit que $(A, +, \cdot_{int}, \cdot_{ext})$ est une $\mathbb{K}$-**algèbre** si et seulement si

- $(A, +, \cdot_{int})$ est un anneau
- $(A, +, \cdot_{ext})$ est un $\mathbb{K}$-espace vectoriel
- $\forall \alpha \in \mathbb{K}, \forall x, y \in A, \alpha(xy) = (\alpha x)y = x(\alpha y)$.

Exemple :

- K, $M_n(\mathbb{K})$ et $\mathbb{K}[X]$ sont des K-algèbres.
- $(\mathcal{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre où E est un $\mathbb{K}$-espace vectoriel.
- $(P(E), \Delta, \cap, \cdot)$ est une $\mathbb{Z}/2\mathbb{Z}$-algèbre.

DÉFINITION : SOUS-ALGÈBRE

Soit A une K-algèbre et $B \subset A$. on dit que B est une **sous-algèbre** de A si et seulement si

- $(B, +, \cdot, \cdot)$ est une K-algèbre.
- $1_B = 1_A$.

CARACTÉRISATION D'UNE SOUS-ALGÈBRE

Soit A une $\mathbb{K}$-algèbre et $B \subset A$ non vide.
Alors B est une sous-algèbre de A si et seulement si B est un sous-espace vectorie et un sous-anneau de A, c'est-à-dire si et seulement si $\forall x, y \in B, \forall \lambda \in \mathbb{K}$

- $\lambda x + y \in B$
- $xy \in B$
- $1_A \in B$

DÉFINITION : MORPHISME D'ALGÈBRES

Soient A_1, A_2 deux algèbres et $\varphi : A_1 \to A_2$.
On dit que φ est un **morphisme d'algèbres** si et seulement si $\forall a, b \in A, \forall \lambda \in \mathbb{K}$,

- $\varphi(\lambda a + b) = \lambda\varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_{A_1}) = 1_{A_2}$

C'est-à-dire φ est une application linéaire et un morphisme d'anneaux.

Exemple :

- Pour $\alpha \in \mathbb{K}$, $\varphi : \left| \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P & \mapsto & P(\alpha) \end{array} \right.$
- Pour B une base de $\ker E$ de dimension n, $\varphi : \left| \begin{array}{ccc} \mathcal{L}(E) & \to & M_n(\mathbb{K}) \\ u & \mapsto & A = M_B(u) \end{array} \right.$

Index Alphabétique